А. Л. Городенцев*

А Л Г Е Б Р А

для студентов-математиков

часть I

Москва, МЦНМО, 2023

*Национальный исследовательский университет «Высшая школа экономики», Независимый Московский университет, Национальный исследовательский центр «Курчатовский институт», e-mail: gorod@itep.ru, http://gorod.bogomolov-lab.ru/.

Оглавление

§1. Множества и отображения

Этот параграф носит вспомогательный характер. В нём собраны некоторые факты о множествах и отображениях, используемые в этой книге. Многие из них, вероятно, знакомы читателю из школы или параллельных курсов анализа и дискретной математики. Нет нужды «учить» материал этого параграфа *перед* тем, как браться за курс алгебры. Но к нему стоит выборочно обращаться всякий раз, когда вы почувствуете себя неуверенно в тех или иных рассуждениях, использующих множества, отображения, отношения или незнакомую вам комбинаторику.

1.1. Множества. В наши цели не входит построение логически строгой теории множеств. Для понимания этого курса достаточно интуитивного школьного представления о множестве как «абстрактной совокупности элементов произвольной природы». Элементы множеств мы часто будем называть *точками*. Все точки в любом множестве, по определению, различны.

Множество X задано, как только про любой объект можно сказать, является он элементом множества X или нет. Принадлежность точки x множеству X записывается как $x \in X$. Два множества *равны*, если они состоят из одних и тех же элементов. Существует единственное множество, не содержащее ни одного элемента. Оно называется *пустым* и обозначается $\varnothing$. Если множество X конечно, то мы обозначаем через $|X|$ количество точек в нём.

Множество X называется *подмножеством* множества Y, если каждый его элемент $x \in X$ лежит также и в Y. В этом случае пишут $X \subset Y$. Отметим, что пустое множество является подмножеством любого множества и всякое множество является подмножеством самого себя. Подмножества, отличные от всего множества, называются *собственными*. В частности, пустое подмножество непустого множества собственное. Если надо указать, что X является собственным подмножеством в Y, используется обозначение $X \subsetneq Y$.

Упражнение 1.1. Сколько всего подмножеств (включая пустое и несобственное) имеется у множества, состоящего из n элементов?

Для заданных множеств X, Y их *объединение* $X \cup Y$ состоит из всех элементов, принадлежащих хотя бы одному из множеств X, Y; *пересечение* $X \cap Y$ состоит из всех элементов, принадлежащих одновременно каждому из множеств X, Y; *разность* $X \smallsetminus Y$ состоит из всех элементов множества X, которые не содержатся в Y.

Упражнение 1.2. Проверьте, что операция пересечения выражается через разность по формуле $X \cap Y = X \smallsetminus (X \smallsetminus Y)$. Можно ли выразить разность через пересечение и объединение?

Если множество X является объединением непересекающихся подмножеств Y и Z, то говорят, что X является *дизъюнктным объединением* Y и Z и пишут $X = Y \sqcup Z$.

Множество $X \times Y$, элементами которого по определению являются всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым* (или *прямым*) *произведением* множеств X и Y.

1.2. Отображения. Отображение $f : X \to Y$ из множества X в множество Y есть правило, однозначно сопоставляющее каждой точке $x \in X$ некоторую точку $y = f(x) \in Y$, которая называется *образом* точки x при отображении f. Множество всех таких точек $x \in X$, образ которых равен заданной точке $y \in Y$, называется *полным прообразом* точки y или *слоем* отображения f над y и обозначается

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in X \mid f(x) = y\}.$$

Полные прообразы различных точек не пересекаются и могут как быть пустыми, так и состоять из многих точек. Множество всех $y \in Y$, имеющих непустой прообраз, называется *образом*

отображения $f : X \to Y$ и обозначается

$$\operatorname{im}(f) \stackrel{\text{def}}{=} \{y \in Y \mid f^{-1}(y) \neq \varnothing\} = \{y \in Y \mid \exists\, x \in X : f(x) = y\}\,.$$

Два отображения $f : X \to Y$ и $g : X \to Y$ *равны*, если $f(x) = g(x)$ для всех $x \in X$. Множество всех отображений из множества X в множество Y обозначается $\operatorname{Hom}(X, Y)$.

Отображение $f : X \to Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\operatorname{im}(f) = Y$, т. е. когда прообраз каждой точки $y \in Y$ не пуст. Мы будем изображать сюръективные отображения стрелками $X \twoheadrightarrow Y$. Отображение f называется *вложением* (а также *инъекцией*, или *мономорфизмом*), если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$, т. е. когда прообраз каждой точки $y \in Y$ содержит не более одного элемента. Инъективные отображения изображаются стрелками $X \hookrightarrow Y$.

Упражнение 1.3. Перечислите все отображения $\{0,\ 1,\ 2\} \to \{0,\ 1\}$ и $\{0,\ 1\} \to \{0,\ 1,\ 2\}$. Сколько среди них вложений и сколько наложений?

Отображение $f : X \to Y$, которое является одновременно и вложением и наложением, называется *взаимно однозначным* (а также *биекцией* или *изоморфизмом*). Биективность отображения f означает, что для каждого $y \in Y$ существует единственный такой $x \in X$, что $f(x) = y$. Мы будем обозначать биекции стрелками $X \xrightarrow{\sim} Y$.

Упражнение 1.4. Из отображений: а) $\mathbb{N} \to \mathbb{N} : x \mapsto x^2$ б) $\mathbb{Z} \to \mathbb{Z} : x \mapsto x^2$ в) $\mathbb{Z} \to \mathbb{Z} : x \mapsto 7x$ г) $\mathbb{Q} \to \mathbb{Q} : x \mapsto 7x$ выделите все инъекции, все сюръекции и все биекции.

Отображения $X \to X$ из множества X в себя обычно называют *эндоморфизмами* множества X. Множество всех эндоморфизмов обозначается $\operatorname{End}(X) \stackrel{\text{def}}{=} \operatorname{Hom}(X, X)$.

Упражнение 1.5 (принцип Дирихле). Покажите, что следующие три условия на множество X равносильны: а) X бесконечно б) существует вложение $X \hookrightarrow X$, не являющееся наложением в) существует наложение $X \twoheadrightarrow X$, не являющееся вложением.

Взаимно однозначные эндоморфизмы $X \xrightarrow{\sim} X$ называются *автоморфизмами* множества X. Множество всех автоморфизмов обозначается через $\operatorname{Aut}(X)$. Автоморфизмы можно воспринимать как *перестановки* элементов множества X. У всякого множества X имеется *тождественный автоморфизм* $\operatorname{Id}_X : X \to X$, который переводит каждый элемент в себя: $\operatorname{Id}_X(x) = x$ для всех $x \in X$.

Упражнение 1.6. Счётно[1] ли множество $\operatorname{Aut}(\mathbb{N})$?

Пример 1.1 (запись отображений словами)
Рассмотрим множества $X = \{1,\ 2,\ \ldots\ ,\ n\}$ и $Y = \{1,\ 2,\ \ldots\ ,\ m\}$, сопоставим каждому отображению $f : X \to Y$ последовательность его значений:

$$w(f) \stackrel{\text{def}}{=} \big(f(x_1),\ f(x_2),\ \ldots\ ,\ f(x_n)\big) \tag{1-1}$$

и будем воспринимать её как n-буквенное слово, написанное при помощи m-буквенного алфавита Y. Так, отображениям $f : \{1,\ 2\} \to \{1,\ 2,\ 3\}$ и $g : \{1,\ 2,\ 3\} \to \{1,\ 2,\ 3\}$, действующим по правилам $f(1) = 3$, $f(2) = 2$ и $g(1) = 1$, $g(2) = 2$, $g(3) = 2$, сопоставятся слова $w(f) = (3, 2)$ и $w(g) = (1, 2, 2)$, составленные из букв алфавита $\{1,\ 2,\ 3\}$. Запись отображения словом задаёт биекцию

$$w : \operatorname{Hom}(X, Y) \xrightarrow{\sim} \{\text{слова из } |X| \text{ букв в алфавите } Y\}\,, \quad f \mapsto w(f)\,. \tag{1-2}$$

[1] Множество M называется *счётным* если существует биекция $\mathbb{N} \xrightarrow{\sim} M$.

Инъективные отображения записываются при этом словами, в которых нет повторяющихся букв, а сюръективные отображения — словами, в которых используются все без исключения буквы алфавита Y. Взаимно однозначным отображениям отвечают слова, в которых каждая буква алфавита Y встречается ровно один раз.

Предложение 1.1
Если множества X и Y конечны, то $|\operatorname{Hom}(X,Y)| = |Y|^{|X|}$.

Доказательство. Пусть X состоит из n элементов, а Y — из m, как в прим. 1.1 выше. Нас интересует количество всех n-буквенных слов, которые можно написать при помощи алфавита из m букв. Обозначим его через $W_m(n)$ и выпишем все эти слова на m страницах, поместив на i-ю страницу все слова, начинающиеся на i-ю букву алфавита. В результате на каждой странице окажется ровно по $W_m(n-1)$ слов. Поэтому

$$W_m(n) = m \cdot W_m(n-1) = m^2 \cdot W(n-2) = \ldots = m^{n-1} \cdot W_m(1) = m^n\,. \qquad \square$$

Замечание 1.1. Принимая во внимание предл. 1.1, множество $\operatorname{Hom}(X,Y)$ отображений $X \to Y$ часто обозначают Y^X. В доказательстве предл. 1.1 мы молчаливо предполагали, что оба множества непусты. Если $X = \varnothing$, то для любого множества Y множество $\operatorname{Hom}(\varnothing, Y)$ по определению состоит из единственного элемента — вложения $\varnothing$ в Y в качестве пустого подмножества или, что то же самое, пустого слова в алфавите Y. В этом случае предл. 1.1 остаётся в силе: $|\operatorname{Hom}(\varnothing,Y)| = 1 = |Y|^0$. В частности, $\operatorname{Hom}(\varnothing,\varnothing)$ тоже состоит из одного элемента[1] — тождественного автоморфизма $\mathrm{Id}_\varnothing$. Если $Y = \varnothing$, а $X \neq \varnothing$, то $\operatorname{Hom}(X,\varnothing) = \varnothing$, что тоже согласуется с предл. 1.1, ибо $0^{|X|} = 0$ при $|X| > 0$.

Предложение 1.2
Если $|X| = n$, то $|\operatorname{Aut}(X)| = n! \stackrel{\text{def}}{=} n \cdot (n-1) \cdot \ldots \cdot 1$.

Доказательство. Пусть $X = \{x_1, \ldots, x_n\}$. Биекции $X \xrightarrow{\sim} X$ записываются n-буквенными словами в n-буквеном алфавите $x_1, \ldots, x_n$, содержащими каждую букву x_i ровно по одному разу. Обозначим количество таких слов через $V(n)$ и выпишем их по алфавиту на n страницах, поместив на i-тую страницу все слова, начинающиеся на x_i. Тогда на каждой странице будет ровно $V(n-1)$ слов, откуда $V(n) = n \cdot V(n-1) = n \cdot (n-1) \cdot V(n-2) = \ldots = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot V(1) = n!$. $\square$

Замечание 1.2. Число $n! = n \cdot (n-1) \cdot \ldots \cdot 1$ называется *n-факториалом*. Так как множество $\operatorname{Aut}(\varnothing)$ состоит из одного элемента $\mathrm{Id}_\varnothing$, мы полагаем $0! \stackrel{\text{def}}{=} 1$.

1.3. Слои отображений. Задание отображения $f : X \to Y$ равносильно указанию подмножества $\operatorname{im}(f) \subset Y$ и разбиению множества X в дизъюнктное объединение занумерованных точками $y \in \operatorname{im}(f)$ непустых подмножеств $f^{-1}(y)$:

$$X = \bigsqcup\nolimits_{y \in \operatorname{im}(f)} f^{-1}(y)\,. \tag{1-3}$$

Такой взгляд на отображения часто оказывается полезным при подсчёте количества элементов в том или ином множестве. Например, когда все непустые слои отображения $f : X \to Y$ состоят

[1] Т. е. 0^0 в этом контексте оказывается равным 1.

из одного и того же числа точек $m = |f^{-1}(y)|$, число элементов в образе отображения f связано с числом элементов в множестве X соотношением

$$|X| = m \cdot |\operatorname{im} f|\,, \tag{1-4}$$

которое при всей своей простоте имеет много разнообразных применений.

Пример 1.2 (мультиномиальные коэффициенты)
При раскрытии скобок в выражении $(a_1+\ldots+a_m)^n$ получится сумма одночленов вида $a_1^{k_1}\ldots a_m^{k_m}$, где каждый показатель k_i заключён в пределах $0 \leqslant k_i \leqslant n$, а общая степень $k_1 + \ldots + k_m = n$. Коэффициент, возникающий при таком одночлене после приведения подобных слагаемых, называется *мультиномиальным коэффициентом* и обозначается $\binom{n}{k_1\ldots k_m}$. Таким образом,

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{k_1+\ldots+k_m=n\\ \forall i\ 0\leqslant k_i\leqslant n}} \binom{n}{k_1\ldots k_m} \cdot a_1^{k_1}\ldots a_m^{k_m}\,, \tag{1-5}$$

Чтобы явно выразить $\binom{n}{k_1\ldots k_m}$ через $k_1, \ldots, k_m$, заметим, что раскрытие n скобок

$$(a_1 + \ldots + a_m)(a_1 + \ldots + a_m)\ldots(a_1 + \ldots + a_m)$$

заключается в выборе внутри каждой из скобок какой-нибудь одной буквы и выписывании их слева направо друг за другом в одно n-буквенное слово. Это надо сделать всеми возможными способами и сложить все полученные слова. Подобные слагаемые, вносящие вклад в коэффициент при $a_1^{k_1}a_2^{k_2}\ldots a_m^{k_m}$, суть слова, состоящие ровно из k_1 букв a_1, k_2 букв a_2, … , k_m букв a_m. Количество таких слов легко подсчитать по формуле (1-4). А именно, сделаем на время k_1 букв a_1 попарно разными, снабдив каждую из них дополнительным верхним индексом; аналогично поступим с k_2 буквами a_2, k_3 буквами a_3 и т. д. В результате получим $n = k_1 + \ldots + k_m$ попарно разных букв:

$$\underbrace{a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(k_1)}}_{k_1 \text{ меченых букв } a_1},\ \underbrace{a_2^{(1)}, a_2^{(2)}, \ldots, a_2^{(k_2)}}_{k_2 \text{ меченых букв } a_2},\ \ldots\ldots\ldots,\ \underbrace{a_m^{(1)}, a_m^{(2)}, \ldots, a_m^{(k_m)}}_{k_m \text{ меченых букв } a_m}.$$

Обозначим через X множество всех n-буквенных слов, которые можно написать этими n различными буквами, используя каждую букву ровно по одному разу. Как мы уже знаем, $|X| = n!$. В качестве Y возьмём интересующее нас множество слов из k_1 одинаковых букв a_1, k_2 одинаковых букв a_2, и т. д. и рассмотрим отображение $f : X \to Y$, стирающее верхние индексы у всех букв. Оно эпиморфно, и полный прообраз каждого слова $y \in Y$ состоит из $k_1! \cdot k_2! \cdot \ \ldots\ \cdot k_m!$ слов, которые получаются из y всевозможными расстановками k_1 верхних индексов у букв a_1, k_2 верхних индексов у букв a_2, и т. д. По формуле (1-4) получаем равенство

$$\binom{n}{k_1\ldots k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \ \ldots\ \cdot k_m!}\,. \tag{1-6}$$

Тем самым, разложение (1-5) имеет вид

$$(a_1 + \ldots + a_m)^n = \sum_{\substack{k_1+\ldots+k_m=n\\ \forall i\ 0\leqslant k_i\leqslant n}} \frac{n! \cdot a_1^{k_1}\ldots a_m^{k_m}}{k_1! \cdot \ldots \cdot k_m!}\,. \tag{1-7}$$

Упражнение 1.7. Сколько всего слагаемых в правой части формулы (1-7) ?

В частности, при $m = 2$ мы получаем известную формулу для раскрытия бинома с натуральным показателем[1]:

$$(a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}\, a^k b^{n-k}\,. \tag{1-8}$$

При $m = 2$ мультиномиальный коэффициент $\binom{n}{k,n-k}$ принято обозначать $\binom{n}{k}$ или C_n^k и называть k-тым *биномиальным коэффициентом* степени n или *числом сочетаний* из n по k. Он равен

$$\binom{n}{k} = C_n^k = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k\cdot(k-1)\cdot\ldots\cdot 1}$$

(сверху и снизу стоит по k последовательно убывающих сомножителей).

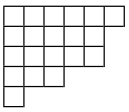
Пример 1.3 (диаграммы Юнга)
Разбиение конечного множества $X = \{1,\,2,\,\ldots\,,\,n\}$ в объединение непересекающихся подмножеств

$$X = X_1 \sqcup X_2 \sqcup \ldots \sqcup X_k \tag{1-9}$$

можно кодировать следующим образом. Занумеруем подмножества в порядке нестрогого убывания их размера и обозначим количество элементов в i-том подмножестве через $\lambda_i = |X_i|$. Получим невозрастающую последовательность чисел

$$\lambda = (\lambda_1, \ldots, \lambda_k)\,, \quad \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_k\,,$$

которая называется *формой* разбиения (1-9). Форму разбиения удобно изображать *диаграммой Юнга* — картинкой вида

 , (1-10)

составленной из выровненных по левому краю горизонтальных клетчатых полосок, занумерованных сверху вниз, так что в i-й сверху полоске λ_i клеток. Общее число клеток в диаграмме λ называется её *весом* и обозначается $|\lambda|$, а количество строк называется *длиной* и обозначается $\ell(\lambda)$. Так, диаграмма Юнга (1-10) отвечает разбиению формы $\lambda = (6,5,5,3,1)$, имеет вес $|\lambda| = 20$ и длину $\ell(\lambda) = 5$.

Упражнение 1.8. Подсчитайте количество всех диаграмм Юнга, умещающихся в прямоугольнике размером $k \times n$ клеток (включая пустую диаграмму и сам прямоугольник).

Будем называть *заполнением* диаграммы λ множеством X из $|X| = |\lambda|$ элементов произвольную расстановку этих элементов в клетки диаграммы по одному элементу в каждую клетку. Таким образом, всякая диаграмма λ веса n имеет $n!$ различных заполнений заданным n-элементным множеством X.

Объединяя элементы, стоящие в i-й строке диаграммы в одно подмножество X_i, мы получаем разбиение множества X в дизъюнктное объединение k непересекающихся подмножеств

[1] Это частный случай *формулы Ньютона*, которую в полной общности мы обсудим в n° 4.3.2 на стр. 69, когда будем заниматься степенными рядами.

$X_1, \dots, X_k$. Поскольку любое разбиение (1-9) заданной формы λ можно получить таким образом, возникает сюръективное отображение из множества заполнений диаграммы λ в множество разбиений множества X формы λ. Покажем, что все слои этого отображения состоят из одного и того же числа элементов. Два заполнения приводят к одинаковым разбиениям тогда и только тогда, когда они получаются друг из друга перестановками элементов внутри строк и перестановками строк одинаковой длины между собою как единого целого. Если обозначить через $m_i = m_i(\lambda)$ число строк длины[1] i в диаграмме λ, то перестановок первого типа будет $\prod \lambda_i! = \prod_{i=1}^n (i!)^{m_i}$ штук, а второго типа — $\prod_{i=1}^n m_i!$ штук. Так как все эти перестановки действуют независимо друг от друга, каждый слой нашего отображения состоит из $\prod_{i=1}^n (i!)^{m_i} m_i!$ элементов. Из формулы (1-4) вытекает

Предложение 1.3
Число разбиений n-элементного множества X в дизъюнктное объединение m_1 1-элементных, m_2 2-элементных, … , m_n n-элементных подмножеств равно

$$\frac{n!}{\prod_{i=1}^n m_i! \cdot (i!)^{m_i}}\,. \tag{1-11}$$

1.4. Классы эквивалентности. Альтернативный способ разбить заданное множество X в дизъюнктное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения «эквивалентными». Формализуется это так. Назовём *бинарным отношением* на множестве X любое подмножество

$$R \subset X \times X = \{(x_1, x_2) \mid x_1, x_2 \in X\}\,.$$

Принадлежность пары (x_1, x_2) отношению R обычно записывают как $x_1 \underset{R}{\sim} x_2$.

Например, на множестве целых чисел $X = \mathbb{Z}$ имеются бинарные отношения

$$\text{равенство} \quad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 = x_2 \tag{1-12}$$

$$\text{неравенство} \quad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \leqslant x_2 \tag{1-13}$$

$$\text{делимость} \quad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \text{ делит } x_2 \tag{1-14}$$

$$\text{сравнимость по модулю } n \quad x_1 \underset{R}{\sim} x_2 \overset{\text{def}}{\iff} x_1 \equiv x_2 \pmod n \tag{1-15}$$

(последнее условие $x_1 \equiv x_2 \pmod n$ читается как «x_1 сравнимо с x_2 по модулю n» и по определению означает, что $x_1 - x_2$ делится на n).

Определение 1.1
Бинарное отношение $\underset{R}{\sim}$ называется *эквивалентностью*, если оно обладает следующими тремя свойствами:

рефлексивность: $\forall\, x \in X \; x \underset{R}{\sim} x$

транзитивность: $\forall\, x_1, x_2, x_3 \in X$ из $x_1 \underset{R}{\sim} x_2$ и $x_2 \underset{R}{\sim} x_3$ вытекает $x_1 \underset{R}{\sim} x_3$

симметричность: $\forall\, x_1, x_2 \in X \; x_1 \underset{R}{\sim} x_2 \iff x_2 \underset{R}{\sim} x_1$.

[1] Отметим, что многие $m_i = 0$, поскольку $|\lambda| = n = m_1 + 2m_2 + \dots + nm_n$.

Среди бинарных отношений (1-12) – (1-15) первое и последнее являются эквивалентностями, а (1-13) и (1-14) не являются (они не симметричны).

Если множество X разбито в объединение непересекающихся подмножеств, то отношение $x_1 \sim x_2$, означающее, что x_1 и x_2 лежат в одном и том же подмножестве этого разбиения, очевидно, является эквивалентностью.

Наоборот, пусть на множестве X задано отношение эквивалентности R. Рассмотрим для каждого $x \in X$ подмножество в X, состоящее из всех элементов, эквивалентных x. Оно называется *классом эквивалентности* элемента x и обозначается

$$[x]_R = \{z \in X \mid x \underset{R}{\sim} z\} = \{z \in X \mid z \underset{R}{\sim} x\}$$

(второе равенство выполняется благодаря симметричности отношения R). Любые два класса $[x]_R$ и $[y]_R$ либо вообще не пересекаются, либо полностью совпадают. В самом деле, если существует элемент z, эквивалентный и x и y, то в силу симметричности и транзитивности отношения $\underset{R}{\sim}$ элементы x и y будут эквивалентны между собой, а значит, любой элемент, эквивалентный x, будет эквивалентен также и y, и наоборот. Таким образом, множество X распадается в дизъюнктное объединение различных классов эквивалентности.

Множество классов эквивалентности по отношению $R \subset X \times X$ обозначается X/R и называется *фактором* множества X по эквивалентности R. Сюрьекция

$$f : X \twoheadrightarrow X/R\,, \quad x \mapsto [x]_R\,, \tag{1-16}$$

сопоставляющая каждому элементу $x \in X$ его класс эквивалентности $[x]_R \in X/R$, называется *отображением факторизации*. Слои этого отображения суть классы эквивалентных элементов. Наоборот, любое сюрьективное отображение $f : X \twoheadrightarrow Y$ является отображением факторизации по отношению эквивалентности $x_1 \sim x_2$, означающему, что $f(x_1) = f(x_2)$.

Пример 1.4 (классы вычетов)
Фиксируем ненулевое целое число $n \in \mathbb{Z}$. Фактор множества целых чисел $\mathbb{Z}$ по отношению сравнимости по модулю n из (1-15) обозначается $\mathbb{Z}/(n)$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$, и опускать индекс n, когда понятно чему он равен. Класс эквивалентности

$$[z]_n \overset{\text{def}}{=} \{x \in \mathbb{Z} \mid (z - x) \text{ делится на } n\} \tag{1-17}$$

называется *классом вычетов по модулю* n. Отображение факторизации

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n)\,, \quad z \mapsto [z]_n$$

называется *приведением по модулю* n. Множество $\mathbb{Z}/(n)$ состоит из n различных классов

$$[0]_n\,,\ [1]_n\,,\ \ldots\,,\ [n-1]_n\,.$$

При желании их можно воспринимать как остатки от деления на n, однако в практических вычислениях удобнее работать именно с *подмножествами*, так как возможность по-разному записывать один и тот же класс часто упрощает вычисления. Например, остаток от деления 12^{100} на 13 можно искать как

$$\left[12^{100}\right]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = \left[(-1)^{100}\right]_{13} = [1]_{13}\,. \tag{1-18}$$

Упражнение 1.9. Докажите правомочность этого вычисления: проверьте, что классы вычетов $[x+y]_n$ и $[xy]_n$ не зависят от выбора чисел $x \in [x]_n$ и $y \in [y]_n$, т. е. правила

$$[x]_n + [y]_n \stackrel{\text{def}}{=} [x+y]_n \tag{1-19}$$

$$[x]_n \cdot [y]_n \stackrel{\text{def}}{=} [xy]_n \tag{1-20}$$

корректно определяют на множестве $\mathbb{Z}/(n)$ операции сложения и умножения[1].

1.4.1. Неявное задание эквивалентности. Для любого семейства отношений эквивалентности $R_\nu \subset X \times X$ пересечение $\bigcap_\nu R_\nu \subset X \times X$ также является отношением эквивалентности. В самом деле, если каждое из множеств $R_\nu \subset X \times X$ содержит диагональ

$$\Delta = \{(x,x) \mid x \in X\} \subset X \times X\,,$$

переходит в себя при симметрии $(x,y) \leftrightarrows (y,x)$ и вместе с каждой парой точек вида (x,y), (y,z) содержит также и точку (x,z), то этими свойствами обладает и пересечение $\bigcap_\nu R_\nu$ всех этих множеств. Поэтому для любого подмножества $R \subset X \times X$ существует *наименьшее по включению* отношение эквивалентности $\overline{R}$, содержащее R, а именно пересечение всех содержащих R отношений эквивалентности. Отношение $\overline{R}$ называется эквивалентностью, *порождённой* отношением R.

Упражнение 1.10. Проверьте, что $(x,y) \in \overline{R}$ если и только если в X существует такая конечная последовательность точек $x = z_0, z_1, z_2, \dots, z_n = y$, что $(z_{i-1}, z_i) \in R$ или $(z_i, z_{i-1}) \in R$ при каждом $i = 1, 2, \dots, n$.

К сожалению, по данному подмножеству $R \subset X \times X$ не всегда легко судить о том, как устроена порождённая им эквивалентность $\overline{R}$. Даже выяснить, не окажутся ли в результате все точки эквивалентными друг другу может быть не просто.

Пример 1.5 (дроби)
Множество рациональных чисел $\mathbb{Q}$ обычно определяют как множество дробей a/b с $a, b \in \mathbb{Z}$ и $b \neq 0$. При этом под *дробью* понимается класс эквивалентности упорядоченных пар (a,b), где $a, b \in \mathbb{Z}$ и $b \neq 0$, по минимальному отношению эквивалентности, содержащему все отождествления

$$(a,b) \sim (ac, bc) \quad \text{с произвольными } c \in \mathbb{Z} \smallsetminus \{0\}\,. \tag{1-21}$$

Отношения (1-21) выражают равенства дробей $a/b = (ac)/(bc)$, но сами по себе не образуют эквивалентности. Например, при $a_1 b_2 = a_2 b_1$ в двухшаговой цепочке отождествлений $(a_1, b_1) \sim (a_1 b_2, b_1 b_2) = (a_2 b_1, b_1 b_2) \sim (a_2, b_2)$ самый левый и самый правый элементы могут не отождествляться напрямую по правилу (1-21), как, например, $3/6$ и $5/10$. Поэтому эквивалентность, порождённая отождествлениями (1-21), обязана содержать все отождествления

$$(a_1, b_1) \sim (a_2, b_2) \quad \text{при} \quad a_1 b_2 = a_2 b_1\,. \tag{1-22}$$

Оказывается, к этим отношениям больше уже ничего добавлять не надо.

[1] Именно такое умножение $[12]^{100} = \underbrace{[12]\cdot[12]\cdot\ldots\cdot[12]}_{100} = \left[12^{100}\right]$ было использовано в (1-18).

Упражнение 1.11. Проверьте, что набор отношений (1-22) рефлексивен, симметричен и транзитивен.

Тем самым, он является минимальным отношением эквивалентности, содержащим все отождествления (1-21). Отметим, что если в отношениях (1-21) разрешить нулевые c, то все пары (a, b) окажутся эквивалентны паре $(0, 0)$.

1.5. Композиции отображений. Отображение $X \to Z$, получающееся в результате последовательного выполнения двух отображений $f : X \to Y$ и $g : Y \to Z$ называется *композицией* отображений g и f и обозначается $g \circ f$ или просто gf. Таким образом, композиция gf определена если и только если образ отображения f содержится в множестве, на котором определено отображение g, и в этом случае $gf : X \to Z$, $x \mapsto g(f(x))$.

Хотя композицию и принято записывать точно так же, как умножение чисел, единственным общим свойством этих операций является их *ассоциативность* или *сочетательный закон*: композиция трёх последовательных отображений

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} T\,,$$

как и произведение трёх чисел, не зависит от того, в каком порядке перемножаются последовательные пары элементов, т. е. $(hg)f = h(gf)$, если хотя бы одна из двух частей этого равенства определена. Действительно, в этом случае вторая часть тоже определена, и обе части действуют на каждую точку $x \in X$ по правилу $x \mapsto h(g(f(x)))$.

В остальном алгебраические свойства композиции весьма далеки от привычных свойств умножения чисел. Если композиция fg определена, то противоположная композиция gf часто бывает не определена. Даже если $f, g : X \to X$ являются эндоморфизмами одного и того же множества X, так что обе композиции fg и gf определены, равенство $fg = gf$ может не выполняться.

Упражнение 1.12. Рассмотрим на плоскости пару различных прямых ℓ_1, ℓ_2, пересекающихся в точке O, и обозначим через σ_1 и σ_2 осевые симметрии относительно этих прямых. Явно опишите движения плоскости, задаваемые композициями $\sigma_1\sigma_2$ и $\sigma_2\sigma_1$. При каком условии на прямые выполняется равенство $\sigma_1\sigma_2 = \sigma_2\sigma_1$?

Общие множители тоже бывает нельзя сокращать, т. е. ни равенство $fg = fh$, ни равенство $gf = hf$, вообще говоря, не влекут равенства $g = h$.

Пример 1.6 (эндоморфизмы двухэлементного множества)
Двухэлементное множество $X = \{1, 2\}$ имеет ровно четыре эндоморфизма. Если кодировать отображение $f : X \to X$ двубуквенным словом $(f(1), f(2))$, как в прим. 1.1 на стр. 7, то эти четыре эндоморфизма запишутся словами $(1, 1)$, $(1, 2) = \mathrm{Id}_X$, $(2, 1)$ и $(2, 2)$. Все композиции между ними определены, и таблица композиций gf имеет вид:

$g \diagdown f$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$
$(1,2)$	$(1,1)$	$(1,2)$	$(2,1)$	$(2,2)$
$(2,1)$	$(2,2)$	$(2,1)$	$(1,2)$	$(1,1)$
$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$	$(2,2)$.

(1-23)

Обратите внимание на то, что $(2, 2) \circ (1, 1) \neq (1, 1) \circ (2, 2)$ и что $(1, 1) \circ (1, 2) = (1, 1) \circ (2, 1)$, хотя $(1, 2) \neq (2, 1)$, и $(1, 1) \circ (2, 2) = (2, 1) \circ (2, 2)$, хотя $(1, 1) \neq (2, 1)$.

Лемма 1.1 (левые обратные отображения)
Если $X \neq \varnothing$, то следующие условия на отображение $f : X \to Y$ эквивалентны:

1) f инъективно

2) существует такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$

3) для любых отображений $g_1, g_2 : Z \to X$ из равенства $fg_1 = fg_2$ вытекает равенство $g_1 = g_2$.

Доказательство. Импликация (1) ⇒ (2): для точек $y = f(x) \in \operatorname{im} f$ положим $g(y) = x$, а в точках $y \notin \operatorname{im} f$ зададим g как угодно[1]. Импликация (2) ⇒ (3): если $fg_1 = fg_2$, то умножая обе части слева на любое такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$, получаем $g_1 = g_2$. Импликация (3) ⇒ (1) доказывается от противного. Пусть $x_1 \neq x_2$, но $f(x_1) = f(x_2)$. Положим $g_1 = \mathrm{Id}_X$, и пусть $g_2 : X \rightrightarrows X$ переставляет между собою точки x_1, x_2, а все остальные точки оставляет на месте. Тогда $g_1 \neq g_2$, но $fg_1 = fg_2$. □

Определение 1.2
Отображение $f : X \to Y$, удовлетворяющее лем. 1.1, называется *обратимым слева*, и всякое такое отображение $g : Y \to X$, что $gf = \mathrm{Id}_X$, называется *левым обратным* к f или *ретракцией* Y на $f(X)$.

Упражнение 1.13. В условиях лем. 1.1 убедитесь, что вложение f тогда и только тогда имеет несколько различных левых обратных, когда оно не сюръективно.

1.5.1. Правое обратное отображение и аксиома выбора. Стремление к гармонии вызывает желание иметь «правую» версию лем. 1.1 — хочется, чтобы следующие три свойства отображения $f : X \to Y$ тоже были эквивалентны:

1) f сюръективно

2) существует такое отображение $g : Y \to X$, что $fg = \mathrm{Id}_Y$

3) для любых отображений $g_1, g_2 : Y \to Z$ из равенства $g_1 f = g_2 f$ вытекает равенство $g_1 = g_2$.

Отображение f, удовлетворяющее свойству (2), называется *обратимым справа*, а такое отображение $g : Y \to X$, что $fg = \mathrm{Id}_Y$, называется *правым обратным* к f или *сечением* эпиморфизма f. Второе название связано с тем, что отображение g, удовлетворяющее свойству (2), переводит каждую точку $y \in Y$ в точку $g(y) \in f^{-1}(y)$, лежащую в слое отображения f над точкой y.

В строгой теории множеств, углубления в которую мы пытаемся избежать, импликация (1) ⇒ (2) постулируется в качестве одной из аксиом. Эта аксиома называется *аксиомой выбора* и утверждает, что в каждом слое любого сюръективного отображения можно выбрать по элементу[2].

Доказательство импликации (2) ⇒ (3) полностью симметрично доказательству аналогичной импликации из лем. 1.1: применяя отображения, стоящие в обеих частях равенства $g_1 f = g_2 f$, вслед за таким отображением $g : Y \to X$, что $fg = \mathrm{Id}_Y$, получаем равенство $g_1 = g_2$.

[1] Например, отобразим их все в одну и ту же произвольно выбранную точку $x \in X$.

[2] Иными словами, если имеется множество попарно непересекающихся множеств, то в каждом из них можно выбрать по элементу.

Импликация (3) ⇒ (1), как и в лем. 1.1, доказывается от противного: если $y \notin \operatorname{im} f$, то свойство (3) не выполняется для отображения $g_1 = \mathrm{Id}_Y$ и любого отображения $g_2 : Y \to Y$, переводящего точку y в какую-нибудь точку из $\operatorname{im} f$ и оставляющего на месте все остальные точки.

Таким образом, перечисленные выше свойства (1) – (3) действительно эквивалентны друг другу, если включить аксиому выбора в список свойств, определяющих множества.

1.5.2. Обратимые отображения. Если отображение $g : X \xrightarrow{\sim} Y$ биективно, то прообраз $g^{-1}(y) \subset X$ каждой точки $y \in Y$ состоит ровно из одной точки. В этом случае правило $y \mapsto g^{-1}(y)$ определяет отображение $g^{-1} : Y \to X$, которое является одновременно и левым, и правым обратным к g в смысле опр. 1.2 и n° 1.5.1, т. е.

$$g \circ g^{-1} = \mathrm{Id}_Y \qquad \text{и} \qquad g^{-1} \circ g = \mathrm{Id}_X \tag{1-24}$$

Отображение g^{-1} называется *обратным* к биективному отображению g.

Предложение 1.4
Следующие условия на отображение $g : X \to Y$ эквивалентны друг другу:

1) g взаимно однозначно

2) существует такое отображение $g' : Y \to X$, что[1] $g \circ g' = \mathrm{Id}_Y$ и $g' \circ g = \mathrm{Id}_X$

3) g обладает левым и правым обратными отображениями[2].

При выполнении этих условий все левые и правые обратные к g отображения равны друг другу и отображению g^{-1}, описанному перед формулировкой предложения.

Доказательство. Импликация (1) ⇒ (2) уже была установлена. Очевидно, что (2) ⇒ (3). Докажем, что (3) ⇒ (2). Если у отображения $g : X \to Y$ есть левое обратное $f : Y \to X$ и правое обратное $h : Y \to X$, то $f = f \circ \mathrm{Id}_Y = f \circ (g \circ h) = (f \circ g) \circ h = \mathrm{Id}_X \circ h = h$ и условие (2) выполнено для $g' = f = h$. Остаётся показать, что (2) ⇒ (1), и $g' = g^{-1}$. Так как $g(g'(y)) = y$ для любого $y \in Y$, прообраз $g^{-1}(y)$ каждой точки $y \in Y$ содержит точку $g'(y)$. С другой стороны, поскольку для всех $x \in g^{-1}(y)$ выполнено равенство $x = \mathrm{Id}_X(x) = g'(g(x)) = g'(y)$, прообраз $f^{-1}(y)$ состоит из единственной точки $g'(y)$, т. е. g — биекция, и $g' = g^{-1}$. □

1.6. Группы преобразований. Непустой набор G взаимно однозначных отображений множества X в себя называется *группой преобразований* множества X, если вместе с каждым отображением $g \in G$ в G лежит и обратное к нему отображение g^{-1}, а вместе с каждыми двумя отображениями $f, g \in G$ в G лежит и их композиция fg. Эти условия гарантируют, что тождественное преобразование Id_X тоже лежит в G, поскольку $\mathrm{Id}_X = g^{-1}g$ для любого $g \in G$. Если группа преобразований G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G. Если подмножество $H \subset G$ тоже является группой, то H называются *подгруппой* группы G.

Пример 1.7 (группы перестановок)
Множество $\mathrm{Aut}(X)$ всех взаимно однозначных отображений $X \to X$ является группой. Эта группа называется *симметрической группой* или *группой перестановок* множества X. Все прочие

[1] Т. е. g' *двусторонне* обратно к g.

[2] Обратите внимание, что совпадения левого обратного отображения с правым обратным отображением не требуется.

группы преобразований множества X являются подгруппами этой группы. Группа перестановок n-элементного множества $\{1,\ 2,\ \dots\ ,\ n\}$ обозначается S_n и называется n-й *симметрической группой*. Согласно предл. 1.2 на стр. 8 порядок $|S_n| = n!$. Перестановки

$$\sigma :\ \{1,\ 2,\ \dots\ ,\ n\} \to \{1,\ 2,\ \dots\ ,\ n\}$$

принято записывать строчками $\sigma = (\sigma_1, \dots, \sigma_n)$ их значений $\sigma_i \stackrel{\text{def}}{=} \sigma(i)$, как в прим. 1.1 на стр. 7. Например, перестановки $\sigma = (3, 4, 2, 1)$ и $\tau = (2, 3, 4, 1)$ представляют собою отображения

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 2 & 1 \end{array} \quad \text{и} \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

а их композиции записываются как $\sigma\tau = (4, 2, 1, 3)$ и $\tau\sigma = (4, 1, 3, 2)$.

Упражнение 1.14. Составьте таблицу умножения шести элементов группы S_3, аналогичную таблице (1-23) на стр. 14.

Пример 1.8 (абелевы группы)
Группа G, в которой любые два элемента $f, g \in G$ перестановочны, т. е. удовлетворяют соотношению $fg = gf$, называется *коммутативной* или *абелевой*. Примерами абелевых групп являются группы параллельных переносов плоскости или пространства, а также группа SO_2 поворотов плоскости вокруг фиксированной точки. Для каждого натурального $n \geqslant 2$ повороты на углы, кратные $2\pi/n$, образуют в группе SO_2 конечную подгруппу. Она называется *циклической группой порядка* n.

1.7. Частично упорядоченные множества. Бинарное отношение[1] $x \leqslant y$ на множестве Z называется *частичным порядком*, если оно рефлексивно и транзитивно[2], но в отличие от эквивалентности не симметрично, а *кососимметрично*, т. е. из $x \leqslant y$ и $y \leqslant x$ вытекает равенство $x = y$. Если на множестве задан частичный порядок, мы пишем $x < y$, когда $x \leqslant y$ и $x \neq y$. Частичный порядок на множестве Z называется *линейным* (или просто *порядком*), если любые два элемента сравнимы, т. е. для всех $x, y \in Z$ выполняется одно из трёх альтернативных условий: или $x < y$, или $x = y$, или $y < x$. Например, обычное неравенство между числами является линейным порядком на множестве натуральных чисел $\mathbb{N}$, тогда как отношение делимости $n \mid m$, означающее, что n делит m, задаёт на $\mathbb{N}$ частичный порядок, который не является линейным. Другим важным примером частичного, но не линейного порядка является отношение включения $X \subseteq Y$ на множестве $\mathcal{S}(M)$ всех подмножеств заданного множества M.

Упражнение 1.15 (предпорядок). *Предпорядком* на множестве Z называется любое рефлексивное транзитивное бинарное отношение $x \prec y$. Убедитесь, что для каждого предпорядка бинарное отношение $x \sim y$, означающее, что одновременно $x \prec y$ и $y \prec x$, является отношением эквивалентности, и на факторе $Z/\sim$ корректно определено[3] бинарное отношение $[x] \leqslant [y]$, которое означает, что $x \prec y$, и является частичным порядком. Продумайте, как всё это работает для отношения делимости $n \mid m$ на множестве целых чисел $\mathbb{Z}$.

[1] См. n° 1.4 на стр. 11.
[2] Ср. с опр. 1.1 на стр. 11.
[3] Т. е. выполнение или невыполнение условия $x \prec y$ не зависит от выбора представителей x и y в классах $[x]$ и $[y]$.

Множество P с зафиксированным на нём частичным порядком называется *частично упорядоченным множеством*, сокращённо — чумом. Если порядок линейный, чум P называется *линейно упорядоченным*. Всякое подмножество X любого чума P также является чумом по отношению к частичному порядку, имеющемуся на P. Если этот индуцированный с P порядок на X оказывается линейным, подмножество $X \subset P$ называют *цепью* в чуме P. Элементы x, y чума P называются *сравнимыми*, если $x \leqslant y$ или $y \leqslant x$. Если же ни одно из этих условий не выполняется, то x и y называются *несравнимыми*. Несравнимые элементы автоматически различны. Частичный порядок линеен тогда и только тогда, когда любые два элемента сравнимы.

Отображение $f : M \to N$ между чумами M, N называется *сохраняющим порядок*[1] или *гоморфизмом* чумов, если $f(x) \leqslant f(y)$ для всех $x \leqslant y$. Два чума M, N называются *изоморфными*, если имеется сохраняющая порядок биекция $M \xrightarrow{\sim} N$. В таком случае мы пишем $M \simeq N$. Отображение f называется *строго возрастающим*, если $f(x) < f(y)$ для всех $x < y$. Всякое сохраняющее порядок вложение является строго возрастающим. Обратное справедливо для возрастающих отображений из линейного упорядоченного множества, однако неверно в общем случае.

Элемент y чума P называется *верхней гранью* подмножества $X \subset P$, если $x \leqslant y$ для всех $x \in X$. Если при этом $y \notin X$, то верхняя грань y называется *внешней*. В таком случае для всех $x \in X$ выполнено строгое неравенство $x < y$.

Элемент $m^* \in X$ называется *максимальным* в подмножестве $X \subset P$, если для $x \in X$ неравенство $m^* \leqslant x$ выполняется только при $x = m^*$. Заметьте, что максимальный элемент не обязан быть сравним со всеми элементами $x \in X$ и, тем самым, может не являться верхней гранью для X. Частично упорядоченное множество может иметь несколько различных максимальных элементов или не иметь их вовсе, как, например, чум $\mathbb{N}$ по отношению к делимости или к обычному неравенству между числами. Линейно упорядоченный чум имеет не более одного максимального элемента, и если такой элемент существует, то он является верхней гранью.

Симметричным образом, элемент $m_* \in X$ называется *минимальным* в X, если для $x \in X$ неравенство $m_* \geqslant x$ выполняется только при $x = m_*$. Аналогично определяются и нижние грани, и всё сказанное выше о максимальных элементах и верхних гранях в равной степени относится и к минимальным элементам и нижним граням.

1.8. Вполне упорядоченные множества. Линейно упорядоченное множество W называется *вполне упорядоченным*, если каждое непустое подмножество $S \subset W$ содержит такой элемент $s_* \in S$, что $s_* \leqslant s$ для всех $s \in S$. Этот элемент автоматически единствен и называется *начальным элементом* подмножества S. Например, множество натуральных чисел $\mathbb{N}$ со стандартным отношением неравенства между числами вполне упорядочено, как и любое дизъюнктное объединение вида $\mathbb{N} \sqcup \mathbb{N} \sqcup \mathbb{N} \sqcup \mathbb{N} \sqcup \ldots$, в котором все элементы каждой копии множества $\mathbb{N}$ полагаются строго большими всех элементов всех предыдущих копий. Пустое множество тоже вполне упорядочено. Напротив, множество $\mathbb{Q}$ со стандартным отношением неравенства между числами не является вполне упорядоченным.

Вполне упорядоченные множества замечательны тем, что их элементы можно рекурсивно перебрать точно также, как и элементы множества $\mathbb{N}$. А именно, пусть некоторое утверждение $\Phi(w)$ зависит от элемента w вполне упорядоченного множества W. Если $\Phi(w)$ истинно для начального элемента w_* множества W, и для каждого $w \in W$ истинность утверждения $\Phi(x)$ при всех $x < w$ влечёт за собою истинность утверждения $\Phi(w)$, то $\Phi(w)$ истинно для всех $w \in W$.

[1] А также *неубывающим* или *нестрого возрастающим*.

Упражнение 1.16. Убедитесь в этом.

Такой способ доказательства утверждения $\Phi(w)$ для всех $w \in W$ называется *трансфинитной индукцией*. Используемые для индуктивного перехода подмножества, состоящие из всех элементов, предшествующих данному элементу w, называются *начальными интервалами* частично упорядоченного множества W и обозначаются

$$[w) \stackrel{\text{def}}{=} \{x \in W \mid x < w\}.$$

Элемент $w \in W$ называется *точной верхней гранью* начального интервала $[w) \subset W$ и однозначно восстанавливается по интервалу $[w)$ как начальный элемент множества $W \smallsetminus [w)$. Отметим, что начальный элемент $w_* \in W$ является точной верхней гранью пустого начального интервала $[w_*) = \varnothing$.

Упражнение 1.17. Покажите, что собственное подмножество $I \subsetneq W$ тогда и только тогда является начальным интервалом вполне упорядоченного множества W, когда $[x) \subset I$ для каждого $x \in I$, и в этом случае точная верхняя грань интервала I однозначно восстанавливается по I как начальный элемент дополнения $W \smallsetminus I$.

Между вполне упорядоченными множествами имеется отношение порядка $U \leqslant W$, означающее, что U можно биективно и с сохранением порядка отобразить на W или на какой-нибудь начальный интервал $[w) \subset W$. Если при этом U и W не изоморфны, мы пишем $U < W$. Хорошим упражнением на трансфинитную индукцию является

Упражнение 1.18. Убедитесь, что для любой пары вполне упорядоченных множеств U, W выполнено ровно одно из соотношений: или $U < W$, или $U \simeq W$, или $W < U$.

Классы изоморфных вполне упорядоченных множеств называют *ординалами*. Множество $\mathbb{N}$ со стандартным порядком можно воспринимать как множество всех конечных ординалов. Все остальные ординалы, включая $\mathbb{N}$, называются *трансфинитными*.

1.9. Лемма Цорна. Рассмотрим произвольное частично упорядоченное множество P и обозначим через $\mathcal{W}(P)$ множество всех подмножеств $W \subset P$, которые вполне упорядочены имеющимся на P отношением $x \leqslant y$. Множество $\mathcal{W}(P)$ непусто и содержит пустое подмножество $\varnothing \subset P$, а также все конечные цепи[1] $C \subset P$, в частности, все элементы множества P.

Лемма 1.2
Не существует такого отображения $\varrho : \mathcal{W}(P) \to P$, что $\varrho(W) > w$ для всех $W \in \mathcal{W}(P)$ и $w \in W$.

Доказательство. Пусть такое отображение ϱ существует. Назовём вполне упорядоченное подмножество $W \subset P$ рекурсивным, если $\varrho([w)) = w$ для всех $w \in W$. Например, подмножество

$$\Big\{\varrho(\varnothing),\ \varrho\big(\{\varrho(\varnothing)\}\big),\ \varrho\Big(\big\{\varrho(\varnothing),\ \varrho(\{\varrho(\varnothing)\})\big\}\Big),\ \ldots\Big\}$$

рекурсивно и его можно расширять дальше вправо, пока P не исчерпается, что противоречит наложенному на ϱ условию. Уточним сказанное. Если два рекурсивных вполне упорядоченных подмножества имеют общий начальный элемент, то либо они совпадают, либо одно из них является начальным интервалом другого.

Упражнение 1.19. Докажите это.

[1] Т. е. конечные линейно упорядоченные подмножества.

Обозначим через $U \subset P$ объединение всех рекурсивных вполне упорядоченных подмножеств в P с начальным элементом $\varrho(\varnothing)$.

Упражнение 1.20. Убедитесь, что подмножество $U \subset P$ вполне упорядочено и рекурсивно.

Поскольку элемент $\varrho(U)$ строго больше всех элементов из U, он не лежит в U. С другой стороны, множество $W = U \cup \{\varrho(U)\}$ вполне упорядочено, рекурсивно, и его начальным элементом является $\varrho(\varnothing)$. Следовательно, $W \subset U$, откуда $\varrho(U) \in U$. Противоречие. □

Предложение 1.5
Если каждое вполне упорядоченное подмножество чума P имеет верхнюю грань[1], то в P есть максимальный элемент[2] (возможно не единственный).

Доказательство. Если максимального элемента нет, то для любого $p \in P$ имеется такой элемент $p' \in P$, что $p < p'$. Тогда для каждого вполне упорядоченного подмножества $W \subset P$ найдётся такой элемент $w^* \in P$, что $w < w^*$ для всех $w \in W$. Сопоставляя каждому $W \in \mathcal{W}$ один[3] из таких элементов w^*, мы получаем отображение $\varrho : \mathcal{W} \to P$, которого не может быть по лем. 1.2. □

Определение 1.3 (полные чумы)
Частично упорядоченное множество называется *полным*, если каждая его цепь имеет верхнюю грань.

Следствие 1.1 (лемма Цорна)
В каждом полном чуме есть максимальный элемент (возможно не единственный). □

Упражнение 1.21 (лемма Бурбаки – Витта о неподвижной точке). Пусть отображение из полного чума в себя $f : P \to P$ таково, что $f(x) \geqslant x$ для всех $x \in P$. Покажите, что существует такое $p \in P$, что $f(p) = p$.

Упражнение 1.22 (теорема Цермелло). Докажите, что каждое множество можно вполне упорядочить.

Упражнение 1.23 (теорема Хаусдорфа о максимальной цепи). Докажите, что в любом чуме каждая цепь содержится в некоторой максимальной по включению цепи.

Задачи для самостоятельного решения к §1

Задача 1.1. Сколько имеется таких отображений из пятиэлементного множества в двухэлементное, чтобы у каждой точки было не менее двух прообразов?

Задача 1.2. Для конечных множеств X, Y с $|X| \geqslant |Y|$ найдите число всех отображений
а) $X \to Y$, являющихся левыми обратными к заданному вложению $Y \hookrightarrow X$
б) $Y \to X$, являющихся правыми обратными к заданному наложению $X \twoheadrightarrow Y$.

[1] Т. е. для любого вполне упорядоченного $W \subset P$ найдётся такой $p \in P$, что $w \leqslant p$ для всех $w \in W$.
[2] Т. е. такой $p^* \in P$, что неравенство $p^* \leqslant x$ выполняется в P только для $x = p^*$, см. последние два абзаца перед n° 1.8 на стр. 18.
[3] Для этого придётся воспользоваться аксиомой выбора из n° 1.5.1 на стр. 15.

Задача 1.3. Фиксируем $m, n \in \mathbb{N}$. Сколько имеется отображений $\{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$
а) произвольных б) биективных в) возрастающих[1] г) инъективных
д) неубывающих[2] е) сюръективных неубывающих ж*) сюръективных?

Задача 1.4. Сколько разных слов (не обязательно осмысленных) можно получить переставляя буквы в словах а) шнурок б) курок в) колобок г) $\underbrace{\text{а}\ldots\text{а}}_{a}\underbrace{\text{б}\ldots\text{б}}_{b}$?

Задача 1.5. Раскройте скобки и приведите подобные слагаемые в выражениях
а) $(a_1 + a_2 + \ldots + a_m)^2$ б) $(a + b + c)^3$.

Задача 1.6. Сколько а) натуральных б) целых неотрицательных решений имеет при заданных натуральных m, n уравнение $x_1 + \ldots + x_m = n$?

Задача 1.7. Сколько имеется различных мономов от n переменных полной степени[3]
а) ровно d б) не больше, чем d?

Задача 1.8. Цело ли число $1000!/\left(100!^{10}\right)$?

Задача 1.9. Вычислите суммы: а) $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$ б) $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \ldots$
в) $\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{k+n}{k}$ г) $\binom{n}{1} + 2\binom{n}{2} + \ldots + n\binom{n}{n}$ д) $\binom{n}{0} + 2\binom{n}{1} + \ldots + (n+1)\binom{n}{n}$
е) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots + (-1)^n\binom{n}{n}$ ж) $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2$.

Задача 1.10. Сколько существует диаграмм Юнга[4]: а) веса 6? б) веса 7, содержащих не более трёх строк? в) без ограничений на вес, но содержащих не более p строк и q столбцов?

Задача 1.11* (Л. Г. Макар–Лиманов). Торговец газировкой коротает время манипулируя пятнадцатью одноразовыми стаканчиками, сложенными перед ним в несколько стопок. Одна манипуляция заключается в том, что он берёт верхний стаканчик из каждой стопки и составляет из них новую стопку[5]. Как разложатся стаканчики после 1000 таких манипуляций?

Задача 1.12. Имеются 4 попарно отличающихся друг от друга чашки, 4 совершенно одинаковых стакана, 10 совершенно одинаковых кусков сахара и 7 попарно разноцветных соломинок. Сколькими способами можно разложить: а) соломинки по чашкам? б) сахар по чашкам? в) сахар по стаканам? г) соломинки по стаканам?

Задача 1.13. Как изменятся ответы в предыдущей задаче, если потребовать, чтобы после раскладывания не оставалось пустых ёмкостей?

Задача 1.14. Стороны плоского проволочного правильного n-угольника раскрашивают в n цветов — каждую сторону в свой цвет. Сколько различных игрушек при этом получится?

Задача 1.15. Сколько бус можно сделать из 5 красных, 7 синих и 11 белых бусин одинаковой формы?

Задача 1.16. Каждую грань а) кубика б) правильного тетраэдра красят одним из шести фиксированных цветов, так чтобы все грани получились разноцветные. Сколько различных игрушек можно получить таким образом?

Задача 1.17. Сколько разных безделушек получится при склейке пары крашеных кубиков из предыдущей задачи по наугад выбираемой грани?

---

[1] Отображение f называется *возрастающим*, если $\forall\, x_1, x_2 \quad x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$.

[2] Отображение f называется *неубывающим*, если $\forall\, x_1, x_2 \quad x_1 \leqslant x_2 \Rightarrow f(x_1) \leqslant f(x_2)$.

[3] *Полной степенью* монома $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_n}$ называется сумма его показателей $m_1 + \ldots + m_n$.

[4] См. формулу (1-10) на стр. 10.

[5] Стопка может состоять из одного стакана, который в этом случае и будет верхним.

Задача 1.18. Покажите, что лемма Цорна[1] эквивалентна аксиоме выбора. А именно, допустим, что для любого полного чума P выполняется сл. 1.1 на стр. 20. Докажите, что тогда у любого сюръективного отображения множеств $f : X \twoheadrightarrow Y$ имеется сечение. Для этого рассмотрите множество P всех пар (U, g), где $U \subset Y$ — любое подмножество, а $g : U \to X$ — такое отображение, что $fg = \mathrm{Id}_U$. Покажите, что отношение $(U, g) \leqslant (W, f)$, означающее, что $U \subset W$, а g является ограничением f с W на U, задаёт на P частичный порядок удовлетворяющий условиям сл. 1.1. Затем покажите, что для максимальной пары (U, g) выполнено равенство $U = Y$.

[1] См. сл. 1.1 на стр. 20.

§2. Поля, коммутативные кольца и абелевы группы

2.1. Определения и примеры. Говоря вольно, поле представляет собою числовую область, где определены четыре стандартных арифметических операции: сложение, вычитание, умножение и деление, которые обладают теми же свойствами, что и соответствующие действия над рациональными числами. Точный перечень этих свойств идёт ниже.

Определение 2.1
Множество $\mathbb{F}$ с двумя операциями $\mathbb{F}\times\mathbb{F}\to\mathbb{F}$: *сложением* $(a,b)\mapsto a+b$ и *умножением* $(a,b)\mapsto ab$ называется *полем*, если выполняются следующие три набора аксиом:

свойства сложения

коммутативность: $a+b=b+a \quad \forall\, a,b\in\mathbb{F}$ (2-1)

ассоциативность: $a+(b+c)=(a+b)+c \quad \forall\, a,b,c\in\mathbb{F}$ (2-2)

наличие нуля: $\exists\, 0\in\mathbb{F}:\quad a+0=a \quad \forall\, a\in\mathbb{F}$ (2-3)

наличие противоположных: $\forall\, a\in\mathbb{F} \quad \exists\,(-a)\in\mathbb{F}:\quad a+(-a)=0$ (2-4)

свойства умножения

коммутативность: $ab=ba \quad \forall\, a,b\in\mathbb{F}$ (2-5)

ассоциативность: $a\,(bc)=(ab)\,c \quad \forall\, a,b,c\in\mathbb{F}$ (2-6)

наличие единицы: $\exists\, 1\in\mathbb{F}:\quad 1\,a=a \quad \forall\, a\in\mathbb{F}$ (2-7)

наличие обратных: $\forall\, a\in\mathbb{F}\smallsetminus 0 \quad \exists\, a^{-1}\in\mathbb{F}:\quad aa^{-1}=1$ (2-8)

свойства, связывающие сложение с умножением

дистрибутивность: $a(b+c)=ab+ac \quad \forall\, a,b,c\in\mathbb{F}$ (2-9)

нетривиальность: $0\neq 1$ (2-10)

Пример 2.1 (поле из двух элементов)
Простейший объект, удовлетворяющий всем аксиомам из опр. 2.1 — это поле $\mathbb{F}_2$, состоящее только из двух таких элементов 0 и 1, что $0+1=1\cdot 1=1$, а все остальные суммы и произведения равны нулю.

Упражнение 2.1. Проверьте, что $\mathbb{F}_2$ действительно является полем.

Элементы этого поля можно воспринимать как классы вычетов по модулю 2, т. е. «чётное» $=0$ и «нечётное» $=1$, со сложением и умножением, заданными формулами (1-19) – (1-20) на стр. 13. С другой стороны, элементы поля $\mathbb{F}_2$ могут интерпретироваться как «ложь» $=0$ и «истина» $=1$, сложение — как логическое «исключающее или»[1], а умножение — как логическое «и»[2]. При такой интерпретации алгебраические вычисления в поле $\mathbb{F}_2$ превращаются в логические манипуляции с высказываниями.

Упражнение 2.2. Напишите многочлен от x с коэффициентами из поля $\mathbb{F}_2$, равный «не x», а

[1] Т. е. высказывание $A+B$ истинно тогда и только тогда, когда истинно *ровно одно* из высказываний A, B: $0+1=1+0=1$, но $0+0=1+1=0$.

[2] Т. е. высказывание $A\cdot B$ истинно если и только если истинны *оба* высказывания A и B : $1\cdot 1=1$, но $0\cdot 1=1\cdot 0=0\cdot 0=0$.

также многочлен от x и y, равный «x или[1] y».

Пример 2.2 (рациональные числа)
Напомню[2], что поле рациональных чисел $\mathbb{Q}$ можно определить как множество дробей a/b, где под «дробью» понимается класс эквивалентности упорядоченной пары (a, b) с $a, b \in \mathbb{Z}$ и $b \neq 0$ по отношению $(a_1, b_1) \sim (a_2, b_2)$ при $a_1 b_2 = a_2 b_1$, которое является минимальным отношением эквивалентности[3], содержащим все отождествления

$$\frac{a}{b} = \frac{ac}{bc} \quad \forall\, c \neq 0\,.$$

Сложение и умножение дробей определяется формулами

$$\frac{a}{b} + \frac{c}{d} \stackrel{\text{def}}{=} \frac{ad + bc}{bd}\,, \quad \frac{a}{b} \cdot \frac{c}{d} \stackrel{\text{def}}{=} \frac{ac}{bd}\,. \tag{2-11}$$

Упражнение 2.3. Проверьте, что эти операции определены корректно (результат не зависит от выбора представителей в классах) и удовлетворяют аксиомам поля.

Пример 2.3 (вещественные числа)
Множество вещественных чисел $\mathbb{R}$ определяется в курсе анализа несколькими различными способами: как множество классов эквивалентности десятичных[4] дробей, как множество дедекиндовых сечений упорядоченного множества $\mathbb{Q}$, или как множество классов эквивалентности рациональных последовательностей Коши. Мы полагаем, что читатель знаком с этими определениями и понимает, как они связаны друг с другом, либо скоро узнает об этом из курса анализа. Какое бы описание множества $\mathbb{R}$ ни использовалось, задание на нём сложения и умножения, равно как и проверка аксиом из опр. 2.1, требуют определённой умственной работы, также традиционно проделываемой в курсе анализа.

2.1.1. Коммутативные кольца. Множество K с операциями сложения и умножения называется *коммутативным кольцом с единицей*, если эти операции обладают всеми свойствами из опр. 2.1 на стр. 23 за исключением свойства (2-8) существования мультипликативно обратных элементов и свойства (2-10), утверждающего, что $1 \neq 0$.

Если помимо этих двух свойств из списка аксиом поля исключаются требование наличия единицы (2-7), то множество K с двумя операциями, удовлетворяющими оставшимся аксиомам, называется просто *коммутативным кольцом*.

Примерами отличных от полей колец с единицами являются кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов с коэффициентами в произвольном коммутативном кольце с единицей. Примеры коммутативных колец без единицы доставляют чётные целые числа, многочлены с чётными целыми коэффициентами, многочлены без свободного члена с коэффициентами в любом коммутативном кольце и т. п.

[1] Здесь имеется в виду обычное, не исключающее «или»: многочлен должен принимать значение 1 тогда и только тогда, когда *хотя бы одна* из переменных равна 1.

[2] См. прим. 1.5 на стр. 13.

[3] См. п° 1.4.1 на стр. 13.

[4] Или привязанных к какой-либо другой позиционной системе счисления, например, двоичных.

2.1.2. Абелевы группы. Множество A *с одной* операцией $A \times A \to A$, удовлетворяющей первым четырём аксиомам сложения из опр. 2.1, называется *абелевой группой*. Таким образом, всякое коммутативное кольцо K является абелевой группой относительно операции сложения. Эта группа называется *аддитивной группой кольца*. Пример абелевой группы, не являющейся кольцом, доставляют *векторы*.

Пример 2.4 (геометрические векторы)
Будем называть *геометрическим вектором* класс направленного отрезка (на плоскости или в пространстве) по отношению эквивалентности, отождествляющему между собой все отрезки, которые получающиеся друг из друга параллельным переносом. Нулевым вектором назовём класс эквивалентности точки — это единственный вектор, имеющий нулевую длину и не имеющий направления. Сложение векторов определяется стандартным образом: надо выбрать представителей векторов a и b так, чтобы конец a совпал с началом b, и объявить $a + b$ равным вектору с началом в начале a и концом в конце b. Коммутативность и ассоциативность этой операции видны из рис. 2⋄1 и рис. 2⋄2.

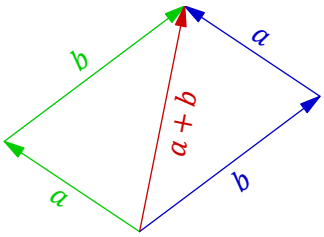


Рис. 2⋄1. Правило параллелограмма.

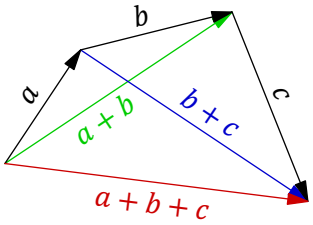


Рис. 2⋄2. Правило четырёхугольника.

Нулевым элементом является нулевой вектор. Вектор $-a$, противоположный вектору a, получается из вектора a изменением его направления на противоположное.

Пример 2.5 (мультипликативная группа поля)
Четыре аксиомы умножения из опр. 2.1 на стр. 23 утверждают, то множество $\mathbb{F}^\times \stackrel{\text{def}}{=} \mathbb{F} \smallsetminus 0$ всех *ненулевых* элементов поля $\mathbb{F}$ является абелевой группой относительно операции умножения. Эту группу называют *мультипликативной группой поля*. Роль нуля из аддитивной группы $\mathbb{F}$ в мультипликативной группе $\mathbb{F}^\times$ исполняет единица. В абстрактной абелевой группе такой элемент называется *нейтральным*. Мультипликативным аналогом перехода к противоположному элементу является переход к обратному элементу.

Лемма 2.1
В любой абелевой группе A нейтральный элемент единствен, и для каждого $a \in A$ противоположный к a элемент $-a$ определяется по a однозначно. В частности, $-(-a) = a$.

Доказательство. Будем записывать операцию в A аддитивно. Если есть два нулевых элемента 0_1 и 0_2, то $0_1 = 0_1 + 0_2 = 0_2$ (первое равенство выплнено, так как 0_2 является нулевым элементом, второе — поскольку нулевым элементом является 0_1). Если есть два элемента $-a$ и $-a'$, противоположных к a, то $-a = (-a) + 0 = (-a) + \big(a + (-a')\big) = \big((-a) + a\big) + (-a') = 0 + (-a') = -a'$. □

Лемма 2.2
В любом коммутативном кольце для любого элемента a выполняется равенство $0 \cdot a = 0$, а в любом коммутативном кольце с единицей — равенство $(-1) \cdot a = -a$.

Доказательство. Так как $a\cdot 0 = a(0+0) = a\cdot 0 + a\cdot 0$, прибавляя к обеим частям элемент, противоположный к $a\cdot 0$, получаем $0 = a\cdot 0$. Второе утверждение проверяется выкладкой $(-1)\cdot a + a = (-1)\cdot a + 1\cdot a = ((-1)+1)\cdot a = 0\cdot a = 0$. □

Замечание 2.1. Аксиома нетривиальности (2-10) в определении поля равносильна требованию $\mathbb{F}\neq 0$, поскольку при $0=1$ для каждого $a\in\mathbb{F}$ получалось бы $a = a\cdot 1 = a\cdot 0 = 0$. Образование, состоящее из одного нуля, согласно предыдущим определениям является коммутативным кольцом, в котором $1=0$, но не полем.

2.1.3. Вычитание и деление. Из лем. 2.1 вытекает, что в любой абелевой группе корректно определена *разность* любых двух элементов

$$a - b \stackrel{\text{def}}{=} a + (-b)\,. \tag{2-12}$$

В частности, операция вычитания имеется в аддитивной группе любого коммутативного кольца. В поле ненулевые элементы образуют абелеву группу по умножению. Поэтому в любом поле имеется ровно один единичный элемент, и для любого ненулевого элемента a обратный к нему элемент a^{-1} однозначно определяется по a. Тем самым, в любом поле помимо сложения, умножения и вычитания (2-12) имеется операция *деления* на любые ненулевые элементы

$$a/b \stackrel{\text{def}}{=} ab^{-1}\,,\quad b\neq 0\,. \tag{2-13}$$

2.2. Делимость в кольце целых чисел. Основным отличием коммутативных колец с единицей от полей является отсутствие обратных элементов к некоторым ненулевым элементам кольца. Элемент a коммутативного кольца K с единицей называется *обратимым*, если в этом кольце существует такой элемент a^{-1}, что $a^{-1}a = 1$. В противном случае элемент a называется *необратимым*. Например, в кольце $\mathbb{Z}$ обратимыми элементами являются только 1 и -1. В кольце $\mathbb{Q}[x]$ многочленов с рациональными коэффициентами обратимыми элементами являются ненулевые константы (многочлены степени нуль) и только они.

Говорят, что элемент a *делится* на элемент b, если в кольце существует такой элемент q, что $a = bq$. Это записывается как $b|a$ (читается «b делит a») или как $a \vdots b$ (читается «a делится на b»). Отношение делимости тесно связано с решением линейных уравнений.

2.2.1. Уравнение $ax+by=k$, НОД и НОК. Зафиксируем какие-нибудь целые числа a и b и обозначим через

$$(a,b) \stackrel{\text{def}}{=} \{ax+by \mid x,y\in\mathbb{Z}\} \tag{2-14}$$

множество всех целых чисел, представимых в виде $ax+by$ с целыми x, y. Это множество замкнуто относительно сложения и вместе с каждым своим элементом содержит все его целые кратные. Кроме того, все числа из (a,b) нацело делятся на каждый общий делитель чисел a и b, а сами a и b тоже входят в (a,b). Обозначим через d наименьшее положительное число в (a,b). Остаток от деления любого числа $z\in(a,b)$ на d лежит в (a,b), поскольку представляется в виде $z-kd$, где и z и $-kd$ лежат в (a,b). Так как этот остаток строго меньше d, он равен нулю. Следовательно, (a,b) совпадает с множеством всех чисел, кратных d.

Таким образом, число d является общим делителем чисел $a,b\in(a,b)$, представляется в виде $d = ax+by$ и делится на любой общий делитель чисел a и b. При этом произвольное число $k\in\mathbb{Z}$ представляется в виде $k = ax+by$ если и только если оно делится на d. Число d называется *наибольшим общим делителем* чисел $a,b\in\mathbb{Z}$ и обозначается нод(a,b).

Упражнение 2.4. Обобщите проделанные только что рассуждения: для любого конечного набора чисел $a_1, \dots, a_m \in \mathbb{Z}$ укажите число $d \in \mathbb{Z}$, которое делит все a_i, делится на любой их общий делитель и представляется в виде $d = a_1x_1 + \dots + a_mx_m$ с целыми x_i. Покажите также, что уравнение $n = a_1x_1 + \dots + a_mx_m$ разрешимо относительно x_i в кольце $\mathbb{Z}$ если и только если $n \vdots d$.

Записывая числа a и b как $a = \alpha d$, $b = \beta d$, где $d = \text{нод}(a, b)$, мы заключаем, что число

$$c = \alpha\beta d = \beta a = \alpha b \tag{2-15}$$

делится на a и на b. Покажем, что c делит все общие кратные чисел a и b. Пусть $m = ka = \ell b$. Так как $\text{нод}(\alpha, \beta) = 1$, существуют такие $x, y \in \mathbb{Z}$, что $\alpha x + \beta y = 1$. Умножая обе части этого равенства на m, мы заключаем, что $m = m\alpha x + m\beta y = \ell b\alpha x + ka\beta y = c(\ell x + ky)$, как и утверждалось. Число c называется *наименьшим общим кратным* чисел a и b и обозначается $\text{нок}(a, b)$.

Упражнение 2.5. Убедитесь, что все целые решения (x, y) уравнения $ax + by = k$ имеют вид $x = x_0 + n\beta$, $y = y_0 - n\alpha$, где α и β те же, что и выше, (x_0, y_0) — какое-то одно решение, а $n \in \mathbb{Z}$ — любое.

2.2.2. Алгоритм Евклида – Гаусса. Найти $\text{нод}(a, b)$ для данных $a, b \in \mathbb{Z}$ и представить его в виде $\text{нод}(a, b) = ax + by$ с целыми x, y можно следующим образом. Составим таблицу

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \tag{2-16}$$

и будем преобразовывать её строки, поэлементно прибавляя к одной строке другую, умноженную на подходящее целое число так, чтобы один из элементов первого столбца каждый раз строго уменьшался по абсолютной величине. Это возможно до тех пор, пока один из элементов в первом столбце не обнулится. После этого, меняя при необходимости строки местами и/или меняя знак у всех элементов одной из строк, можем переписать полученную таблицу в виде

$$\begin{pmatrix} d & x & y \\ 0 & k & \ell \end{pmatrix}, \tag{2-17}$$

где $x, y, k, \ell \in \mathbb{Z}$ и $d \in \mathbb{N}$. Это означает, что $\text{нод}(a, b) = d = ax + by$, а $\text{нок}(a, b) = |ka| = |\ell b|$, причём $\text{нод}(k, \ell) = 1$. Например, для чисел $a = 5\,073$ и $b = 1\,064$ получаем[1]:

$$\begin{pmatrix} 5\,073 & 1 & 0 \\ 1\,064 & 0 & 1 \end{pmatrix} \qquad (1) \mapsto (1) - 5 \cdot (2)$$

$$\begin{pmatrix} -247 & 1 & -5 \\ 1\,064 & 0 & 1 \end{pmatrix} \qquad (2) \mapsto (2) + 4 \cdot (1)$$

$$\begin{pmatrix} -247 & 1 & -5 \\ 76 & 4 & -19 \end{pmatrix} \qquad (1) \mapsto (1) + 3 \cdot (2)$$

$$\begin{pmatrix} -19 & 13 & -62 \\ 76 & 4 & -19 \end{pmatrix} \qquad (2) \mapsto (2) + 4 \cdot (1)$$

$$\begin{pmatrix} -19 & 13 & -62 \\ 0 & 56 & -267 \end{pmatrix} \qquad (1) \mapsto -(1)$$

$$\begin{pmatrix} 19 & -13 & 62 \\ 0 & 56 & -267 \end{pmatrix}.$$

[1] Запись вроде $(1) \mapsto (1) - 5 \cdot (2)$ означает, что к 1-й строке прибавляется 2-я, умноженная на -5.

Тем самым, нод$(5\,073,\ 1\,064) = 19 = -13 \cdot 5\,073 + 62 \cdot 1\,064$, нок$(5\,073,\ 1\,064) = 5\,073 \cdot 56 = 1\,064 \cdot 267$.

Упражнение 2.6. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$$

кроме, может быть, итоговой (полученной перестановкой строк и/или сменой знака в одной из строк) выполняются равенства $m = ax + by$, $n = as + bt$ и $xt - sy = 1$.

Из упражнения вытекает, что элементы возникающей в конце вычисления таблице вида

$$\begin{pmatrix} d' & x & y \\ 0 & s & t \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & s & t \\ d' & x & y \end{pmatrix}$$

(где $d' \in \mathbb{Z}$ может отличаться от итогового $d \in \mathbb{N}$ лишь знаком) выполняются равенства

$$d' = ax + by\,, \quad sa = -tb\,, \quad tx - sy = 1\,. \tag{2-18}$$

Из первого следует, что d' делится на все общие делители чисел a и b. Умножая последнее равенство на a и на b и пользуясь первыми двумя равенствами, заключаем, что

$$a = atx - asy = atx + bty = td' \quad \text{и} \quad b = btx - bsy = -asx - bsy = -sd'$$

оба делятся на d', откуда $d = |d'| =$ нод(a, b). Второе равенство (2-18) показывает, что число $c' = sa = -tb$ является общим кратным a и b. Умножая третье равенство (2-18) на любое общее кратное $m = ka = \ell b$ чисел a и b, убеждаемся, что $m = mtx - msy = \ell btx - kasy = -c'(\ell x + ky)$ делится на c', откуда $c = |c'| =$ нок(a, b).

Замечание 2.2. С вычислительной точки зрения отыскание нод(a, b) и нок(a, b) по алгоритму Евклида – Гаусса *несопоставимо* быстрее разложения чисел a и b на простые множители. Читателю предлагается убедиться в этом, попробовав вручную разложить на простые множители числа 10 203 и 4 687. Вычисление по алгоритму Евклида – Гаусса занимает 6 строк:

$$\begin{aligned}
&\begin{pmatrix} 10\,203 & 1 & 0 \\ 4\,687 & 0 & 1 \end{pmatrix} && (1) \mapsto (1) - 2 \cdot (2) \\
&\begin{pmatrix} 829 & 1 & -2 \\ 4\,687 & 0 & 1 \end{pmatrix} && (2) \mapsto (2) - 6 \cdot (1) \\
&\begin{pmatrix} 829 & 1 & -2 \\ -287 & -6 & 13 \end{pmatrix} && (1) \mapsto (1) + 3 \cdot (2) \\
&\begin{pmatrix} -32 & -17 & 37 \\ -287 & -6 & 13 \end{pmatrix} && (2) \mapsto (2) - 9 \cdot (1) \\
&\begin{pmatrix} -32 & -17 & 37 \\ 1 & 147 & -320 \end{pmatrix} && (1) \mapsto (1) + 32 \cdot (2) \\
&\begin{pmatrix} 0 & 4\,687 & 10\,203 \\ 1 & 147 & -320 \end{pmatrix}, &&
\end{aligned} \tag{2-19}$$

откуда нод$(10\,203, 4\,687) = 1 = 147 \cdot 10\,203 - 320 \cdot 4\,687$, нок$(10\,203, 4\,687) = 10\,203 \cdot 4\,687$. Если известно произведение двух *очень* больших простых чисел, то извлечь из него сами эти числа за разумное время не под силу даже мощным компьютерам. Это обстоятельство лежит в основе многих популярных систем шифрования данных.

2.3. Взаимная простота. Выше мы видели, что в кольце $\mathbb{Z}$ условие нод$(a, b) = 1$ равносильно разрешимости в целых числах уравнения $ax + by = 1$. Числа a, b, обладающие этим свойством, называются *взаимно простыми*. В произвольном коммутативном кольце K с единицей из разрешимости уравнения $ax + by = 1$ также вытекает отсутствие у элементов a и b необратимых общих делителей: если $a = d\alpha$, $b = d\beta$, и $ax + by = 1$, то $d(\alpha + \beta) = 1$ и d обратим. Однако, отсутствие у a и b необратимых общих делителей, вообще говоря, не гарантирует разрешимости уравнения $ax + by = 1$. Например, в кольце многочленов от двух переменных $\mathbb{Q}[x, y]$ одночлены x и y не имеют общих делителей, отличных от констант, однако равенство $f(x, y) \cdot x + g(x, y) \cdot y = 1$ невозможно ни при каких $f, g \in \mathbb{Q}[x, y]$.

Упражнение 2.7. Объясните почему.

Оказывается, что именно разрешимость уравнения $ax + by = 1$ влечёт за собою наличие у элементов a, b многих приятных свойств, которыми обладают взаимно простые целые числа.

Определение 2.2
Элементы a и b произвольного коммутативного кольца K с единицей называются *взаимно простыми*, если уравнение $ax + by = 1$ разрешимо в K относительно x и y.

Лемма 2.3
В произвольном коммутативном кольце K с единицей для любого $c \in K$ и любых взаимно простых $a, b \in K$ справедливы импликации:

(1) если ac делится на b, то c делится на b

(2) если c делится и на a, и на b, то c делится и на ab.

Кроме того, если $a \in K$ взаимно прост с каждым из элементов $b_1, \dots, b_n$, то он взаимно прост и с их произведением $b_1 \dots b_m$.

Доказательство. Умножая обе части равенства $ax + by = 1$ на c, получаем соотношение

$$c = acx + bcy\,,$$

из которого вытекают обе импликации (1), (2). Если $\forall\, i\ \exists\, x_i, y_i \in K :\ ax_i + b_i y_i = 1$, то перемножая все эти равенства и раскрывая скобки, получим в левой части сумму, в которой все слагаемые, кроме $(b_1 \dots b_n) \cdot (y_1 \dots y_n)$, делятся на a. Вынося a за скобку, приходим к соотношению $a \cdot X + (b_1 \dots b_n) \cdot (y_1 \dots y_n) = 1$. □

Упражнение 2.8. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\mathbb{Z}$: всякое необратимое целое число $z \neq 0$ является произведением конечного числа простых[1], причём любые два таких представления

$$p_1 \dots p_k = z = q_1 \dots q_m$$

имеют одинаковое число сомножителей $k = m$, и эти сомножители можно перенумеровать так, чтобы $p_i = \pm q_i$ для всех i.

Замечание 2.3. (нод и нок в произвольном кольце) В произвольном коммутативном кольце K принято называть *наибольшим общим делителем* элементов $a, b \in K$ любой элемент $d \in K$,

[1]Напомним, что ненулевое необратимое целое число называется *простым*, если оно не раскладывается в произведение двух необратимых целых чисел.

который делит a и b и делится на все их общие делители. Это определение не гарантирует ни существования, ни единственности наибольшего общего делителя, ни его представимости в виде $d = ax + by$. Аналогично, *наименьшим общим кратным* элементов $a, b \in K$ называется любой элемент $c \in K$, который делится на a и b и делит все их общие кратные. Такого элемента тоже может не быть, а если он есть, то не обязательно единствен.

2.4. Кольцо вычетов $\mathbb{Z}/(n)$. Напомню[1], что числа $a, b \in \mathbb{Z}$ называются *сравнимыми* по модулю n, что записывается как $a \equiv b \pmod n$, если их разность $a - b$ делится на n. Сравнимость по модулю n является отношением эквивалентности[2] и разбивает множество целых чисел на непересекающиеся классы сравнимых по модулю n чисел. Эти классы называются *классами вычетов по модулю* n, а их совокупность обозначается через $\mathbb{Z}/(n)$. Мы будем писать $[a]_n \in \mathbb{Z}/(n)$ для обозначения класса, содержащего число $a \in \mathbb{Z}$. Такое обозначение не однозначно: разные числа $x \in \mathbb{Z}$ и $y \in \mathbb{Z}$ задают один и тот же класс $[x]_n = [y]_n$ если и только если $x = y + dn$ для некоторого $d \in \mathbb{Z}$. Всего в $\mathbb{Z}/(n)$ имеется n различных классов: $[0]_n$, $[1]_n$, … , $[(n-1)]_n$. Сложение и умножение классов вычетов задаётся правилами:

$$[a] + [b] \stackrel{\text{def}}{=} [a + b]\,, \quad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\,. \tag{2-20}$$

Согласно упр. 1.9 на стр. 13, эти операции определены корректно[3]. Они очевидным образом удовлетворяют аксиомам коммутативного кольца с единицей — формулы (2-20) сводят операции над вычетами к операциям над целыми числами, для которых аксиомы выполнены.

2.4.1. Делители нуля и нильпотенты. В $\mathbb{Z}/(10)$ произведение классов $[2]$ и $[5]$ равно нулю, хотя *каждый* из них отличен от нуля, а в кольце $\mathbb{Z}/(8)$ ненулевой класс $[2]$ имеет нулевой куб $[2]^3 = [8] = [0]$. Элемент a произвольного коммутативного кольца K называется *делителем нуля*, если $ab = 0$ для некоторого ненулевого $b \in K$. Тривиальным делителем нуля является нуль. Обратимый элемент $a \in K$ не может быть делителем нуля, поскольку, умножая обе части равенства $ab = 0$ на a^{-1}, мы получаем $b = 0$. Тем самым, кольцо с ненулевыми делителями нуля не может быть полем. Кольцо с единицей без ненулевых делителей нуля называется *целостным*.

Элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Тривиальным нильпотентом является нуль. Всякий нильпотент автоматически делит нуль. Кольцо с единицей без ненулевых нильпотентов называется *приведённым*. Например, каждое целостное кольцо приведено.

2.4.2. Обратимые элементы кольца вычетов. Обратимость класса $[m]_n \in \mathbb{Z}/(n)$ означает существование такого класса $[x]_n$, что $[m]_n[x]_n = [mx]_n = [1]_n$. Последнее равенство равносильно наличию таких $x, y \in \mathbb{Z}$, что $mx + ny = 1$ в $\mathbb{Z}$. Тем самым, класс $[m]_n$ обратим в $\mathbb{Z}/(n)$ если и только если нод$(m, n) = 1$ в кольце $\mathbb{Z}$.

Проверить, обратим ли данный класс $[m]_n$, и если да, вычислить $[m]_n^{-1}$, можно при помощи алгоритма Евклида – Гаусса[4]. Так, проделанное в форм. (2-19) на стр. 28 вычисление показывает, что класс $[10\,203]$ обратим в $\mathbb{Z}/(4\,687)$ и $10\,203^{-1} = 147 \pmod{4\,687}$, а класс $[4\,687]$ обратим в $\mathbb{Z}/(10\,203)$ и $4\,687^{-1} = -320 \pmod{10\,203}$.

[1] См. прим. 1.4 на стр. 12.

[2] См. n° 1.4 на стр. 11.

[3] Т. е. не зависят от способа записи классов или, что то же самое — от выбора представителей $a \in [a]$ и $b \in [b]$.

[4] См. n° 2.2.2 на стр. 27.

Обратимые элементы кольца $\mathbb{Z}/(n)$ образуют мультипликативную абелеву группу. Она называется *группой обратимых вычетов* по модулю n и обозначается $\mathbb{Z}/(n)^\times$. Порядок этой группы равен количеству натуральных чисел, меньших n и взаимно простых с n. Он обозначается

$$\varphi(n) \stackrel{\text{def}}{=} \left|\mathbb{Z}/(n)^\times\right|$$

и называется *функцией Эйлера* числа $n \in \mathbb{Z}$.

Пример 2.6 (теорема Эйлера и порядок обратимого вычета)
Умножение на фиксированный обратимый вычет $[a] \in \mathbb{Z}/(n)^\times$ задаёт биекцию[1]

$$a:\ \mathbb{Z}/(n)^\times \xrightarrow{\sim} \mathbb{Z}/(n)^\times, \quad [x] \mapsto [ax], \tag{2-21}$$

обратной к которой является умножение на вычет $[a]^{-1}$. Последовательно применяя отображение (2-21) к произвольному элементу $[z] \in \mathbb{Z}/(n)^\times$, получаем цепочку его образов

$$[z] \overset{a}{\mapsto} [az] \overset{a}{\mapsto} [a^2z] \overset{a}{\mapsto} [a^3z] \overset{a}{\mapsto} \dots, \tag{2-22}$$

которые начнут повторяться, ибо множество вычетов конечно. В силу биективности отображения (2-21), самым первым повторно встретившимся элементом цепочки (2-22) станет её начальный элемент $[z]$, т. е. цепочка (2-22) является циклом. В силу всё той же биективности отображения (2-21) два таких цикла, проходящие через классы $[x]$ и $[y]$, либо не пересекаются, либо полностью совпадают. Кроме того, все циклы имеют одинаковую длину.

Упражнение 2.9. Убедитесь, что отображения умножения на $[x]^{-1}[y]$ и на $[y]^{-1}[x]$ суть взаимно обратные биекции между циклами, проходящими через классы $[x]$ и $[y]$.

Мы заключаем, что $\mathbb{Z}/(n)^\times$ распадается в объединение непересекающихся циклов (2-22) *одинаковой длины* m, которая таким образом является делителем числа $\varphi(n) = |\mathbb{Z}/(n)^\times|$. Умножая обе части равенства $[z] = [a]^m[z]$ на $[z]^{-1}$, получаем $[a^m] = [1]$, откуда и $[a^{\varphi(n)}] = [1]$. Иными словами, для любых взаимно простых целых чисел a и n выполняется сравнение $a^{\varphi(n)} \equiv 1 \pmod{n}$. Этот факт известен как *теорема Эйлера*. Число m однозначно характеризуется как наименьшее такое $k \in \mathbb{N}$, что $[a]^k = 1$, и называется *порядком* обратимого вычета $[a] \in \mathbb{Z}/(n)^\times$. Как мы видели, порядок каждого обратимого вычета в $\mathbb{Z}/(n)^\times$ делит $\varphi(n)$.

2.4.3. Поля вычетов $\mathbb{F}_p = \mathbb{Z}/(p)$. Из сказанного в начале n° 2.4.2 вытекает, что кольцо вычетов $\mathbb{Z}/(n)$ является полем тогда и только тогда, когда n является *простым числом*. В самом деле, если $n = mk$ составное, ненулевые классы $[m], [k] \in \mathbb{Z}/(n)$ делят нуль и не могут быть обратимы. Напротив, если p простое, то $\text{нод}(m, p) = 1$ для всех m, не кратных p, и значит, каждый ненулевой класс $[m] \in \mathbb{Z}/(p)$ обратим. Поле $\mathbb{Z}/(p)$, где p простое, принято обозначать $\mathbb{F}_p$.

Пример 2.7 (бином Ньютона по модулю p)
В поле $\mathbb{F}_p = \mathbb{Z}/(p)$ выполняется замечательное равенство

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ раз}} = 0\,. \tag{2-23}$$

Из него вытекает, что для любых $a, b \in \mathbb{F}_p$ выполняется равенство

$$(a + b)^p = a^p + b^p\,. \tag{2-24}$$

[1] См. n° 1.5.2 на стр. 16.

В самом деле, раскрывая скобки в биноме $(a+b)^p$, мы для каждого k получим $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ одночленов $a^k b^{p-k}$, сумма которых равна $(1+\ldots+1)\cdot a^k b^{p-k}$, где внутри скобок складываются $\binom{p}{k}$ единиц поля $\mathbb{F}_p$. Такая сумма равна нулю при $0 < k < p$ в силу следующей леммы.

Лемма 2.4
При простом p и любом натуральном k в пределах $1 \leqslant k \leqslant (p-1)$ биномиальный коэффициент $\binom{p}{k}$ делится на p.

Доказательство. Так как число p взаимно просто со всеми числами от 1 до $p-1$, оно по лем. 2.3 взаимно просто с произведением $k!(p-k)!$. Поскольку $p!$ делится на $k!(p-k)!$, из той же лем. 2.3 следует, что $(p-1)!$ делится на $k!(p-k)!$, а значит, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p. □

Следствие 2.1 (малая теорема Ферма)
Для любого $a \in \mathbb{Z}$ и любого простого $p \in \mathbb{N}$ выполняется сравнение $a^p \equiv a \pmod p$.

Доказательство. Надо показать, что $[a^p] = [a]$ в поле $\mathbb{F}_p$. Согласно (2-24)

$$[a]^p = \underbrace{\bigl([1]+\ldots+[1]\bigr)^p}_{a \text{ раз}} = \underbrace{[1]^p+\ldots+[1]^p}_{a \text{ раз}} = \underbrace{[1]+\ldots+[1]}_{a \text{ раз}} = [a]\,.$$

□

Упражнение 2.10. Выведите малую теорему Ферма из теоремы Эйлера[1].

Упражнение 2.11. Покажите, что $\binom{mp^n}{p^n} \equiv m \pmod p$ для простого $p \nmid m$.

2.5. Гомоморфизмы. Отображение абелевых групп $\varphi\colon A \to B$ называется *гомоморфизмом*, если для любых $a_1, a_2 \in A$ в группе B выполнено соотношение

$$\varphi(a_1+a_2) = \varphi(a_1)+\varphi(a_2)\,. \tag{2-25}$$

В частности, этим условиям удовлетворяет *нулевой* (или *тривиальный*) гомоморфизм, отображающий все элементы группы A в нулевой элемент группы B.

Упражнение 2.12. Убедитесь, что композиция[2] гомоморфизмов — это тоже гомоморфизм.

Любой гомоморфизм $\varphi\colon A \to B$ переводит нулевой элемент группы A в нулевой элемент группы B, так как из равенств $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$ вытекает, что $0 = \varphi(0)$. Выкладка

$$\varphi(a)+\varphi(-a) = \varphi(a+(-a)) = \varphi(0) = 0$$

показывает, что $\varphi(-a) = -\varphi(a)$. Тем самым, *образ* $\operatorname{im}\varphi = \varphi(A) \subset B$ любого гомоморфизма $\varphi\colon A \to B$ является абелевой подгруппой в B.

2.5.1. Ядро. Полный прообраз нулевого элемента группы B при гомоморфизме $\varphi\colon A \to B$ называется *ядром* гомоморфизма φ и обозначается

$$\ker\varphi = \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}\,.$$

Ядро образует в A подгруппу, так как из равенств $\varphi(a_1) = 0$ и $\varphi(a_2) = 0$ вытекает равенство

$$\varphi(a_1 \pm a_2) = \varphi(a_1) \pm \varphi(a_2) = 0 \pm 0 = 0\,.$$

[1] См. прим. 2.6 на стр. 31.
[2] См. п° 1.5 на стр. 14.

Предложение 2.1
Каждый непустой слой[1] гомоморфизма абелевых групп $\varphi\colon A \to B$ является сдвигом его ядра:

$$\varphi^{-1}(\varphi(a)) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\} \text{ для всех } a \in A.$$

В частности, все непустые слои находятся в биекции друг с другом, и инъективность гомоморфизма φ равносильна равенству $\ker\varphi = \{0\}$.

Доказательство. Равенства $\varphi(a_1) = \varphi(a_2)$ и $\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) = 0$ равносильны. Поэтому элементы $a_1, a_2 \in A$ переходят в один и тот же элемент из B тогда и только тогда, когда $a_1 - a_2 \in \ker(\varphi)$. □

Пример 2.8 (квадраты в поле $\mathbb{F}_p$)
Зафиксируем простое $p > 2$. Отображение $\varphi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^2$, является гомоморфизмом мультипликативной группы ненулевых элементов поля $\mathbb{F}_p$ в себя. Его ядро состоит из таких $x \in \mathbb{F}_p^\times$, что $x^2 = 1$. Поскольку в поле равенство $x^2 - 1 = (x+1)(x-1) = 0$ возможно только для $x = \pm 1$, мы заключаем, что $\ker\varphi = \{\pm 1\}$, и все непустые слои гомоморфизма φ состоят из двух элементов. Поэтому $|\operatorname{im}\varphi| = (p-1)/2$, т. е. ровно половина ненулевых элементов поля $\mathbb{F}_p$ является квадратами. Узнать, является ли квадратом заданное число $a \in \mathbb{F}_p^\times$ можно при помощи другого гомоморфизма $\psi\colon \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, $x \mapsto x^{\frac{p-1}{2}}$. По малой теореме Ферма[2] все $(p-1)/2$ ненулевых квадратов лежат в его ядре. Поэтому $|\operatorname{im}\psi| \leqslant 2$.

Упражнение 2.13. Покажите, что ненулевой многочлен степени m с коэффициентами в произвольном поле $\Bbbk$ имеет в этом поле не более m различных корней.

Из упражнения вытекает, что равенство $x^{\frac{p-1}{2}} = 1$ не может выполняться сразу для всех $p-1$ элементов группы $\mathbb{F}_p^\times$. Поэтому $|\operatorname{im}\psi| = 2$ и $|\ker\psi| = (p-1)/2$. Мы заключаем, что $\ker\psi$ состоит в точности из ненулевых квадратов поля $\mathbb{F}_p$. Иными словами, $a \in \mathbb{F}_p^\times$ является квадратом если и только если $a^{\frac{p-1}{2}} = 1$. Например, -1 является квадратом в поле $\mathbb{F}_p$ если и только если $(p-1)/2$ чётно.

Упражнение 2.14. Покажите, что $\operatorname{im}\psi = \{\pm 1\}$.

2.5.2. Группа гомоморфизмов. Для абелевых групп A, B через $\operatorname{Hom}(A,B)$ мы обозначаем множество всех *гомоморфизмов* $A \to B$. Это множество является абелевой группой относительно операции поточечного сложения значений, т. е. $\varphi_1+\varphi_2\colon a \mapsto \varphi_1(a)+\varphi_2(a)$. Нулевым элементом группы $\operatorname{Hom}(A,B)$ является *нулевой гомоморфизм*, отображающий все элементы группы A в нулевой элемент группы B.

2.5.3. Гомоморфизмы колец. Отображение колец $\varphi\colon A \to B$ называется *гомоморфизмом колец*, если для любых $a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$\begin{aligned} f(a_1 + a_2) &= f(a_1) + f(a_2) \\ f(a_1 a_2) &= f(a_1) f(a_2)\,. \end{aligned} \tag{2-26}$$

Поскольку гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом аддитивных абелевых групп, он обладает всеми свойствами гомоморфизмов абелевых групп. В частности, $\varphi(0) = 0$,

[1] Ср. с n° 1.3 на стр. 8.
[2] См. сл. 2.1 на стр. 32.

$\varphi(-a) = -\varphi(a)$, и все непустые слои φ являются сдвигами слоя над нулём: если $\varphi(a) = b$, то $\varphi^{-1}(b) = a + \ker\varphi = \{a + a' \mid a' \in \ker\varphi\}$. Поэтому гомоморфизм φ инъективен тогда и только тогда, когда $\ker\varphi = \{0\}$. Ядро гомоморфизма колец $\varphi\colon A \to B$ вместе с каждым элементом $a \in \ker\varphi$ содержит и все кратные ему элементы aa', поскольку $\varphi(aa') = \varphi(a)\varphi(a') = 0$. В частности, ядро $\ker\varphi$ является подкольцом в A. Образ гомоморфизма колец $\varphi\colon A \to B$ является подкольцом в B, но он может не содержать единицы, и $1 \in A$ может не перейти в $1 \in B$.

Упражнение 2.15. Убедитесь, что отображение $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$, $[0] \mapsto [0]$, $[1] \mapsto [3]$, является гомоморфизмом колец.

Предложение 2.2
Любой ненулевой гомоморфизм произвольного кольца с единицей в любое целостное[1] кольцо переводит единицу в единицу.

Доказательство. Из равенств $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$ вытекает, что $\varphi(1)\big(1 - \varphi(1)\big) = 0$. В целостном кольце такое возможно либо при $\varphi(1) = 1$, либо при $\varphi(1) = 0$. Во втором случае $\varphi(a) = \varphi(1 \cdot a) = \varphi(1) \cdot \varphi(a) = 0$ для всех $a \in A$. □

2.5.4. Гомоморфизмы полей. Если кольца A и B являются полями, то всякий ненулевой гомоморфизм колец $\varphi\colon A \to B$ является гомоморфизмом мультипликативных групп этих полей. В частности, $\varphi(1) = 1$ и $\varphi(a/b) = \varphi(a)/\varphi(b)$ для всех a и всех $b \neq 0$.

Предложение 2.3
Любой ненулевой гомоморфизм из поля в произвольное кольцо является вложением.

Доказательство. Если $\varphi(a) = 0$ для какого-нибудь $a \neq 0$, то для каждого b

$$\varphi(b) = \varphi\left(ba^{-1}a\right) = \varphi\left(ba^{-1}\right)\varphi(a) = 0\,.$$

Поэтому любой ненулевой гомоморфизм из поля имеет нулевое ядро. □

2.5.5. Характеристика. Для любого кольца K с единицей имеется канонический гомоморфизм колец $\varkappa\colon \mathbb{Z} \to K$, заданный правилом

$$\varkappa(\pm n) = \pm\underbrace{(1 + \ldots + 1)}_{n}, \quad \text{где} \quad n \in \mathbb{N}\,. \tag{2-27}$$

Его образ $\operatorname{im}\varkappa$ является наименьшим по включению подкольцом в K с единицей, равной единице кольца K. Если гомоморфизм $\varkappa$ инъективен, то говорят, что кольцо K имеет *характеристику нуль*. В противном случае *характеристикой* $\operatorname{char}(K)$ кольца K называют наименьшее $m \in \mathbb{N}$, для которого $\underbrace{1 + 1 + \cdots + 1}_{m} = 0$. Равенство

$$\underbrace{1 + 1 + \cdots + 1}_{mn} = \underbrace{(1 + 1 + \cdots + 1)}_{m} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{n}$$

[1] Напомню, что *целостным* называется кольцо с единицей без ненулевых делителей нуля, см. n° 2.4.1 на стр. 30.

показывает, что характеристика целостного кольца либо равна нулю, либо является простым числом. Для целостного кольца K характеристики $p > 0$ гомоморфизм $\varkappa$ переводит все числа, кратные p, в нуль и корректно факторизуется до гомоморфизма поля вычетов

$$\varkappa_p : \mathbb{Z}/(p) \to K\,, \quad a \,(\mathrm{mod}\, p) \mapsto \varkappa(a)\,. \tag{2-28}$$

По предл. 2.3 гомоморфизм (2-28) инъективен, и значит, $\operatorname{im}\varkappa = \operatorname{im}\varkappa_p \simeq \mathbb{F}_p$. Таким образом, наименьшее содержащее единицу подкольцо целостного кольца K положительной характеристики является полем, изоморфным полю вычетов $\mathbb{Z}/(p)$ по простому модулю $p \in \mathbb{N}$, равному характеристике $\operatorname{char} K$.

2.5.6. Простое подполе. Пусть теперь $K = \mathbb{F}$ является полем. Его наименьшее по включению подполе называется *простым подполем* в $\mathbb{F}$. В силу своего определения простое подполе содержит образ $\operatorname{im}(\varkappa)$ гомоморфизма (2-27). Если $\operatorname{char}(\mathbb{F}) = p > 0$, то простое подполе совпадает с $\operatorname{im}\varkappa = \operatorname{im}\varkappa_p$ и изоморфно полю вычетов $\mathbb{Z}/(p)$. Если $\operatorname{char}(\mathbb{F}) = 0$, то гомоморфизм $\varkappa$ инъективно вкладывает $\mathbb{Z}$ в $\mathbb{F}$. Так как простое подполе содержит обратные ко всем элементам из $\operatorname{im}\varkappa$, правило $p/q \mapsto \varkappa(p)/\varkappa(q)$ продолжает $\varkappa$ до вложения полей $\varkappa : \mathbb{Q} \hookrightarrow \mathbb{F}$, образ которого совпадает с простым подполем. Тем самым, простое подполе поля характеристики нуль изоморфно полю рациональных чисел $\mathbb{Q}$.

Упражнение 2.16. Покажите, что а) каждый ненулевой гомоморфизм из поля в себя тождественно действует на простом подполе б) между полями разной характеристики не существует ненулевых гомоморфизмов.

Пример 2.9 (автоморфизмы поля $\mathbb{R}$)
Покажем, что каждый ненулевой гомоморфизм $\varphi : \mathbb{R} \to \mathbb{R}$ тождествен. Поскольку неравенство $x_1 < x_2$ равносильно тому, что $x_2 - x_1 = a^2$ для некоторого $a \neq 0$, мы заключаем, что для всех $x_1 < x_2$ выполняется неравенство $\varphi(x_1) < \varphi(x_2)$, ибо $\varphi(x_2) - \varphi(x_1) = \varphi(x_2 - x_1) = \varphi(a^2) = \varphi(a)^2 > 0$. Таким образом, φ является строго монотонной функцией, совпадающей с тождественным отображением $\varphi(x) = x$ на простом подполе $\mathbb{Q} \subset \mathbb{R}$.

Упражнение 2.17 (по анализу). Покажите, что строго монотонная функция $\mathbb{R} \to \mathbb{R}$, совпадающая с функцией $\varphi(x) = x$ на подмножестве $\mathbb{Q} \subset \mathbb{R}$, совпадает с нею всюду.

Пример 2.10 (гомоморфизм Фробениуса)
В поле $\mathbb{F}$ характеристики $\operatorname{char}(\mathbb{F}) = p > 0$ отображение возведения в p-тую степень

$$F_p : \mathbb{F} \to \mathbb{F}\,, \quad x \mapsto x^p\,, \tag{2-29}$$

является гомоморфизмом, поскольку $\forall\, a, b \in \mathbb{F}$ выполняются равенства $(ab)^p = a^p b^p$ и

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \underbrace{(1+1+\cdots+1)}_{\binom{p}{k}} \cdot a^k b^{p-k} = a^p + b^p$$

(ср. с прим. 2.7 и лем. 2.4 на стр. 32). Гомоморфизм (2-29) называется *гомоморфизмом Фробениуса*. Как и всякий ненулевой гомоморфизм из поля в себя, он тождественно действует на простом подполе $\mathbb{F}_p \subset \mathbb{F}$, что ещё раз доказывает малую теорему Ферма[1].

[1] См. сл. 2.1 на стр. 32.

2.6. Прямые произведения. Прямое произведение абелевых групп $A_1, \dots, A_m$

$$\prod_\nu A_\nu = A_1 \times \dots \times A_\nu \stackrel{\text{def}}{=} \{(a_1, \dots, a_m) \mid a_\nu \in A_\nu \ \forall\, \nu\} \tag{2-30}$$

состоит из упорядоченных наборов $(a_1, \dots, a_m)$ элементов $a_\nu \in A_\nu$ и наделяется структурой абелевой группы посредством покомпонентных операций:

$$(a_1, \dots, a_m) + (b_1, \dots, b_m) \stackrel{\text{def}}{=} (a_1 + b_1, \dots, a_m + b_m)\,. \tag{2-31}$$

Упражнение 2.18. Проверьте, что так определённая операция коммутативна и ассоциативна, нулевым элементом для неё является набор нулей $(0, \dots, 0)$, а противоположным к набору $(a_1, \dots, a_m)$ является набор $(-a_1, \dots, -a_m)$.

Абелева группа (2-30) называется *прямым произведением* абелевых групп A_i. Если все группы A_i конечны, прямое произведение (2-30) тоже конечно и имеет порядок

$$\left|\prod A_i\right| = \prod |A_i|\,.$$

Прямое произведение имеет смысл не только для конечного набора, но и для произвольного семейства абелевых групп A_x, занумерованных элементами $x \in X$ какого-нибудь множества X. Такое произведение обозначается через $\prod_{x\in X} A_x$.

Аналогичным образом, для любого семейства коммутативных колец $\{K_x\}_{x\in X}$ определено прямое произведение $\prod K_x$, элементами которого являются семейства $(a_x)_{x\in X}$, где каждый элемент a_x лежит в своём кольце K_x. Операции сложения и умножения определяются также покомпонентно:

$$(a_x)_{x\in X} + (b_x)_{x\in X} \stackrel{\text{def}}{=} (a_x + b_x)_{x\in X}\ , \qquad (a_x)_{x\in X} \cdot (b_x)_{x\in X} \stackrel{\text{def}}{=} (a_x \cdot b_x)_{x\in X}\ .$$

Упражнение 2.19. Убедитесь, что $\prod K_x$ является кольцом, причём если все кольца K_x имеют единицы, то $\prod K_x$ тоже имеет единицу $(1, \dots, 1)$.

Например, если $X = \mathbb{R}$ и все $K_x = \mathbb{R}$, т. е. перемножается континуальное семейство одинаковых экземпляров поля $\mathbb{R}$, занумерованных действительными числами $x \in \mathbb{R}$, то прямое произведение $\prod_{x\in\mathbb{R}} \mathbb{R}_x$ изоморфно кольцу функций $f : \mathbb{R} \to \mathbb{R}$ с обычными операциями поточечного сложения и умножения значений функций. Этот изоморфизм переводит семейство вещественных чисел $(f_x) \in \prod_{x\in\mathbb{R}} \mathbb{R}_x$, занумерованное вещественным числом x, в функцию $f : \mathbb{R} \to \mathbb{R}$, значение которой в точке $x \in \mathbb{R}$ равно x-тому элементу семейства: $f(x) = f_x$.

В прямом произведении колец любой ненулевой элемент, имеющий хотя бы одну нулевую компоненту, является делителем нуля. Например, $(0, 1, \dots, 1)$ делит нуль:

$$(0, 1, \dots, 1)(1, 0, \dots, 0) = (0, \dots, 0)\,.$$

Поэтому произведение нескольких колец никогда не является полем. Например, в произведении $\mathbb{F}_p \times \mathbb{F}_q$ конечных полей $\mathbb{F}_p$ и $\mathbb{F}_q$, состоящих из p и q элементов, есть $(p-1)(q-1)$ обратимых пар (a, b), составляющих мультипликативную группу $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$, а также есть $p + q - 1$ делителей нуля, имеющих вид $(a, 0)$ и $(0, b)$.

В общем случае элемент $a = (a_1, \dots, a_m) \in K_1 \times \dots \times K_m$ обратим если и только если каждая его компонента $a_\nu \in K_\nu$ обратима в своём кольце K_ν. Поэтому группа обратимых элементов кольца $\prod K_\nu$ является прямым произведением групп обратимых элементов колец K_ν:

$$\left(\prod K_\nu\right)^\times = \prod K_\nu^\times \tag{2-32}$$

2.7. Китайская теорема об остатках. Пусть целое число $n = n_1 \dots n_m$ является произведением попарно взаимно простых чисел $n_1, \dots, n_m \in \mathbb{Z}$. Отображение, переводящее вычет $z \pmod n$ в набор вычетов $z \pmod{n_i}$:

$$\varphi : \mathbb{Z}/(n) \to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m), \quad [z]_n \mapsto \big([z]_{n_1}, \dots, [z]_{n_m}\big), \tag{2-33}$$

l корректно определено, поскольку при выборе другого представителя $z_1 \equiv z_2 \pmod n$ разность $z_1 - z_2$ делится на произведение $n = n_1 \dots n_m$, и $[z_1]_{n_i} = [z_2]_{n_i}$ при всех i. Легко видеть, что φ перестановочно со сложением:

$$\begin{aligned}\varphi\big([z]_n + [w]_n\big) = \varphi\big([z+w]_n\big) = \big([z+w]_{n_1}, \dots, [z+w]_{n_m}\big) = \\ = \big([z]_{n_1} + [w]_{n_1}, \dots, [z]_{n_m} + [w]_{n_m}\big) = \\ = \big([z]_{n_1}, \dots, [z]_{n_m}\big) + \big([w]_{n_1}, \dots, [w]_{n_m}\big) = \varphi\big([z]_n\big) + \varphi\big([w]_n\big).\end{aligned}$$

Аналогично проверяется, что φ перестановочно с умножением, т. е. является гомоморфизмом колец. Если $[z]_n \in \ker\varphi$, то z делится на каждое n_i, а значит, по лем. 2.3 на стр. 29, делится и на их произведение $n = n_1 \dots n_m$, откуда $[z]_n = 0$. Так как гомоморфизм с нулевым ядром инъективен и в кольцах $\mathbb{Z}/(n)$ и $\prod \mathbb{Z}/(n_i)$ одинаковое число элементов $n = n_1 \dots n_m$, отображение (2-33) биективно. Этот факт известен как *китайская теорема об остатках*.

На житейском языке он означает, что для любого набора остатков $r_1, \dots, r_m$ от деления на попарно взаимно простые числа $n_1, \dots, n_m$ всегда найдётся число z, имеющее остаток r_i от деления на n_i одновременно для всех i, причём любые два таких числа z_1, z_2 различаются на целое кратное числа $n = n_1 \dots n_k$. Практическое отыскание такого z осуществляется с помощью алгоритма Евклида – Гаусса следующим образом. Из взаимной простоты числа n_i с остальными числами n_ν вытекает[1], что n_i взаимно просто с произведением $m_i = \prod_{\nu \neq i} n_\nu$. Поэтому для каждого i найдутся такие $x_i, y_i \in \mathbb{Z}$, что $n_i x_i + m_i y_i = 1$. Число $b_i = m_i y_i$ даёт остаток 1 от деления на n_i и делится на все n_ν с $\nu \neq i$. Число $z = r_1 b_1 + \dots + r_m b_m$ решает задачу.

Пример 2.11

Найдём наименьшее натуральное число, имеющее остатки $r_1 = 2$, $r_2 = 7$ и $r_3 = 43$ от деления, соответственно, на $n_1 = 57$, $n_2 = 91$ и $n_3 = 179$. Сначала найдём число, обратное к $91 \cdot 179$ по модулю 57: замечаем, что $91 \cdot 179 \equiv 34 \cdot 8 \equiv -13 \pmod{57}$, применяем алгоритм Евклида – Гаусса[2] к $a = 57$ и $b = 13$ и приходим к равенству $22 \cdot 13 - 5 \cdot 57 = 1$. Таким образом, число

$$b_1 = -22 \cdot 91 \cdot 179 \quad (\equiv 22 \cdot 13 \pmod{57})$$

даёт при делении на 57, 91 и 179 остатки $(1,\ 0,\ 0)$. Аналогично находим числа

$$\begin{aligned} b_2 &= -33 \cdot 57 \cdot 179 \quad (\equiv 33 \cdot 11 \pmod{91}) \\ b_3 &= -45 \cdot 57 \cdot 91 \quad (\equiv 45 \cdot 4 \pmod{179}) \end{aligned}$$

дающие при делении на 57, 91 и 179 остатки $(0,\ 1,\ 0)$ и $(0,\ 0,\ 1)$ соответственно. Требуемые остатки $(2,\ 7,\ 43)$ имеет число

$$\begin{aligned} z = 2\,b_1 + 7\,b_2 + 43\,b_3 = -(2 \cdot 22 \cdot 91 \cdot 179 + 7 \cdot 33 \cdot 57 \cdot 179 + 43 \cdot 45 \cdot 57 \cdot 91) = \\ = -(716\,716 + 2\,356\,893 + 10\,036\,845) = -13\,110\,454, \end{aligned}$$

[1] По всё той же лем. 2.3 на стр. 29.

[2] См. n° 2.2.2 на стр. 27.

а также все числа, отличающиеся от него на целые кратные числа $n = 57 \cdot 91 \cdot 179 = 928\,473$. Наименьшим положительным среди них является $z + 15\,n = 816\,641$.

Задачи для самостоятельного решения к §2

Задача 2.1. Вычислите нод(a, b) и подберите такие целые x, y, α, β, что нод$(a, b) = ax + by$ и нок$(a, b) = \alpha a = \beta b$ для чисел а) $a = 221$, $b = -323$ б) $a = 8\,888\,888$, $b = 8\,888$ в) $a = -44\,863$, $b = 70\,499$ г) $a = 8\,385\,403$, $b = 2\,442\,778$ д) $a = 2^n - 1$, $b = 2^m - 1$.

Задача 2.2. Вычислите а) нод(665, 684, 741) б) нод(924, 1540, 3003, 5005) и представьте его в виде целочисленной линейной комбинации данных чисел.

Задача 2.3. Найдите все целые решения уравнений: а) $1537\,x + 1387\,y = 1$ б) $169\,x + 221\,y = 26$ в) $nx + (2n - 1)y = 3$ г) $28\,x + 30\,y + 31\,z = 365$

Задача 2.4. Найдите все натуральные решения уравнений:
а) $173\,x + 95\,y = 20000$ б) $57\,x + 102\,y = 10000$.

Задача 2.5. Составьте таблицы умножения для колец $\mathbb{Z}/(m)$ с $4 \leqslant m \leqslant 8$. В каждом из них найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов постройте таблицу обратных.

Задача 2.6. Покажите, что: а) $a^2 + b^2 \vdots 7 \Rightarrow a \vdots 7$ и $b \vdots 7$ б) $a^3 + b^3 + c^3 \vdots 7 \Rightarrow abc \vdots 7$ в) $a^2 + b^2 + c^2 + d^2 + e^2 \vdots 9 \Rightarrow abcde \vdots 9$.

Задача 2.7. Делится ли а) $2222^{5555} + 5555^{2222}$ на 7 б) $2^{70} + 3^{70}$ на 13?

Задача 2.8. Какой остаток от деления на 179 имеет число $2021^{2022^{2023}}$?

Задача 2.9. Вычислите остатки всех степеней десятки от деления на 2, 5, 4, 3, 9, 11, 7, 13 и укажите как можно более простые способы отыскания остатка данного числа от деления на 2, 5, 4, 3, 9, 11, 7, 13 по цифрам его десятичной записи[1].

Задача 2.10. Имеют ли уравнения а) $x^2 + y^2 + z^2 = 2\,xyz$ б) $x^2 + y^2 + z^2 = 999\,999$ соответственно ненулевые и хоть какие-нибудь решения в целых числах?

Задача 2.11. Верно ли, что
а) ни одно число вида $4k + 3$ не является суммой квадратов двух целых чисел?
б) ни одно число вида 10^{3k+1} не является суммой кубов двух целых чисел?

Задача 2.12. Верно ли что: а) $2^n - 1$ просто $\Rightarrow n$ просто б) $2^n + 1$ просто $\Rightarrow n = 2^m$?
в) Верны ли обратные импликации?

Задача 2.13. Существуют ли на числовой прямой сколь угодно длинные отрезки, не содержащие ни одного простого числа?

Задача 2.14. Верно ли, что среди чисел вида а) $10\ldots03$ б) $3\ldots31$ бесконечно много составных?

Задача 2.15. Найдите все натуральные числа, кратные тридцати и имеющие ровно тридцать различных натуральных делителей[2].

Задача 2.16. Чему равно третье по величине натуральное число с остатками

[1] Например: остаток от деления на 3 равен остатку суммы цифр десятичной записи.
[2] Включая единицу и само число.

а) 2 и 7 от деления на 57 и 179 б) 2, 4, 5 от деления на 5, 7, 8
в) 4, 5, 6 от деления на 6, 7, 8 г) 2, 4, 6 и 8 от деления на 5, 7, 8 и 9?

Задача 2.17. В кольце $\mathbb{Z}/(360)$ найдите все решения уравнений а) $x^2 = 1$ б*) $x^3 = 1$ в*) $x^2 = 49$.

Задача 2.18. Сколько решений имеет уравнение $x^{76} = 1$ в кольце $\mathbb{Z}/(2320)$?

Задача 2.19. Докажите, что для любого $m \in \mathbb{N}$ существует такое $n \in \mathbb{N}$, что уравнение $x^2 = 1$ имеет в $\mathbb{Z}/(n)$ не менее m решений.

Задача 2.20 (порядки вычетов). Покажите, что вычет $a \in \mathbb{Z}/(n)$ обратим если и только если существует такое $k \in \mathbb{N}$, что $a^k = 1$ в $\mathbb{Z}/(n)$. Наименьшее такое k называется *порядком* обратимого вычета a. Найдите порядок произведения $a = a_1 \dots a_n$ обратимых вычетов попарно взаимно простых порядков $k_1, \dots, k_n$ и для любых двух обратимых вычетов a и b порядков k и m постройте вычет порядка нок(k, m).

Задача 2.21 (первообразные корни). Обратимый вычет порядка $\varphi(n)$ в $\mathbb{Z}/(n)$ называется *первообразным корнем* по модулю n. а) Существует ли первообразный корень в $\mathbb{Z}/(21)$?
б*) Докажите существование первообразного корня по любому простому модулю.
в*) Пусть r — первообразный корень по простому модулю $p > 2$. Докажите, что существует такое $t \in \mathbb{N}$, что $(r + pt)^{p-1} = 1$ в $\mathbb{Z}/(p)$, но $(r + pt)^{p-1} \neq 1$ в $\mathbb{Z}/(p^2)$, и вычет $r + pt$ является первообразным корнем в $\mathbb{Z}/(p^k)$ для всех $k \in \mathbb{N}$.
г*) Докажите существование первообразного корня в $\mathbb{Z}/(2p^k)$ для простых $p > 2$ и $k \in \mathbb{N}$.

Задача 2.22 (простое поле). Рассмотрим поле $\mathbb{F}_p = \mathbb{Z}/(p)$, где $p > 2$ — целое простое число.
а) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$, вычислите произведение всех ненулевых элементов из $\mathbb{F}_p$ и докажите *теорему Вильсона*: натуральное $m \geqslant 2$ просто если и только если $(m-1)! + 1 \vdots m$.
б) Опишите множества значений многочленов $x^p - x$, x^{p-1} и $x^{(p-1)/2}$ на всём поле $\mathbb{F}_p$ и на множестве квадратов поля $\mathbb{F}_p$.
в) Сколько в $\mathbb{F}_p$ квадратов? Всегда ли в $\mathbb{F}_p$ разрешимо уравнение $x^2 + y^2 = -1$?
г) (лемма Гаусса о квадратичных вычетах) Выпишем элементы поля $\mathbb{F}_p$ в виде «числовой прямой»: $-(p-1)/2, \dots, -1, 0, 1, \dots, (p-1)/2$. Покажите, что $a \in \mathbb{F}_p$ является квадратом если и только если количество «положительных» точек, которые становятся «отрицательными» от умножения на a, чётно.
д) При каких p в $\mathbb{F}_p$ разрешимы уравнения $x^2 = -1$ и $x^2 = 2$?

Задача 2.23 (идемпотенты). Элемент a коммутативного кольца A с единицей называется *идемпотентом*, если $a^2 = a$. Покажите, что а) любой идемпотент является делителем нуля б) a идемпотент если и только если $1 - a$ идемпотент. в) Обозначим через $a : A \to A$, $x \mapsto ax$, отображение умножения на фиксированный идемпотент $a \in A$. Покажите, что это гомоморфизм относительно сложения, причём $\ker a = \operatorname{im}(1-a)$, $\operatorname{im} a = \ker(1-a)$ и аддитивная абелева группа кольца A раскладывается в прямое произведение $A = \ker a \times \operatorname{im} a$. г) При каких n в кольце $\mathbb{Z}/(n)$ имеются идемпотенты?

Задача 2.24. Найдите все идемпотенты в кольце $\mathbb{Z}/(n)$ для а) $n = 6$ б) $n = 36$ в) $n = p_1 \dots p_n$ г) $n = p_1^{m_1} \dots p_n^{m_n}$, где p_i различные простые числа.

Задача 2.25 (функция Эйлера). Функция $f : \mathbb{Z} \to \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ при взаимно простых m, n. Покажите, что
а) функция Эйлера[1] $\varphi(n)$ является мультипликативным характером
б) для $n = p_1^{k_1} \dots p_n^{k_n}$, где все p_i просты и различны, $\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$.

[1] См. n° 2.4.2 на стр. 30.

в) Найдите все n с $\varphi(n) = 10$.

Задача 2.26 (функция Мёбиуса). Функция Мёбиуса $\mu(n)$ сопоставляет числу $n \in \mathbb{N}$ нуль, если n делится на квадрат простого числа, и $(-1)^s$, где s — количество натуральных простых делителей числа n, если n не делится на квадраты простых чисел. Кроме того, $\mu(1) \stackrel{\text{def}}{=} 1$. Покажите, что

а) $\mu(n)$ является мультипликативным характером числа n

б) $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{при } n = 1 \\ 0 & \text{при } n > 1 \end{cases}$, где суммирование ведётся по всем натуральным делителям d числа n, включая 1 и n.

Задача 2.27 (обращение Мёбиуса). Пусть для функции $g : \mathbb{N} \to \mathbb{C}$ при каждом $n \in \mathbb{N}$ известно значение суммы $\sigma(n) = \sum_{d|n} g(d)$. Покажите, что функция g восстанавливается по функции σ по формуле $g(n) = \sum_{d|n} \sigma(d) \cdot \mu(n/d)$.

Задача 2.28. Для произвольного $m \in \mathbb{N}$ вычислите $\sum_{d|m} \varphi(d)$.

§3. Многочлены и расширения полей

Всюду в этом параграфе мы обозначаем через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

3.1. Ряды и многочлены. Бесконечное выражение вида

$$A(x) = \sum_{\nu \geqslant 0} a_\nu x^\nu = a_0 + a_1 x + a_2 x^2 + \dots \text{, где } a_i \in K, \tag{3-1}$$

называется *формальным степенным рядом* от x с коэффициентами в кольце K. Ряды

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \dots \\ B(x) &= b_0 + b_1 x + b_2 x^2 + \dots \end{aligned} \tag{3-2}$$

равны, если $a_i = b_i$ для всех i. Сложение и умножение рядов (3-2) осуществляется по стандартными правилами раскрытия скобок и приведения подобных слагаемых: коэффициенты s_m и p_m рядов $S(X) = A(x) + B(x) = s_0 + s_1 x + s_2 x^2 + \dots$ и $P(x) = A(x)B(x) = p_0 + p_1 x + p_2 x^2 + \dots$ суть[1]

$$\begin{aligned} s_m &= a_m + b_m \\ p_m &= \sum_{\alpha+\beta=m} a_\alpha b_\beta = a_0 b_m + a_1 b_{m-1} + \dots + a_0 b_m \end{aligned} \tag{3-3}$$

Упражнение 3.1. Убедитесь, что эти две операции удовлетворяют аксиомам коммутативного кольца с единицей.

Кольцо формальных степенных рядов от переменной x с коэффициентами в кольце K обозначается через $K[\![x]\!]$. Начальный коэффициент a_0 ряда (3-1) называется *свободным членом* этого ряда. Самый левый ненулевой коэффициент в (3-1) называется *младшим* коэффициентом ряда A, а степень переменной, на которую умножается, называется *порядком* ряда. Если в кольце K нет делителей нуля, младший коэффициент произведения двух рядов равен произведению младших коэффициентов сомножителей, а порядок равен сумме порядков. Поэтому кольцо формальных степенных рядов с коэффициентами из целостного кольца тоже является целостным.

Кольцо $K[\![x_1, \dots, x_n]\!]$ формальных степенных рядов от n переменных определяется по индукции: $K[\![x_1, \dots, x_n]\!] \stackrel{\text{def}}{=} K[\![x_1, \dots, x_{n-1}]\!][\![x_n]\!]$ и представляет собою множество формальных сумм вида $F(x) = \sum_{\nu_1,\dots,\nu_n \in \mathbb{Z}_{\geqslant 0}} a_{\nu_1 \dots \nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n}$.

3.1.1. Алгебраические операции над рядами. Назовём *n-арной алгебраической операцией* в $K[\![x]\!]$ правило, сопоставляющее n рядам $f_1, \dots, f_n$ новый ряд f так, что каждый коэффициент ряда f вычисляется по коэффициентам рядов $f_1, \dots, f_n$ при помощи конечного числа[2] операций в K. Например, сложение и умножение рядов — это бинарные алгебраические операции, а подстановка вместо x численного значения $\alpha \in K$ алгебраической операцией обычно не является[3].

[1] Говоря формально, операции, о которых тут идёт речь, являются операциями над *последовательностями* (a_ν) и (b_ν) элементов кольца K. Буква x служит лишь для облегчения их восприятия.

[2] Которое может зависеть от номера коэффициента.

[3] Очевидным исключением из этого правила служит вычисление значения ряда $f(x)$ при $x = 0$, дающее в качестве результата свободный член этого ряда. Однако при произвольных α и f вычисление $f(\alpha)$ требует, вообще говоря, выполнения бесконечно большого количества сложений.

Пример 3.1 (замена переменной)
Подстановка в ряд $f(x)$ вместо x любого ряда $g(x) = b_1x + b_2x^2 + \dots$ с нулевым свободным членом является бинарной алгебраической операцией, дающей на выходе ряд

$$\begin{aligned} f(g(x)) = \sum a_k(b_1x + b_2x^2 + \dots)^k = \\ = a_0 + a_1(b_1x + b_2x^2 + \dots) + a_2(b_1x + b_2x^2 + \dots)^2 + a_3(b_1x + b_2x^2 + \dots)^3 + \dots = \\ = a_0 + (a_1b_1)\cdot x + (a_1b_2 + a_2b_1^2)\cdot x^2 + (a_1b_3 + 2\,a_2b_1b_2 + a_3b_1^3)\cdot x^3 + \dots , \end{aligned}$$

в котором на коэффициент при x^m влияют лишь начальные члены первых m слагаемых в f.

Пример 3.2 (обращение)
Покажем, что ряд $f(x) = a_0 + a_1x + a_2x^2 + \dots \in K[\![x]\!]$ обратим в $K[\![x]\!]$ если и только если его свободный член a_0 обратим в K, и в этом случае обращение $f \mapsto f^{-1}$ является унарной алгебраической операцией над обратимым рядом f. Пусть

$$(a_0 + a_1x + a_2x^2 + \dots)\cdot(b_0 + b_1x + b_2x^2 + \dots) = 1\,.$$

Приравнивая коэффициенты при одинаковых степенях x в левой и правой части, получаем бесконечную систему уравнений

$$\begin{aligned} a_0b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0 \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \end{aligned} \tag{3-4}$$

на коэффициенты b_i. Разрешимость первого уравнения равносильна обратимости a_0, и в этом случае $b_0 = a_0^{-1}$ и $b_k = -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \dots + a_kb_0)$ при всех $k \geqslant 1$.

Упражнение 3.2. Вычислите в $\mathbb{Q}[\![x]\!]$ а) $(1-x)^{-1}$ б) $(1-x^2)^{-1}$ в) $(1-x)^{-2}$.

3.1.2. Многочлены. Ряды с конечным числом ненулевых коэффициентов называются *многочленами*. Многочлены от $x_1, \dots, x_n$ с коэффициентами в K образуют в кольце степенных рядов подкольцо, которое обозначается $K[x_1, \dots, x_n] \subset K[\![x_1, \dots, x_n]\!]$. Многочлен от одной переменной x представляет собою формальное выражение вида $f(x) = a_0 + a_1x + \dots + a_nx^n$. Самый правый ненулевой коэффициент в нём называется *старшим*, а его номер — *степенью* многочлена f и обозначается $\deg f$. Многочлены со старшим коэффициентом 1 называются *приведёнными*, а многочлены степени нуль — *константами*.

Так как старший коэффициент произведения равен произведению старших коэффициентов сомножителей, для многочленов f_1, f_2 с коэффициентами в целостном[1] кольце K выполняется равенство $\deg(f_1f_2) = \deg(f_1) + \deg(f_2)$. В частности, кольцо $K[x]$ тоже целостное, и обратимыми элементами в нём являются только обратимые константы.

Упражнение 3.3. Покажите, что $y^n - x^n$ делится в $\mathbb{Z}[x, y]$ на $y - x$ и найдите частное.

[1] Т. е. с единицей и без делителей нуля.

3.1.3. Дифференциальное исчисление. Заменим в $f(x) = a_0 + a_1x + a_2x^2 + \dots$ переменную x на $x + t$, где t — ещё одна переменная. Получим ряд

$$f(x+t) = a_0 + a_1(x+t) + a_2(x+t)^2 + \dots \in K[\![x,t]\!] .$$

Раскроем в нём все скобки, затем сгруппируем слагаемые по степеням переменной t и обозначим через $f_m(x) \in K[\![x]\!]$ ряд, возникающий как коэффициент при t^m:

$$f(x+t) = f_0(x) + f_1(x)\cdot t + f_2(x)\cdot t^2 + f_3(x)\cdot t^3 + \dots = \sum\nolimits_{m\geqslant 0} f_m(x)\cdot t^m . \tag{3-5}$$

Упражнение 3.4. Убедитесь, что $f_0(x) = f(x)$ совпадает с исходным рядом f.

Ряд $f_1(x)$ называется *производной* от исходного ряда f и обозначается f' или $\frac{d}{dx}f$. Он однозначно определяется равенством

$$f(x+t) = f(x) + f'(x)\cdot t + (\text{члены, делящиеся на } t^2)$$

и может быть вычислен при помощи упр. 3.3 как результат подстановки $t = 0$ в ряд

$$\frac{f(x+t)-f(x)}{t} = \sum_{k\geqslant 1} a_k \frac{(x+t)^k - t^k}{t} = \sum_{k\geqslant 1} a_k\big((x+t)^{k-1} + (x+t)^{k-2}x + \dots + x^{k-1}\big) ,$$

что даёт

$$f'(x) = \sum_{k\geqslant 1} k\,a_k x^{k-1} = a_1 + 2a_2x + 3a_3x^2 + \dots . \tag{3-6}$$

Пример 3.3 (ряды с нулевой производной)
Из формулы (3-6) вытекает, что производная от константы равна нулю. Если[1] $\operatorname{char} K = 0$, то верно и обратное: $f' = 0$ тогда и только тогда, когда $f = a_0$. Но если $\operatorname{char} K = p > 0$, то производная от каждого монома вида x^{kp} занулится, поскольку коэффициент m при x^{m-1} в формуле (3-6) представляет собою сумму m единиц кольца K. Мы заключаем, над целостным кольцом K характеристики $p > 0$ равенство $f'(x) = 0$ означает, что $f(x) = g(x^p)$ для некоторого $g \in K[\![x]\!]$.

Упражнение 3.5. Покажите, что при простом $p \in \mathbb{N}$ для любого ряда $g \in \mathbb{F}_p[\![x]\!]$ выполняется равенство $g(x^p) = g(x)^p$.

Предложение 3.1 (правила дифференцирования)
Для любого $\alpha \in K$ и любых $f, g \in K[\![x]\!]$ справедливы равенства

$$(\alpha f)' = \alpha\cdot f' , \quad (f+g)' = f' + g' , \quad (fg)' = f'\cdot g + f\cdot g' . \tag{3-7}$$

Кроме того, если ряд g не имеет свободного члена, то

$$\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big) , \tag{3-8}$$

а если ряд f обратим, то

$$\frac{d}{dx}f^{-1} = -f'/f^2 . \tag{3-9}$$

[1] См. n° 2.5.5 на стр. 34.

Доказательство. Первые два равенства в (3-7) вытекают прямо из формулы (3-6). Для доказательства третьего перемножим ряды

$$f(x+t) = f(x) + t\cdot f'(x) + (\text{члены, делящиеся на } t^2)$$
$$g(x+t) = g(x) + t\cdot g'(x) + (\text{члены, делящиеся на } t^2)\,.$$

С точностью до членов, делящихся на t^2, получим

$$f(x+t)g(x+t) = f(x)g(x) + t\cdot(f'(x)g(x) + f(x)g'(x)) + (\text{члены, делящиеся на } t^2)\,,$$

откуда $(fg)' = f'\cdot g + f\cdot g'$. Формула (3-8) доказывается похожим образом: подставляя в $f(x)$ вместо x ряд $g(x+t)$, получаем $f\big(g(x+t)\big) = f\big(g(x) + t\cdot g'(x) + (\text{члены, делящиеся на } t^2)\big)$. Полагая $\tau(x,t) \stackrel{\text{def}}{=} g(x+t) - g(x) = t\cdot g'(x) + (\text{члены, делящиеся на } t^2)$ и переписывая правую часть предыдущего ряда как

$$\begin{aligned} f\big(g(x+t)\big) = f\big(g(x)+\tau(x,t)\big) = \\ = f(g(x)) + \tau(x,t)\cdot f'(g(x)) + (\text{члены, делящиеся на } \tau(x,t)^2) = \\ = f(g(x)) + t\cdot g'(x)\cdot f'(g(x)) + (\text{члены, делящиеся на } t^2)\,, \end{aligned}$$

заключаем, что $\big(f(g(x))\big)' = g'(x)\cdot f'\big(g(x)\big)$. Для доказательства формулы (3-9) достаточно продифференцировать обе части равенства $f\cdot f^{-1} = 1$. □

Упражнение 3.6. Покажите, что при $\operatorname{char}\Bbbk = 0$ в разложении (3-5) каждый ряд $f_m(x)$ равен $\frac{1}{m!}\big(\frac{d}{dx}\big)^m f(x)$, где $\big(\frac{d}{dx}\big)^m$ означает m-кратное применение операции $\frac{d}{dx}$.

3.2. Делимость в кольце многочленов. Школьный алгоритм «деления уголком» работает для многочленов с коэффициентами в произвольном коммутативном кольце с единицей при условии, что многочлен-делитель имеет обратимый старший коэффициент.

Предложение 3.2 (деление с остатком)
Пусть K — произвольное коммутативное кольцо с единицей, и старший коэффициент многочлена $u\in K[x]$ обратим. Тогда для любого $f\in K[x]$ существуют такие $q, r\in K[x]$, что $f = uq + r$ и $\deg(r) < \deg(u)$ или $r = 0$. Если кольцо K целостное, то q, r однозначно определяются этими свойствами по f, u.

Доказательство. Пусть $f = a_n x^n + \ldots + a_1 x + a_0$ и $u = b_k x^k + \ldots + b_1 x + b_0$, где b_k обратим. Если $n < k$, можно взять $q = 0$ и $r = f$. Если $k = 0$, т. е. $u = b_0$, можно взять $r = 0$, $q = b_0^{-1} f$. Пусть $n \geqslant k > 0$, и по индукции предложение справедливо для всех многочленов f с $\deg f < n$. Тогда $f - a_n b_k^{-1} x^{n-k} u = qu + r$, где $\deg r < \deg u$ или $r = 0$, ибо $\deg(f - a_n b_k^{-1} x^{n-k} u) < n$. Тем самым, $f = (q + a_n b_k^{-1} x^{n-k})\cdot u + r$, как и утверждалось. Если кольцо K целостное и $p, s\in K[x]$ таковы, что $\deg(s) < \deg(u)$ и $up + s = f = uq + r$, то $u(q-p) = r - s$. При $p - q \neq 0$ степень левой части не менее $\deg u$, что строго больше степени правой. Поэтому, $p - q = 0$, откуда и $r - s = 0$. □

Определение 3.1
Многочлены q и r, удовлетворяющие условиям предл. 3.2 называются *неполным частным* и *остатком* от деления f на u в $K[x]$.

Следствие 3.1
Для любых многочленов f, g с коэффициентами в любом поле $\Bbbk$ существует единственная такая пара многочленов $q, r \in \Bbbk[x]$, что $f = g \cdot q + r$ и $\deg(r) < \deg(g)$ или $r = 0$. □

Пример 3.4 (вычисление значения многочлена в точке)
Остаток от деления многочлена $f(x) = a_n x^n + \ldots + a_1 x + a_0$ на линейный двучлен $x - \alpha$ имеет степень нуль и равен значению $f(\alpha)$ многочлена f при $x = \alpha$, в чём легко убедиться, подставляя $x = \alpha$ в равенство $f(x) = (x - \alpha) \cdot q(x) + r$. При «делении уголком» значение $f(\alpha)$ вычисляется в виде

$$f(\alpha) = \alpha\Big(\ldots \alpha\big(\alpha(\alpha a_n + a_{n-1}) + a_{n-2}\big) + \ldots\Big) + a_0\,,$$

что гораздо эффективнее «лобовой подстановки» значения $x = \alpha$ в $a_n x^n + \ldots + a_1 x + a_0$.

Предложение 3.3
Над произвольным полем $\Bbbk$ для любого набора многочленов $f_1, \ldots, f_n \in \Bbbk[x]$ существует единственный приведённый многочлен $d \in \Bbbk[x]$, который делит каждый из многочленов f_i и делится на любой многочлен, делящий каждый из многочленов f_i. Он представляется в виде

$$d = f_1 h_1 + \ldots + f_n h_n\,, \quad \text{где} \quad h_i \in \Bbbk[x]\,. \tag{3-10}$$

Произвольный многочлен $g \in \Bbbk[x]$ представим в виде (3-10) если и только если $d \mid g$.

Доказательство. Единственность очевидна: два многочлена, каждый из которых делится на другой, имеют равные степени и могут различаться лишь постоянным множителем, который равен единице, коль скоро оба многочлена приведены. Существование доказывается тем же рассуждением, что и в n° 2.4.2 на стр. 30. Обозначим множество всех многочленов $g \in \Bbbk[x]$, представимых в виде (3-10), через $(f_1, \ldots, f_n) \stackrel{\text{def}}{=} \big\{ f_1 h_1 + \ldots + f_n h_n \;\big|\; h_i \in \Bbbk[x] \big\}$. Это подкольцо в $\Bbbk[x]$, содержащее вместе с каждым многочленом g и все кратные ему многочлены hg с любым $h \in \Bbbk[x]$. Кроме того, $(f_1, \ldots, f_n)$ содержит каждый из многочленов f_i, и все многочлены из $(f_1, \ldots, f_n)$ делятся на любой общий делитель всех многочленов f_i. Возьмём в качестве d приведённый многочлен наименьшей степени в $(f_1, \ldots, f_n)$. Для любого $g \in (f_1, \ldots, f_n)$ остаток $r = g - qd$ от деления g на d лежит в $(f_1, \ldots, f_n)$, и так как неравенство $\deg r < \deg d$ невозможно, мы заключаем, что $r = 0$, т. е. все $g \in (f_1, \ldots, f_n)$ делятся на d. □

Определение 3.2
Многочлен d из предл. 3.3 называется *наибольшим общим делителем*[1] многочленов f_i и обозначается нод$(f_1, \ldots, f_n)$.

3.2.1. Взаимная простота. Из предл. 3.3 вытекает, что для любого поля $\Bbbk$ взаимная простота[2] многочленов $f_1, \ldots, f_m \in \Bbbk[x]$, т. е. наличие таких $h_1, \ldots, h_m \in \Bbbk[x]$, что $h_1 f_1 + \ldots + h_n f_n = 1$, равносильна отсутствию у многочленов $f_1, \ldots, f_n$ общих делителей положительной степени — точно также, как это происходит в кольце целых чисел $\mathbb{Z}$.

Определение 3.3
Необратимый многочлен $f \in K[x]$ с коэффициентами в целостном[3] кольце K называется *неприводимым*, если из равенства $f = gh$ вытекает, что g или h является обратимой константой.

[1] Ср. с зам. 2.3. на стр. 29.
[2] См. опр. 2.2 на стр. 29.
[3] Т. е. с единицей и без делителей нуля.

Упражнение 3.7. Пусть $\Bbbk$ — любое поле. Пользуясь лем. 2.3, докажите следующую теорему об однозначности разложения на простые множители в кольце $\Bbbk[x]$: каждый многочлен f положительной степени является произведением конечного числа неприводимых многочленов, причём в любых двух таких представлениях $p_1 \dots p_k = f = q_1 \dots q_m$ одинаковое количество множителей $k = m$, и их можно перенумеровать так, чтобы при всех i выполнялись равенства $p_i = \lambda_i q_i$ для некоторых ненулевых констант $\lambda_i \in \Bbbk$.

3.2.2. Алгоритм Евклида – Гаусса из n° 2.2.2 также применим к многочленам с коэффициентами из любого поля $\Bbbk$. Покажем, как он работает, вычислив нод(f, g) для

$$f = x^7 + 3x^6 + 4x^5 + x^4 + 5x^2 + 3x^3 + 3x + 4 \text{ и } g = x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4\,.$$

Как и в n° 2.2.2 на стр. 27, составляем таблицу

$$\begin{pmatrix} f & 1 & 0 \\ g & 0 & 1 \end{pmatrix} = \begin{pmatrix} x^7 + 3x^6 + 4x^5 + x^4 + 3x^3 + 5x^2 + 3x + 4 & 1 & 0 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}.$$

и преобразуем её строки, умножая какую-нибудь из них на ненулевую константу и прибавляя к результату другую строку, умноженную на подходящий многочлен, так, чтобы степень одного из многочленов в левом столбце строго уменьшалась, пока один из них не обнулится:

$$(1) \mapsto (1) - x^2 \cdot (2): \quad \begin{pmatrix} -2x^6 - 7x^5 - 11x^4 - 4x^3 + x^2 + 3x + 4 & 1 & -x^2 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}$$

$$(1) \mapsto (1) + 2x \cdot (2): \quad \begin{pmatrix} 3x^5 + 11x^4 + 20x^3 + 15x^2 + 11x + 4 & 1 & -x^2 + 2x \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}$$

$$(1) \mapsto (1) - 3 \cdot (2): \quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^5 + 5x^4 + 11x^3 + 12x^2 + 7x + 4 & 0 & 1 \end{pmatrix}$$

$$(2) \mapsto 4 \cdot (2) + x \cdot (1): \quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ 7x^4 + 23x^3 + 38x^2 + 20x + 16 & x & -x^3 + 2x^2 - 3x + 4 \end{pmatrix}$$

$$(2) \mapsto 4 \cdot (2) + 7 \cdot (1): \quad \begin{pmatrix} -4x^4 - 13x^3 - 21x^2 - 10x - 8 & 1 & -x^2 + 2x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix}$$

$$(1) \mapsto (1) + 4x \cdot (2): \quad \begin{pmatrix} 7x^3 + 19x^2 + 22x - 8 & 16x^2 + 28x + 1 & -16x^4 + 4x^3 + 7x^2 - 18x - 3 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix}$$

$$(1) \mapsto (1) - 7 \cdot (1): \quad \begin{pmatrix} -16x^2 - 48x - 64 & 16x^2 - 48 & -16x^4 + 32x^3 - 32x + 32 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix}$$

$$(1) \mapsto -(1)/16: \quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ x^3 + 5x^2 + 10x + 8 & 4x + 7 & -4x^3 + x^2 + 2x - 5 \end{pmatrix}$$

$$(2) \mapsto (2) - x \cdot (1): \quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 2x^2 + 6x + 8 & x^3 + x + 7 & -x^5 + 2x^4 - 4x^3 - x^2 + 4x - 5 \end{pmatrix}$$

$$(2) \mapsto (2) - 2 \cdot (1): \quad \begin{pmatrix} x^2 + 3x + 4 & -x^2 + 3 & x^4 - 2x^3 + 2x - 2 \\ 0 & x^3 + 2x^2 + x + 1 & -x^5 - x^2 - 1 \end{pmatrix}$$

Полученный результат означает, что нод$(f, g) = x^2 + 3x + 4 = -(x^2 - 3) \cdot f + (x^4 - 2x^3 + 2x - 2) \cdot g$, а нок$(f, g) = (x^3 + 2x^2 + x + 1) \cdot f = (x^5 + x^2 + 1) \cdot g$.

Упражнение 3.8. Убедитесь, что в каждой возникающей по ходу вычисления таблице

$$\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$$

выполняются равенства $p = rf + sg$, $q = uf + wg$, а многочлен $rw - us$ является ненулевой константой, и выведите из них, что в итоговой таблице вида

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} 0 & m_1 & m_2 \\ d' & h_1 & h_2 \end{pmatrix}$$

многочлен $d' = fh_1 + gh_2$ делит f и g, а многочлен $c' = fm_1 = -gm_2$ делит любое общее кратное f и g.

Теорема 3.1 (китайская теорема об остатках)
Пусть $\Bbbk$ — произвольное поле, и многочлен $f = f_1 \dots f_m \in \Bbbk[x]$ является произведением m попарно взаимно простых многочленов $f_i \in \Bbbk[x]$. Тогда отображение

$$\varphi : \frac{\Bbbk[x]}{(f)} \to \frac{\Bbbk[x]}{(f_1)} \times \dots \times \frac{\Bbbk[x]}{(f_m)}, \quad [g]_f \mapsto ([g]_{f_1}, \dots, [g]_{f_m}), \tag{3-11}$$

корректно определено и является изоморфизмом колец.

Доказательство. Проверка того, что отображение (3-11) корректно определено[1], является гомоморфизмом колец и имеет нулевое ядро, дословно та же, что в n° 2.7 на стр. 37, и мы оставляем её читателям. Докажем, что гомоморфизм (3-11) сюръективен. Для каждого i обозначим через $F_i = f/f_i$ произведение всех многочленов f_ν кроме i-го. Так как f_i взаимно прост с каждым f_ν при $\nu \neq i$, многочлены F_i и f_i взаимно просты по лем. 2.3 на стр. 29. Поэтому существует такой многочлен $h_i \in \Bbbk[x]$, что $[1]_{f_i} = [F_i]_{f_i}[h_i]_{f_i} = [F_i h_i]_{f_i}$ в $\Bbbk[x]/(f_i)$. Мы заключаем, что класс многочлена $F_i h_i$ нулевой во всех кольцах $\Bbbk[x]/(f_\nu)$ с $\nu \neq i$ и равен единице в $\Bbbk[x]/(f_i)$. Поэтому для любого набора классов $[r_i]_{f_i} \in \Bbbk[x]/(f_i)$ многочлен $g = \sum_i r_i F_i h_i$ таков, что $[g]_{f_i} = [r_i]_{f_i}$ сразу для всех i. □

3.3. Корни многочленов. Число $\alpha \in K$ называется *корнем* многочлена $f \in K[x]$, если $f(\alpha) = 0$. Как мы видели в прим. 3.4 на стр. 45, это равносильно тому, что $f(x)$ делится в $K[x]$ на $x - \alpha$.

Упражнение 3.9. Пусть $\Bbbk$ — поле. Проверьте, что многочлен степени 2 или 3 неприводим в $\Bbbk[x]$ если и только если у него нет корней в поле $\Bbbk$.

Предложение 3.4
Пусть K — целостное кольцо и $f \in K[x]$ имеет s различных корней $\alpha_1, \dots, \alpha_s \in K$. Тогда f делится в $K[x]$ на произведение $\prod_i (x - \alpha_i)$. В частности, $\deg(f) \geqslant s$ или $f = 0$.

Доказательство. Так как в K нет делителей нуля и $(\alpha_i - \alpha_1) \neq 0$ при $i \neq 1$, подставляя в равенство $f(x) = (x - \alpha_1) \cdot q(x)$ значения $x = \alpha_2, \dots, \alpha_s$, убеждаемся, что они являются корнями многочлена $q(x)$, и применяем индукцию. □

[1] Т. е. $\varphi([g]_f) = \varphi([h]_f)$ при $[g]_f = [h]_f$.

Следствие 3.2
Пусть кольцо K целостное, и $f, g \in K[x]$ имеют степени, не превосходящие n. Если $f(\alpha_i) = g(\alpha_i)$ для более, чем n попарно разных $\alpha_i \in K$, то $f = g$ в $K[x]$.

Доказательство. Так как $\deg(f-g) \leqslant n$, и у $f-g$ больше n корней, $f-g=0$. □

Пример 3.5 (интерполяционный многочлен Лагранжа)
Пусть $\Bbbk$ — поле. По сл. 3.2 для любых наборов из $n+1$ различных чисел $a_0, a_1, \dots, a_n \in \Bbbk$ и произвольных значений $b_0, b_1, \dots, b_n \in \Bbbk$ имеется не более одного многочлена $f \in \Bbbk[x]$ степени $\leqslant n$ со значениями $f(a_i) = b_i$ при всех i. Единственный такой многочлен всегда существует и называется *интерполяционным многочленом Лагранжа*. Чтобы выписать его явно заметим, что произведение $\prod_{\nu\neq i}(x-a_\nu)$ зануляется во всех точках a_ν кроме i-той, где его значение отлично от нуля. Деля на него, получаем многочлен $f_i(x) = \prod_{\nu\neq i}(x-a_\nu)/\prod_{\nu\neq i}(a_i-a_\nu)$ со значениями $f_i(a_\nu) = 0$ при $\nu \neq i$ и $f_i(a_i) = 1$. Искомый многочлен Лагранжа имеет вид

$$\sum_{i=0}^{n} b_i \cdot f_i(x) = \sum_{i=0}^{n} b_i \prod_{\nu\neq i} \frac{x-a_\nu}{a_i-a_\nu}\,.$$

3.3.1. Присоединение корней. Зафиксируем произвольный отличный от константы многочлен $f \in \Bbbk[x]$. Кольцо вычетов $\Bbbk[x]/(f)$ определяется аналогично кольцу[1] $\mathbb{Z}/(n)$. А именно, обозначим через $(f) = \{fh \mid h \in \Bbbk[x]\}$ подкольцо в $\Bbbk[x]$, состоящее из всех многочленов, делящихся на f. Сдвиги этого подкольца на всевозможные элементы $g \in \Bbbk[x]$ обозначаются $[g]_f = g + (f) = \{g + fh \mid h \in \Bbbk[x]\}$ и называются *классами вычетов* по модулю f. Два таких класса $[g]_f$ и $[h_f]$ либо не пересекаются, либо совпадают, причём последнее означает, что $g_1 - g_2 \in (f)$.

Упражнение 3.10. Убедитесь, что отношение $g_1 \equiv g_2 \pmod f$, означающее, что $g_1 - g_2 \in (f)$, является эквивалентностью[2].

Множество классов вычетов обозначается через $\Bbbk[x]/(f)$. Сложение и умножение в нём задаётся формулами $[g]_f + [h]_f \stackrel{\text{def}}{=} [g+h]_f$, $[g]_f \cdot [h]_f \stackrel{\text{def}}{=} [gh]_f$.

Упражнение 3.11. Проверьте корректность[3] этого определения и выполнение в $\Bbbk[x]/(f)$ всех аксиом коммутативного кольца с единицей.

Нулём кольца $\Bbbk[x]/(f)$ является класс $[0]_f = (f)$, единицей — класс $[1]_f = 1 + (f)$. Так как константы не делятся на многочлены положительной степени, классы всех констант $c \in \Bbbk$ различны по модулю f. Иначе говоря, поле $\Bbbk$ гомоморфно вкладывается в кольцо $\Bbbk[x]/(f)$ в качестве подполя, образованного классами констант. Поэтому классы чисел $c \in \Bbbk$ обычно записываются как c, а не $[c]_f$.

Упражнение 3.12. Покажите, что поле $\Bbbk[x]/(x-\alpha)$ изоморфно полю $\Bbbk$.

Каждый многочлен $g \in \Bbbk[x]$ однозначно представляется в виде $g = fh + r$, где $\deg r < \deg f$. Поэтому в каждом классе $[g]_f$ есть ровно один многочлен $r \in [g]_f$ с $\deg(r) < \deg(f)$. Таким образом, каждый элемент кольца $\Bbbk[x]/(f)$ однозначно записывается в виде

$$[a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_f = a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}\,,\ \text{где } \vartheta = [x]_f \text{ и } a_i \in \Bbbk\,.$$

[1] См. n° 2.4 на стр. 30.
[2] См. опр. 1.1 на стр. 11.
[3] Т. е. независимость классов $[g+h]_f$ и $[gh]_f$ от выбора представителей $g \in [g]_f$ и $h \in [h]_f$.

Класс $\vartheta = [x]_f$ удовлетворяет в кольце $\Bbbk[x]/(f)$ уравнению $f(\vartheta) = 0$, ибо

$$f(\vartheta) = f\left([x]_f\right) = [f(x)]_f = [0]_f\,.$$

В таких обозначениях сложение и умножение вычетов представляет собою формальное сложение и умножение записей $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$ по стандартным правилам раскрытия скобок и приведения подобных слагаемых с учётом соотношения $f(\vartheta) = 0$. По этой причине кольцо $\Bbbk[x]/(f)$ часто обозначают через $\Bbbk[\vartheta]$, где $f(\vartheta) = 0$, и называют *расширением* поля $\Bbbk$ путём *присоединения* к нему корня ϑ многочлена $f \in \Bbbk[x]$.

Например, кольцо $\mathbb{Q}[x]/(x^2-2)$ можно воспринимать как множество формальных записей вида $a + b\sqrt{2}$, где $\sqrt{2} \stackrel{\text{def}}{=} [x]$. Сложение и умножение таких записей происходит по стандартным правилам раскрытия скобок с учётом того, что $\sqrt{2}\cdot\sqrt{2} = 2$:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (cb + ad)\sqrt{2}\,.$$

Упражнение 3.13. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем, и выясните, являются ли полями кольца $\mathbb{Q}[\vartheta]$, в которых а) $\vartheta^3 + 1 = 0$ б) $\vartheta^3 + 2 = 0$.

Предложение 3.5
Пусть $\Bbbk$ — произвольное поле и $f \in \Bbbk[x]$. Кольцо $\Bbbk[x]/(f)$ является полем если и только если f неприводим в $\Bbbk[x]$.

Доказательство. Если $f = gh$, где $\deg g$, $\deg h$ строго меньше $\deg f$, то ненулевые классы $[g]$, $[h]$ являются делителями нуля в кольце $\Bbbk[x]/(f)$, что невозможно в поле. Если f неприводим, то $\text{нод}(f, g) = 1$ для любого $g \notin (f)$, и значит, $fh + gq = 1$ для некоторых $h, q \in \Bbbk[x]$, откуда $[q]\cdot[g] = [1]$, т. е. класс $[g]$ обратим в $\Bbbk[x]/(f)$. □

Упражнение 3.14. Найдите $(1+\vartheta)^{-1}$ в поле $\mathbb{Q}[\vartheta]$, где $\vartheta^2 + \vartheta + 1 = 0$.

Теорема 3.2
Для любого поля $\Bbbk$ и произвольного $f \in \Bbbk[x]$ существует такое поле $\mathbb{F} \supset \Bbbk$, что в кольце $\mathbb{F}[x]$ многочлен f разлагается в произведение $\deg f$ линейных множителей.

Доказательство. Индукция по $n = \deg f$. Пусть для любого поля $\Bbbk$ и каждого многочлена степени $< n$ из $\Bbbk[x]$ искомое поле имеется[1]. Рассмотрим многочлен f степени n. Если он приводим, т. е. $f = gh$ и $\deg g, \deg h < n$, то по индуктивному предположению существует поле $\mathbb{L} \supset \Bbbk$ над которым g полностью разлагается на линейные множители, а также поле $\mathbb{F} \supset \mathbb{L}$ над которым полностью разлагается h, а с ним и f. Если f неприводим, рассмотрим поле $\mathbb{L} = \Bbbk[x]/(f)$. Оно содержит $\Bbbk$ в качестве классов констант, и многочлен f делится в $\mathbb{L}[x]$ на $(x - \vartheta)$, где $\vartheta = [x]_f \in \mathbb{L}$. Частное от этого деления имеет степень $n-1$ и по индукции раскладывается на линейные множители над некоторым полем $\mathbb{F} \supset \mathbb{L}$. Тем самым и f полностью раскладывается над $\mathbb{F}$. □

[1] Заметим, что при $n = 2$ это так: достаточно взять $\mathbb{F} = \Bbbk$.

3.3.2. Общие корни нескольких многочленов $f_1, \ldots, f_m \in \Bbbk[x]$ с коэффициентами в поле $\Bbbk$ искать обычно проще, чем корни каждого из многочленов f_i в отдельности, так как общие корни являются корнями многочлена нод$(f_1, \ldots, f_m)$, который находится при помощи алгоритма Евклида и как правило имеет меньшую степень, чем любой из f_i. Отметим, что при нод$(f_1, \ldots, f_m) = 1$ многочлены f_i не имеют общих корней не только в поле $\Bbbk$, но и ни в каком большем кольце $K \supset \Bbbk$, поскольку существуют такие $h_i \in \Bbbk[x]$, что $f_1h_1 + \ldots + f_mh_m = 1$.

3.3.3. Кратные корни. Пусть $\Bbbk$ — произвольное поле. Число $\alpha \in \Bbbk$ называется m-кратным корнем многочлена $f \in \Bbbk[x]$, если $f(x) = (x-\alpha)^m \cdot g(x)$ и $g(\alpha) \neq 0$. Корни кратности $m = 1$ называются *простыми*, а более высоких кратностей — *кратными*.

Предложение 3.6
Число α является кратным корнем многочлена f если и только если $f(\alpha) = f'(\alpha) = 0$.

Доказательство. Если корень α кратный, то $f(x) = (x-\alpha)^2 g(x)$. Дифференцируя, получаем

$$f'(x) = (x-\alpha)\big(2g(x) + (x-\alpha)g'(x)\big),$$

откуда $f'(\alpha) = 0$. Если корень α не кратный, то $f(x) = (x-\alpha)g(x)$, где $g(\alpha) \neq 0$. Подставляя $x = \alpha$ в $f'(x) = (x-\alpha)g'(x) + g(x)$, получаем $f'(\alpha) = g(\alpha) \neq 0$. □

Предложение 3.7
Если $\operatorname{char}\Bbbk = 0$, то $\alpha \in \Bbbk$ является m-кратным корнем многочлена $f \in \Bbbk[x]$ если и только если

$$f(\alpha) = \frac{d}{dx}f(\alpha) = \ldots = \frac{d^{m-1}}{dx^{m-1}}f(\alpha) = 0 \quad \text{и} \quad \frac{d^m}{dx^m}f(\alpha) \neq 0\,.$$

Доказательство. Если $f(x) = (x-\alpha)^m g(x)$, то $f'(x) = (x-\alpha)^{m-1}\big(mg(x) + (x-\alpha)g'(x)\big)$. При $g(\alpha) \neq 0$ второй множитель в последнем равенстве ненулевой при $x = \alpha$. Поэтому α является m-кратным корнем f если и только если α является $(m-1)$-кратным корнем f'. □

3.3.4. Сепарабельность. Многочлен $f \in \Bbbk[x]$ называется *сепарабельным*, если он взаимно прост со своей производной. Это равносильно отсутствию у f кратных корней в любом кольце $K \supset \Bbbk$. В самом деле, если $\deg$ нод$(f, f') \geqslant 1$ или $f' = 0$, то по теор. 3.2 нод(f, f') или, соответственно, сам f имеет корень в некотором поле $\mathbb{F} \supset \Bbbk$, и по предл. 3.6 этот корень кратный для f. Наоборот, если нод$(f, f') = 1$, то $pf + qf' = 1$ для подходящих $p, q \in \Bbbk[x]$, и поэтому f и f' не могут одновременно обратиться в нуль ни в каком расширении $K \supset \Bbbk$.

Пример 3.6 (сепарабельность и несепарабельность неприводимых многочленов)
Если многочлен $f \in \Bbbk[x]$ неприводим, то он взаимно прост со всеми ненулевыми многочленами меньшей степени. Поэтому нод$(f, f') = 1$, если $f' \neq 0$ в $\Bbbk[x]$. Поскольку над полем характеристики нуль каждый многочлен положительной степени имеет ненулевую производную, все неприводимые многочлены над таким полем сепарабельны. Если $\operatorname{char}\Bbbk = p > 0$, то $f' = 0$ если и только если[1] $f(x) = g(x^p)$ для некоторого $g(x) = b_mx^m + \ldots + b_1x + b_0 \in \Bbbk[x]$. Когда $\Bbbk = \mathbb{F}_p$ является простым конечным полем, $g(x^p) = b_mx^{pm} + \ldots + b_1x^p + b_0 = b_m^px^{pm} + \ldots + b_1^px^p + b_0^p = (b_mx^m + \ldots + b_1x + b_0)^p = g^p(x)$, ибо в характеристике p возведение в p-тую степень является гомоморфизмом колец[2] и тождественно действует на простом поле $\mathbb{F}_p$. Таким образом,

[1] См. прим. 3.3 на стр. 43.
[2] См. прим. 2.7 на стр. 31.

в $\mathbb{F}_p[x]$ каждый многочлен с нулевой производной является чистой p-той степенью и тем самым приводим. Следовательно, все неприводимые многочлены над $\mathbb{F}_p$ тоже сепарабельны. Над бесконечными полями положительной характеристики существуют несепарабельные неприводимые многочлены. Например, можно показать, что над полем $\Bbbk = \mathbb{F}_p(t)$ рациональных функций от одной переменной t с коэффициентами в поле $\mathbb{F}_p$ многочлен $f(x) = x^p - t$ неприводим, но так как $f' = 0$, многочлен f не сепарабелен.

3.4. Поле комплексных чисел $\mathbb{C} \stackrel{\text{def}}{=} \mathbb{R}[t]/(t^2+1)$ получается из поля $\mathbb{R}$ присоединением корня неприводимого над $\mathbb{R}$ многочлена $t^2+1=0$ и состоит из элементов $x+iy$, где $x, y \in \mathbb{R}$, а $i \stackrel{\text{def}}{=} [t]$ удовлетворяет соотношению $i^2 = -1$. Обратным к ненулевому числу $x + yi$ является число

$$\frac{1}{x+yi} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}\cdot i\,.$$

Комплексное число $z = x + yi$ удобно изображать на плоскости $\mathbb{R}^2$ с фиксированной прямоугольной системой координат (x, y) *радиус вектором* z, ведущим из начала координат в точку $z = (x, y)$, как на рис. 3◇1. Координаты (x, y) называются *действительной* и *мнимой* частями числа $z \in \mathbb{C}$ и обозначаются через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$, а длина $|z| \stackrel{\text{def}}{=} \sqrt{x^2+y^2}$ называется *модулем* или *абсолютной величиной* комплексного числа z. Множество всех таких $\vartheta \in \mathbb{R}$, что поворот плоскости вокруг нуля на угол ϑ совмещает направление координатной оси x с направлением вектора z, называется *аргументом* числа z и обозначается $\mathrm{Arg}(z) = \{\alpha + 2\pi k \mid k \in \mathbb{Z}\}$, где $\alpha \in \mathbb{R}$ — ориентированная длина какой-нибудь дуги единичной окружности, ведущей из точки $(1, 0)$ в точку[1] $z/|z|$. Таким образом, каждое комплексное число имеет вид $z = |z|\cdot(\cos\alpha + i\cdot\sin\alpha)$, где $\alpha \in \mathrm{Arg}(z)$, и $\mathrm{Re}(z) = |z|\cdot\cos\alpha$, а $\mathrm{Im}(z) = |z|\cdot\sin\alpha$.

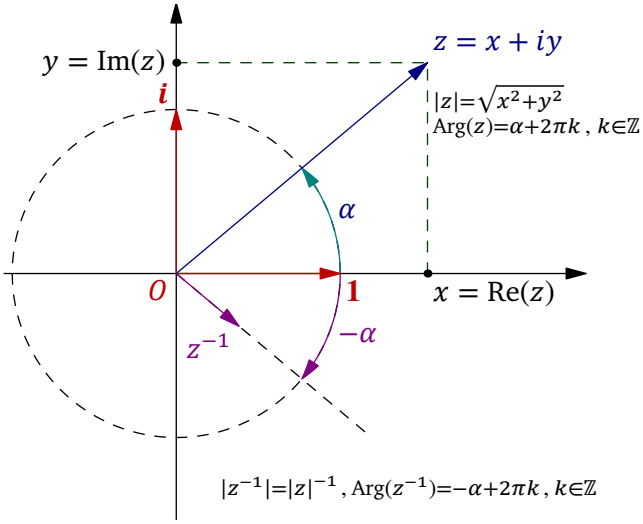


Рис. 3◇1. Числа $z = |z|\cdot(\cos\alpha + i\sin\alpha)$ и $z^{-1} = |z|^{-1}(\cos\alpha - i\sin\alpha)$.

На множестве векторов в $\mathbb{R}^2$ имеется своя внутренняя операция сложения векторов, относительно которой радиус векторы точек $z \in \mathbb{R}^2$ образуют абелеву группу. Зададим на множестве векторов в $\mathbb{R}^2$ операцию умножения требованием, чтобы длины перемножаемых векторов

[1] Любые две таких дуги отличаются друг от друга на целое число оборотов, а «ориентированность» означает, что длину дуги следует брать со знаком «+», если движение вдоль неё происходит против часовой стрелки, и со знаком «−» если по часовой стрелке.

перемножались, а аргументы — складывались, т. е.

$$\begin{gathered} |z_1 z_2| = |z_1| \cdot |z_2| \\ \operatorname{Arg}(z_1 z_2) = \operatorname{Arg}(z_1) + \operatorname{Arg}(z_2) \stackrel{\text{def}}{=} \{\vartheta_1 + \vartheta_2 \mid \vartheta_1 \in \operatorname{Arg}(z_1),\ \vartheta_2 \in \operatorname{Arg}(z_2)\}. \end{gathered} \tag{3-12}$$

Упражнение 3.15. Проверьте корректность нижней формулы, т. е. убедитесь, что любые два числа в правом множестве отличаются на целое кратное 2π.

Лемма 3.1
Множество радиус векторов точек z евклидовой координатной плоскости $\mathbb{R}^2$ с описанными выше сложением и умножением является полем. Отображение $\mathbb{C} \to \mathbb{R}^2$, сопоставляющее комплексному числу $x + iy \in \mathbb{C}$ точку $z = (x, y) \in \mathbb{R}^2$, является изоморфизмом полей.

Доказательство. Радиус векторы точек плоскости образуют абелеву группу по сложению. Очевидно также, что ненулевые векторы образуют абелеву группу относительно операции умножения, задаваемой формулами (3-12). Единицей этой группы служит единичный направляющий вектор оси x, а обратный к ненулевому z вектор z^{-1} имеет $|z^{-1}| = 1/|z|$ и $\operatorname{Arg}(z^{-1}) = -\operatorname{Arg}(z)$ (см. рис. 3⋄1). Для проверки дистрибутивности заметим, что для любого $a \in \mathbb{R}^2$ отображение

$$a\colon \mathbb{R}^2 \to \mathbb{R}^2, \quad z \mapsto az,$$

состоящее в умножении всех векторов на a по формулам (3-12), представляет собою *поворотную гомотетию*[1] плоскости $\mathbb{R}^2$ относительно начала координат на угол $\operatorname{Arg}(a)$ с коэффициентом $|a|$. Аксиома дистрибутивности $a(b + c) = ab + ac$ утверждает, что поворотная гомотетия перестановочна со сложением векторов[2]. Но это действительно так, поскольку и повороты и гомотетии переводят параллелограммы в параллелограммы. Таким образом, радиус векторы точек евклидовой координатной плоскости $\mathbb{R}^2$ образуют поле. Векторы, параллельные горизонтальной координатной оси, составляют в нём подполе, изоморфное полю $\mathbb{R}$. Если обозначить через i единичный направляющий вектор вертикальной координатной оси, то радиус вектор каждой точки $z = (x, y) \in \mathbb{R}^2$ однозначно запишется в виде $z = x + iy$, где числа $x, y \in \mathbb{R}$ понимаются как векторы, параллельные горизонтальной координатной оси, а сложение и умножение происходят по правилам поля $\mathbb{R}^2$. При этом $i^2 = -1$ и для любых векторов $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ выполняются равенства $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$ и

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1),$$

которыми описывается сложение и умножение вычетов $[x + yt]$ в поле $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$. □

3.4.1. Комплексное сопряжение. Числа $z = x + iy$ и $\overline{z} \stackrel{\text{def}}{=} x - iy$ называются *комплексно сопряжёнными*. В терминах комплексного сопряжения обратное к ненулевому $z \in \mathbb{C}$ число можно записать как $z^{-1} = \overline{z}/|z|^2$. На геометрическом языке комплексное сопряжение $z \mapsto \overline{z}$ представляет собою симметрию комплексной плоскости относительно вещественной оси x. С алгебраической точки зрения сопряжение является инволютивным[3] автоморфизмом поля $\mathbb{C}$, т. е. $\overline{\overline{z}} = z$ для всех $z \in \mathbb{C}$, а $\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2$ и $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$ для всех $z_1, z_2 \in \mathbb{C}$

[1] *Поворотной гомотетией* относительно точки 0 на угол α с коэффициентом $\varrho > 0$ называется композиция поворота на угол α вокруг точки 0 и растяжения в ϱ раз относительно 0. Так такие растяжения и повороты коммутируют друг с другом, неважно в каком порядке выполняется эта композиция.

[2] Т. е. является гомоморфизмом аддитивных групп.

[3] Эндоморфизм $\iota\colon X \to X$ произвольного множества X называется *инволюцией*, если $\iota \circ \iota = \mathrm{Id}_X$. По предл. 1.4 на стр. 16 всякая инволюция автоматически биективна.

3.4.2. Тригонометрия. Почти вся школьная тригонометрия представляет собою трудную для восприятия закодированную запись заурядных алгебраических вычислений с комплексными числами, лежащими на единичной окружности.

Пример 3.7 (формулы сложения аргументов)
Произведение z_1z_2 чисел $z_1 = \cos\varphi_1 + i\sin\varphi_1$ и $z_2 = \cos\varphi_2 + i\sin\varphi_2$ согласно лем. 3.1 равно $\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)$, а лобовое перемножение этих чисел путём раскрытия скобок даёт $z_1z_2 = (\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)$, откуда $\cos(\varphi_1+\varphi_2) = \cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2$ и $\sin(\varphi_1+\varphi_2) = \cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2$. Таким образом мы *доказали* тригонометрические формулы сложения аргументов.

Пример 3.8 (тригонометрические функции кратных углов)
По лем. 3.1 число $z = \cos\varphi + i\sin\varphi \in \mathbb{C}$ имеет $z^n = \cos(n\varphi) + i\sin(n\varphi)$. Раскрывая скобки в биноме $(\cos\varphi + i\sin\varphi)^n$ по форм. (1-8) на стр. 10, получаем равенство

$$\begin{aligned}\cos(n\varphi) + i\sin(n\varphi) &= (\cos\varphi + i\sin\varphi)^n = \\ &= \cos^n\varphi + i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi - i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \ldots = \\ &= \left(\binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots\right) + \\ &\quad + i\cdot\left(\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots\right)\end{aligned}$$

заключающее в себе сразу все мыслимые формулы для кратных углов:

$$\begin{aligned}\cos(n\varphi) &= \binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \cdots \\ \sin(n\varphi) &= \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \cdots\end{aligned}$$

Например, $\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\cdot\sin^2\varphi = 4\cos^3\varphi - 3\cos^2\varphi$.

Упражнение 3.16. Выразите $\sin(2\pi/5)$ и $\cos(2\pi/5)$ через радикалы от рациональных чисел.

3.4.3. Корни из единицы и круговые многочлены. Решим в поле $\mathbb{C}$ уравнение $z^n = 1$. Сравнивая модули левой и правой части, заключаем, что $|z| = 1$. Сравнивая аргументы, получаем $n\operatorname{Arg}(z) = \operatorname{Arg}(1) = \{2\pi k \mid k \in \mathbb{Z}\}$. С точностью до прибавления целых кратных 2π существует ровно n различных вещественных чисел, попадающих при умножении на n в множество $\{2\pi k \mid k \in \mathbb{Z}\}$. Это все геометрически различные углы $2\pi k/n$ с $0 \leqslant k \leqslant n-1$. Мы заключаем, что уравнение $z^n = 1$ имеет ровно n корней

$$\zeta_k = \cos(2\pi k/n) + i\sin(2\pi k/n), \quad \text{где} \quad k = 0, 1, \ldots, (n-1), \tag{3-13}$$

расположенных в вершинах правильного n-угольника, вписанного в единичную окружность так, что его вершина ζ_0 находится в точке 1, см. рис. 3⋄2 и рис. 3⋄3 на стр. 54. Корни (3-13) образуют абелеву группу относительно операции умножения. Эта группа обозначается $\boldsymbol{\mu}_n$ и называется *группой корней n-й степени из единицы*. Корень $\zeta \in \boldsymbol{\mu}_n$ называются *первообразным корнем* степени n из единицы, если все остальные элементы группы $\boldsymbol{\mu}_n$ представляются в виде ζ^k с

$k \in \mathbb{N}$. Например, первообразным является корень $\zeta_1 = \cos(2\pi/n) + i\sin(2\pi/n)$, имеющий наименьший положительный аргумент. Но бывают и другие: на рис. 3⋄2 все четыре отличных от 1 корня пятой степени из единицы являются первообразными, тогда как в группе $\boldsymbol{\mu}_6$ на рис. 3⋄3 первообразными являются только ζ_1 и $\zeta_5 = \zeta_1^{-1} = \zeta_1^4$. Множество всех первообразных корней обозначается через $R_n \subset \boldsymbol{\mu}_n$.

Упражнение 3.17. Покажите, что $\zeta_1^k = \cos(2\pi k/n) + i\sin(2\pi k/n) \in R_n$ если и только если $\text{нод}(k, n) = 1$.

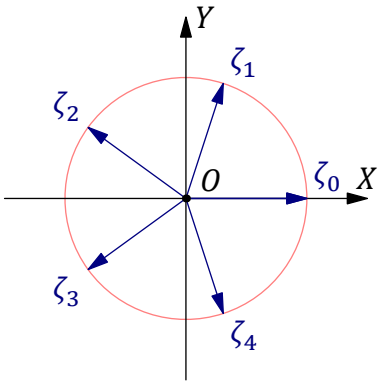


Рис. 3⋄2. Группа $\boldsymbol{\mu}_5$.

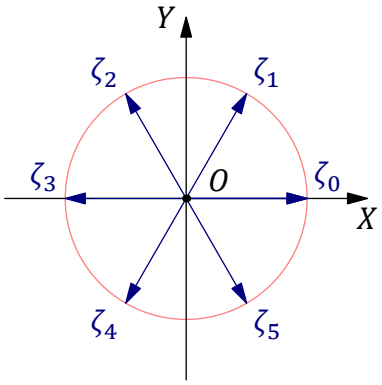


Рис. 3⋄3. Группа $\boldsymbol{\mu}_6$.

Приведённый многочлен $\Phi_n(z) = \prod_{\zeta \in R_n}(z - \zeta)$, корнями которого являются все первообразные корни n-й степени из единицы и только они, называется n-тым *круговым* или *циклотомическим* многочленом. Например, пятый и шестой круговые многочлены имеют вид

$$\Phi_5(z) = (z-\zeta_1)(z-\zeta_2)(z-\zeta_3)(z-\zeta_4) = z^4 + z^3 + z^2 + z + 1$$
$$\Phi_6(z) = (z-\zeta_1)(z-\zeta_4) = z^2 - z + 1\,.$$

Упражнение 3.18*. Попытайтесь доказать, что $\Phi_n \in \mathbb{Z}[x]$ и неприводим[1] в $\mathbb{Q}[x]$ при всех n.

Пример 3.9 (уравнение $z^n = a$)
Число $z = |z| \cdot (\cos\varphi + i\sin\varphi) \in \mathbb{C}$ является корнем уравнения $z^n = a$ если и только если $|z|^n = |a|$ и $n\varphi \in \operatorname{Arg}(a)$. При $a \neq 0$ имеется ровно n таких чисел. Они выражаются через $r = |a|$ и $\alpha \in \operatorname{Arg} a$ по формуле

$$z_k = \sqrt[n]{r} \cdot \left(\cos\frac{\alpha + 2\pi k}{n} + i\,\sin\frac{\alpha + 2\pi k}{n}\right), \quad 0 \leqslant k \leqslant n-1\,,$$

и располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{r}$ с центром в нуле так, что радиус вектор одной из его вершин образует с осью x угол α/n.

3.5. Конечные поля можно строить присоединяя к $\mathbb{F}_p = \mathbb{Z}/(p)$ корень какого-нибудь неприводимого многочлена $f \in \mathbb{F}_p[x]$. Если $\deg f = n$, то получающееся таким образом поле вычетов $\mathbb{F}_p[x]/(f)$ состоит из p^n элементов вида $a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$, где $a_i \in \mathbb{F}_p$ и $f(\vartheta) = 0$.

[1] Т. е. не являются произведениями многочленов строго меньшей степени.

Пример 3.10 (поле $\mathbb{F}_9$)
Многочлен $x^2+1 \in \mathbb{F}_3[x]$ неприводим, так как не имеет корней в $\mathbb{F}_3$. Присоединяя к $\mathbb{F}_3$ его корень, получаем поле $\mathbb{F}_9 \stackrel{\text{def}}{=} \mathbb{F}_3[x]/(x^2+1)$, состоящее из девяти элементов вида $a+bi$, где $a, b \in \mathbb{F}_3 = \{-1, 0, 1\}$ и $i^2 = -1$. Расширение $\mathbb{F}_3 \subset \mathbb{F}_9$ похоже на расширение $\mathbb{R} \subset \mathbb{C}$. Аналогом комплексного сопряжения в поле $\mathbb{F}_9$ является гомоморфизм Фробениуса[1] $F_3 : \mathbb{F}_9 \to \mathbb{F}_9, z \mapsto z^3$, тождественно действующий на простом подполе $\mathbb{F}_3 \subset \mathbb{F}_9$ и переводящий i в $-i$.

Упражнение 3.19. Составьте для поля $\mathbb{F}_9$ таблицы умножения и обратных элементов, перечислите в $\mathbb{F}_9$ все квадраты и кубы и убедитесь, что мультипликативная группа $\mathbb{F}_9^\times$ изоморфна $\boldsymbol{\mu}_8$.

Пример 3.11 (поле $\mathbb{F}_4$)
Многочлен $x^2+x+1 \in \mathbb{F}_2[x]$ неприводим, так как не имеет корней в $\mathbb{F}_2$. Присоединяя к $\mathbb{F}_2$ его корень, получаем поле $\mathbb{F}_4 \stackrel{\text{def}}{=} \mathbb{F}_2[x]/(x^2+x+1)$, состоящее из 0, 1, $\omega = [x]$ и $1+\omega = \omega^2 = \omega^{-1}$, причём[2] $\omega^2+\omega+1 = 0$. Расширение $\mathbb{F}_2 \subset \mathbb{F}_4$ тоже похоже на $\mathbb{R} \subset \mathbb{C}$, если понимать второе расширение как результат присоединения к $\mathbb{R}$ первообразного комплексного кубического корня ω из единицы, который также удовлетворяет уравнению $\omega^2+\omega+1=0$. В поле $\mathbb{F}_4$ аналогом комплексного сопряжения $\mathbb{C} \to \mathbb{C}$, переводящего $\omega \in \mathbb{C}$ в $\overline{\omega} = \omega^2$, также является гомоморфизм Фробениуса[3] $F_2 : \mathbb{F}_4 \to \mathbb{F}_4, z \mapsto z^2$, который тождественно действует на простом подполе $\mathbb{F}_2 \subset \mathbb{F}_4$ и переводит корни многочлена x^2+x+1 друг в друга.

Упражнение 3.20. Убедитесь, что мультипликативная группа $\mathbb{F}_4^\times$ изоморфна $\boldsymbol{\mu}_3$.

Теорема 3.3
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ существует конечное поле $\mathbb{F}_q$ из $q = p^n$ элементов.

Доказательство. Рассмотрим в $\mathbb{F}_p[x]$ многочлен $f(x) = x^q - x$. По теор. 3.2 существует такое поле $\mathbb{F} \supset \mathbb{F}_p$, что f полностью раскладывается в $\mathbb{F}[x]$ в произведение q линейных множителей. Так как $f'(x) = -1$, многочлен f сепарабелен[4], и все эти множители различны. Таким образом, в поле $\mathbb{F}$ имеется ровно q таких чисел α, что $\alpha^q = \alpha$. Обозначим множество этих чисел через $\mathbb{F}_q$ и покажем, что $\mathbb{F}_q \subset \mathbb{F}$ является подполем. Очевидно, что нуль и единица поля $\mathbb{F}$ лежат в $\mathbb{F}_q$ и если $\alpha \in \mathbb{F}_q$, то $-\alpha \in \mathbb{F}_q$ и $\alpha^{-1} \in \mathbb{F}_q$, так как $(-\alpha)^q = -\alpha^q = -\alpha$ и $\left(\alpha^{-1}\right)^q = \left(\alpha^q\right)^{-1} = \alpha^{-1}$. Если $\alpha, \beta \in \mathbb{F}_q$, то $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, т. е. $\alpha\beta \in \mathbb{F}_q$. Поскольку $\operatorname{char}\mathbb{F} = p$, в поле $\mathbb{F}$ выполняется равенство[5] $(\alpha+\beta)^p = \alpha^p + \beta^p$. Применяя его n раз, заключаем, что для всех $\alpha, \beta \in \mathbb{F}_q$ выполняется равенство $(\alpha+\beta)^q = (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$, т. е. $\alpha+\beta \in \mathbb{F}_q$. □

Упражнение 3.21. Покажите, что число элементов в любом конечном поле является степенью его характеристики.

[1] См. прим. 2.10 на стр. 35.
[2] Отметим, что $-1 = 1$ в $\mathbb{F}_2$, что позволяет обходиться без минусов.
[3] См. прим. 2.10 на стр. 35.
[4] См. n° 3.3.4 на стр. 50.
[5] См. прим. 2.10 на стр. 35.

3.5.1. Циклические группы и порядки элементов. Рассмотрим абелеву группу A, операцию в которой будем записывать мультипликативно. Если группа A конечна, то среди степеней любого элемента $b \in A$ встречаются одинаковые, скажем $b^n = b^k$ с $n > k$. Умножая обе части этого равенства на b^{-k}, заключаем, что $b^{n-k} = 1$. Таким образом, для каждого $b \in A$ существует такое $m \in \mathbb{N}$, что $b^m = 1$. Наименьшее из этих m называется *порядком* элемента b и обозначается $\operatorname{ord} b$. Если $\operatorname{ord} b = n$, то элементы $b^0 = 1$, $b^1 = b$, b^2, …, b^{n-1} попарно различны, и каждая целая степень b^k совпадает с одним из них: если $k = nq + r$, где r — остаток от деления k на n, то $b^k = (b^n)^q b^r = b^r$. В частности, $b^m = 0$ если и только если $m \vdots \operatorname{ord} b$.

Упражнение 3.22. Покажите, что порядок любого элемента из конечной абелевой группы A делит $|A|$.

Группа A называется *циклической*, если она исчерпывается целыми степенями какого-нибудь элемента $a \in A$, т. е. $A = \{a^n \mid n \in \mathbb{Z}\}$. Для конечной группы A это условие равносильно равенству $\operatorname{ord} a = |A|$, т. е. совпадению порядка элемента a с порядком группы. Каждый обладающий этим свойством элемент $a \in A$ называется *образующей* циклической группы A. Например, группа $\boldsymbol{\mu}_n \subset \mathbb{C}$ комплексных корней n-й степени из единицы[1] циклическая, и её образующими являются первообразные корни.

Упражнение 3.23. Пусть циклическая группа A порядка n порождается элементом a. Убедитесь, что элемент $b = a^k$ тоже является образующей если и только если $\operatorname{нод}(k, n) = 1$.

Предложение 3.8
Если порядки элементов мультипликативной абелевой группы A ограничены сверху, то максимальный из них делится на порядок любого элемента $a \in A$.

Доказательство. Достаточно для любых двух элементов $a_1, a_2 \in A$, имеющих порядки m_1, m_2, построить элемент $b \in A$, порядок которого равен $\operatorname{нок}(m_1, m_2)$. Если $\operatorname{нод}(m_1, m_2) = 1$, положим $b = a_1 a_2$. Тогда $b^{m_1 m_2} = a^{m_1} a^{m_2} = 1$. Если $b^k = 1$, то $a_1^k = a_2^{-k}$, откуда $1 = a_1^{m_1} = a_2^{-km_1}$, и значит, $km_1 \vdots m_2$. Так как m_1 и m_2 взаимно просты, $k \vdots m_2$. Меня ролями a_1 и a_2, заключаем, что $k \vdots m_1$, а значит, $k \vdots m_1 m_2$. Тем самым, $\operatorname{ord}(b) = m_1 m_2 = \operatorname{нок}(m_1, m_2)$.

Если $\operatorname{нод}(m_1, m_2) \neq 1$, то для каждого простого $p \in \mathbb{N}$ обозначим через $\nu_i(p)$ показатель, с которым p входит в разложение числа m_i на простые множители[2]. Тогда

$$\operatorname{нок}(m_1, m_2) = \prod\nolimits_p p^{\max(\nu_1(p), \nu_2(p))}.$$

Обозначим через ℓ_1 произведение $\prod p^{\nu_1(p)}$ по всем простым $p \in \mathbb{N}$ с $\nu_1(p) > \nu_2(p)$ и положим $\ell_2 = \operatorname{нок}(m_1, m_2)/\ell_1$. По построению $\operatorname{нод}(\ell_1, \ell_2) = 1$ и $m_1 = k_1 \ell_1$, $m_2 = k_2 \ell_2$ для некоторых $k_1, k_2 \in \mathbb{N}$. Элементы $b_1 = a_1^{k_1}$, $b_2 = a_2^{k_2}$ имеют взаимно простые порядки ℓ_1, ℓ_2, и по уже доказанному их произведение $b = b_1 b_2$ имеет порядок $\ell_1 \ell_2 = \operatorname{нок}(m_1, m_2)$. □

Следствие 3.3
Любая конечная подгруппа A в мультипликативной группе $\Bbbk^\times$ произвольного поля $\Bbbk$ является циклической.

[1] См. n° 3.4.3 на стр. 53.
[2] См. упр. 2.8 на стр. 29.

Доказательство. Обозначим через m максимальный из порядков элементов группы A. Согласно предл. 3.8, все элементы группы A являются корнями многочлена $x^m - 1 = 0$. Поэтому их не более m и все они исчерпываются степенями имеющегося в A элемента m-того порядка. □

Теорема 3.4
Всякое конечное поле изоморфно одному из полей $\mathbb{F}_q$, построенных в теор. 3.3 на стр. 55.

Доказательство. Пусть поле $\mathbb{F}$ имеет характеристику p и состоит из q элементов. По сл. 3.3 мультипликативная группа $\mathbb{F}^\times$ является циклической. Обозначим её образующую через $\zeta \in \mathbb{F}^\times$. Тогда $\mathbb{F} = \{0, 1, \zeta, \zeta^2, \dots, \zeta^{q-2}\}$ и $\zeta^{q-1} = 1$. Чтобы доказать теорему, построим ещё одно поле из q элементов, изоморфное как полю $\mathbb{F}$, так и подходящему полю из теор. 3.3. Для этого обозначим через $g \in \mathbb{F}_p[x]$ приведённый многочлен минимальной степени с корнем ζ.

Упражнение 3.24. Убедитесь, что такой многочлен g существует, неприводим в $\mathbb{F}_p[x]$ и делит все многочлены $f \in \mathbb{F}_p[x]$ с корнем ζ.

Из упражнения вытекает, что кольцо $\mathbb{F}_p[x]/(g)$ является полем, а правило $[h]_g \mapsto h(\zeta)$ корректно задаёт ненулевой гомоморфизм колец $\mathbb{F}_p[x]/(g) \to \mathbb{F}$. Он инъективен по предл. 2.3 на стр. 34 и сюръективен, так как все ζ^m содержатся в его образе. Тем самым, $\mathbb{F} \simeq \mathbb{F}_p[x]/(g)$. В частности, поле $\mathbb{F}$ состоит из $q = p^n$ элементов $a_{n-1}\zeta^{n-1} + \dots + a_1\zeta + a_0$, где $a_i \in \mathbb{F}_p$, $n = \deg g$.

Так как ζ является корнем многочлена $f(x) = x^q - x$, из упр. 3.24 вытекает, что $f = gu$ для некоторого $u \in \mathbb{F}_p[x]$. Подставляя в это равенство q элементов поля $\mathbb{F}_q$, построенного в теор. 3.3 и состоящего в точности из q корней многочлена f, мы заключаем, что хотя бы один из них — назовём его $\xi \in \mathbb{F}_q$ — является корнем многочлена g. Правило $[h]_g \mapsto h(\xi)$ корректно задаёт вложение полей $\mathbb{F}_p[x]/(g) \hookrightarrow \mathbb{F}_q$, сюръективное, поскольку оба поля состоят из q элементов. Тем самым, $\mathbb{F}_p[x]/(g) \simeq \mathbb{F}_q$. □

Следствие 3.4 (из доказательства теор. 3.4)
Для каждого $n \in \mathbb{N}$ и простого $p \in \mathbb{N}$ в $\mathbb{F}_p[x]$ имеется неприводимый многочлен степени n. □

Следствие 3.5
Каждое конечное поле $\mathbb{F}$ состоит из p^n элементов, где простое $p = \operatorname{char}\mathbb{F}$, и для каждого $n \in \mathbb{N}$ и простого p имеется единственное с точностью до изоморфизма поле из p^n элементов. □

Задачи для самостоятельного решения к §3

Задача 3.1. Найдите остатки от деления многочлена $x^{179} + x^{57} + x^2 + 1$ в кольце $\mathbb{Z}[x]$ на многочлены а) $x + 1$ б) $x^2 - 1$ в) $x^2 + 1$ г) $x^2 + x + 1$ д) $x^2 - x + 1$ е*) $x^2 + x - 1$.

Задача 3.2. Вычислите $\text{нод}(f_1, f_2)$ в кольце $\mathbb{Q}[x]$ и подберите такие $h_1, h_2 \in \mathbb{Q}[x]$, что $\text{нод}(f_1, f_2) = f_1h_1 + f_2h_2$ и $\deg h_1 < \deg f_2 - d$, $\deg h_2 < \deg f_1 - d$, где $d = \deg \text{нод}(f_1, f_2)$, для многочленов а) $f_1 = x^{30} - 1$, $f_2 = x^8 - 1$ б) $f_1 = x^5 - 1$, $f_2 = x^4 + x^2 + 1$.

Задача 3.3. Найдите в $\mathbb{Q}[x]$ все многочлены с остатками а) $1 + x$, $1 + x^2$ от деления на $1 + x^2$, $1 + x^4$ б) 1, 2, x от деления на $(x - 1)^2$, $(x + 1)^2$, $x^2 + 1$ соответственно.

Задача 3.4. Подберите $f \in \mathbb{Q}[x]$ с $\deg f = 2$ и $f(1) = 2$, $f(2) = 20$, $f(3) = 200$. Много ли таких f?

Задача 3.5. Пусть поле $\mathbb{F}$ бесконечно. Докажите, что любой ненулевой многочлен $f \in \mathbb{F}[x_1, \ldots, x_n]$ задаёт ненулевую функцию $\mathbb{F}^n \to \mathbb{F}$.

Задача 3.6. Пусть поле $\mathbb{F}$ конечно. Верно ли, что любая функция а) $\mathbb{F} \to \mathbb{F}$ б*) $\mathbb{F}^n \to \mathbb{F}$ является многочленом? Существует ли ненулевой многочлен $f \in \mathbb{F}[x_1, \ldots, x_n]$, задающий тождественно нулевую функцию $\mathbb{F}^n \to \mathbb{F}$?

Задача 3.7. Является ли кольцо вычетов а) $\mathbb{R}[x]/(x^4+1)$ б) $\mathbb{Q}[x]/(x^4+1)$ в) $\mathbb{Q}[x]/(x^3+x+1)$ полем? Найдите в этих кольцах $[1+x]^{-1}$ и $[1+x^2]^{-1}$ если они существуют.

Задача 3.8. Могут ли два разных приведённых неприводимых многочлена $f, g \in \mathbb{Q}[x]$ одинаковой степени $\deg f = \deg g \geqslant 2$ задавать изоморфные поля $\mathbb{Q}[x]/(f)$ и $\mathbb{Q}[x]/(g)$?

Задача 3.9. Есть ли среди полей $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ и $\mathbb{Q}[\sqrt[3]{2}]$ изоморфные между собой?

Задача 3.10 (минимальный многочлен). Пусть $\Bbbk \subset \mathbb{F}$ два поля. Элемент $\alpha \in \mathbb{F}$ называется *алгебраическим* над $\Bbbk$, если $f(\alpha) = 0$ для некоторого многочлена $f(a) \in \Bbbk[x]$, и приведённый многочлен наименьшей степени с таким свойством называется *минимальным многочленом* элемента α над полем $\Bbbk$. Докажите, что минимальный многочлен неприводим в $\Bbbk[x]$ и делит в $\Bbbk[x]$ все многочлены, для которых α является корнем.

Задача 3.11. Найдите минимальный многочлен числа а) $2-3i \in \mathbb{C}$ над $\mathbb{R}$ б) $\sqrt{2}+\sqrt{3} \in \mathbb{R}$ над $\mathbb{Q}$.

Задача 3.12 (формулы Виета). Выразите коэффициенты a_k приведённого многочлена

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

через его корни α_ν и подберите такое $c = c(a_1, \ldots, a_n)$, чтобы у многочлена $f(t-c)$ занулился коэффициент при t^{n-1}.

Задача 3.13. Найдите вещественную и мнимую часть, модуль, аргумент и по возможности точно нарисуйте комплексные числа

а) $\dfrac{(5+i)(7-6i)}{3+i}$ б) $\dfrac{(1+i)^5}{(1-i)^3}$ в) $\left(\dfrac{\sqrt{3}+i}{1-i}\right)^{30}$ г) $z = (1+i)^{50}$ д) все такие z, что $z^2 = -1+i\sqrt{3}$.

Задача 3.14. Вычислите $z^m + 1/z^m$, если $z + 1/z = 2\cos\theta$.

Задача 3.15. Найдите все $\lambda \in \mathbb{C}$, при которых многочлен $x^4 - 4x + \lambda$ имеет кратный корень.

Задача 3.16. Найдите все кратные комплексные корни многочлена

$$x^7 + 7x^5 - 36x^4 + 15x^3 - 216x^2 + 9x - 324.$$

Задача 3.17. Куда переводят отображения $z \mapsto z^2$ и $z \mapsto 1/z$

а) прямые $x = c$, $y = c$, $y = cx$, где $c \in \mathbb{R}$

б) окружности $|z-1| = 1$ и $|z-i| = 1$

в) кошку с рис. рис. 3◇4?

Задача 3.18. Покажите, что четыре различные неколлинеарные точки $z_1, \ldots, z_4 \in \mathbb{C}$ лежат на одной окружности если и только если их *двойное отношение* $\frac{(z_1-z_3)(z_2-z_4)}{(z_1-z_4)(z_2-z_3)} \in \mathbb{R}$.

Задача 3.19. Решите в поле $\mathbb{C}$ уравнения:

а) $z^3 = -i$ б) $\overline{z} = z^3$ в) $(z+1)^n - (z-1)^n = 0$

г) $(z+i)^n + (z-i)^n = 0$.

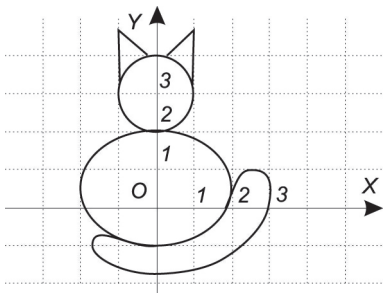


Рис. 3◇4. Комплексная кошка.

Задача 3.20. Вычислите суммы: а) $\binom{n}{0}+\binom{n}{4}+\binom{n}{8}+\ldots$ б) $\binom{n}{1}+\binom{n}{5}+\binom{n}{9}+\ldots$

Задача 3.21. Выразите $\sin 5\varphi$ через $\sin\varphi$ и получите для $\sin(4\pi/5)$ и $\cos(2\pi/5)$ явные выражения в радикалах от рациональных чисел.

Задача 3.22 (алгебраическая замкнутость поля $\mathbb{C}$). Для произвольного многочлена $f\in\mathbb{C}[x]$ положительной степени докажите, что:

а) для любого $c\in\mathbb{R}$ найдётся такой круг $D\subset\mathbb{C}$, что $|f(z)|>c$ для всех $z\notin D$

б) в любом круге $D\subset\mathbb{C}$ есть такая точка $z_0\in D$, что $|f(z)|\geqslant|f(z_0)|$ для всех $z\in D$

в) существует такое $z_0\in\mathbb{C}$, что $|f(z)|\geqslant|f(z_0)|$ для всех $z\in\mathbb{C}$

г) если $f(z_0)\neq 0$, то вблизи z_0 найдётся такое $z\in\mathbb{C}$, что $|f(z)|<|f(z_0)|$

д) f имеет корень в $\mathbb{C}$.

Задача 3.23. Покажите, что всякий многочлен $f\in\mathbb{R}[x]$ раскладывается в произведение линейных двучленов и квадратных трёхчленов с отрицательным дискриминантом. Разложите в $\mathbb{R}[x]$ на неприводимые множители многочлены x^4+4 и x^8+128.

Задача 3.24. Используя только сложение, вычитание, умножение, деление и извлечение квадратных корней из вещественных чисел явно выразите действительные и мнимые части комплексных корней уравнения $z^2=a$ через действительную и мнимую части числа a.

Задача 3.25. Для всех $n,s\in\mathbb{N}$ вычислите в поле $\mathbb{C}$ а) сумму б) произведение s-тых степеней всех корней n-той степени из 1.

Задача 3.26. Покажите, что $\sin mx/\sin x$ при нечётном $m\in\mathbb{N}$ является многочленом от $\sin^2 x$ и найдите степень, корни и старший коэффициент этого многочлена.

Задача 3.27 (эйлеровы разложения). При помощи предыдущей задачи докажите тождества

а) $\dfrac{\sin(mx)}{\sin x}=(-4)^{\frac{m-1}{2}}\prod\limits_{j=1}^{\frac{m-1}{2}}\left(\sin^2 x-\sin^2\left(\dfrac{2\pi j}{m}\right)\right)$ б) $(-1)^{\frac{m-1}{2}}\sin(mx)=2^{m-1}\prod\limits_{j=0}^{m-1}\sin\left(x+\dfrac{2\pi j}{m}\right)$

Задача 3.28 (квадратичная взаимность по Эйзенштейну). Зафиксируем простое $p\in\mathbb{N}$. Число

$$\left(\frac{n}{p}\right)\stackrel{\text{def}}{=}[n]_p^{(p-1)/2}=\begin{cases}1 & \text{если } [n] \text{ ненулевой квадрат в } \mathbb{F}_p\\ 0 & \text{если } [n]=[0] \text{ в } \mathbb{F}_p\\ -1 & \text{если } [n] \text{ не квадрат в } \mathbb{F}_p\end{cases}$$

называется *символом Лежандра* числа n по модулю p. а) Докажите, что $\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$. б) Вычислите $\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)$. в*) Сравните знак $\left(\frac{m}{p}\right)$ со знаком произведения

$$\prod_{j=1}^{\frac{p-1}{2}}\frac{\sin(2\pi mj/p)}{\sin(2\pi j/p)},$$

разложите в нём каждое отношение синусов по формулам из зад. 3.27 и докажите для простых натуральных $p,q>2$ *квадратичный закон взаимности*:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

г) Найдите $\left(\frac{43}{179}\right)$.

Задача 3.29. Найдите все обратимые элементы в кольцах
а) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a+bi \in \mathbb{C} \mid a,b \in \mathbb{Z},\ i^2=-1\}$
б) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a+b\omega \in \mathbb{C} \mid a,b \in \mathbb{Z},\ \omega^2+\omega+1=0\ \}$.

Задача 3.30. Выпишите все неприводимые многочлены степени $\leqslant 5$ над полем $\mathbb{F}_2$ и все неприводимые приведённые многочлены степени $\leqslant 4$ над полем $\mathbb{F}_3$.

Задача 3.31. В $\mathbb{F}_2[x]$ разложите на неприводимые множители или докажите неприводимость многочленов а) $x^6+x^5+x^4+x^3+1$ б) x^7+x^3+1.

Задача 3.32. У скольких многочленов степени $\leqslant n$ из кольца $\mathbb{F}_2[x]$ нет корней в $\mathbb{F}_2$?

Задача 3.33. Какие из колец а) $\mathbb{F}_5[x]/(x^3+x^2+x+1)$ б) $\mathbb{F}_5[x]/(x^3+x+1)$ в) $\mathbb{F}_5[x]/(x^3+x^2+1)$ являются полями? Найдите в этих кольцах $[1+x]^{-1}$ и $[1+x^2]^{-1}$ если они существуют.

Задача 3.34. Предъявите примеры полей из а) 4 б) 8 в) 9 г) 16 элементов. Укажите в них все квадраты, все кубы и все образующие мультипликативной группы.

Задача 3.35. Изоморфны ли поля $\mathbb{F}_2[x]/(x^3+x+1)$ и $\mathbb{F}_2[x]/(x^3+x^2+1)$? Если да, предъявите изоморфизм явно. Тот же вопрос про поля из зад. 3.33.

Задача 3.36. Используя подходящую модификацию обращения Мёбиуса[1], докажите, что число неприводимых многочленов степени n в $\mathbb{F}_p[x]$ равно $\frac{1}{n}\sum_{d|n} p^d \mu(n/d)$.

Задача 3.37. Обозначим через ι_m число неприводимых приведённых многочленов степени m в $\mathbb{F}_p[x]$. Докажите в $\mathbb{Q}[\![t]\!]$ равенство $(1-pt)^{-1} = \prod_{m\in\mathbb{N}} \left(1-t^m\right)^{-\iota_m}$.

Задача 3.38. Пусть $\mathbb{F}_q$ — конечное поле из $q=p^n$ элементов и $\mathbb{F}_p \subset \mathbb{F}_q$ — его простое подполе. Покажите, что:
а) все элементы поля $\mathbb{F}_q$ алгебраичны[2] над $\mathbb{F}_p$
б) порядок любого элемента в мультипликативной группе $\mathbb{F}_q^\times$ делит $q-1$.
в) Пользуясь обращением Мёбиуса найдите число элементов d-го порядка в $\mathbb{F}^\times$.
г) Сколько в $\mathbb{F}^\times$ элементов $(q-1)$-го порядка[3] и какова степень минимального многочлена каждого такого элемента?

Задача 3.39. Обобщите результаты прим. 2.8 на стр. 33 на произвольное конечное поле $\mathbb{F}_q$: докажите, что ровно половина элементов мультипликативной группы $\mathbb{F}_q^\times$ является квадратами, и что $a \in \mathbb{F}_q^\times$ квадрат если и только если $a^{\frac{q-1}{2}} = 1$.

Задача 3.40. Пусть $\Bbbk$ — поле характеристики p и $a \in \Bbbk$. Покажите, что $f(x) = x^p - a$ либо неприводим в $\Bbbk[x]$, либо имеет p-кратный корень в $\Bbbk$.

Задача 3.41. Пусть многочлен $f(x)=x^p-x-a \in \mathbb{F}_p[x]$ имеет в некотором поле $\mathbb{K} \supset \mathbb{F}_p$ корень ζ. Явно укажите в $\mathbb{K}$ ещё $p-1$ корней многочлена f и покажите, что над $\mathbb{F}_p$ многочлен f либо неприводим, либо полностью разлагается на линейные множители.

Задача 3.42. Напишите приведённый[4] многочлен $x^m+a_1x^{m-1}+\ldots+a_m$ минимальной возможной степени с коэффициентами $a_i \in \mathbb{Z}/(n)$, имеющий ровно n различных корней в кольце $\mathbb{Z}/(n)$ для а) $n=101$ б) $n=111$ в) $n=121$

[1] См. зад. 2.27 на стр. 40.
[2] Т. е. являются корнями некоторых многочленов из $\mathbb{F}_p[x]$, см. зад. 3.10 на стр. 58.
[3] Обратите внимание, что таким образом получается новое доказательство того, что мультипликативная группа конечного поля циклическая.
[4] Т. е. со старшим коэффициентом 1.

Задача 3.43 (круговые многочлены). Напомню[1], что n-тый *круговой* многочлен Φ_n — это приведённый многочлен, корнями которого являются комплексные первообразные корни n-той степени из 1 и только они. Покажите, что

а) $\Phi_{2n}(x) = \Phi_n(-x)$ при нечётном n

б) $x^n - 1 = \prod_{d|n} \Phi_d(x)$

в) $\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$

г) $\Phi_p(x) = x^{p-1} + \ldots + x + 1$, а $\Phi_{p^k}(x) = \Phi_p\left(x^{p^{k-1}}\right)$ при простом p и всех $k \in \mathbb{N}$

д) $\Phi_{pm}(x) = \Phi_m\left(x^p\right) / \Phi_m(x)$ при простом $p \nmid m$

е) $\Phi_{p_1^{k_1} \ldots p_n^{k_n}}(x) = \Phi_{p_1 \ldots p_n}\left(x^{p_1^{k_1-1} \ldots p_n^{k_n-1}}\right)$ для попарно разных простых p_i

ж) $\Phi_n(x) \in \mathbb{Z}[x]$ при всех n.

[1] См. n° 3.4.3 на стр. 53.

§4. Дроби и ряды

В этом параграфе мы продолжаем обозначать через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

4.1. Кольца частных. Способ изготовления поля $\mathbb{Q}$ из кольца $\mathbb{Z}$ как множества дробей с целым числителем и ненулевым целым знаменателем[1] применим в любом коммутативном кольце K с единицей. Подмножество $S \subset K$ называется *мультипликативным*, если $1 \in S$ и $st \in S$ для всех $s, t \in S$. Например, множество всех целых неотрицательных степеней q^k любого элемента $q \in K$ мультипликативно[2]. Множество $K^\circ \subset K$, состоящее из всех не делящих нуль ненулевых элементов, тоже мультипликативно. В частности, множество всех ненулевых элементов любого целостного кольца мультипликативно. Каждое мультипликативное подмножество $S \subset K$ задаёт на множестве упорядоченных пар $K \times S$ отношение эквивалентности $\sim_S$, порождённое[3] отождествлениями $(a, s) \sim_S (at, st)$ для всех $t \in S$. Класс эквивалентности пары (a, s) по модулю этого отношения называется *дробью* со знаменателем в S и обозначается a/s. Множество всех таких дробей обозначается KS^{-1} или $K[S^{-1}]$ и называется *кольцом частных* или *локализацией* кольца K со знаменателями в S.

Пример 4.1
Пусть $K = \mathbb{Z}/(6)$ и $S = \{[1], [2], [-2]\}$. Каждая дробь в KS^{-1} имеет представление со знаменателем $[1]$:

$$[a]/[\pm 2] = [a][\mp 2]/[\pm 2][\mp 2] = [\mp a][2]/[1][2] = [\mp a]/[1]\,.$$

В частности, $[0]/[\pm 2] = [0]/[1]$. Далее,

$$[\pm 2]/[1] = [\pm 2][2]/[1][2] = [\mp 1][2]/[1][2] = [\mp 1]/[1]\,.$$

Наконец, $[3]/[1] = [3][2]/[1][2] = [0]/[2] = [0]/[1]$. Тем самым, KS^{-1} исчерпывается тремя дробями: $[0]/[1]$, $[1]/[1]$ и $[-1]/[1]$.

Упражнение 4.1. Убедитесь, что эти три дроби различны.

Лемма 4.1
$a/s = b/t$ в KS^{-1} если и только если $atu = bsu$ в K для некоторого $u \in S$.

Доказательство. Положим $(a, s) \approx (b, t)$, если $atu = bsu$ для некоторого $u \in S$. Двухшаговая цепочка отождествлений $(a, s) \sim_S (atu, stu) = (bsu, tsu) \sim_S (b, t)$ показывает, что отношение $\approx$ содержится в отношении $\sim_S$. Остаётся проверить, что отношение $\approx$ является отношением эквивалентности — тогда оно совпадёт с $\sim_S$ в силу минимальности последнего. Рефлексивность и симметричность очевидны. Докажем транзитивность. Пусть $(a, s) \approx (b, t)$ и $(b, t) \approx (c, r)$, т. е. существуют такие $u, w \in S$, что $atu = bsu$ и $brw = ctw$. Тогда

$$ar(tuw) = (atu)rw = (bsu)rw = (brw)su = (ctw)su = cs(tuw)\,,$$

т. е. $(a, s) \approx (c, r)$. □

[1] См. прим. 1.5 на стр. 13 и прим. 2.2 на стр. 24.
[2] Мы по определению полагаем $q^0 = 1$.
[3] Т. е. наименьшее по включению отношение эквивалентности $R \subset (K \times S) \times (K \times S)$, содержащее все пары вида $\big((a, s), (at, st)\big)$, где $t \in S$, см. n° 1.4.1 на стр. 13.

Лемма 4.2
Операции $\frac{a}{r} + \frac{b}{s} \stackrel{\text{def}}{=} \frac{as+br}{rs}$ и $\frac{a}{r} \cdot \frac{b}{s} \stackrel{\text{def}}{=} \frac{ab}{rs}$ корректно задают на KS^{-1} структуру коммутативного кольца с единицей $1/1$ и нулём $0/1$.

Доказательство. Так каждое отождествление $\sim_S$ является цепочкой элементарных отождествлений $(a, r) \sim_S (au, ru)$, где $u \in S$, достаточно проверить, что результаты операций не меняются при замене $\frac{a}{r}$ на $\frac{au}{ru}$, а $\frac{b}{s}$ — на $\frac{bw}{sw}$, где $u, w \in S$, что очевидно:

$$\frac{au}{ru} + \frac{bw}{sw} = \frac{ausw + bwru}{rusw} = \frac{(as + br) \cdot wu}{rs \cdot wu} = \frac{as + br}{rs}$$
$$\frac{au}{ru} \cdot \frac{bw}{sw} = \frac{aubw}{rusw} = \frac{(ab) \cdot wu}{rs \cdot wu} = \frac{ab}{rs}.$$

Проверку выполнения в KS^{-1} всех аксиом коммутативного кольца с единицей мы оставляем читателю в качестве упражнения. □

Следствие 4.1
Кольцо KS^{-1} нулевое если и только если S содержит нуль.

Доказательство. Если $0 \in S$, то любая дробь $a/s = (a \cdot 0)/(s \cdot 0) = 0/0 = (0 \cdot 1)/(1 \cdot 0) = 0/1$ эквивалентна нулю. С другой стороны, $1/1 = 0/1$ только если существует такой $s \in S$, что $1 \cdot 1 \cdot s = 0 \cdot 1 \cdot s = 0$, откуда $s = 0 \in S$. □

Теорема 4.1
Отображение $\iota_S \colon K \to KS^{-1}$, переводящее $a \in K$ в дробь $a/1$, является гомоморфизмом колец с ядром $\ker \iota_S = \{a \in K \mid \exists s \in S \colon as = 0\}$. Образ $\iota_S(s)$ любого элемента $s \in S$ обратим в KS^{-1}. Для любого гомоморфизма $\varphi \colon K \to R$ в целостное кольцо R, переводящего каждый элемент из S в обратимый элемент из R, существует единственный такой гомоморфизм колец $\varphi_S \colon KS^{-1} \to R$, что $\varphi = \varphi_S \circ \iota_S$.

Доказательство. Очевидно, что ι_S является гомоморфизмом. Дробь $\iota_S(a) = a/1$ равна $0/1$ если и только если найдётся такой $s \in S$, что $a \cdot 1 \cdot s = 0 \cdot 1 \cdot s = 0$. Обратным к $\iota_S(s) = s/1$ элементом является дробь $1/s$. Остаётся доказать последнее утверждение. Для продолжения гомоморфизма $\varphi \colon K \to R$ до гомоморфизма $\varphi_S \colon KS^{-1} \to R$ нет иного выбора как положить $\varphi_S(1/s) = 1/\varphi(s)$, так как в кольце R должны выполняться равенства $\varphi_S(1/s) \cdot \varphi_S(s) = \varphi_S\big(s \cdot (1/s)\big) = \varphi(1) = 1$. Следовательно, искомое продолжение обязано задаваться формулой $\varphi_S(a/s) \stackrel{\text{def}}{=} \varphi(a)/\varphi(s)$. Она корректна, поскольку при замене $\frac{a}{s}$ на $\frac{au}{su}$ с $u \in S$ имеем $\varphi_S\left(\frac{au}{su}\right) = \frac{\varphi(au)}{\varphi(su)} = \frac{\varphi(a)\varphi(u)}{\varphi(s)\varphi(u)} = \frac{\varphi(a)}{\varphi(s)}$. Бесхитростную проверку того, что построенное отображение φ_S перестановочно со сложением и умножением, мы оставляем читателю. □

Упражнение 4.2. Пусть $K = \mathbb{Z}/(30)$, а $S = \{[2^k]_{30} \mid k = 0, \dots, 4\}$. Покажите, что $KS^{-1} \simeq \mathbb{Z}/(15)$.

Пример 4.2 (поле частных целостного кольца)
Если кольцо K не имеет делителей нуля, его ненулевые элементы образуют мультипликативную систему. Кольцо частных со знаменателями в этой системе является полем. Оно называется *полем частных* целостного кольца K и обозначается Q_K. Равенство $a/b = c/d$ в Q_K равносильно равенству $ac = bd$ в K, а гомоморфизм $\iota \colon K \hookrightarrow Q_K$, $a \mapsto a/1$, инъективен, и любой гомоморфизм $\varphi \colon K \to R$ в целостное кольцо R, переводящий все ненулевые элементы из K в обратимые элементы кольца R, единственным способом продолжается до вложения поля частных $\widetilde{\varphi} \colon Q_K \hookrightarrow R$.

Пример 4.3 (поле $\mathbb{Q}$)
Полем частных целостного кольца $\mathbb{Z}$ является поле рациональных чисел $\mathbb{Q} = Q_{\mathbb{Z}}$, которое канонически вкладывается в любое поле характеристики нуль в качестве простого подполя[1].

Пример 4.4 (поле рядов Лорана)
Поле частных кольца формальных степенных рядов $\Bbbk[\![x]\!]$ с коэффициентами в произвольном поле $\Bbbk$ обозначается $\Bbbk(\!(x)\!) \stackrel{\text{def}}{=} Q_{\Bbbk[\![x]\!]}$. Так как любой ряд с ненулевым свободным членом обратим[2] в $\Bbbk[\![x]\!]$, каждая дробь $p(x)/q(x) \in \Bbbk(\!(x)\!)$ однозначно представляется в виде $x^m h(x)$, где $h \in \Bbbk[\![x]\!]$ имеет ненулевой свободный член, а показатель $m \in \mathbb{Z}$ равен разности показателей младших членов рядов p и q. Иначе говоря, поле $\Bbbk(\!(x)\!)$ состоит из формальных степенных рядов вида $f(x) = \sum_{k \geqslant m(f)} a_k x^k$, в которых допускается конечное число мономов отрицательной степени. Такие ряды называются *рядами Лорана*, а поле $\Bbbk(\!(x)\!)$ — *полем рядов Лорана*. Номер $m(f) \in \mathbb{Z}$ самого левого ненулевого коэффициента ряда Лорана f называется *порядком* ряда f.

4.2. Рациональные функции. Поле частных кольца $\Bbbk[x]$ обозначается через $\Bbbk(x)$ и называется *полем рациональных функций* от x. Его элементами являются дроби вида $p(x)/q(x)$ с $p, q \in \Bbbk[x]$.

Предложение 4.1
Если $g = g_1 \dots g_m$, где $\text{нод}(g_i, g_j) = 1$ при $i \neq j$, то при любом f дробь f/g единственным образом представляется в виде суммы

$$\frac{f}{g} = h + \frac{f_1}{g_1} + \dots + \frac{f_m}{g_m}, \tag{4-1}$$

где $h \in \Bbbk[x]$ и $\deg f_i < \deg g_i$ при всех i.

Доказательство. Деля f на g с остатком[3], заключаем, что $f/g = h + r/g$, где h — неполное частное, а остаток r имеет степень $\deg r < \deg g$. Если $g = g_1 g_2$ и $\text{нод}(g_1, g_2) = 1$, то $[g_2]_{g_1}$ обратим в $\Bbbk[x]/(g_1)$. Представим $[r]_{g_1}/[g_2]_{g_1} = [f_1]_{g_1}$ многочленом f_1 степени $\deg f_1 < \deg g_1$. Тогда $r = f_1 \cdot g_2 + f_2 \cdot g_1$ для некоторого $f_2 \in \Bbbk[x]$. Сравнивая степени, заключаем, что $\deg f_2 < \deg g_2$. Таким образом, $r/g = f_1/g_1 + f_2/g_2$ и к каждой из этих дробей применимо то же рассуждение, если её знаменатель является произведением взаимно простых многочленов. Это доказывает существование разложения (4-1). Для доказательства его единственности, умножим обе части разложения (4-1) на g. Получим равенство вида $f = hg + f_1 G_1 + \dots + f_m G_m$, где через $G_i = g/g_i$ обозначено произведение всех многочленов g_ν кроме i-го. Так как $\deg(f_1 G_1 + \dots + f_m G_m) < \deg g$, многочлен h является неполным частным, а $r = f_1 G_1 + \dots + f_m G_m$ — остатком от деления f на g. Каждый f_i является тем единственным многочленом степени $< \deg g_i$, класс которого в $\Bbbk[x]/(g_i)$ равен $[f]_{g_i}/[G_i]_{g_i}$. Таким образом, все ингредиенты формулы (4-1) однозначно определяются многочленами f и $g_1, \dots, g_n$. □

Предложение 4.2
Любую дробь вида f/g^m, в которой $\deg f < \deg g^m = m \deg g$, можно единственным образом представить в виде суммы

$$\frac{f}{g^m} = \frac{f_1}{g} + \frac{f_2}{g^2} + \dots + \frac{f_m}{g^m}, \tag{4-2}$$

где $\deg f_i < \deg g$ при всех i.

[1] См. n° 2.5.6 на стр. 35.
[2] См. прим. 3.2 на стр. 42.
[3] См. n° 3.2 на стр. 44.

Доказательство. Представление (4-2) равносильно записи f в виде

$$f = f_1 g^{m-1} + f_2 g^{m-2} + \ldots + f_{m-1} g + f_m\,, \tag{4-3}$$

аналогичном записи целого числа f в g-ичной позиционной системе исчисления: f_m является остатком от деления f на g, f_{m-1} — остатком от деления частного $(f - f_m)/g$ на g, f_{m-2} — остатком от деления частного $\left(\frac{f-f_m}{g} - f_{m-1}\right)/g$ на g и т. д. □

4.2.1. Разложение на простейшие дроби. Из предыдущих двух предложений вытекает, что каждая дробь $f/g \in \Bbbk(x)$ допускает *единственное* представление в виде суммы неполного частного от деления f на g и дробей вида p/q^m, где q пробегает неприводимые делители знаменателя g, показатель m меняется от 1 до кратности вхождения q в разложение g на неприводимые множители, и в каждой из таких дробей $\deg p < \deg q$. Такое представление называется *разложением f/g на простейшие дроби* и бывает полезно в практических вычислениях с рациональными функциями.

Пример 4.5
Вычислим 2022-ю производную, а также первообразную[1] от $1/(1+x^2)$. Разложим эту дробь в поле $\mathbb{C}(x)$ на простейшие:

$$\frac{1}{1+x^2} = \frac{\alpha}{1+ix} + \frac{\beta}{1-ix}\,, \quad \text{где} \quad \alpha, \beta \in \mathbb{C}\,.$$

Подставляя $x = \pm i$ в равенство $1 = \alpha(1-ix) + \beta(1+ix)$, находим $\alpha = \beta = 1/2$, т. е.

$$\frac{1}{1+x^2} = \frac{1}{2}\left(\frac{1}{1+ix} + \frac{1}{1-ix}\right).$$

Теперь дифференцируем каждое слагаемое:

$$\left(\frac{d}{dx}\right)^{2022} \frac{1}{1+x^2} = \frac{2022!}{2}\left(\frac{(-i)^{2022}}{(1+ix)^{2023}} + \frac{i^{2022}}{(1-ix)^{2023}}\right) =$$
$$= -2022! \cdot \frac{1}{2}\frac{(1-ix)^{2023} + (1+ix)^{2023}}{(1+x^2)^{2023}} = 2022! \cdot \sum_{\nu=0}^{1011} \binom{2023}{2\nu} \cdot \frac{(-1)^{\nu+1} x^{2\nu}}{(1+x^2)^{2023}}\,,$$

и интегрируем каждое слагаемое:

$$\int \frac{dx}{1+x^2} = \frac{1}{2}\int \frac{dx}{1+ix} + \frac{1}{2}\int \frac{dx}{1-ix} = \frac{\ln(1+ix) - \ln(1-ix)}{2i} = \frac{1}{2i}\ln\frac{1+ix}{1-ix} = \operatorname{arctg} x\,.$$

Подчеркнём, что все проделанные вычисления корректно определены в кольце $\mathbb{C}[\![x]\!]$, а все написанные равенства суть равенства между элементами этого кольца[2].

[1] Т. е. такой ряд f без свободного члена, что $f'(x) = 1/(1+x^2)$. Подробнее см. в n° 4.3 на стр. 68.

[2] В частности, последнее равенство вытекает из определения тангенса:

$$\operatorname{tg} t \stackrel{\text{def}}{=} \frac{\sin t}{\cos t} = \frac{1}{i}\cdot\frac{e^{it} - e^{-it}}{e^{it} + e^{-it}} = \frac{1}{i}\cdot\frac{e^{2it} - 1}{e^{2it} + 1} \in \mathbb{C}[\![t]\!]\,.$$

Полагая $\operatorname{tg} t = x$, получаем $e^{2it} = \frac{1+ix}{1-ix}$. Про экспоненту и логарифм мы ещё подробно поговорим в n° 4.3 на стр. 68 ниже.

4.2.2. Разложение рациональной функции в степенной ряд. По теор. 4.1 на стр. 63 существует единственное вложение $\Bbbk(x) \hookrightarrow \Bbbk((x))$, переводящее каждый многочлен в себя. Иначе говоря, каждую рациональную функцию можно разложить в ряд Лорана. Если основное поле $\Bbbk$ алгебраически замкнуто[1], такое разложение описывается довольно явными формулами. Пусть $\deg f < \deg g$ и знаменатель дроби f/g имеет вид:

$$g(x) = 1 + a_1 x + a_2 x^2 + \ldots + a_n x^n = \prod (1 - \alpha_i x)^{m_i}, \tag{4-4}$$

где все числа $\alpha_i \in \Bbbk$ попарно различны.

Упражнение 4.3. Убедитесь, что при $a_n \neq 0$ числа α_i из разложения (4-4) суть корни многочлена $t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n = \prod (t - \alpha_i)^{m_i}$.

По предл. 4.1 и предл. 4.2 функция f/g является суммой простейших дробей

$$\frac{\beta_{ij}}{(1 - \alpha_i x)^{k_{ij}}}, \tag{4-5}$$

где при каждом i показатели k_{ij} лежат в пределах $1 \leqslant k_{ij} \leqslant m_i$, а $\beta_{ij} \in \Bbbk$.

Если все кратности $m_i = 1$, то разложение на простейшие дроби имеет вид

$$\frac{f(x)}{(1 - \alpha_1 x) \ldots (1 - \alpha_n x)} = \frac{\beta_1}{1 - \alpha_1 x} + \ldots + \frac{\beta_n}{1 - \alpha_n x}.$$

Чтобы найти β_i, умножим обе части на общий знаменатель и подставим $x = \alpha_i^{-1}$. Получим

$$\beta_i = \frac{f\left(\alpha_i^{-1}\right)}{\prod_{\nu \neq i} \left(1 - (\alpha_\nu / \alpha_i)\right)} = \frac{\alpha_i^{n-1} f\left(\alpha_i^{-1}\right)}{\prod_{\nu \neq i} \left(\alpha_i - \alpha_\nu\right)}. \tag{4-6}$$

Мы заключаем, что когда все $m_i = 1$, дробь f/g является суммой $n = \deg g$ геометрических прогрессий:

$$\frac{f(x)}{g(x)} = \sum \left(\beta_1 \alpha_1^k + \beta_2 \alpha_2^k + \ldots + \beta_n \alpha_n^k\right) \cdot x^k, \tag{4-7}$$

где β_i находятся по формулам (4-6).

Простейшая дробь (4-5) с показателем $k_{ij} = m > 1$ раскладывается в ряд при помощи формулы Ньютона для бинома с отрицательным показателем

$$\frac{1}{(1 - x)^m} = \sum_{k \geqslant 0} \frac{(k + m - 1)(k + m - 2) \cdots (k + 1)}{(m - 1)!} \cdot x^k = \sum_{k \geqslant 0} \binom{k + m - 1}{m - 1} \cdot x^k, \tag{4-8}$$

которая получается $(m-1)$-кратным дифференцированием обеих частей разложения геометрической прогрессии $(1 - x)^{-1} = 1 + x + x^2 + x^3 + \ldots$.

Упражнение 4.4. Убедитесь, что $\left(\frac{d}{dx}\right)^n (1 - x)^{-1} = n! / (1 - x)^{n+1}$.

Таким образом, разложение простейшей дроби (4-5) имеет вид

$$\frac{\beta}{(1 - \alpha_i x)^m} = \beta \sum_{k \geqslant 0} \alpha_i^k \binom{k + m - 1}{m - 1} \cdot x^k. \tag{4-9}$$

[1] Т. е. каждый многочлен из $\Bbbk[x]$ полностью раскладывается в $\Bbbk[x]$ на линейные множители.

4.2.3. Решение линейных рекуррентных уравнений. Предыдущие вычисления можно использовать для отыскания «формулы k-того члена» последовательности z_k, заданной *линейным рекуррентным уравнением n-того порядка*:

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0\,, \tag{4-10}$$

где коэффициенты $a_1, \ldots, a_n \in \mathbb{C}$ — заданные числа. При $k \geqslant n$ уравнению (4-10) удовлетворяют коэффициенты z_k любого степенного ряда вида

$$z_0 + z_1 x + z_2 x^2 + \ldots = \frac{b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}}{1 + a_1 x + a_2 x^2 + \ldots + a_n x^k}\,.$$

Если в числителе правой части подобрать коэффициенты $b_0, b_1, \ldots, b_{n-1} \in \mathbb{C}$ так, чтобы первые n коэффициентов $z_0, \ldots, z_{n-1}$ разложения полученной дроби в степенной ряд совпали с первыми n членами последовательности (4-10), то формулы (4-6) и (4-9) дадут явные выражения элементов последовательности z_k через k.

Пример 4.6 (числа Фибоначчи)
Найдём явное выражение через k для элементов последовательности z_k, в которой

$$z_0 = 0\,,\ z_1 = 1 \text{ и } z_k = z_{k-1} + z_{k-2} \text{ при } k \geqslant 2\,.$$

Рекуррентное уравнение $z_k - z_{k-1} - z_{k-2} = 0$ описывает коэффициенты ряда

$$x + z_2 x^2 + z_3 x^3 + \ldots = \frac{b_0 + b_1 x}{1 - x - x^2}\,,$$

у которого $z_0 = 0$ и $z_1 = 1$. Умножая обе части на знаменатель и сравнивая коэффициенты при x^0 и x^1, заключаем, что $b_0 = 0$, а $b_1 = 1$. Таким образом,

$$z(x) = \frac{x}{1 - x - x^2} = \frac{\beta_+}{1 - \alpha_+ x} + \frac{\beta_-}{1 - \alpha_- x}\,,$$

где $\alpha_\pm = (1 \pm \sqrt{5})/2$ суть корни многочлена $t^2 - t - 1$, а $\beta_+ = -\beta_- = 1/(\alpha_+ - \alpha_-) = 1/\sqrt{5}$ по формуле (4-6). Разложение $z(x)$ в ряд имеет вид

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1 - \alpha_+ x} - \frac{1}{1 - \alpha_- x}\right) = \sum_{k \geqslant 0} \frac{\alpha_+^k - \alpha_-^k}{\sqrt{5}} \cdot x^k\,,$$

т. е.

$$z_k = \frac{(1 + \sqrt{5})^k - (1 - \sqrt{5})^k}{2^k \sqrt{5}}\,.$$

Предложение 4.3
Если последовательность чисел $z_k \in \mathbb{C}$ удовлетворяет при $k \geqslant n$ рекуррентному уравнению

$$z_k + a_1 z_{k-1} + a_2 z_{k-2} + \ldots + a_n z_{k-n} = 0 \tag{4-11}$$

с постоянными коэффициентами $a_i \in \mathbb{C}$, то $z_k = \alpha_1^k \varphi_1(k) + \ldots + \alpha_r^k \varphi_r(k)$, где $\alpha_1, \ldots, \alpha_r$ — это все различные корни многочлена[1]

$$t^n + a_1 t^{n-1} + \ldots + a_n\,, \tag{4-12}$$

а $\varphi_i(x) \in \mathbb{C}[x]$ и $\deg \varphi_i$ строго меньше кратности соответствующего корня α_i.

[1] Он называется *характеристическим многочленом* рекуррентного уравнения (4-10).

Доказательство. Ряд $\sum z_k x^k \in \mathbb{C}[\![x]\!]$, коэффициенты которого решают уравнение (4-11), является суммой дробей вида $\beta(1-\alpha x)^{-m}$, где α пробегает различные корни многочлена (4-12), показатель m лежит в пределах от 1 до кратности соответствующего корня α, и для каждой пары α, m комплексное число $\beta = \beta(\alpha, m)$ однозначно вычисляется по α, m и первым n коэффициентам последовательности z_k. Согласно формуле (4-9) коэффициент при x^k у разложения дроби $(1-\alpha x)^{-m}$ в степенной ряд имеет вид $\alpha^k \varphi(k)$, где $\varphi(k) = \binom{k+m-1}{m-1}$ является многочленом степени $m-1$ от k. □

4.3. Логарифм и экспонента. Всюду в этом разделе мы рассматриваем ряды с коэффициентами в поле $\Bbbk$ характеристики $\operatorname{char}\Bbbk = 0$. В этом случае для любого ряда $f(x) = a_0 + a_1 x + a_2 x^2 + \dots$ существует единственный ряд без свободного члена, производная от которого равна $f(x)$. Он называется *первообразной* или *интегралом* от f и обозначается

$$\int f(x)\,dx \stackrel{\text{def}}{=} a_0 x + \frac{a_1}{2}x^2 + \frac{a_2}{3}x^3 + \dots = \sum_{k\geqslant 1} \frac{a_{k-1}}{k}\,x^k\,. \tag{4-13}$$

Первообразный ряд от знакопеременной геометрической прогрессии называется *логарифмом* и обозначается

$$\ln(1+x) \stackrel{\text{def}}{=} \int \frac{dx}{1+x} = \int \left(1 - x + x^2 - x^3 + \dots\right) dx = \\ = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \dots = \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{k} x^k\,. \tag{4-14}$$

Единственный ряд со свободным членом 1, совпадающий со своей производной, называется *экспонентой* и обозначается

$$e^x \stackrel{\text{def}}{=} \sum_{k\geqslant 0} x^k/k! = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \dots\,. \tag{4-15}$$

4.3.1. Логарифмирование и экспоненцирование. Обозначим через $N = (x) \subset \Bbbk[\![x]\!]$ аддитивную абелеву группу всех рядов без свободного члена, а через $U = 1+N \subset \Bbbk[\![x]\!]$ — мультипликативную абелеву группу всех рядов с единичным свободным членом. Подстановка в аргумент логарифма вместо $1+x$ произвольного ряда $u(x) \in U$ означает подстановку в логарифмический ряд (4-14) вместо переменной x ряда $u(x) - 1$ без свободного члена и тем самым является алгебраической операцией[1]. Мы получаем отображение *логарифмирования*

$$\ln :\ U \to N\,, \quad u \mapsto \ln u\,. \tag{4-16}$$

Упражнение 4.5. Убедитесь, что $(\ln u)' = u'/u$ и $\ln(1/u) = -\ln u$ для всех $u \in U$.

Подстановка в экспоненту (4-15) вместо x любого ряда $\tau(x) \in N$ даёт ряд $e^{\tau(x)}$ со свободным членом 1. Мы получаем *экспоненциальное отображение*

$$\exp :\ N \to U\,, \quad \tau \mapsto e^{\tau}\,. \tag{4-17}$$

Лемма 4.3
Для рядов $u, w \in U$ равенства $u = w$, $u' = w'$, $\ln(u) = \ln(w)$ и $u'/u = w'/w$ попарно эквивалентны друг другу.

[1] См. n° 3.1.1 на стр. 41.

Доказательство. Первое равенство влечёт за собой все остальные. Поскольку ряды с равными свободными членами совпадают если и только если совпадают их производные, первые два равенства и последние два равенства равносильны друг другу. Остаётся показать, что из последнего равенства следует первое. Но последнее равенство утверждает, что $u'/u - w'/w = (u'w - w'u)/uw = (w/u)\cdot(u/w)' = 0$ откуда $(u/w)' = 0$, т. е. $u/w = \mathrm{const} = 1$. □

Теорема 4.2
Экспоненциальное и логарифмическое отображения (4-17) и (4-16) являются взаимно обратными изоморфизмами абелевых групп, т. е. для любых рядов u, u_1, u_2 из U и τ, τ_1, τ_2 из N выполняются тождества $\ln e^{\tau} = \tau$, $e^{\ln u} = u$, $\ln(u_1u_2) = \ln(u_1) + \ln(u_2)$, $e^{\tau_1+\tau_2} = e^{\tau_1}e^{\tau_2}$.

Доказательство. Равенство $\ln e^{\tau} = \tau$ проверяется сравнением производных от обеих частей:

$$\left(\ln e^{\tau}\right)' = \frac{\left(e^{\tau}\right)'}{e^{\tau}} = \frac{e^{\tau}\tau'}{e^{\tau}} = \tau',$$

а равенство $e^{\ln u} = u$ — сравнением логарифмических производных:

$$\frac{\left(e^{\ln u}\right)'}{e^{\ln u}} = \frac{e^{\ln u}(\ln u)'}{e^{\ln u}} = \frac{u'}{u}.$$

Тем самым, экспоненцирование и логарифмирование являются взаимно обратными биекциями. Ряды $\ln(u_1u_2)$ и $\ln u_1 + \ln u_2$ совпадают, поскольку имеют нулевые свободные члены и равные производные:

$$\left(\ln(u_1u_2)\right)' = \frac{(u_1u_2)'}{u_1u_2} = \frac{u_1'u_2 + u_1u_2'}{u_1u_2} = \frac{u_1'}{u_1} + \frac{u_2'}{u_2} = \left(\ln u_1 + \ln u_2\right)'.$$

Поэтому логарифмирование — гомоморфизм, а значит, и обратное к нему экспоненцирование — тоже. □

Упражнение 4.6. Докажите в $\Bbbk[\![x,y]\!]$ равенство $e^{x+y} = e^xe^y$ непосредственным сравнением коэффициентов этих двух рядов.

4.3.2. Степенная функция и бином. В этом разделе мы продолжаем считать, что поле $\Bbbk$ имеет характеристику нуль. Для любого числа $\alpha \in \Bbbk$ определим *биномиальный ряд* с показателем α формулой

$$(1+x)^{\alpha} \stackrel{\text{def}}{=} e^{\alpha\ln(1+x)}.$$

Подставляя вместо $1+x$ произвольные ряды $u \in U$, мы для любого числа $\alpha \in \Bbbk$ получаем алгебраическую операцию *возведения в α-тую степень* $U \to U$, $u \mapsto u^{\alpha}$, обладающую всеми интуитивно ожидаемыми от степенной функции свойствами. В частности, для любых рядов $u, v \in U$ и чисел $\alpha, \beta \in \Bbbk$ выполняются равенства

$$u^{\alpha}\cdot u^{\beta} = e^{\alpha\ln u}e^{\beta\ln u} = e^{\alpha\ln u+\beta\ln u} = e^{(\alpha+\beta)\ln u} = u^{\alpha+\beta}$$
$$\left(u^{\alpha}\right)^{\beta} = e^{\beta\ln(u^{\alpha})} = e^{\beta\ln\left(e^{\alpha\ln u}\right)} = e^{\alpha\beta\ln u} = u^{\alpha\beta}$$
$$(uv)^{\alpha} = e^{\alpha\ln(uv)} = e^{\alpha(\ln u+\ln v)} = e^{\alpha\ln u+\alpha\ln v} = e^{\alpha\ln u}\cdot e^{\alpha\ln v} = u^{\alpha}v^{\alpha}.$$

Например, для любого ряда u с единичным свободным членом ряд $u^{1/n}$ представляет собою $\sqrt[n]{u}$ в том смысле, что $\left(u^{1/n}\right)^n = u$. Чтобы найти коэффициенты a_i биномиального ряда

$$(1+x)^{\alpha} = a_0 + a_1x + a_2x^2 + \ldots$$

рассмотрим его логарифмическую производную

$$\frac{\bigl((1+x)^\alpha\bigr)'}{(1+x)^\alpha} = \frac{d}{dx}\ln(1+x)^\alpha = \alpha\frac{d}{dx}\ln(1+x) = \frac{\alpha}{1+x}\,.$$

Умножая левую и правую части на $(1+x)^{\alpha+1}$, получаем равенство

$$\bigl(a_1 + 2a_2x + 3a_3x^2 + \ldots\bigr)\cdot(1+x) = \alpha\cdot(1 + a_1x + a_2x^2 + a_3x^3 + \ldots)\,.$$

Сравнивая коэффициенты при x^{k-1} в правой и левой части, приходим к рекуррентному соотношению $ka_k + (k-1)a_{k-1} = \alpha a_{k-1}$, из которого

$$a_k = \frac{\alpha-(k-1)}{k}\cdot a_{k-1} = \frac{(\alpha-(k-1))(\alpha-(k-2))}{k(k-1)}\cdot a_{k-2} = \ldots$$
$$\ldots = \frac{(\alpha-(k-1))(\alpha-(k-2))\cdots(\alpha-1)\alpha}{k!}\,.$$

Стоящая в правой части дробь имеет в числителе и знаменателе по k множителей, представляющих собою последовательно уменьшающиеся на единицу числа: в знаменателе — от k до 1, в числителе — от α до $(\alpha-k+1)$. Эта дробь называется *биномиальным коэффициентом* и обозначается

$$\binom{\alpha}{k} \stackrel{\text{def}}{=} \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!} \tag{4-18}$$

Таким образом, для любого $\alpha\in\Bbbk$ имеется разложение

$$(1+x)^\alpha = \sum_{k\geqslant 0}\binom{\alpha}{k}x^k = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + \frac{\alpha(\alpha-1)(\alpha-2)}{6}x^3 + \ldots\,,$$

известное как *формула Ньютона*.

Пример 4.7 (бином с рациональным показателем)
Если $\alpha = n\in\mathbb{N}$, то при $k>n$ в числителе дроби (4-18) появится нулевой сомножитель. Поэтому разложение бинома в этом случае конечно и имеет вид

$$(1+x)^n = 1 + n\,x + \frac{n(n-1)}{2}\,x^2 + \ldots + x^n = \sum_{k=0}^{n}\binom{n}{k}\cdot x^k\,,$$

знакомый нам из форм. (1-8) на стр. 10. При $\alpha = -m$, где $m\in\mathbb{N}$, мы получаем разложение из форм. (4-8) на стр. 66

$$(1+x)^{-m} = 1 - m\,x + \frac{m(m+1)}{2}\,x^2 - \frac{m(m+1)(m+2)}{6}\,x^3 + \ldots = \sum_{k\geqslant 0}(-1)^k\binom{k+m-1}{k}\cdot x^k\,.$$

При $\alpha = 1/n$, где $n\in\mathbb{N}$, формула Ньютона разворачивает в степенной ряд радикал

$$\sqrt[n]{1+x} = 1 + \frac{1}{n}\,x + \frac{\frac{1}{n}\left(\frac{1}{n}-1\right)}{2}\,x^2 + \frac{\frac{1}{n}\left(\frac{1}{n}-1\right)\left(\frac{1}{n}-2\right)}{6}\,x^3 + \cdots =$$
$$= 1 + \frac{x}{n} - \frac{n-1}{2}\cdot\frac{x^2}{n^2} + \frac{(n-1)(2n-1)}{2\cdot 3}\cdot\frac{x^3}{n^3} - \frac{(n-1)(2n-1)(3n-1)}{2\cdot 3\cdot 4}\cdot\frac{x^4}{n^4} + \cdots$$

Например, при $n = 2$ и $k \geqslant 1$ в качестве коэффициента при x^k получается дробь

$$(-1)^{k-1} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-3)}{2^k k!} = \frac{(-1)^{k-1}}{2k} \cdot \frac{1}{4^{k-1}} \cdot \binom{2k-2}{k-1},$$

т. е.

$$\sqrt{1+x} = 1 + \sum\nolimits_{k\geqslant 1} \frac{(-1)^{k-1}}{k} \cdot \binom{2k-2}{k-1} \cdot \frac{x^k}{4^{k-1}}. \tag{4-19}$$

Пример 4.8 (числа Каталана)
Воспользуемся разложением (4-19) для получения явной формулы для *чисел Каталана*, часто возникающих в комбинаторных задачах. Вычислим произведение $n+1$ чисел

$$a_0 a_1 \ldots a_n, \tag{4-20}$$

делая за один шаг ровно одно из n умножений и заключая перемножаемые числа в скобки. В результате мы расставим n пар скобок в выражении (4-20). Количество различных расстановок скобок, возникающих таким образом, называется n-ым *числом Каталана* c_n. При $n = 1$ есть лишь одна расстановка скобок $(a_0 a_1)$, при $n = 2$ — две $(a_0(a_1 a_2))$ и $((a_0 a_1)a_2)$, при $n = 3$ — пять: $(a_0(a_1(a_2 a_3)))$, $(a_0((a_1 a_2)a_3))$, $((a_0 a_1)(a_2 a_3))$, $((a_0(a_1 a_2))a_3)$, $(((a_0 a_1)a_2)a_3)$. Множество всевозможных расстановок скобок в произведении (4-20) распадается в дизъюнктное объединение n подмножеств, в которых конфигурации наружных скобок имеют вид

$$(a_0(a_1 \ldots a_n)),\ ((a_0 a_1)(a_2 \ldots a_n)),\ \ldots,\ ((a_0 \ldots a_{n-2})(a_{n-1} a_n)),\ ((a_0 \ldots a_{n-1})a_n)$$

и которые состоят, соответственно, из c_{n-1}, $c_1 c_{n-2}$, $c_2 c_{n-3}$, …, $c_{n-2} c_1$, c_{n-1} элементов. Если дополнить последовательность чисел Каталана числом $c_0 \stackrel{\text{def}}{=} 1$, то получится соотношение

$$c_n = c_0 c_{n-1} + c_1 c_{n-2} + \ldots + c_{n-2} c_1 + c_{n-1} c_0,$$

означающее, что *ряд Каталана* $c(x) \stackrel{\text{def}}{=} \sum_{k\geqslant 0} c_k x^k = 1 + c_1 x + c_2 x^2 + \ldots \in \mathbb{Z}[\![x]\!]$ удовлетворяет уравнению $c(x)^2 = (c(x) - 1)/x$, т. е. является лежащим в кольце $\mathbb{Z}[\![x]\!]$ корнем квадратного трёхчлена $xt^2 - t - 1 = 0$ от переменной t. В поле рядов Лорана $\mathbb{Q}(\!(x)\!) \supset \mathbb{Z}[\![x]\!]$ корни находятся по стандартной школьной формуле $t = (1 \pm \sqrt{1-4x})/2x$. Так как $1 + \sqrt{1-4x}$ не делится на $2x$ в $\mathbb{Z}[\![x]\!]$, корень $(1 + \sqrt{1-4x})/(2x) \notin \mathbb{Z}[\![x]\!]$. Тем самым, $c(x) = (1 - \sqrt{1-4x})/(2x)$, откуда по формуле (4-19)

$$c_k = \frac{1}{k+1}\binom{2k}{k}.$$

Отметим, что даже не сразу понятно, что это число — целое.

4.4. Действие $\mathbb{Q}[[d/dt]]$ на $\mathbb{Q}[t]$. Рассмотрим кольцо формальных степенных рядов $\mathbb{Q}[\![x]\!]$ от переменной x и кольцо многочленов $\mathbb{Q}[t]$ от переменной t. Обозначим через

$$D = \frac{d}{dt} : \mathbb{Q}[t] \to \mathbb{Q}[t], \quad g \mapsto g',$$

оператор дифференцирования. Оператор D можно подставить вместо переменной x в любой степенной ряд $\Phi(x) = \sum_{k\geqslant 0} \varphi_k x^k \in \mathbb{Q}[\![x]\!]$. Результатом такой подстановки, по определению, является линейное отображение

$$\Phi(D) : \mathbb{Q}[t] \to \mathbb{Q}[t], \quad f \mapsto \sum_{k\geqslant 0} \varphi_k D^k f = \varphi_0 f + \varphi_1 f' + \varphi_2 f'' + \ldots. \tag{4-21}$$

Поскольку каждое дифференцирование уменьшает степень многочлена на единицу, все слагаемые в правой части (4-21) обратятся в нуль при $k > \deg f$. Таким образом, для каждого многочлена $f \in \mathbb{Q}[t]$, правая часть (4-21) является корректно определённым многочленом, каждый коэффициент которого вычисляется конечным числом действий с коэффициентами исходного многочлена f и первыми $\deg(f)$ коэффициентами ряда Φ. Линейность отображения (4-21) означает, что $\Phi(D)(\alpha f + \beta g) = \alpha\Phi(D)f + \beta\Phi(D)g$ для всех $\alpha, \beta \in \mathbb{Q}$ и $f, g \in \mathbb{Q}[t]$. Результатом подстановки оператора D в произведение рядов $\Phi(x)\Psi(x) \in \mathbb{Q}[\![x]\!]$ является *композиция* $\Phi(D) \circ \Psi(D) = \Psi(D) \circ \Phi(D)$ отображений $\Phi(D)$ и $\Psi(D)$.

Упражнение 4.7. Убедитесь в этом.

Таким образом, все отображения вида $\Phi(D)$ перестановочны друг с другом, и для биективности отображения $\Phi(D)$ необходимо и достаточно, чтобы степенной ряд $\Phi(x)$ был обратим[1] в кольце $\mathbb{Q}[\![x]\!]$. В силу линейности значение отображения $\Phi(D)$ на произвольном многочлене выражается через его значения $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ на базисных одночленах t^m:

$$\Phi(D)\left(a_0 + a_1 t + \ldots + a_n t^n\right) = a_0 + a_1\Phi_1(t) + \ldots + a_n\Phi_n(t)\,.$$

Многочлен $\Phi_m(t) \stackrel{\text{def}}{=} \Phi(D)t^m$ называется m-тым *многочленом Аппеля* ряда Φ. Его степень не превосходит m, а коэффициенты зависит лишь от первых $m+1$ коэффициентов ряда Φ.

Пример 4.9 (операторы сдвига)
Экспонента $e^D = 1 + D + D^2/2 + D^3/6 + \ldots$ имеет многочлены Аппеля

$$e^D t^m = \sum_{k\geqslant 0} \frac{1}{k!} D^k t^m = \sum_{k\geqslant 0} \frac{m(m-1)\ldots(m-k+1)}{k!}\, t^{m-k} = \sum_{k=0}^{m} \binom{m}{k} t^{m-k} = (t+1)^m\,.$$

Поэтому $e^D : f(t) \mapsto f(t+1)$ — это *оператор сдвига*. Так как ряды e^x и e^{-x} обратны друг другу в $\mathbb{Q}[\![x]\!]$, операторы e^D и e^{-D} тоже обратны друг другу, т. е. $e^{-D} : f(t) \mapsto f(t-1)$.

Упражнение 4.8. Убедитесь, что $e^{\alpha D} : f(t) \mapsto f(t+\alpha)$ при любом $\alpha \in \mathbb{Q}$.

Пример 4.10 (вычисление суммы степеней)
Для произвольно зафиксированного $m \in \mathbb{Z}_{\geqslant 0}$ рассмотрим сумму

$$S_m(n) \stackrel{\text{def}}{=} 0^m + 1^m + 2^m + 3^m + \ldots + n^m = \sum_{k=0}^{n} k^m \tag{4-22}$$

как функцию от n. При $m = 0, 1, 2, 3$ функции $S_m(n)$ достаточно известны:

$$\begin{aligned} S_0(n) &= 1 + \ldots + 1 = n \\ S_1(n) &= 1 + 2 + \ldots + n = n(n+1)/2 \\ S_2(n) &= 1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6 \\ S_3(n) &= 1^3 + 2^3 + \ldots + n^3 = n^2(n+1)^2/4 = S_1(n)^2\,. \end{aligned} \tag{4-23}$$

Чтобы получить для $S_m(t)$ явное выражение, применим к этой функции *разностный оператор*

$$\nabla : \varphi(t) \mapsto \varphi(t) - \varphi(t-1)\,. \tag{4-24}$$

[1] Т. е. имел ненулевой свободный член, см. прим. 3.2 на стр. 42.

Функция $\nabla S_m(t)$ принимает при всех $t \in \mathbb{Z}_{\geqslant 0}$ те же значения, что и многочлен t^m. Если существует такой многочлен $S_m(t) \in \mathbb{Q}[t]$, что $S_m(0) = 0$ и $\nabla S_m(t) = t^m$, то его значения в точках $t = 0,\ 1,\ 2,\ \ldots$ последовательно вычисляются, начиная с $S_m(0) = 0$, по формуле

$$S_m(n) = S_m(n-1) + \nabla S_m(n) = S_m(n-1) + n^m$$

и совпадают с суммами (4-22). Покажем, что уравнение $\nabla S_m(t) = t^m$ имеет в $\mathbb{Q}[t]$ единственное решение $S_m(t)$ с $S_m(0) = 0$. Согласно прим. 4.9 оператор $\nabla\colon\ \mathbb{Q}[t] \to \mathbb{Q}[t]$ имеет вид

$$\nabla = 1 - e^{-D} = \frac{1 - e^{-D}}{D} \circ D\,.$$

Ряд $(1 - e^{-x})/x$ имеет свободный член 1 и обратим в $\mathbb{Q}[\![x]\!]$. Обратный ему ряд

$$\mathrm{td}(x) \stackrel{\text{def}}{=} \frac{x}{1 - e^{-x}} \in \mathbb{Q}[\![x]\!]$$

называется *рядом Тодда*. Подставляя $x = D$ в равенство $\mathrm{td}(x) \cdot (1 - e^{-x}) = x$, получаем соотношение $\mathrm{td}(D) \circ \nabla = D$. Стало быть, $DS_m(t) = \mathrm{td}(D)\nabla S_m(t) = \mathrm{td}(D)t^m = \mathrm{td}_m(t)$ является многочленом Аппеля ряда Тодда, а искомый нами многочлен $S_m(t) = \int \mathrm{td}_m(t)\,dt$ получается из него интегрированием. Запишем ряд Тодда в «экспоненциальной форме»

$$\mathrm{td}(x) = \sum_{k \geqslant 0} \frac{a_k}{k!}\, x^k. \tag{4-25}$$

Сумма m-тых степеней первых t натуральных чисел равна

$$S_m(t) = \int \Bigl(\sum_{k=0}^{m} \frac{a_k}{k!} D^k t^m\Bigr)\,dt = \int \Bigl(\sum_{k=0}^{m} \binom{m}{k} a_k t^{m-k}\Bigr)\,dt = \sum_{k=0}^{m} \binom{m}{k} \frac{a_k t^{m-k+1}}{m-k+1} =$$
$$= \frac{1}{m+1}\left(\binom{m+1}{1} a_m t + \binom{m+1}{2} a_{m-1} t^2 + \ldots + \binom{m+1}{m} a_1 t^m + \binom{m+1}{m+1} a_0 t^{m+1}\right).$$

Эту формулу часто символически пишут в виде

$$(m+1) \cdot S_m(t) = (a^{\downarrow} + t)^{m+1} - a_{m+1}\,,$$

где стрелка у $a^{\downarrow}$ предписывает при раскрытии бинома $(a+t)^{m+1}$ заменять a^k на a_k. Коэффициенты a_k рекурсивно вычисляются из равенства $\mathrm{td}(x) \cdot (1 - e^{-x})/x = 1$, которое имеет вид

$$\Bigl(1 + a_1 x + \frac{a_2}{2} x^2 + \frac{a_3}{6} x^2 + \frac{a_4}{24}\, x^4 + \ldots\Bigr) \cdot \Bigl(1 - \frac{1}{2}\, x + \frac{1}{6}\, x^2 - \frac{1}{24}\, x^3 + \frac{1}{120}\, x^4 - \ldots\Bigr) = 1\,.$$

Упражнение 4.9. Найдите первую дюжину чисел a_k, проверьте формулы (4-23), дополните их явными формулами для $S_4(n)$ и $S_5(n)$ и вычислите[1] $S_{10}(1000)$.

[1] Яков Бернулли (1654–1705), пользуясь лишь пером и бумагой, сложил 10-е степени первой тысячи натуральных чисел примерно за 7 минут, о чём не без гордости написал в своём манускрипте «Ars Conjectandi», изданном в 1713 году уже после его кончины.

Замечание 4.1. (числа Бернулли) Название «ряд Тодда» вошло в обиход во второй половине XX века после работ Хирцебруха и Гротендика, где он использовался для формулировки и доказательства теоремы Римана – Роха. Во времена Бернулли и Эйлера предпочитали пользоваться рядом $\mathrm{td}(-x) = x/(e^x - 1)$, который отличается от $\mathrm{td}(x)$ ровно в одном члене, поскольку

$$\mathrm{td}(x) - \mathrm{td}(-x) = \frac{x}{1-e^{-x}} + \frac{x}{1-e^{x}} = x \cdot \frac{2 - e^x - e^{-x}}{(1-e^{-x})\cdot(1-e^x)} = x\,.$$

Тем самым, коэффициенты при x в $\mathrm{td}(x)$ и в $\mathrm{td}(-x)$ равны соответственно $1/2$ и $-1/2$, а все прочие коэффициенты при нечётных степенях x^{2k+1} с $k \geqslant 1$ в обоих рядах нулевые. Коэффициенты B_k в экспоненциальном представлении

$$\frac{x}{e^x - 1} = \sum_{k\geqslant 0} \frac{B_k}{k!}\, x^k$$

называются *числами Бернулли*. Таким образом, $B_k = a_k$ при $k \neq 1$ и обращаются в нуль при всех нечётных $k \geqslant 3$, а $B_1 = -a_1 = -1/2$. Со времён своего открытия числа Бернулли вызывают неослабевающий интерес. Им посвящена обширная литература[1] и специальный интернет-ресурс[2], на котором среди прочего есть программа для быстрого вычисления чисел B_k в виде несократимых рациональных дробей. Однако, не смотря на множество красивых теорем о числах Бернулли, про явную зависимость B_n от n известно немного, и любой содержательный новый взгляд в этом направлении был бы интересен.

Упражнение 4.10. Получите для чисел Бернулли рекурсивную формулу

$$(n+1)B_n = -\sum_{k=0}^{n-1} \binom{n+1}{k} \cdot B_k\,.$$

4.5. Ряды Пюизо. Дробно степенной ряд вида $f(t) = \sum_{k\geqslant m} a_k t^{k/q}$, у которого показатели степеней ограничены снизу и имеют конечный общий знаменатель $q \in \mathbb{N}$, называется *рядом Пюизо*. Можно воспринимать ряд Пюизо как ряд Лорана от формальной переменной $\sqrt[q]{t}$, где $q \in \mathbb{N}$ может быть любым. Ряды Пюизо с коэффициентами a_i из поля $\Bbbk$ образуют поле, которое мы будем обозначать через $\Bbbk\{\!\{x\}\!\}$. Основным результатом этого раздела является

Теорема 4.3
Если поле $\Bbbk$ алгебраически замкнуто и $\mathrm{char}\,\Bbbk = 0$, то поле рядов Пюизо $\Bbbk\{\!\{t\}\!\}$ тоже алгебраически замкнуто.

Другими словами, теор. 4.3 утверждает, что корни любого многочлена

$$a_n(t)\,x^n + a_{n-1}(t)\,x^{n-1} + \ldots + a_1(t)\,x + a_0(t)\,,$$

коэффициенты которого являются рядами Пюизо от t, раскладываются в ряды Пюизо по t. Например, любой многочлен $f(x,y) \in \Bbbk[x,y]$ можно рассматривать как многочлен от y с коэффициентами в $\Bbbk[x]$. По теор. 4.3 существует такой ряд Пюизо $\varphi(x) \in \Bbbk\{\!\{x\}\!\}$, что $f(x,\varphi(x)) = 0$

[1] Начать знакомство с которой я советую с гл. 15 книги *К. Айрлэнд, М. Роузен*. «Классическое введение в современную теорию чисел» и § 8 гл. V книги *З. И. Боревич, И Р. Шафаревич*. «Теория чисел».

[2] http://www.bernoulli.org/

в $\Bbbk\{\{x\}\}$. Неформально говоря, это означает, что «неявная алгебраическая функция» $y = y(x)$, заданная полиномиальным соотношением $f(x, y) = 0$, всегда может быть *явно выписана* в виде ряда Пюизо от x, если только поле $\Bbbk$, над которым происходит дело, алгебраически замкнуто и имеет характеристику нуль.

Доказательство теор. 4.3 является комбинацией двух соображений, представленных ниже в лем. 4.4 и лем. 4.5. Завершение доказательства см. в n° 4.5.1 на стр. 77. В n° 4.5.2 приведён пример, показывающий, что при $\operatorname{char}\Bbbk = p > 0$ теор. 4.3 не верна.

Лемма 4.4 (лемма Гензеля)
Пусть $G(t, x) \in \Bbbk[\![t]\!]\,[x]$ — приведённый многочлен от переменной x с коэффициентами в формальных степенных рядах от переменной t над произвольным полем $\Bbbk$. Если при $t = 0$ многочлен $G(0, x) \in \Bbbk[x]$ раскладывается в $\Bbbk[x]$ в произведение взаимно простых приведённых множителей $a(x)$ и $b(x)$ положительных степеней, то существуют единственные такие приведённые многочлены $A(t, x)$, $B(t, x) \in \Bbbk[\![t]\!]\,[x]$, что $\deg A = \deg a$, $\deg B = \deg b$, $A(0, x) = a(x)$, $B(0, x) = b(x)$ и $G(t, x) = A(t, x)\,B(t, x)$ в $\Bbbk[\![t]\!]\,[x]$. Эти многочлены взаимно просты.

Доказательство. Запишем данный ряд $G(t, x)$ и искомые ряды $A(t, x)$ и $B(t, x)$ в виде рядов от переменной t с коэффициентами в $\Bbbk[x]$:

$$\begin{aligned} G(t, x) &= g_0(x) + g_1(x)\,t + g_2(x)\,t^2 + \dots \\ A(t, x) &= a_0(x) + a_1(x)\,t + a_2(x)\,t^2 + \dots \\ B(t, x) &= b_0(x) + b_1(x)\,t + b_2(x)\,t^2 + \dots\,. \end{aligned}$$

Сравнивая коэффициенты при t^k в равенстве $G(t, x) = A(t, x)\,B(t, x)$, видим, что $a_0 b_0 = g_0$ и

$$a_0 b_k + b_0 a_k = g_k - \sum_{i=1}^{k-1} a_i b_{k-i} \quad \text{при } k \geqslant 1\,. \tag{4-26}$$

Взаимно простые приведённые многочлены $a_0 = a(x)$ и $b_0 = b(x)$, удовлетворяющие равенству $a_0 b_0 = g_0$, имеются по условию. Равенство (4-26) однозначно определяет многочлены a_k и b_k степеней $\deg a_k < \deg a$ и $\deg b_k < \deg b$, как только известны все предыдущие многочлены a_i и b_i и $\deg a_i < \deg a$, $\deg b_i < \deg b$ при всех $0 < i < k$. В самом деле, раз G приведён как многочлен от x, то $\deg g_i < \deg g_0$ при всех $i > 0$, и степень многочлена в правой части (4-26) строго меньше $\deg a_0 \cdot \deg b_0$. Тем самым, b_k — это единственный многочлен степени $< \deg b_0$, класс которого по модулю b_0 равен отношению класса правой части формулы (4-26) к классу $a_0 \pmod{b_0}$, а класс a_k играет аналогичную роль по модулю a_0 (ср. с доказательством предл. 4.1 на стр. 64). Это доказывает первое утверждение.

Чтобы доказать взаимную простоту многочленов A и B, построим для каждого $i \geqslant 0$ такие многочлены $p_i, q_i \in \Bbbk[x]$ с $\deg p < \deg a$, $\deg q_i < \deg b$, что ряды $P(t, x) = \sum_{k\geqslant 0} p_k(x)\,t^k$ и $Q(t, x) = \sum_{k\geqslant 0} q_k(x)\,t^k$ удовлетворяют равенству $AP + BQ = 1$. Сравнивая в нём коэффициенты при t^k, заключаем, что $a_0 p_0 + b_0 q_0 = 1$ и $a_0 p_k + b_0 q_k = -\sum_{i=1}^{k-1}(a_i p_{k-i} + b_i q_{k-i})$ при $k \geqslant 1$. Так как $a_0 = a$ и $b_0 = b$ взаимно просты и $\deg a_i < \deg a$, $\deg b_i < \deg b$ при всех $i > 0$, эти соотношения однозначно задают искомые многочлены p_i и q_i. □

Лемма 4.5
Над алгебраически замкнутым полем $\Bbbk$ характеристики нуль для любого многочлена

$$F(t, x) = a_n(t)\,x^n + a_{n-1}(t)\,x^{n-1} + \dots + a_0(x) \in \Bbbk(\!(t)\!)\,[x]$$

существуют такие $m \in \mathbb{N}$ и $\vartheta(t) \in \Bbbk(\!(t)\!)$, что $F\left(t^m, \vartheta(t)\right) = 0$ в $\Bbbk(\!(t)\!)$. Иными словами, каждый многочлен с коэффициентами в поле рядов Лорана от t имеет при некотором $m \in \mathbb{N}$ корень в поле $\Bbbk(\!(\sqrt[m]{t})\!)$.

Доказательство. Умножая многочлен F на подходящее t^k, мы можем и будем считать, что все коэффициенты a_i лежат в $\Bbbk[\![t]\!]$. Далее, умножая F на a_n^{n-1} и заменяя x на $a_n x$, сделаем F приведённым. Наконец, пользуясь тем, что $\operatorname{char}\Bbbk = 0$, заменим x на $x - a_{n-1}/n$, что занулит коэффициент при x^{n-1}.

Упражнение 4.11. Убедитесь, в этом.

Таким образом, достаточно доказать теорему для многочлена вида

$$F(t,x) = x^n + a_{n-2}(t)\,x^{n-2} + \ldots + a_0(t) \tag{4-27}$$

с коэффициентами $a_i \in \Bbbk[\![t]\!]$. Если все $a_i = 0$, что так при $n = 1$, можно взять $m = 1$ и $\vartheta = 0$. Поэтому мы можем и будем считать, что имеются $a_i \neq 0$ и тем самым $n \geqslant 2$, а для всех многочленов степени меньше n теорема верна.

Если среди коэффициентов a_i имеется ряд с ненулевым свободным членом, то при $t = 0$ многочлен $F(0,x)$ отличен от x^n. Так как $\operatorname{char}\Bbbk = 0$, многочлен $F(0,x)$ отличен и от всех многочленов $(x-\alpha)^n$ с $\alpha \neq 0$, ибо все они имеют ненулевой коэффициент при x^{n-1}. Мы заключаем, что многочлен $F(0,x) \in \Bbbk[x]$ имеет в алгебраически замкнутом поле $\Bbbk$ по крайней мере два разных корня, а значит, имеет вид $F(0,x) = a(x)b(x)$, где $\operatorname{нод}(a,b) = 1$ и $\deg a, \deg b < \deg F$. Тогда по лемме Гензеля[1] $F(t,x) = A(t,x)B(t,x)$ в кольце $\Bbbk[\![t]\!]\,[x]$, где A, B приведены и оба имеют степень меньше n. По индукции теорема верна для многочлена A, а значит, и для F.

Пусть каждый ненулевой ряд a_i делится на t. Покажем, что этот случай можно свести к предыдущему заменой параметра t на t^q, а переменной x на $t^p x$ с подходящими $p, q \in \mathbb{N}$. Чтобы указать такие p и q, обозначим через $\mu_i = \operatorname{ord} a_i(t)$ порядок[2] каждого ненулевого коэффициента a_i по t и приведём все дроби $\mu_i/(n-i)$ к общему знаменателю. В качестве q возьмём этот общий знаменатель, а качестве p — наименьший из полученных после приведения числителей. Таким образом, $q\mu_i \geqslant p(n-i)$ при всех i, причём при некотором $i = \ell$ это неравенство обращается в равенство. Заменяя в многочлене F параметр t на t^q, а переменную x — на $t^p x$, получаем многочлен

$$\begin{aligned} G(t,x) = F(t^q, t^p x) &= t^{pn}\,x^n + \sum_{i=0}^{n-2} a_i(t^q)\,t^{pi}x^i = \\ &= t^{pn}\,x^n + \sum_{i=0}^{n-2} t^{pi}\left(\alpha_{\mu_i}\,t^{q\mu_i} + \text{члены большей степени по } t\right)\cdot x^i = \\ &= t^{pn}\Big(x^n + \sum_{i=0}^{n-2} t^{q\mu_i - p(n-i)}\,(\alpha_{\mu_i} + \text{ члены, делящиеся } t\,)\cdot x^i\Big), \end{aligned}$$

который делится в $\Bbbk[\![t]\!]\,[x]$ на t^{pn}. После сокращения этого множителя коэффициент при x^ℓ у частного будет иметь ненулевой свободный член, так как $q\mu_\ell = p(n-\ell)$. По уже доказанному, приведённый многочлен $G(t,x)/t^{pn}$ приводим в $\Bbbk[\![t]\!][x]$, и тем самым существуют такие $d \in \mathbb{N}$

[1] См. лем. 4.4 на стр. 75.

[2] Т. е. наименьшую степень t, входящую в ряд с ненулевым коэффициентом, ср. с прим. 4.4 на стр. 64.

и $\tau(t) \in \Bbbk(\!(t)\!)$, что $G\left(t^d, \tau(t)\right) = 0$ в $\Bbbk(\!(t)\!)$. Тогда для $m = qd$ и $\vartheta(t) = t^p\,\tau(t)$ имеем $F\left(t^m, \vartheta(t)\right) = F\left(t^{qd}, t^p\,\tau(t)\right) = G\left(t^d, \tau(t)\right) = 0$, что и требовалось. □

4.5.1. Окончание доказательства теор. 4.3. Пусть многочлен

$$f(x) = a_0(t) + a_1(t)\,x + \ldots + a_n(t)\,x^n$$

имеет коэффициенты $a_i(t)$ в поле рядов Пюизо. Обозначим общий знаменатель всех показателей всех рядов a_i через N и положим $t = u^N$. Тогда $a_i(t) = a_i(u^m) \in \Bbbk(\!(u)\!)$ и по лем. 4.5 после ещё одной подстановки $u = s^q$ у многочлена f появится корень в поле $\Bbbk(\!(s)\!)$. Возвращаясь к исходному параметру $t = s^{qm}$ получаем корень многочлена f в виде ряда Лорана от $t^{\frac{1}{qm}}$, что и требуется.

4.5.2. Контрпример к теор. 4.3 в положительной характеристике. Если $\operatorname{char}\Bbbk = p > 0$, то лем. 4.5 и теор. 4.3 перестают быть верны. Например, многочлен $x^p - x - t^{-1} \in \mathbb{F}_p(\!(t)\!)\,[x]$ не имеет корня в поле рядов Пюизо от t. В самом деле, пусть ряд Пюизо $x(t) = c_1 t^{\lambda_1} + c_2 t^{\lambda_2} + \ldots$ с $\lambda_1 < \lambda_2 < \ldots$ и ненулевыми $c_i \in \mathbb{F}_p$ удовлетворяет равенству $x^p - x = t^{-1}$. Так как $c^p = c$ для всех $c \in \mathbb{F}_p$, это равенство переписывается в виде

$$c_1 t^{p\lambda_1} + c_2 t^{p\lambda_2} - c_1 t^{\lambda_1} + c_3 t^{p\lambda_3} - c_2 t^{\lambda_2} + \text{ большие степени } = t^{-1}\,.$$

Мы заключаем, что $\lambda_1 < 0$ и член минимальной степени $c_1 t^{p\lambda}$ ни с чем в левой части не сокращается. Поэтому $c_1 t^{p\lambda} = t^{-1}$, откуда $c_1 = 1$ и $\lambda_1 = -1/p$. Следующие два члена обязаны сокращать друг друга, откуда $c_2 = c_1 = 1$, а $\lambda_2 = \lambda_1/p = -1/p^2$. Следующие два члена также обязаны сокращать друг друга, откуда $c_3 = 1$, а $\lambda_3 = -1/p^3$ и т. д. Таким образом, ряд $x(t) = \sum_{k\geqslant 1} t^{-1/p^k}$ содержит бесконечно много членов отрицательной степени, а у его показателей нет общего знаменателя, т. е. он не является рядом Пюизо вопреки предположению.

4.5.3. Метод Ньютона. Пусть у приведённого многочлена

$$F(t,x) = x^n + a_{n-1}(t)\,x^{n-1} + \ldots + a_0(t) \in \Bbbk[\![t]\!]\,[x]\,, \tag{4-28}$$

свободный член $a_0(0) = 0$, и тем самым, $F(0,x) \in \Bbbk[x]$ имеет корень $x = 0$. Метод Ньютона строит ряд Пюизо

$$x(t) = c_1 t^{\varepsilon_1} + c_2 t^{\varepsilon_1+\varepsilon_2} + c_3 t^{\varepsilon_1+\varepsilon_2+\varepsilon_3} + \ldots = t^{\varepsilon_1}\Big(c_1 + t^{\varepsilon_2}\big(c_2 + t^{\varepsilon_3}(c_3 + \ldots)\big)\Big)\,, \tag{4-29}$$

последовательно вычисляя поправки $\varepsilon_1, \varepsilon_2, \ldots \in \mathbb{Q}$ к показателям его степеней и соответствующие этим поправкам коэффициенты $c_1, c_2, \ldots \in \Bbbk$ так, чтобы при каждом $k \in \mathbb{N}$ при подстановке в $F(t,x)$ вместо x выражения

$$t^{\varepsilon_1}\Big(c_1 + t^{\varepsilon_2}\big(c_2 + \ldots + t^{\varepsilon_k}(c_k + x(t))\,\ldots\big)\Big)\,,$$

где $x(t)$ — произвольный ряд Пюизо строго положительного порядка[1], получался ряд, порядок которого строго больше некоторого числа $N_k \in \mathbb{Q}$, монотонно возрастающего с ростом k. Если $N_k \to \infty$ при $k \to \infty$, то ряд (4-29) будет корнем многочлена (4-28).

[1] Напомню, что порядком ряда называется минимальный из показателей степеней, представленных в нём с ненулевыми коэффициентами, см. n° 3.1 на стр. 41.

Главным инструментом вычисления является *многоугольник Ньютона* многочлена $F(t,x)$ — выпуклая оболочка таких целых точек $(p,q) \in \mathbb{Z}^2$ на координатной плоскости $\mathbb{R}^2$, что $F(t,x)$ содержит с ненулевым с ненулевым коэффициентом моном[1] $t^q x^p$. Например, многоугольник Ньютона многочлена

$$(-t^3+t^4) - 2t^2\,x - t\,x^2 + 2t\,x^4 + x^5 \tag{4-30}$$

изображён на рис. 4◇1. Видимый из начала координат участок границы многоугольника Ньютона называется *ломаной Ньютона*. Так, ломаная Ньютона многочлена (4-30) состоит из двух красных отрезков, ортогональных векторам $(1,1)$ и $(1,3)$. Каждая лежащая на ломаной Ньютона целая точка (i,μ_i) обязательно является показателем начального члена одного из служащих коэффициентами многочлена $F(t,x)$ рядов

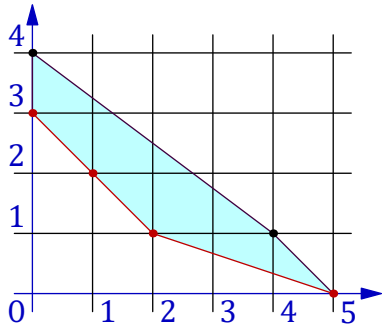


Рис. 4◇1.

$$a_i(t) = \alpha_{\mu_i}\, t^{\mu_i} + \text{старшие степени } t\,,$$

однако показатели начальных членов некоторых из этих коэффициентов, вообще говоря, могут располагаться и строго выше ломаной Ньютона, как это происходит с коэффициентом $a_4 = 2t$ многочлена (4-30). Если подставить в $F(t,x)$ вместо x ряд $x(t) = t^\varepsilon(c + y(t))$, где $y(t)$ — ряд строго положительного порядка, то младший член каждого произведения $a_i(t)x^i(t)$ получится равным $a_{\mu_i}c^i t^{i\varepsilon+\mu_i}$. Если несколько таких членов имеют одинаковую степень по t, то их можно сократить друг с другом, надлежащим образом подобрав коэффициенты c. Равенство степеней $i\varepsilon+\mu_i = j\varepsilon+\mu_j$ означает, что точки (i,μ_i) и (j,μ_j) лежат на одной прямой $\varepsilon p + q = \text{const}$. Это заведомо происходит для всех целых точек, лежащих на одном звене Z ломаной Ньютона при $\varepsilon = \delta_1/\delta_2$ равном наклону вектора $\delta = (\delta_1,\delta_2) \in \mathbb{N}^2$, перпендикулярного звену Z и направленному внутрь многоугольника Ньютона. Если подобрать c так, чтобы начальные члены всех мономов с показателями на звене Z сократились, то порядок ряда $F(t,t^\varepsilon(c+y(t)))$ будет строго больше значения, которое линейная форма $\varepsilon p + q$ принимает на звене Z.

На первом шаге вычисления по методу Ньютона выбирается какое-нибудь звено Z. Пусть его вектор нормали, направленный внутрь многоугольника Ньютона, имеет координаты

$$(\delta_1,\delta_2) \in \mathbb{N}^2\,, \quad \text{где} \quad \text{нод}(\delta_1,\delta_2) = 1\,.$$

Группируя вместе мономы, показатели которых лежат на прямых $\delta_1 p + \delta_2 q = \text{const}$, перепишем $F(t,x)$ в виде

$$F(t,x) = \sum\nolimits_{k\geqslant\gamma} f_k(t,x)\,, \quad \text{где} \quad f_k(t,x) = \sum\nolimits_{\delta_1 p+\delta_2 q=k} \alpha_{p,q}x^p t^q\,, \tag{4-31}$$

а $\gamma \in \mathbb{N}$ равно значению линейной формы $\delta_1 p+\delta_2 q$ на звене Z. Положим $\varepsilon_1 = \delta_1/\delta_2$ и подставим в $F(t,x)$ вместо x ряд $x(t) = c_1 t^{\varepsilon_1} + \text{старшие степени } t$. Так как $\varepsilon_1 p + q = k/\delta_2$ при $\delta_1 p+\delta_2 q = k$, мы заключаем, что $f_k(t,x(t)) = f_k(1,c_1)t^{k/\delta_2} + \text{старшие степени } t$. Таким образом, младший член ряда $F(t,x(t))$ равен $f_\gamma(1,c_1)t^{\gamma/\delta_2}$, и чтобы занулить его, следует положить c_1 равным одному из ненулевых корней многочлена $f_\gamma(1,x) \in \Bbbk[x]$. Каждому такому корню c_1 будет отвечать свой корень (4-29), начинающийся с $c_1 t^{\varepsilon_1}$.

[1] Обратите внимание, что показатели при x откладываются вдоль *горизонтальной* оси.

Упражнение 4.12. Убедитесь, что многочлен $f_\gamma(1,x)$ делится в $\Bbbk[x]$ на x^m, где m — абсцисса левого конца звена Z.

Для многочлена (4-30) это вычисление выглядит следующим образом. Выберем в качестве Z левое звено красной ломаной на рис. 4◇1. Его вектор нормали $(1,1)$, что даёт $\varepsilon_1 = 1$ и $\gamma = 3$. На звене Z лежат показатели мономов $-t^3$, $-2t^2x$ и $-tx^2$, откуда $f_3(1,x) = -1-2x-x^2 = -(x+1)^2$, что даёт единственно возможное $c_1 = -1$. Полностью разложение (4-31) многочлена (4-30) имеет вид

$$\begin{gathered} F(t,x) = f_3(t,x) + f_4(t,x) + f_5(t,x)\,,\ \text{где} \\ f_3(t,x) = -t^3 - 2t^2x - tx^2,\ f_4(t,x) = t^4,\ f_5(t,x) = 2tx^4 + x^5\,. \end{gathered} \tag{4-32}$$

На втором шаге метода Ньютона переменные t и x в $F(t,x)$ заменяются соответственно на t^{δ_2} и $t^{\delta_1}(c_1+x)$. Получающийся в результате такой замены многочлен $F(t^{\delta_2}, t^{\delta_1}(c_1+x))$ делится на t^γ и с полученным частным $F_2(t,x)$ проделываются те же вычисления, что производились на первом шагу с многочленом $F_1(t,x) = F(t,x)$. В результате получается вторая поправка ε_2 к показателю и второй коэффициент c_2 искомого ряда Пюизо, которые, вообще говоря, тоже можно выбирать по разному в виду произвола в выборе звена ломаной Ньютона многочлена $F_2(t,x)$ и произвола в выборе корня отвечающего этому звену многочлена $f_\gamma(1,x)$.

Так, для продолжения начатого нами вычисления корня многочлена (4-30) следует заменить в (4-32) переменную x на $t(x-1)$ и поделить результат на t^3. Получится многочлен

$$\begin{gathered} F_2(t,x) = f_3(1,(x-1)) + tf_4(1,(x-1)) + t^2f_5(1,(x-1)) = \\ = -x^2 + t + t^2\big(2(x-1)^4 + (x-1)^5\big) = \\ = (t+t^2) - 3t^2x + (-1+2t^2)\,x^2 + 2t^2x^3 - 3t^2x^4 + t^2x^5 \end{gathered}$$

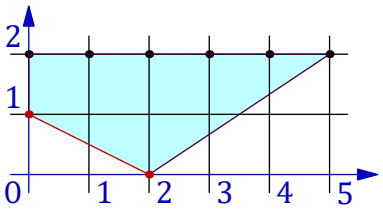


Рис. 4◇2.

с изображённым на рис. 4◇2 многоугольником Ньютона. Его ломаная Ньютона состоит из единственного звена с вектором нормали $(1,2)$, что даёт $\varepsilon_2 = 1/2$ и $\gamma = 2$. Перепишем многочлен $F_2(t,x)$ в виде

$$\begin{gathered} F_2(t,x) = f_2(t,x) + f_4(t,x) + f_5(t,x) + f_6(t,x) + f_7(t,x) + f_8(t,x) + f_9(t,x)\,,\quad \text{где} \\ f_2(t,x) = t - x^2,\ f_4(t,x) = t^2,\ f_5(t,x) = -3t^2x,\ f_6(t,x) = 2t^2x^2, \\ f_7(t,x) = 2t^2x^3,\ f_8(t,x) = -3t^2x^4,\ f_9(t,x) = t^2x^5. \end{gathered} \tag{4-33}$$

Двучлен $f_2(1,x) = 1 - x^2$ имеет два корня ±1. Положим $c_2 = 1$, заменим в (4-33) переменные t и x соответственно на t^2 и $t(x+1)$ и поделим результат на t^2. Получим следующий многочлен

$$\begin{gathered} F_3(t,x) = f_2(1,x) + t^2f_4(1,x) + t^3f_5(1,x) + t^4f_6(1,x) + t^5f_7(1,x) + t^6f_8(1,x) + t^7f_9(1,x) = \\ = -x^2 - 2x + t^2 - 3t^3(x+1) + 2t^4(x+1)^2 + 2t^5(x+1)^3 - 3t^6(x+1)^4 + t^7(x+1)^5 = \\ = (t^2 - 3t^3 + 2t^4 + 2t^5 - 3t^6 + t^7) + (-2 - 3t^3 + 4t^4 + 6t^5 + 5t^7 - 12t^6)\,x + \\ +(-1 + 2t^4 + 6t^5 - 18t^6 + 10t^7)\,x^2 + (2t^5 - 12t^6 + 10t^7)\,x^3 + (-3t^6 + 5t^7)\,x^4 + t^7x^5, \end{gathered}$$

ломаная Ньютона которого состоит из единственного звена с концами в точках $(0,2)$ и $(1,0)$.

Упражнение 4.13. Выведите отсюда, что и на всех последующих шагах ломаная Ньютона будет состоять из единственного звена, соединяющего точки вида $(0,m)$ и $(1,0)$, а значит, при $i \geqslant 3$ все $\varepsilon_i \in \mathbb{N}$.

Мы заключаем, что вычисляемый нами ряд Пюизо является степенным рядом от $t^{1/2}$. Записывая этот ряд с неопределёнными коэффициентами и подставляя его в F, получаем явные рекуррентные формулы для последовательного отыскания всех коэффициентов.

Упражнение 4.14. Выпишите эти рекуррентные формулы явно.

Упражнение 4.15. Убедитесь в том, что решение, отвечающее выбору $c_2 = -1$, тоже является степенным рядом от $t^{1/2}$.

Если на первом шаге вычисления корня многочлена (4-30) выбрать в качестве Z правое звено с вектором нормали $(1,3)$, то мы получим $\varepsilon_1 = 1/3$ и $\gamma = 5$. Отвечающие такому выбору коэффициенты c_1 являются корнями многочлена $f_5(1,x)/x^2 = -1 + x^3$, коих имеется три: 1, ω и ω^2, где $\omega \in \Bbbk$ — первообразный кубический корень из единицы. Положим $c_2 = \omega$ и заменим в

$$F_1(t,x) = (-t^3 + t^4) - 2t^2x - tx^2 + 2tx^4 + x^5 = f_5(t,x) + f_7(t,x) + f_9(t,x) + f_{12}(t,x), \text{ где}$$
$$f_5(t,x) = -tx^2 + x^5,\ f_7(t,x) = -2t^2x + 2tx^4,\ f_9(t,x) = -t^3,\ f_{12}(t,x) = t^4,$$

переменные t и x соответственно на t^3 и $t(x+\omega)$. Деля результат на t^5, получим

$$\begin{aligned} F_2(t,x) &= f_5(1,x+\omega) + t^2 f_7(1,x+\omega) + t^4 f_9(1,x+\omega) + t^7 f_{12}(1,x+\omega) = \\ &= (\omega+x)^2(3\omega^2x + 3\omega x^2 + x^3) - 2t^2(\omega+x)(3\omega^2x + 3\omega x^2 + x^3) - t^4 + t^7 = \\ &= (-t^4 + t^7) + (\omega + 6t^2)\,x + (9 + 12\omega^2t^2)\,x^2 + (10\omega^2 + 8\omega t^2)\,x^3 + (5\omega + 2t^2)\,x^4 + x^5. \end{aligned}$$

Ломаная Ньютона этого многочлена состоит из единственного звена, соединяющего точки $(0,4)$ и $(1,0)$. Согласно упр. 4.13 возникающий на этом пути ряд Пюизо будет степенным рядом от $t^{1/3}$, и его можно явно найти методом неопределённых коэффициентов.

Упражнение 4.16. Убедитесь, что ряды Пюизо, отвечающие $c_2 = 1, -\omega$ также являются степенными рядами от $t^{1/3}$.

Мы заключаем, что пять корней многочлена (4-30) суть два степенных ряда от $t^{1/2}$ с начальными членами $-t + t^{3/2} + \ldots$ и $-t - t^{3/2} + \ldots$, а также три степенных ряда от $t^{1/3}$ с начальными членами $t^{1/3} + \ldots$, $\omega t^{1/3} + \ldots$ и $\omega^2 t^{1/3} + \ldots$.

Вернёмся к общему случаю и покажем, что метод Ньютона действительно строит корень многочлена $F(t,x)$ в поле рядов Пюизо.

Предложение 4.4
Вычисленный методом Ньютона ряд (4-29):

$$x(t) = t^{\varepsilon_1}\Big(c_1 + t^{\varepsilon_2}\big(c_2 + t^{\varepsilon_3}(c_3 + \ldots)\big)\Big) = c_1 t^{\varepsilon_1} + c_2 t^{\varepsilon_1+\varepsilon_2} + c_3 t^{\varepsilon_1+\varepsilon_2+\varepsilon_3} + \ldots$$

является рядом Пюизо и корнем многочлена[1] $F(t,x)$.

Доказательство. Сначала убедимся, что показатели ряда $x(t)$ имеют общий знаменатель. Для этого достаточно проверить, что среди чисел ε_i имеется лишь конечное число дробных. Заметим, что знаменатель очередной поправки $\varepsilon_i = \delta_1/\delta_2$ не превосходит длины $\ell(Z_i)$ горизонтальной проекции выбранного для его вычисления ребра Z_i ломаной Ньютона многочлена $F_i(t,x)$,

[1] Отметим, что из это предложение даёт альтернативное доказательство лем. 4.5.

а степень многочлена $f_\gamma(1,x)/x^\lambda$, корнем которого является очередной коэффициент c_i, равна количеству отрезков, на которые звено Z_i разбивается лежащими на нём целыми точками, и тоже не превышает $\ell(Z_i)$. Если выбранный в качестве c_i корень имеет кратность d, т. е. $f_\gamma(1,x) = (x-c_1)^d g(x) x^m$, где m — абсцисса левого конца звена Z_i, а $g(c_1)\neq 0$, то многочлен

$$f_\gamma(t^{\delta_2}, t^{\delta_1}(c_1+x))/t^\gamma = c_1^m g(c_1) x^d + \text{старшие степени } x$$

содержит ненулевой член $g(c_1)c_1^m x^d$ с показателем $(d,0)$. Поэтому ломаная Ньютона возникающего на следующем шаге многочлена $F_{i+1} = F_i(t^{\delta_2}, t^{\delta_1}(c_1+x))/t^\gamma$ выйдет на горизонтальную ось не правее точки $(d,0)$, откуда длины горизонтальных проекций всех её рёбер не больше кратности d, которая в свою очередь, не больше $\ell(Z_i)$. Таким образом, $\ell(Z_{i+1}) \leqslant \ell(Z_i)$, и это неравенство нестрого, только если c_i является $\ell(Z_i)$-кратным корнем многочлена $f_\gamma(x,1)/x^m$ и степень этого многочлена тоже равна $\ell(Z_i)$. В этом случае $f_\gamma(x,1)/x^m = \alpha\cdot(x-c_i)^{\ell(Z_i)}$ с ненулевым $\alpha\in\Bbbk$, и абсциссы лежащих на ребре Z_i целых точек принимают все без исключения целые значения от m до $m+\ell(Z_i)$, что возможно только если вектор нормали ребру Z_i имеет вид $(\delta,1)$ с $\delta\in\mathbb{N}$, откуда $\varepsilon_{i+1} = \delta\in\mathbb{N}$. Таким образом, либо $\ell(Z_{i+1}) < \ell(Z_i)$, либо $\varepsilon_{i+1}\in\mathbb{N}$. Мы заключаем, что все ε_i станут целыми, начиная с некоторого номера, откуда получающийся на выходе ряд $x(t)$ будет рядом Пюизо.

Равенство $F(t,x(t)) = 0$ вытекает из этого по построению: на i-том шагу алгоритма Ньютона устанавливается, что степень младшего ненулевого члена ряда $F(t,x(t))$ не меньше суммы всех дробей γ/δ_2, возникших на первых i шагах. Поскольку все $\gamma\geqslant 1$, а знаменатели δ_2, начиная с некоторого шага, становятся единичными, эта сумма неограниченно растёт. □

Задачи для самостоятельного решения к §4

Задача 4.1. Чему равен коэффициент при $x_1^{\alpha_1}\dots x_m^{\alpha_m}$ у $(x_1+\dots+x_m)^n$? У какого из многочленов $(1+x^2-x^3)^{1000}$ или $(1-x^2+x^3)^{1000}$ больше коэффициент при x^{17}?

Задача 4.2. Найдите коэффициент при x^m у $\sum_{i=k}^n (1+x)^i$.

Задача 4.3. Пусть $(1+x+x^2)^n = \sum_{k\geqslant 0} a_k x^k$. Найдите: а) $a_0a_1 - a_1a_2 + a_2a_3 - \dots - a_{2n-1}a_{2n}$ б) $a_0^2 - a_1^2 + a_2^2 - \dots + (-1)^{n-1}a_{n-1}^2$ в) $\sum_{k\geqslant 0} a_{2k}$ г) $\sum_{k\geqslant 0} a_{2k+1}$.

Задача 4.4. Докажите для любого многочлена $f\in\Bbbk[x]$ степени $\deg f < n$ равенства:

а) $\dfrac{f(x)}{g(x)} = \sum_{i=1}^n \dfrac{f(\alpha_i)/g'(\alpha_i)}{x-\alpha_i}$, если $g(x) = (x-\alpha_1)\dots(x-\alpha_n)$ и все $\alpha_i\in\Bbbk$ различны

б) $\dfrac{f(x)}{(x-\alpha)^n} = \sum_{i=0}^{n-1} \dfrac{f^{(i)}(\alpha)/i!}{(x-\alpha)^{n-i}}$, где $f^{(i)} = \left(\dfrac{d}{dx}\right)^i f$.

Задача 4.5. Разложите на простейшие дроби следующие рациональные функции:
а) $(3x^2+x+1)/(-6x^3-7x^2+1)$ б) $(x^4+1)/(x^2+x-6)$ в) $(x^3-1)/(x^4-4x+6x^2-4x^3+1)$.

Задача 4.6. Пусть $g(x) = \prod(x-\alpha_i)$, где все α_i попарно различны. Покажите, что для любого $f\in\Bbbk[x]$ с $\deg f < \deg g$ разложение рациональной функции f/g в сумму простейших дробей из предл. 4.1 имеет вид:

$$\frac{f}{g} = \sum \frac{f(\alpha_i)/g'(\alpha_i)}{(x-\alpha_i)}$$

где g' — производная от g.

Задача 4.7 (формула Тейлора). Покажите, что над любым полем $\Bbbk$ характеристики нуль для произвольно заданных точки $a \in \Bbbk$ и $n+1$ значений $b_0, b_1, \dots, b_n \in \Bbbk$ существует единственный такой многочлен $f \in \Bbbk[x]$ степени $\deg f \leqslant n$, что $f(a) = b_0$ и $(d/dx)^i f(a) = b_i$ при всех $i = 1, \dots, n$. Напишите для него явную формулу.

Задача 4.8. Явно разложите в ряды в $\mathbb{Q}[\![x]\!]$ все дроби из зад. 4.5, а также функции:
а) $1/(1+x+x^2)$ б) $1/(1+x+x^2)^2$ в) $1/(2x^2-3x+1)$ г) $1/(x^4+2x^3-7x^2-20x-12)$
д) $\sqrt[3]{1+2x}$ е) $1/\sqrt{1-3x}$ ж) $\cos x \stackrel{\text{def}}{=} (e^{ix}+e^{-ix})/2$ з) $\sin x \stackrel{\text{def}}{=} (e^{ix}-e^{-ix})/(2i)$
и) $\operatorname{ch} x \stackrel{\text{def}}{=} (e^x+e^{-x})/2$ к) $\operatorname{sh} x \stackrel{\text{def}}{=} (e^x-e^{-x})/2$.

Задача 4.9. Найдите первообразную и 1000-ю производную от $x^4/(1+x^2)$.

Задача 4.10. Найдите k-тый член последовательности a_k, если:
а) $a_0 = 1$, $a_1 = -1$ и $a_k = 2a_{k-1} - a_{k-2}$ при $k \geqslant 2$
б) $a_0 = 1$, $a_1 = -7$ и $a_k = 5a_{k-1} - 6a_{k-2}$ при $k \geqslant 2$
в) $a_0 = 2$, $a_1 = 4$ и $a_k = 4a_{k-1} - 4a_{k-2}$ при $k \geqslant 2$
г) $a_0 = -1/4$, $a_1 = -1/2$ и $a_k = -a_{k-1} - a_{k-2}$ при $k \geqslant 2$
д) $a_0 = 1$, $a_1 = -3$, $a_2 = -29$ и $a_k = 9a_{k-1} - 26a_{k-2} + 24a_{k-3}$ при $k \geqslant 3$.

Задача 4.11. Пользуясь разложениями $(1-x)^{\pm 1/2}$ в $\mathbb{Q}[\![x]\!]$, вычислите:
а) $\binom{2k}{k} + \binom{2}{1}\binom{2k-2}{k-1} + \binom{4}{2}\binom{2k-4}{k-2} + \dots + \binom{2k-2}{k-1}\binom{2}{1} + \binom{2k}{k}$
б) $\binom{2k-2}{k-1} + \frac{1}{2}\binom{2}{1}\binom{2k-4}{k-2} + \frac{1}{3}\binom{4}{2}\binom{2k-6}{k-3} + \dots + \frac{1}{k-1}\binom{2k-4}{k-2}\binom{2}{1} + \frac{1}{k}\binom{2k-2}{k-1}$
в) $\frac{2^{2k-1}}{1} - \frac{2^{2k-3}}{2}\binom{2}{1} - \frac{2^{2k-5}}{3}\binom{4}{2} - \dots - \frac{2}{k}\binom{2k-2}{k-1}$
г) $\frac{1}{1\cdot(k-1)}\binom{2k-4}{k-2} + \frac{1}{2\cdot(k-2)}\binom{2}{1}\binom{2k-6}{k-3} + \frac{1}{3\cdot(k-3)}\binom{4}{2}\binom{2k-8}{k-4} + \dots$
$\dots + \frac{1}{(k-2)\cdot 2}\binom{2k-6}{k-3}\binom{2}{1} + \frac{1}{(k-1)\cdot 1}\binom{2k-4}{k-2}$

Задача 4.12. Для всех $m, n \in \mathbb{N}$ вычислите $\sum_{k\geqslant 0}(-1)^k\binom{m}{k}\binom{k}{n}$.

Задача 4.13*. Лежат ли ряды а) e^x б) $\ln(1+x)$ в) $\sqrt{1+x}$ в подполе $\mathbb{Q}(x) \subset \mathbb{Q}(\!(x)\!)$?

Задача 4.14. Является ли рациональной функцией ряд $\sum_{n\geqslant 0}(-n^3-9n^2-19n-16)\cdot x^n$? Если да, явно запишите его несократимой дробью p/q с $p, q \in \mathbb{Z}[x]$, если нет, объясните, почему.

Задача 4.15. Напишите степенной ряд, который не является рациональной функцией и все ненулевые коэффициенты которого равны 1.

Задача 4.16. Обозначим через $p_m(n)$ число n-клеточных диаграмм Юнга из не более m строк и пусть $p(0) \stackrel{\text{def}}{=} 1$. Выразите $p_m(n)$ через $p_{m-1}(n)$ и $p_m(n-m)$ и покажите, что производящая функция $P_m(t) = \sum_{n\geqslant 0} p_m(n)\, t^n$ лежит в $\mathbb{Q}(t)$.

Задача 4.17 (теорема Эйлера о пятиугольных числах). Обозначим через $p(n)$ число всех диаграмм Юнга веса[1] n, а через $\hat{p}_{\text{ч}}(n)$ и $\hat{p}_{\text{н}}(n)$ — количества таких диаграмм Юнга веса n, у которых длины всех строк различны и которые состоят, соответственно, из чётного и нечётного количества строк. Положим $p(0) \stackrel{\text{def}}{=} 1$ и образуем производящую функцию

$$P(t) = \sum_{n\geqslant 0} p(n)t^n \in \mathbb{Q}[\![t]\!]\,.$$

[1] число $p(n)$ также называется *числом разбиений* числа n

Докажите равенства

$$P(t) = \prod_{k\geqslant 1}(1-t^k)^{-1}$$

$$\frac{1}{P(t)} = 1 + \sum_{n\geqslant 1}\left(\hat{p}_{\text{ч}}(n) - \hat{p}_{\text{н}}(n)\right)\cdot t^n$$

$$p(n) = \sum_{k\geqslant 1}(-1)^{k+1}\left(p\left(n-\frac{3k^2-k}{2}\right)+p\left(n-\frac{3k^2+k}{2}\right)\right) =$$

$$= p(n-1)+p(n-2)-p(n-5)-p(n-7)+p(n-12)+p(n-15)-\ldots$$

и вычислите $p(10)$.

Задача 4.18. В выпуклом n угольнике проводят максимально возможное число диагоналей так, чтобы они не пересекались нигде, кроме вершин. Сколькими способами это можно сделать?

Задача 4.19. Докажите, что у ряда $\operatorname{td}(-t) = t/(e^t-1) = \sum_{k\geqslant 0} b_k t^k/k! \in \mathbb{Q}[\![x]\!]$ коэффициенты b_{2n} знакопеременны, а $b_{2n+1} = 0$ при $n \geqslant 1$.

Задача 4.20*. Выразите через числа b_k из предыдущей задачи коэффициенты рядов
а) $(t/2)\cdot\operatorname{cth}(t/2)$, где $\operatorname{cth} t \stackrel{\text{def}}{=} \operatorname{ch} t/\operatorname{sh} t = (e^t+e^{-t})/(e^t-e^{-t})$ б) $(t/2)\cdot\operatorname{ctg}(t/2)$ в) $(t/2)\cdot\operatorname{tg}(t/2)$.

Задача 4.21*. Убедитесь, что ряд $\operatorname{tg}(t) = \sin(t)/\cos(t) = -i(e^{it}-e^{-it})/(e^{it}+e^{-it}) \in \mathbb{C}[\![x]\!]$ имеет рациональные коэффициенты. Есть ли среди них отрицательные?

Задача 4.22. Найдите первую дюжину коэффициентов ряда Тодда $\operatorname{td}(x) = x/(1-e^{-x})$ и вычислите $\operatorname{td}(x) - \operatorname{td}(-x)$.

Задача 4.23. Найдите $\operatorname{td}(d/dx)\,x^n$ и $\sum_{k=0}^m k^n$ для всех $0 \leqslant n \leqslant 6$.

Задача 4.24. Пусть $\nabla\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$, $f(x) \mapsto f(x) - f(x-1)$. Покажите, что для любого степенного ряда $\psi(t) \in \mathbb{Q}[\![t]\!]$ корректно определено линейное отображение $\psi(\nabla)\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$, и укажите такой ряд φ, что $\varphi(\nabla) = d/dx$. Много ли таких φ?

Задача 4.25. Покажите, что следующие свойства линейного отображения $F\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$ эквивалентны: а) F перестановочно с d/dx б) F перестановочно с ∇
в) $F = \varphi(d/dx)$ для некоторого $\varphi(t) \in \mathbb{Q}[\![t]\!]$ г) $F = \psi(\nabla)$ для некоторого $\psi(t) \in \mathbb{Q}[\![t]\!]$
д) F перестановочно со сдвигом $T_1\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$, $f(x) \mapsto f(x+1)$
е) F перестановочно со всеми сдвигами $T_\alpha\colon f(x) \mapsto f(x+\alpha)$, где $\alpha \in \mathbb{Q}$.

Задача 4.26. Верно ли, что любые два коммутирующих со сдвигами линейных отображения $\mathbb{Q}[x] \to \mathbb{Q}[x]$ коммутируют между собой?

Задача 4.27. Пусть $\varphi(t) = \sum_{k\geqslant 0}\varphi_k t^k/k! \in \mathbb{Q}[\![t]\!]$. Образ базисного монома $x^m \in \mathbb{Q}[x]$ под действием оператора $\varphi(d/dx)\colon \mathbb{Q}[x] \to \mathbb{Q}[x]$ называется m-м *многочленом Аппеля*[1] ряда φ и обозначается $f_m(x) = \varphi(d/dx)\,x^m$. Покажите, что при всех целых $n \geqslant 0$:
а) $\varphi_n = f_n(0)$
б) $f_n'(x) = nf_{n-1}(x)$
в) $f_n(x+y) = \sum_{k=0}^n \binom{n}{k} f_{n-k}(x)y^k$
г) $f_n(x) = \sum_{k=0}^n \binom{n}{k}\varphi_{n-k}x^k = (\varphi^{\downarrow}+x)^n$, где стрелка у $\varphi^{\downarrow}$ предписывает раскрывать бином $(\varphi+x)^n$ заменяя все φ^k на φ_k.

[1] Многочлены f_k называются *многочленами Аппеля* ряда φ, ср. с прим. 4.9 на стр. 72.

Задача 4.28. Найдите по три ненулевых начальных члена разложений Пюизо каждого из корней $x(t)$ многочленов

а) $(t^7 + t^6) - t^3\,x + t\,x^2 - x^3$

б) $t^3 + (-t + t^2)\,x + x^3$

в) $t^4 - t^3\,x + 3t^2\,x^3 - 3t\,x^5 + x^7$

г) $(t^2 + 4t^3 + 6t^4) - 4t^4\,x + (-2t - 4t^2 - 2t^3)\,x^2 + x^4$

д) $2t^5 - t^3\,x + 2t^2\,x^2 - t\,x^3 + 2x^5$

и нарисуйте все встречающиеся по ходу дела многоугольники Ньютона.

§5. Идеалы, фактор кольца и разложение на множители

5.1. Идеалы. Подкольцо I коммутативного кольца K называется *идеалом*, если вместе с каждым своим элементом оно содержит и все его кратные. В n° 2.5.3 мы видели, что этим свойством обладает ядро любого гомоморфизма колец. Множество всех элементов кольца, кратных фиксированному элементу $a \in K$, также является идеалом. Этот идеал обозначается

$$(a) = \{ka \mid k \in K\}, \tag{5-1}$$

и называется *главным* идеалом, порождённым a. Мы встречались с главными идеалами при построении колец вычетов[1] $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$, где они возникали как ядра гомоморфизмов факторизации $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n), m \mapsto [m]_n$, и $\Bbbk[x] \twoheadrightarrow \Bbbk[x]/(f), g \mapsto [g]_f$, которые сопоставляют целому числу (соотв. многочлену) его класс вычетов. Среди главных идеалов имеются *тривиальный* идеал (0), состоящий только из нулевого элемента, и *несобственный* идеал (1), совпадающий со всем кольцом. Идеалы, отличные от всего кольца, называются *собственными*.

Упражнение 5.1. Покажите, что следующие условия на идеал I в коммутативном кольце K с единицей эквивалентны: а) $I = K$ б) $1 \in I$ в) I содержит обратимый элемент.

Предложение 5.1
Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных собственных идеалов.

Доказательство. Из упр. 5.1 вытекает, что в поле таких идеалов нет. Наоборот, если в кольце нет нетривиальных собственных идеалов, то главный идеал (b), состоящий из всех кратных произвольно взятого элемента $b \neq 0$, совпадает со всем кольцом. В частности, он содержит единицу, т. е. $1 = ab$ для некоторого a. Тем самым, любой ненулевой элемент b обратим. □

5.1.1. Нётеровость. Любое подмножество $M \subset K$ порождает идеал $(M) \subset K$, состоящий из всех элементов кольца K, представимых в виде $b_1a_1 + \ldots + b_ma_m$, где $a_1, \ldots, a_m$ — произвольные элементы множества M, а $b_1, \ldots, b_m$ — произвольные элементы кольца K, и число слагаемых $m \in \mathbb{N}$ также произвольно.

Упражнение 5.2. Убедитесь, что $(M) \subset K$ это и в самом деле идеал, совпадающий с пересечением всех идеалов, содержащих множество M.

Любой идеал $I \subset K$ имеет вид (M) для подходящего множества образующих $M \subseteq I$: например, всегда можно положить $M = I$. Идеалы $I = (a_1, \ldots, a_k) = \{b_1a_1 + \ldots + b_ka_k \mid b_i \in K\}$, допускающие конечное множество образующих, называются *конечно порождёнными*. Мы встречались с такими идеалами, когда доказывали существование наибольшего общего делителя в кольцах целых чисел и многочленов с коэффициентами в поле.

Лемма 5.1
Следующие свойства коммутативного кольца K попарно эквивалентны:

1) любое подмножество $M \subset K$ содержит конечный набор элементов, порождающий тот же идеал, что и M

2) любой идеал $I \subset K$ конечно порождён

[1] См. n° 2.4 на стр. 30 и n° 3.3.1 на стр. 48.

3) любая бесконечная возрастающая цепочка вложенных идеалов $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ в K стабилизируется в том смысле, что найдётся такое $n \in \mathbb{N}$, что $I_\nu = I_n$ для всех $\nu \geqslant n$.

Доказательство. Ясно, что (1) влечёт (2). Чтобы получить (3) из (2), заметим, что объединение $I = \bigcup I_\nu$ всех идеалов цепочки тоже является идеалом. Согласно (2), идеал I порождён конечным набором элементов. Все они принадлежат некоторому идеалу I_n. Тогда $I_n = I = I_\nu$ при $\nu \geqslant n$. Чтобы вывести (1) из (3), будем по индукции строить цепочку идеалов $I_n = (a_1, \ldots, a_n)$, начав с произвольного элемента $a_1 \in M$ и добавляя на k-том шагу очередную образующую $a_k \in M \setminus I_{k-1}$ до тех пор, пока это возможно, т. е. пока $M \not\subset I_k$. Так как $I_{k-1} \subsetneq I_k$, этот процесс не может продолжаться бесконечно, и на каком-то шагу мы получим идеал, содержащий всё множество M, а значит, совпадающий с (M). □

Определение 5.1
Кольцо K, удовлетворяющее условиям лем. 5.1, называется *нётеровым*. Отметим, что любое поле нётерово.

Теорема 5.1 (теорема Гильберта о базисе идеала)
Если кольцо K нётерово, то кольцо многочленов $K[x]$ также нётерово.

Доказательство. Рассмотрим произвольный идеал $I \subset K[x]$ и обозначим через $L_d \subset K$ множество старших коэффициентов всех многочленов степени не выше d из I, а через $L_\infty = \bigcup_d L_d$ — множество старших коэффициентов вообще всех многочленов из I.

Упражнение 5.3. Убедитесь, что все L_d (включая L_∞) являются идеалами в K.

Поскольку кольцо K нётерово, все идеалы L_d конечно порождены. Для каждого d (включая $d = \infty$) обозначим через $f_1^{(d)}, \ldots, f_{m_d}^{(d)} \in K[x]$ многочлены, старшие коэффициенты которых порождают соответствующий идеал $L_d \subset K$. Пусть наибольшая из степеней многочленов $f_i^{(\infty)}$, старшие коэффициенты которых порождают идеал L_∞, равна D. Покажем, что идеал I порождается многочленами $f_i^{(\infty)}$ и $f_j^{(d)}$ с $d < D$.

Каждый многочлен $g \in I$ сравним по модулю многочленов $f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)}$ с многочленом, степень которого строго меньше D. В самом деле, поскольку старший коэффициент многочлена g лежит в идеале L_∞, он имеет вид $\sum \lambda_i a_i$, где $\lambda_i \in K$, а a_i — старшие коэффициенты многочленов $f_i^{(\infty)}$. При $\deg g \geqslant D$ все разности $\delta_i = \deg g - \deg f_i^{(\infty)} \geqslant 0$, и можно образовать многочлен $h = g - \sum \lambda_i \cdot f_i^{(\infty)}(x) \cdot x_i^{\delta_i}$, сравнимый с g по модулю I и имеющий $\deg h < \deg g$. Заменяем g на h и повторяем процедуру, пока не получим многочлен $h \equiv g \pmod{(f_1^{(\infty)}, \ldots, f_{m_\infty}^{(\infty)})}$ с $\deg h < D$. Теперь старший коэффициент многочлена h лежит в идеале L_d с $d < D$, и мы можем строго уменьшать его степень, тем же способом сокращая старший член путём вычитания из h подходящих комбинаций многочленов $f_j^{(d)}$ с $0 \leqslant d < D$. □

Следствие 5.1
Если K нётерово, то кольцо многочленов $K[x_1, \ldots, x_n]$ также нётерово. □

Упражнение 5.4. Покажите, что кольцо формальных степенных рядов над нётеровым кольцом нётерово.

Следствие 5.2
Любая система полиномиальных уравнений с коэффициентами в нётеровом кольце эквивалентна некоторой конечной своей подсистеме.

Доказательство. Если кольцо K нётерово, то кольцо $K[x_1,\dots,x_n]$ тоже нётерово, и в любом множестве многочленов $M \subset K[x_1,\dots,x_n]$ можно указать такой конечный набор многочленов $f_1,\dots,f_m \in M$, что каждый многочлен $g \in M$ представляется в виде $g = h_1f_1 + \dots + h_mf_m$ для некоторых $h_i \in K[x_1,\dots,x_n]$. Поэтому любое уравнение вида $g(x_1,\dots,x_n) = 0$ с $g \in M$ является следствием m уравнений $f_1(x_1,\dots,x_n) = \dots = f_m(x_1,\dots,x_n) = 0$. □

5.1.2. Примеры ненётеровых колец. Кольцо многочленов от счётного множества переменных $\mathbb{Q}[x_1, x_2, x_3, \dots]$, элементы которого суть конечные линейные комбинации с рациональными коэффициентами всевозможных мономов вида $x_{\nu_1}^{m_1}x_{\nu_2}^{m_2}\dots x_{\nu_s}^{m_s}$ не является нётеровым: его идеал $(x_1, x_2, \dots)$, состоящий из всех многочленов без свободного члена, нельзя породить конечным множеством многочленов.

Упражнение 5.5. Докажите это и выясните, является ли конечно порождённым идеал, образованный в кольце бесконечно гладких функций $\mathbb{R} \to \mathbb{R}$ всеми функциями, которые обращаются в нуле в нуль вместе со всеми своими производными.

Предостережение 5.1. Подкольцо нётерова кольца может не быть нётеровым. Например, кольцо формальных степенных рядов $\mathbb{C}[\![z]\!]$ нётерово по упр. 5.4, тогда как его подкольцо образованное рядами, сходящимися всюду в $\mathbb{C}$, нётеровым не является.

Упражнение 5.6. Приведите пример бесконечной возрастающей цепочки строго вложенных идеалов в кольце сходящихся всюду в $\mathbb{C}$ степенных рядов из $\mathbb{C}[\![x]\!]$.

5.2. Фактор кольца. Пусть на коммутативном кольце K задано отношение эквивалентности, разбивающее K в дизъюнктное объединение классов эквивалентных элементов. Обозначим множество классов через X и рассмотрим сюръективное отображение факторизации

$$\pi : K \twoheadrightarrow X, \quad a \mapsto [a], \tag{5-2}$$

переводящее элемент $a \in K$ в его класс эквивалентности $[a] \subset K$, являющийся элементом множества X. Мы хотим задать на множестве X структуру коммутативного кольца, определив сложение и умножение теми же сами правилами

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab], \tag{5-3}$$

которые мы использовали в кольцах вычетов. Если эти правила корректны, то аксиомы коммутативного кольца в X будут автоматически выполнены, как и для колец вычетов, поскольку формулы (5-3) сводят их проверку к проверке аксиом коммутативного кольца в K. В частности, нулевым элементом кольца X будет класс $[0]$. С другой стороны, если формулы (5-3) корректны, то они утверждают, что отображение (5-2) является гомоморфизмом колец. Но если это так, то согласно n° 2.5.3 на стр. 33 класс нуля $[0] = \ker\pi$, служащий ядром этого гомоморфизма, является идеалом в K, а класс $[a] \subset K$ произвольного элемента $a \in K$, служащий прообразом точки $[a] \in X$ при гомоморфизме (5-2), является аддитивным сдвигом ядра на элемент a:

$$[a] = \pi^{-1}(\pi(a)) = a + \ker\pi = a + [0] = \{a + b \mid b \in [0]\}.$$

Оказывается, что этих необходимых условий на классы также и достаточно для того, чтобы правила (5-3) были корректны, т. е. для любого идеала $I \subset K$ множество классов

$$[a]_I = a + I \stackrel{\text{def}}{=} \{a + b \mid b \in I\} \tag{5-4}$$

образует разбиение кольца K, и правила (5-3) корректно определяют на классах этого разбиения структуру коммутативного кольца с нулевым элементом $[0]_I = I$.

Упражнение 5.7. Убедитесь, что отношение сравнимости по модулю идеала $a_1 \equiv a_2 \pmod I$, означающее, что $a_1 - a_2 \in I$, является отношением эквивалентности, и проверьте, что формулы (5-3) корректны.

Определение 5.2
Классы эквивалентности (5-4) называются *классами вычетов* (или *смежными классами*) по модулю идеала I. Множество этих классов с операциями (5-3) называется *фактор кольцом* кольца K по идеалу I и обозначается K/I. Эпиморфизм $K \twoheadrightarrow K/I$, $a \mapsto [a]_I$, сопоставляющий каждому элементу кольца его класс вычетов, называется *гомоморфизмом факторизации*.

Пример 5.1 (кольца вычетов)
Рассматривавшиеся выше кольца $\mathbb{Z}/(n)$ и $\Bbbk[x]/(f)$ суть фактор кольца кольца целых числел и кольца многочленов по главным идеалам $(n) \subset \mathbb{Z}$ и $(f) \subset \Bbbk[x]$ соответственно.

Пример 5.2 (образ гомоморфизма)
Согласно n° 2.5.3, для любого гомоморфизма коммутативных колец $\varphi : A \to B$ имеется канонический изоморфизм колец $\overline{\varphi} : A/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$, $[a]_{\ker\varphi} \mapsto \varphi(a)$, переводящий каждый класс

$$[a]_{\ker\varphi} = a + \ker\varphi = \varphi^{-1}(\varphi(a))$$

в его образ $\varphi(a) = \varphi([a])$ при гомоморфизме φ.

Пример 5.3 (максимальные идеалы и гомоморфизмы вычисления)
Идеал $\mathfrak{m} \subset K$ называется *максимальным*, если фактор кольцо $K/\mathfrak{m}$ является полем. Название связано с тем, что собственный[1] идеал $\mathfrak{m} \subset K$ максимален если и только если он не содержится ни в каком строго большем собственном идеале, т. е. является максимальным элементом в чуме[2] собственных идеалов кольца K, частично упорядоченных по включению. В самом деле, обратимость всех ненулевых классов $[a]_\mathfrak{m}$ в фактор кольце $K/\mathfrak{m}$ означает, что для любого $a \notin \mathfrak{m}$ найдутся такие $b \in K$, $m \in \mathfrak{m}$, что $ab + m = 1$ в K. Последнее равносильно тому, что идеал $(\mathfrak{m}, a) \supsetneq \mathfrak{m}$, порождённый $\mathfrak{m}$ и элементом $a \notin \mathfrak{m}$, содержит 1 и совпадает с K, т. е. что идеал $\mathfrak{m}$ не содержится ни в каком строго большем собственном идеале.

Покажем, что любой собственный идеал произвольного коммутативного кольца с единицей содержится в некотором максимальном идеале. В самом деле, множество всех собственных идеалов, содержащих данный идеал $I \subset K$, тоже составляет чум по включению.

Упражнение 5.8. Убедитесь, что он полный, т. е. для любого линейно упорядоченного множества[3] M содержащих I собственных идеалов в K существует собственный идеал J^*, содержащий все идеалы из M.

По лемме Цорна[4] существует такой собственный идеал $\mathfrak{m} \supset I$, который не содержится ни в каком большем собственном идеале, содержащем I. Идеал $\mathfrak{m}$ автоматически максимален по включению и в чуме всех собственных идеалов кольца K.

[1] Т. е. отличный от всего кольца.
[2] См. n° 1.7 на стр. 17.
[3] В данном случае это означает, что для любых $J_1, J_2 \in M$ выполняется включение $J_1 \subseteq J_2$ или включение $J_2 \subseteq J_1$.
[4] См. сл. 1.1 на стр. 20.

Максимальные идеалы возникают в кольцах функций как ядра *гомоморфизмов вычисления*. А именно, пусть X — произвольное множество, $\Bbbk$ — любое поле, а K — подкольцо в кольце всех функций $X \to \Bbbk$, содержащее тождественно единичную функцию 1 и вместе с каждой функцией $f \in K$ содержащее и все пропорциональные ей функции cf, $c \in \Bbbk$. Для любой точки $p \in X$ гомоморфизм вычисления[1] $\mathrm{ev}_p : K \to \Bbbk$ переводит функцию $f \in K$ в её значение $f(p) \in \Bbbk$. В силу сделанных предположений о кольце K он сюръективен, и его ядро $\ker \mathrm{ev}_p = \{f \in K \mid f(p) = 0\}$ является максимальным идеалом в K.

Упражнение 5.9. Убедитесь, что: а) каждый максимальный идеал кольца $\mathbb{C}[x]$ имеет вид $\ker \mathrm{ev}_p$ для некоторого $p \in \mathbb{C}$ б) в кольце непрерывных функций $[0,1] \to \mathbb{R}$ каждый максимальный идеал имеет вид $\ker \mathrm{ev}_p$ для некоторой точки $p \in [0,1]$. в) Укажите в кольце $\mathbb{R}[x]$ максимальный идеал, отличный от всех идеалов вида $\ker \mathrm{ev}_p$, где $p \in \mathbb{R}$.

Пример 5.4 (простые идеалы и гомоморфизмы в поля)
Идеал $\mathfrak{p} \subset K$ называется *простым*, если в факторкольце $K/\mathfrak{p}$ нет делителей нуля. Иначе говоря, идеал $\mathfrak{p} \subset K$ прост если и только если из $ab \in \mathfrak{p}$ вытекает, что $a \in \mathfrak{p}$ или $b \in \mathfrak{p}$. Например, главные идеалы $(p) \subset \mathbb{Z}$ и $(q) \subset \Bbbk[x]$, где $\Bbbk$ — поле, просты тогда и только тогда, когда число p просто, а многочлен q неприводим.

Упражнение 5.10. Убедитесь в этом.

Согласно определениям, всякий максимальный идеал прост. Обратное неверно: скажем, главный идеал $(x) \subset \mathbb{Q}[x,y]$ прост, так как кольцо $\mathbb{Q}[x,y]/(x) \simeq \mathbb{Q}[y]$ целостное, но не максимален, поскольку строго содержится в идеале (x,y) многочленов без свободного члена[2]. Простые идеалы кольца K являются ядрами гомоморфизмов из кольца K во всевозможные поля. В самом деле, образ любого такого гомоморфизма, будучи подкольцом в поле, не имеет делителей нуля, и стало быть ядро любого такого гомоморфизма является простым идеалом. Наоборот, факторкольцо $K/\mathfrak{p}$ по простому идеалу $\mathfrak{p} \subset K$ является подкольцом своего поля частных $Q_{K/\mathfrak{p}}$, и композиция факторизации и вложения $K \twoheadrightarrow K/\mathfrak{p} \hookrightarrow Q_{K/\mathfrak{p}}$ задаёт гомоморфизм из K в поле $Q_{K/\mathfrak{p}}$ с ядром $\mathfrak{p}$.

Упражнение 5.11. Убедитесь, что пересечение конечного множества идеалов содержится в простом идеале $\mathfrak{p}$ только если хотя бы один из пересекаемых идеалов содержится в $\mathfrak{p}$.

Пример 5.5 (конечно порождённые коммутативные алгебры)
Пусть K — произвольное коммутативное кольцо с единицей. Всякое кольцо вида

$$A = K[x_1, \dots, x_n]/I\,,$$

где $I \subset K[x_1, \dots, x_n]$ — произвольный идеал, называется *конечно порождённой K-алгеброй*[3]. Классы $a_i = [x_i]_I$ называются *образующими* K-алгебры A, а многочлены $f \in I$ — *алгебраическими соотношениями* между этими образующими. Говоря неформально, K-алгебра состоит из всевозможных выражений, которые можно составить из элементов кольца K и коммутирующих букв $a_1, \dots, a_n$ при помощи операций сложения и умножения, производимых с учётом полиномиальных соотношений $f(a_1, \dots, a_n) = 0$ для всех f из I. Из сл. 5.1 и идущего следом упр. 5.12:

[1] Обозначение ev происходит от «*evaluation*».

[2] Т. е. в ядре гомоморфизма вычисления в нуле: $\mathrm{ev}_{(0,0)} : \mathbb{Q}[x,y] \twoheadrightarrow \mathbb{Q}$, $f(x,y) \mapsto f(0,0)$.

[3] Или, более торжественно, *конечно порождённой коммутативной алгеброй* над кольцом K.

Упражнение 5.12. Покажите, что факторкольцо нётерова кольца тоже нётерово.

мы получаем

Следствие 5.3
Всякая конечно порождённая коммутативная алгебра над нётеровым коммутативным кольцом нётерова, и все соотношения между её образующими являются следствиями конечного числа соотношений. □

5.3. Кольца главных идеалов. Целостное кольцо с единицей называется *областью главных идеалов*, если каждый его идеал является главным. Наблюдавшийся нами в §§ 1, 2 параллелизм между кольцами $\mathbb{Z}$ и $\Bbbk[x]$, где $\Bbbk$ — поле, объясняется тем, что оба кольца являются областями главных идеалов. Мы фактически установили это[1] при описании наибольших общих делителей, ключевым моментом в котором была возможность *деления с остатком*.

5.3.1. Евклидовы кольца. Целостное кольцо K с единицей называется *евклидовым*, если на нём можно задать *функцию высоты* $\nu\colon K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\}$ со свойствами:

1) $\nu(a) = 0 \iff a = 0$

2) для любых ненулевых $a, b \in K$ найдётся такое $q \in K$, что $\nu(a - bq) < \nu(b)$.

Удовлетворяющее второму свойству число q называются *неполным частным*, а разность $r = a - bq$ — *остатком* от деления a на b относительно высоты ν. Подчеркнём, что никакой их единственности для заданных a, b не предполагается.

Упражнение 5.13. Докажите евклидовость колец: а) $\mathbb{Z}$ с $\nu(z) = |z|$ б) $\Bbbk[x]$ с $\nu(f) = \deg f + 1$
в) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mid a, b \in \mathbb{Z},\ i^2 = -1\}$ с $\nu(z) = |z|^2$
г) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\ \}$ с $\nu(z) = |z|^2$.

Предложение 5.2
Каждое евклидово кольцо является областью главных идеалов.

Доказательство. В любом идеале I евклидова кольца K имеется ненулевой элемент $d \in I$ наименьшей в I высоты. Поскольку для любого $a \in I$ найдётся такое $q \in K$, что $\nu(a - dq) < \nu(d)$, и при этом $a - dq \in I$, мы заключаем, что $a - dq = 0$, т. е. $a \vdots d$. Поэтому $I = (d)$. □

Определение 5.3
Функция высоты $\nu\colon K \to \mathbb{Z}_{\geqslant 0}$ называется *приведённой*, если $\nu(ab) \geqslant \nu(a)$ для всех ненулевых $a, b \in K$.

Предложение 5.3
На любом евклидовом кольце K существует приведённая функция высоты.

Доказательство. Для произвольной высоты ν' и каждого ненулевого $a \in K$ положим

$$\nu(a) = \min_{x \in K^\times} \nu'(ax)\,.$$

[1] См. n° 2.2.1 на стр. 26 и предл. 3.3 на стр. 45.

Очевидно, что $\nu(ab) \geqslant \nu(a)$ для всех ненулевых $a, b \in K$. Пусть $\nu(b) = \nu'(bc)$ для ненулевого $c \in K$. Поскольку существует такое $q \in K$, что $\nu'(ac - bcq) < \nu'(bc)$, мы заключаем, что

$$\nu(a - bq) \leqslant \nu'\big((a - bq)c\big) < \nu'(bc) = \nu(b)\,.$$

Тем самым ν тоже является функцией высоты. □

Упражнение 5.14. Покажите, что в евклидовом кольце с приведённой высотой ν равенство $\nu(ab) = \nu(a)$ для ненулевых a, b равносильно тому, что b обратим.

Предостережение 5.2. Существуют области главных идеалов, которые не являются евклидовыми кольцами. Например, таковым является кольцо всех чисел вида $a + b\zeta \in \mathbb{C}$, где $a, b \in \mathbb{Z}$, а $\zeta = (1+\sqrt{-19})/2$, см. зад. 5.12 на стр. 99. В прим. 5.6 на стр. 93 будет дана характеризация областей главных идеалов в терминах высот, обладающих более слабым свойством, чем евклидова высота.

5.3.2. НОД и взаимная простота. В кольце главных идеалов K идеал

$$(a_1, \ldots, a_n) = \{x_1a_1 + \ldots + x_na_n \mid x_i \in K\}\,,$$

порождённый любым набором элементов $a_1, \ldots, a_n$, является главным и имеет вид (d) для некоторого $d \in K$. Таким образом, элемент d представляется в виде $d = a_1b_1 + \ldots + a_nb_n$, где $b_i \in K$, делит все элементы a_i и делится на любой общий делитель элементов a_i, т. е. является *наибольшим общим делителем*[1] элементов $a_1, \ldots, a_n$. Отметим, что наибольший общий делитель определён не однозначно, а с точностью до умножения на произвольный обратимый элемент из K.

Упражнение 5.15. Убедитесь, что в любом целостном коммутативном кольце K главные идеалы (a) и (b) совпадают если и только если $a = sb$ для некоторого обратимого $s \in K$.

Поэтому всюду далее обозначение нод$(a_1, \ldots, a_n)$ подразумевает целый класс элементов, получающихся друг из друга умножениями на обратимые константы, и все формулы, которые будут писаться, относятся к произвольно выбранному конкретному представителю этого класса[2]. В частности, равенство нод$(a_1, \ldots, a_n) = 1$ означает, что у элементов a_i нет необратимых общих делителей. Так как в этом случае $1 = a_1b_1 + \ldots + a_nb_n$ с $b_i \in K$, отсутствие необратимых общих делителей у элементов a_i в кольце главных идеалов равносильно их *взаимной простоте* в смысле опр. 2.2 на стр. 29.

Упражнение 5.16. Проверьте, что идеалы $(x, y) \subset \mathbb{Q}[x, y]$ и $(2, x) \in \mathbb{Z}[x]$ не являются главными.

5.4. Факториальность. Всюду в этом разделе мы по умолчанию обозначаем через K целостное[3] кольцо. Ненулевые элементы $a, b \in K$ называются *ассоциированными*, если b делится на a, и a делится на b или, что то же самое, если $(a) = (b)$. Из упр. 5.15 выше вытекает, что a и b ассоциированы если и только если они получаются друг из друга умножением на обратимый элемент кольца. Например, целые числа a и b ассоциированы в кольце $\mathbb{Z}$ если и только если $a = \pm b$, а многочлены $f(x)$ и $g(x)$ с коэффициентами из поля $\Bbbk$ ассоциированы в $\Bbbk[x]$ если и только если $f(x) = cg(x)$, где $c \in \Bbbk^\times$ — ненулевая константа.

[1] См. зам. 2.3. на стр. 29.

[2] Что, конечно же, требует проверки корректности всех таких формул, которую мы, как правило, будем оставлять читателю в качестве упражнения.

[3] См. n° 2.4.1 на стр. 30.

5.4.1. Неприводимые элементы. Ненулевой необратимый элемент $q \in K$ называется *неприводимым*, если из равенства $q = mn$ вытекает, что m или n обратим. Другими словами, неприводимость элемента q означает, что главный идеал (q) собственный и не содержится строго ни в каком другом собственном главном идеале, т. е. максимален в частично упорядоченном отношением включения множестве собственных главных идеалов. Неприводимыми элементами в кольце $\mathbb{Z}$ являются простые числа, а в кольце $\Bbbk[x]$, где $\Bbbk$ — поле, — неприводимые многочлены.

В кольце главных идеалов любые два неприводимых элемента p, q либо взаимно просты[1], либо ассоциированы, поскольку идеал $(p, q) = (d)$ для некоторого $d \in K$, и в виду максимальности (p) и (q) включения $(p) \subset (d)$ и $(q) \subset (d)$ влекут либо равенство $(d) = (K) = (1)$, либо равенство $(d) = (p) = (q)$. Обратите внимание, что в произвольном целостном кольце два неассоциированных неприводимых элемента могут и не быть взаимно простыми. Например, в $\mathbb{Q}[x, y]$ неприводимые многочлены x и y не взаимно просты и не ассоциированы.

Предложение 5.4
В кольце главных идеалов K следующие свойства ненулевого элемента $p \in K$ эквивалентны:

1) идеал (p) максимален, т. е. факторкольцо $K/(p)$ является полем

2) идеал (p) прост, т. е. в факторкольце $K/(p)$ нет делителей нуля

3) p неприводим, т. е. из равенства $p = ab$ вытекает, что a или b обратим в K.

Доказательство. Импликация (1) $\Rightarrow$ (2) очевидна и имеет место в любом коммутативном кольце с единицей. Импликация (2) $\Rightarrow$ (3) имеет место в любом целостном кольце K. Действительно, из $p = ab$ следует, что $[a][b] = 0$ в $K/(p)$, и так как в $K/(p)$ нет делителей нуля, один из сомножителей, скажем $[a]$, равен $[0]$. Тогда $a = ps = abs$ для некоторого $s \in K$, откуда $a(1 - bs) = 0$. Поскольку в K нет делителей нуля, $bs = 1$, т. е. b обратим.

Покажем теперь, что в кольце главных идеалов (3) $\Rightarrow$ (1). Так как каждый собственный идеал в K главный, максимальность идеала (p) в чуме собственных главных идеалов означает его максимальность в чуме всех собственных идеалов. В прим. 5.3 на стр. 88 мы видели, что это равносильно тому, что $K/(p)$ поле. □

Предложение 5.5
Каждый необратимый элемент целостного нётерова кольца является произведением конечного числа неприводимых.

Доказательство. Если элемент a неприводим, доказывать нечего. Пусть a приводим. Запишем его в виде произведения необратимых элементов. Каждый приводимый сомножитель этого произведения снова запишем в виде произведения необратимых элементов и т. д. Эта процедура закончится, когда все сомножители станут неприводимы, что и требуется. Если же она никогда не закончится, мы сможем образовать бесконечную последовательность строго вложенных друг в друга главных идеалов $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$, что противоречит нётеровости. □

Определение 5.4
Целостное кольцо K называется *факториальным*, если каждый его ненулевой необратимый элемент является произведением конечного числа неприводимых, причём любые два таких разложения $p_1 p_2 \dots p_m = q_1 q_2 \dots q_k$ состоят из одинакового числа $k = m$ сомножителей, после

[1] В смысле опр. 2.2 на стр. 29, т. е. существуют такие $x, y \in K$, что $px + qy = 1$.

надлежащей перенумерации которых можно указать такие обратимые элементы $s_\nu \in K$, что $q_\nu = p_\nu s_\nu$ при всех ν.

5.4.2. Простые элементы. Ненулевой элемент $p \in K$ называется *простым*, если порождённый им главный идеал $(p) \subset K$ прост, т. е. в факторкольце $K/(p)$ нет делителей нуля. Это означает, что для любых $a, b \in K$ произведение ab делится на p только если a или b делится на p. Каждый простой элемент p автоматически неприводим: если $p = xy$, то один из сомножителей, скажем x, делится на p, и тогда $p = pyz$, откуда $yz = 1$ и y обратим. Согласно предл. 5.4 в кольце главных идеалов верно и обратное: все неприводимые элементы кольца главных идеалов просты. Однако в произвольном целостном кольце могут быть неприводимые непростые элементы. Например, в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)$ таковым является число 2, так как в факторе

$$\mathbb{Z}[\sqrt{5}]/(2) \simeq \mathbb{Z}[x]/(2, x^2 - 5) = \mathbb{Z}[x]/(2, x^2 + 1) \simeq \mathbb{F}_2[x]/(x^2 + 1) \simeq \mathbb{F}_2[x]/\big((x+1)^2\big)$$

есть нильпотент — класс $[x + 1] \in \mathbb{Z}[x]/(2, x^2 + 5)$. Среди прочего это означает, что квадрат $(1 + \sqrt{5})^2 = 6 + 2\sqrt{5}$ делится в кольце $\mathbb{Z}[\sqrt{5}]$ на 2, хотя $1 + \sqrt{5}$ не делится на 2, при том что 2 и $\sqrt{5} + 1$ неприводимы и не ассоциированы друг с другом в кольце $\mathbb{Z}[\sqrt{5}]$.

Упражнение 5.17. Убедитесь в этом, и покажите, что $2 \cdot 2 = 4 = \big(\sqrt{5} + 1\big) \cdot \big(\sqrt{5} - 1\big)$ суть два *различных* разложения числа 4 на неприводимые множители в $\mathbb{Z}[\sqrt{5}]$.

Предложение 5.6
Целостное нётерово кольцо K факториально если и только если все его неприводимые элементы просты.

Доказательство. Покажем сначала, что если K факториально, то любой неприводимый элемент $q \in K$ прост. Пусть произведение ab делится на q. Тогда разложение ab на неприводимые множители содержит множитель, ассоциированный с q, и в силу своей единственности является произведением разложений a и b на неприводимые множители. Поэтому q ассоциирован с одним из неприводимых делителей a или b, т. е. a или b делится на q. Наоборот, пусть все неприводимые элементы в K просты. Тогда по предл. 5.5 на стр. 92 каждый элемент кольца K является произведением конечного числа простых. Покажем, что в целостном кольце равенство $p_1 \dots p_k = q_1 \dots q_m$, в котором все сомножители просты, возможно только если $k = m$ и после надлежащей перенумерации каждый $p_i = s_i q_i$, где s_i обратим. Поскольку произведение $q_1 \dots q_m$ делится на p_1, один из его сомножителей делится на p_1. Будем считать, что это $q_1 = sp_1$. Так как q_1 неприводим, элемент s обратим. Пользуясь целостностью K, сокращаем обе части равенства $p_1 \dots p_k = q_1 \dots q_m$ на p_1 и получаем более короткое равенство $p_2 p_3 \dots p_k = (sq_2)q_3 \dots q_m$, к которому применимы те же рассуждения. □

Следствие 5.4
Всякое кольцо главных идеалов факториально. □

Пример 5.6 (характеризация областей главных идеалов, продолжение № 5.3.1 на стр. 90)
Покажем, что целостное кольцо K является областью главных идеалов если и только если на K можно задать функцию высоты $\nu : K \to \mathbb{Z}_{\geqslant 0} = \mathbb{N} \cup \{0\}$ со свойствами: (1) $\nu(a) = 0 \Longleftrightarrow a = 0$ (2) если $b \nmid a$, то такие найдутся $x, y \in K$, что $0 < \nu(ax + by) < \nu(b)$. Пусть такая высота существует. Тогда в каждом идеале $I \subset K$ есть элемент d наименьшей в I положительной

высоты. Если $a \in I$ не делится на d, то $0 < \nu(ax+dy) < \nu(b)$ для некоторых $x, y \in K$, что невозможно, так как $ax+dy \in I$. Поэтому $I = (d)$ и тем самым K является областью главных идеалов. Наоборот, пусть K — область главных идеалов. Выберем в каждом классе ассоциированных простых элементов какого-нибудь представителя p и для каждого $a \in K$ обозначим через $\nu_p(a)$ показатель, с которым p входит в разложение $a = \prod_p p^{\nu_p(a)}$ на простые множители. Положим $\nu(a) = 2^{\sum_p \nu_p(a)}$. Так как $\nu_p(a) = 0$ для всех p кроме конечного числа, это определение корректно. Если $b \nmid a$, то $d = \text{нод}(a,b) = ax+by = \prod_p p^{\min(\nu_p(a),\nu_p(b))}$ имеет $0 < \nu(d) < \nu(b)$, что и требуется. Более того, высота ν *приведённая*[1], т. е. $\nu(a) \leqslant \nu(ab)$ для всех ненулевых a, b, и обращение этого неравенства в равенство равносильно обратимости b.

Пример 5.7 (гауссовы числа и суммы двух квадратов)
Элементы кольца $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1) \simeq \{x+iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$ из упр. 5.13 (в) на стр. 90 называются *целыми гауссовыми числами*.

Упражнение 5.18. Убедитесь, что: а) в $\mathbb{Z}[i]$ обратимы только ± 1 и $\pm i$ б) $z \in \mathbb{Z}$ прост если и только если прост $\bar{z}$.

Из упражнения вытекает, что разложение вещественного целого числа $n \in \mathbb{Z}$ на простые множители в области $\mathbb{Z}[i]$, будучи инвариантным относительно комплексного сопряжения, вместе с каждым невещественным неприводимым множителем содержит и его сопряжённый. Поэтому вещественное простое $p \in \mathbb{Z}$ становится приводимым в $\mathbb{Z}[i]$ если и только если оно имеет вид $p = (a+ib)(a-ib) = a^2+b^2$ с ненулевыми $a, b \in \mathbb{Z}$. С другой стороны, неприводимость $p \in \mathbb{Z}[i]$ означает, что факторкольцо $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[x]/(p, x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$ является полем[2], что равносильно неприводимости многочлена x^2+1 над $\mathbb{F}_p$. Последнее равносильно тому, что -1 не является квадратом в $\mathbb{F}_p$, что имеет место[3] если и только если $p = 4k+3$. Мы заключаем, что неприводимость простого $p \in \mathbb{Z}$ в области $\mathbb{Z}[i]$ равносильна тому, что $p = 4k+3$, и тому, что p не представляется в виде суммы двух квадратов целых чисел.

Упражнение 5.19. Покажите, что произвольное $n \in \mathbb{N}$ является квадратом или суммой двух квадратов натуральных чисел если и только если в его разложении на простые множители в кольце $\mathbb{Z}$ простые числа $p = 4k+3$ присутствуют только в чётных степенях.

5.4.3. НОД в факториальном кольце. Каждый конечный набор элементов $a_1, \ldots, a_m$ любого факториального кольца K обладает наибольшим общим делителем[4], который имеет следующее явное описание. Зафиксируем, как в прим. 5.6 выше, в каждом классе ассоциированных простых элементов кольца K некоторого представителя p и для каждого $a \in K$ обозначим через $\nu_p(a) \in \mathbb{Z}_{\geqslant 0}$ показатель, с которым p входит в разложение a на простые множители[5]. Тогда, с точностью до умножения на обратимые элементы, $\text{нод}(a_1, \ldots, a_m) = \prod_p p^{\min_i \nu_p(a_i)}$.

Упражнение 5.20. Убедитесь, что правая часть делит каждое a_i и делится на любой общий делитель всех a_i.

Отметим, что если K не является областью главных идеалов, то $\text{нод}(a_1, \ldots, a_m)$ может не представляться в виде линейной комбинации элементов a_i с коэффициентами из K. Например, эле-

[1] Ср. с n° 5.3.1 на стр. 90.
[2] См. предл. 5.4 на стр. 92.
[3] См. прим. 2.8 на стр. 33.
[4] В смысле зам. 2.3. на стр. 29, т. е. числом, которое делит все a_i и делится на любой их общий делитель.
[5] Обратите внимание, что для каждого a показатель $\nu_p(a) \neq 0$ только для конечного множества простых чисел p.

менты x, y факториального кольца[1] $\mathbb{Q}[x,y]$ имеют нод$(x,y) = 1$, но нет таких $f, g \in \mathbb{Q}[x,y]$, что $fx + gy = 1$, поскольку подставляя в это равенство $x = y = 0$, получим $0 = 1$.

5.5. Многочлены над факториальным кольцом. Пусть K — факториальное кольцо. Обозначим через Q_K его поле частных. Кольцо $K[x]$ является подкольцом в $Q_K[x]$. Назовём *содержанием* многочлена $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ наибольший общий делитель его коэффициентов:

$$\operatorname{cont}(f) \stackrel{\text{def}}{=} \text{нод}(a_0, a_1, \ldots, a_n)\,.$$

Лемма 5.2
$\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ для любых $f, g \in K[x]$.

Доказательство. Достаточно для каждого простого $q \in K$ убедиться в том, что q делит все коэффициенты произведения fg если и только если q делит все коэффициенты хотя бы одного из многочленов f, g. Для этого положим $R = K/(q)$ и применим к произведению fg гомоморфизм

$$K[x] \to R[x]\,, \quad a_0 + a_1 x + \ldots + a_n x^n \mapsto [a_0]_q + [a_1]_q x + \ldots [a_n]_q x^n\,,$$

заменяющий коэффициенты каждого многочлена их вычетами по модулю q.

Упражнение 5.21. Проверьте, что это и в самом деле гомоморфизм колец.

В силу простоты q кольцо R целостное. Поэтому $R[x]$ тоже целостное, и $[fg]_q = [f]_q [g]_q$ нулевое если и только если $[f]_q$ или $[g]_q$ нулевой. □

Лемма 5.3 (приведённое представление)
Каждый $f \in Q_K[x]$ представляется в виде $f(x) = (a\,/\,b) \cdot f_{\text{red}}(x)$, где $f_{\text{red}} \in K[x]$, $a, b \in K$ и $\operatorname{cont}(f_{\text{red}}) = \text{нод}(a,b) = 1$, причём a, b и f_{red} определяются по f однозначно с точностью до умножения на обратимые элементы кольца K.

Доказательство. Вынесем из коэффициентов f их общий знаменатель, потом вынесем из всех коэффициентов полученного многочлена их наибольший общий делитель. В результате мы получим многочлен содержания 1, умноженный на число из Q_K, которое запишем несократимой дробью a/b. Докажем единственность такого представления. Если $(a/b)\cdot f_{\text{red}}(x) = (c/d)\cdot g_{\text{red}}(x)$ в $Q_K[x]$, то $ad \cdot f_{\text{red}}(x) = bc \cdot g_{\text{red}}(x)$ в $K[x]$. Сравнивая содержание обеих частей, получаем $ad = bc$. Поэтому $f_{\text{red}}(x) = g_{\text{red}}(x)$, а дроби $a\,/\,b$ и $c\,/\,d$ совпадают друг с другом. □

Следствие 5.5 (лемма Гаусса)
Многочлен $f \in K[x]$ содержания 1 неприводим в $Q_K[x]$ если и только если он неприводим в $K[x]$.

Доказательство. Пусть $f(x) = g(x) \cdot h(x)$ в $Q_K[x]$. Записывая многочлены g и h в приведённом виде из лем. 5.3 и сокращая возникающую дробь, приходим к равенству

$$f(x) = \frac{a}{b} \cdot g_{\text{red}}(x) \cdot h_{\text{red}}(x)\,, \tag{5-5}$$

в котором $g_{\text{red}}, h_{\text{red}} \in K[x]$ имеют содержание 1, и нод$(a,b) = 1$. По лем. 5.2

$$\operatorname{cont}(g_{\text{red}} h_{\text{red}}) = \operatorname{cont}(g_{\text{red}}) \cdot \operatorname{cont}(h_{\text{red}}) = 1\,,$$

[1] См. сл. 5.6 на стр. 96.

т. е. правая часть в (5-5) является приведённым представлением многочлена f. В силу единственности приведённого представления элементы a и b обратимы в K, а $f = g_{\text{red}} h_{\text{red}}$ с точностью до умножения на обратимую константу. □

Теорема 5.2
Кольцо многочленов над факториальным кольцом факториально.

Доказательство. Будучи кольцом главных идеалов, кольцо $Q_K[x]$ факториально, и каждый многочлен $f \in K[x] \subset Q_K[x]$ раскладывается в $Q_K[x]$ в произведение неприводимых множителей $f_\nu \in Q_K[x]$. Записывая их в приведённом виде из лем. 5.3 и сокращая возникающую при этом числовую дробь, получаем равенство $f = \frac{a}{b} \prod f_{\nu,\text{red}}$, в котором $a, b \in K$ имеют нод$(a, b) = 1$, а все $f_{\nu,\text{red}} \in K[x]$ неприводимы в $Q_K[x]$ и $\operatorname{cont}(f_{\nu,\text{red}}) = 1$. Тогда $\operatorname{cont}\left(\prod f_{\nu,\text{red}}\right) = 1$ по лем. 5.3, и правая часть равенства является приведённым представлением многочлена $f = \operatorname{cont}(f) \cdot f_{\text{red}}$. В силу единственности приведённого представления $b = 1$ и $f = a \prod f_{\nu,\text{red}}$ с точностью до умножения на обратимые константы из K. Раскладывая $a \in K$ в произведение неприводимых констант, получаем разложение f в произведение неприводимых множителей в кольце $K[x]$. Докажем единственность такого разложения. Пусть в $K[x]$

$$a_1 \dots a_k \cdot p_1 \dots p_s = b_1 \dots b_m \cdot q_1 \dots q_r\,,$$

где $a_\alpha, b_\beta \in K$ — неприводимые константы, а $p_\mu, q_\nu \in K[x]$ — неприводимые многочлены. Поскольку неприводимые многочлены имеют содержание 1, сравнивая содержание обеих частей, приходим к равенству $a_1 \dots a_k = b_1 \dots b_m$ в K. Так как K факториально, мы заключаем, что $k = m$ и после надлежащей перенумерации сомножителей $a_i = s_i b_i$, где все $s_i \in K$ обратимы. Следовательно, с точностью до умножения на обратимую константу из K, в кольце $K[x]$ выполняется равенство $p_1 \dots p_s = q_1 \dots q_r$. Так как все p_i и q_i неприводимы в факториальном кольце $Q_K[x]$, мы заключаем, что $r = s$ и после надлежащей перенумерации сомножителей $p_i = q_i$ с точностью до постоянных множителей из поля Q_K. Из единственности приведённого представления[1] вытекает, что эти постоянные множители являются обратимыми константами из кольца K. □

Следствие 5.6
Кольцо многочленов $K[x_1, \dots, x_n]$ над факториальным кольцом[2] K факториально. □

5.6. Разложение многочленов с целыми коэффициентами. Разложение многочлена $f \in \mathbb{Z}[x]$ на множители в $\mathbb{Q}[x]$ разумно начать с отыскания его рациональных корней, что делается за конечное число проб.

Упражнение 5.22. Покажите, что несократимая дробь $p/q \in \mathbb{Q}$ является корнем многочлена $a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ только если $p \mid a_0$ и $q \mid a_n$.

Точное знание комплексных корней многочлена f тоже весьма полезно.

Упражнение 5.23. Разложите $x^4 + 4$ в произведение двух квадратных трёхчленов из $\mathbb{Z}[x]$.

После того, как эти простые соображения будут исчерпаны, следует подключать более трудоёмкие способы.

[1] См. лем. 5.3 на стр. 95.

[2] В частности, над полем или над областью главных идеалов.

5.6.1. Редукция коэффициентов многочленов по модулю $m \in \mathbb{Z}$

$$\mathbb{Z}[x] \to \frac{\mathbb{Z}}{(m)}[x], \quad a_0 + a_1 x + \ldots + a_n x^n \mapsto [a_0]_m + [a_1]_m x + \ldots [a_n]_m x^n, \tag{5-6}$$

является гомоморфизмом колец[1]. Поэтому равенство $f = gh$ в $\mathbb{Z}[x]$ влечёт за собой равенства $[f]_m = [g]_n \cdot [h]_m$ во всех кольцах $\big(\mathbb{Z}/(m)\big)[x]$. Таким образом из неприводимости многочлена $[f]_m$ хотя бы при одном m вытекает его неприводимость в $\mathbb{Z}[x]$. Если число $m = p$ простое, кольцо коэффициентов $\mathbb{Z}/(m) = \mathbb{F}_p$ является полем, и кольцо многочленов $\mathbb{F}_p[x]$ в этом случае факториально. При малых p разложение многочлена небольшой степени на неприводимые множители в $\mathbb{F}_p[x]$ можно осуществить простым перебором, и анализ такого разложения может дать существенную информацию о возможном разложении в $\mathbb{Z}[x]$.

Пример 5.8
Покажем, что многочлен $f(x) = x^5 + x^2 + 1$ неприводим в кольце $\mathbb{Z}[x]$. Поскольку у f нет целых корней, нетривиальное разложение $f = gh$ в $\mathbb{Z}[x]$ возможно только с $\deg(g) = 2$ и $\deg(h) = 3$. Сделаем редукцию по модулю 2. Так как у $[f]_2 = x^5 + x^2 + 1$ нет корней и в $\mathbb{F}_2$, оба многочлена $[g]_2$, $[h]_2$ неприводимы в $\mathbb{F}_2[x]$. Но единственный неприводимый многочлен второй степени в $\mathbb{F}_2[x]$ это $x^2 + x + 1$, и $x^5 + x^2 + 1$ на него не делится. Тем самым, $[f]_2$ неприводим над $\mathbb{F}_2$, а значит, и над $\mathbb{Z}$.

Пример 5.9 (критерий Эйзенштейна)
Пусть все коэффициенты приведённого многочлена $f \in \mathbb{Z}[x]$ делятся на простое число $p \in \mathbb{N}$, а младший коэффициент, делясь на p, не делится при этом на p^2. Покажем, что f неприводим в $\mathbb{Z}[x]$. В силу сделанных об f предположений при редукции по модулю p от f остаётся только старший моном $[f(x)]_p = x^n$. Если $f(x) = g(x)h(x)$ в $\mathbb{Z}[x]$, то в силу единственности разложения на простые множители в $\mathbb{F}_p[x]$ оба сомножителя g, h тоже редуцируются в некоторые степени переменной: $[g]_p = x^k$ и $[h]_p = x^m$. Это означает, что все коэффициенты многочленов g и h кроме старшего делятся на p. Тогда младший коэффициент многочлена f, будучи произведением младших коэффициентов многочленов g и h, должен делиться на p^2, что не так.

Пример 5.10 (неприводимость кругового многочлена Φ_p)
Покажем, что при простом $p \in \mathbb{N}$ круговой многочлен $\Phi_p(x) = x^{p-1} + \ldots + x + 1 = (x^p - 1)/(x - 1)$ неприводим в $\mathbb{Z}[x]$. Для этого перепишем его как многочлен от переменной $t = x - 1$:

$$f(t) = \Phi_p(t+1) = (t+1)^p - 1/t = t^{p-1} + \binom{p}{1} t^{p-2} + \ldots + \binom{p}{p-1}.$$

Поскольку при простом p все биномиальные коэффициенты $\binom{p}{k}$ с $1 \leqslant k \leqslant p-1$ делятся[2] на p, а свободный член $\binom{p}{p-1} = p$ не делится на p^2, многочлен $f(t)$ неприводим по критерию Эйзенштейна из прим. 5.9. Поэтому и $\Phi_p(x) = f(x-1)$ неприводим.

[1] Мы уже пользовались этим в доказательстве лем. 5.2 на стр. 95, см. упр. 5.21.
[2] См. сл. 2.1 на стр. 32.

5.6.2. Алгоритм Кронекера позволяет путём довольно трудоёмкого, но вполне конечного вычисления либо явно разложить многочлен $f \in \mathbb{Z}[x]$ на множители в кольце $\mathbb{Z}[x]$, либо убедиться, что f неприводим в $\mathbb{Z}[x]$. Пусть $\deg f = 2n$ или $\deg f = 2n+1$. Тогда в любом нетривиальном разложении $f = gh$ степень одного из делителей, пусть это будет h, не превосходит n. Чтобы выяснить, делится ли f в $\mathbb{Z}[x]$ на какой-нибудь многочлен степени не выше n, подставим в f произвольные $n+1$ различных чисел $z_0, \dots, z_n \in \mathbb{Z}$ и выпишем все возможные наборы чисел $d_0, \dots, d_n \in \mathbb{Z}$, в которых каждое d_i делит соответствующее $f(z_i)$. Таких наборов имеется конечное число, и если искомый многочлен h существует, то набор его значений $h(z_0), \dots, h(z_n)$ на числах z_i является одним из выписанных наборов $d_0, \dots, d_n$. Для каждого такого набора в $\mathbb{Q}[x]$ есть ровно один многочлен h степени не выше n, принимающий значения $h(z_i) = d_i$ при всех i — это *интерполяционный многочлен Лагранжа*[1]

$$h(x) = \sum_{i=0}^{n} d_i \cdot \prod_{\nu \neq i} \frac{(x - z_\nu)}{(z_i - z_\nu)}\,. \tag{5-7}$$

Таким образом, делитель h многочлена f, если он существует, совпадает с одним из тех многочленов (5-7), что имеют целые коэффициенты. Остаётся явно разделить f на все такие многочлены и либо убедиться, что они не делят f, либо обнаружить среди них делитель f.

Задачи для самостоятельного решения к §5

Задача 5.1. Перечислите все идеалы в кольце степенных рядов $\Bbbk[\![t]\!]$ над произвольным полем $\Bbbk$. Какие из них максимальны? Какие просты?

Задача 5.2. Являются ли кольца многочленов $\mathbb{Q}[x,y]$ и $\mathbb{Z}[x]$ областями главных идеалов? Есть ли в них простые немаксимальные идеалы?

Задача 5.3. Обязательно ли конечно кольцо $\mathbb{Z}[x]/(f,g)$, если $f, g \in \mathbb{Z}[x]$:
а) имеют нод$(f,g) = 1$ в $\mathbb{Z}[x]$ б) взаимно просты в $\mathbb{Q}[x]$?

Задача 5.4. Укажите непростой неприводимый элемент в кольце $\mathbb{Z}[\sqrt{13}]$.

Задача 5.5. В кольце $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ найдите а) нод$(5+3i, 6-4i)$. б) наименьшее $n \in \mathbb{N}$, кратное данному $a+bi \in \mathbb{Z}[i]$. в) Разложите 3, 5, 7, $7+i$ на простые множители.

Задача 5.6. Докажите эквивалентность друг другу следующих свойств простого $p \in \mathbb{N}$:
а) $p \not\equiv 3 \pmod 4$ б) -1 квадрат в поле $\mathbb{F}_p$ в) существует ненулевой гомоморфизм $\mathbb{Z}[i] \to \mathbb{F}_p$
г) p приводимо в кольце $\mathbb{Z}[i]$ д) p является суммой двух квадратов натуральных чисел.

Задача 5.7. Какие простые $p \in \mathbb{Z}$ остаются таковыми в кольце $\mathbb{Z}[\omega] = \mathbb{Z}[x]/(x^2+x+1)$?

Задача 5.8. Покажите, что простое $p \in \mathbb{Z}$ имеет вид x^2+xy+y^2, где $x, y \in \mathbb{Z}$, если и только если $p = 3$ или $p \equiv 1 \pmod 3$.

Задача 5.9. Сколько решений $(x,y) \in \mathbb{Z}^2$ имеют уравнения а) $x^2+y^2 = n$ б) $x^2+xy+y^2 = n$ в зависимости от $n \in \mathbb{N}$?

Задача 5.10. Сколько элементов может быть в конечном факторе кольца а) $\mathbb{Z}[i]$ б) $\mathbb{Z}[\omega]$?

[1] См. прим. 3.5 на стр. 48.

Задача 5.11. Является ли кольцо $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2-2) \simeq \{a+b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ евклидовым относительно высоты $\nu(a+b\sqrt{2}) = |a^2-2b^2|$?

Задача 5.12. Пусть $d \in \mathbb{N}$ не делится на квадраты. Обозначим через $\mathcal{O}_{\sqrt{-d}} \subset \mathbb{C}$ множество чисел вида $a+b\zeta_d$, где $a, b \in \mathbb{Z}$, а

$$\zeta_d = \begin{cases} (1+i\sqrt{d})/2 & \text{при } d \equiv 3 \pmod 4 \\ i\sqrt{d} & \text{при } d \equiv 1, 2 \pmod 4. \end{cases}$$

Убедитесь, что $\mathcal{O}_{\sqrt{-d}}$ является подкольцом в $\mathbb{C}$ и докажите, что

а) оно евклидово для высоты $\nu(z) = |z|^2$ если и только если $\mathbb{C}$ покрывается сдвигами единичного круга на векторы из $\mathcal{O}_{\sqrt{-d}}$

б*) это так для $d = 1, 2, 3, 7, 11$ и только для них

в*) для всех прочих d кольцо $\mathcal{O}_{\sqrt{-d}}$ не евклидово ни для какой высоты[1].

г*) Для $d = 19$ кольцо $\mathcal{O}_{\sqrt{-d}}$ является областью главных идеалов.

Задача 5.13. Убедитесь, что каждый гомоморфизм колец $\varphi : K \to L$ задаёт гомоморфизм колец многочленов $K[x] \to L[x]$, $f \mapsto f^\varphi$, состоящий в применении φ ко всем коэффициентам. Пусть оба кольца K, L целостные, и $f \in K[x]$ таков, что $\deg f^\varphi = \deg f$ и f^φ неприводим в $Q_L[x]$, где Q_L — поле частных кольца L. Докажите, что f неприводим в $K[x]$.

Задача 5.14. Найдите все рациональные корни многочлена $2x^4 - 7x^3 + 4x^2 - 2x - 3$.

Задача 5.15. Укажите разложение на неприводимые в $\mathbb{Z}[x]$ множители или докажите неприводимость многочленов: а) $x^4 - 8x^3 + 12x^2 - 6x + 2$ б) $x^5 - 12x^3 + 36x - 12$ в) $x^4 + x + 1$ г) $x^5 + x^4 + x^2 + x + 2$ д) $x^6 + x^3 + 1$ е) $x^4 + 4x^3 + 8x^2 + 8x + 4$ ж) $x^{179} - 9$.

Задача 5.16. Пусть $a_1, \ldots, a_n \in \mathbb{Z}$ все различны. Приводимы ли в $\mathbb{Q}[x]$ многочлены:
а) $(x-a_1)\ldots(x-a_n) - 1$ б) $(x-a_1)^2 \ldots (x-a_n)^2 + 1$

Задача 5.17. Пусть A — коммутативное кольцо с единицей, $I, J \subset A$ — произвольные идеалы. Положим[2] $\sqrt{I} \stackrel{\text{def}}{=} \{a \in A \mid \exists\, n \in \mathbb{N} :\ a^n \in I\}$, $I + J \stackrel{\text{def}}{=} (I, J) = \{a + b \mid a \in I,\ b \in J\}$ и обозначим через IJ идеал, порождённый произведениями[3] ab с $a \in I$, $b \in J$. Верно ли, что[4]
а) произведения ab с $a \in I$, $b \in J$ уже и сами по себе образуют идеал
б) $\sqrt{I}$ это идеал в) $IJ = I \cap J$ г) $I + J = A \Rightarrow IJ = I \cap J$
д) $\sqrt{IJ} = \sqrt{I \cap J}$ е) $\sqrt{IJ} = \sqrt{I}\sqrt{J}$ ж) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Задача 5.18 (китайская теорема об остатках). Пусть идеалы $I_1, \ldots, I_m$ коммутативного кольца A с единицей таковы, что $I_i + I_j = A$ для всех $i \neq j$. Покажите, что $I_1 \ldots I_m = I_1 \cap \ldots \cap I_m$ и постройте изоморфизм $A/I_1 \ldots I_m \xrightarrow{\sim} (A/I_1) \times \ldots \times (A/I_m)$.

Задача 5.19. Докажите, что а) простой идеал $\mathfrak{p}$ содержит пересечение конечного набора идеалов если и только если $\mathfrak{p}$ содержит один из них б) идеал I содержится в объединении конечного набора простых идеалов если и только если I лежит в одном из них.

---

[1] подсказка: пусть $a \in \mathcal{O}_{\sqrt{-d}}$ — необратимый элемент наименьшей *приведённой* высоты; покажите, что любое $b \in \mathcal{O}_{\sqrt{-d}}$ сравнимо с 0, 1 или -1 по модулю (a).

[2] $\sqrt{I}$ называется *радикалом* идеала I.

[3] Т. е. пересечение всех идеалов, содержащих эти произведения, или (что то же самое) — множество всевозможных сумм вида $a_1b_1 + \cdots + a_mb_m$, где $m \in \mathbb{N}$, $a_i \in I$, $b_i \in J$.

[4] Верные утверждение докажите, к неверным приведите явные контрпримеры.

Задача 5.20*. Сопоставим вещественному числу $p \in [0\,,1]$ множество $\mathfrak{m}_p$ всех таких непрерывных функций $f : [0\,,1] \to \mathbb{R}$, что $f(p) = 0$. Покажите, что это задаёт биекцию между точками отрезка $[0\,,1]$ и максимальными идеалами в кольце непрерывных функций $[0\,,1] \to \mathbb{R}$.

Задача 5.21*. Всякий ли простой идеал кольца непрерывных функций $[0\,,1] \to \mathbb{R}$ максимален?

Задача 5.22* (теорема Крулля). Докажите, что целостное нётерово кольцо факториально если и только если все его минимальные по включению ненулевые простые идеалы являются главными.

Задача 5.23* (нильрадикал). Множество всех нильпотентных элементов коммутативного кольца K с единицей называется *нильрадикалом* кольца K и обозначается $\mathfrak{n} = \mathfrak{n}(K) \stackrel{\text{def}}{=} \sqrt{(0)}$. Докажите, что $\mathfrak{n}(K)$ является пересечением всех простых идеалов кольца K.

§6. Модули над коммутативными кольцами

6.1. Определения и примеры. Аддитивная абелева группа[1] M называется *модулем* над коммутативным кольцом K или K-*модулем*, если задана операция умножения *векторов на скаляры*[2]

$$K \times M \to M\,, \quad (x, v) \mapsto xv\,,$$

с теми же свойствами, что известное из геометрии умножение векторов[3] на числа:

$$\forall\, x, y \in K \quad \forall\, v \in M \quad x(yv) = (xy)v \tag{6-1}$$

$$\forall\, x, y \in K \quad \forall\, v \in M \quad (x + y)v = xv + yv \tag{6-2}$$

$$\forall\, x \in K \quad \forall\, u, w \in M \quad x(v + w) = xv + xw\,. \tag{6-3}$$

Если в кольце K есть единица и выполняется дополнительное свойство

$$\forall\, v \in V \quad 1v = v\,, \tag{6-4}$$

то модуль M называется *унитальным*. Всюду в этом курсе мы по умолчанию будем иметь дело именно с такими модулями. Унитальные модули над полями называются *векторными пространствами*. Часто бывает удобно записывать произведение вектора $v \in M$ на скаляр $x \in K$ не как xv, а как vx. Когда кольцо скаляров K коммутативно, мы по определению считаем эти две записи эквивалентными обозначениями $xv = vx$ для одного и того же вектора из M.

Упражнение 6.1. Выведите из свойств (6-1) – (6-3), что в любом K-модуле M для всех $v \in M$ и $x \in K$ выполняются равенства $0v = 0$, где $0 \in K$, и $x0 = 0$, где $0 \in V$, а в унитальном модуле над коммутативным кольцом с единицей — равенство $(-1)\,v = -v$, где $-1 \in K$, $-v \in V$.

Аддитивная абелева подгруппа $N \subseteq M$ в K-модуле M называется K-*подмодулем*, если она образует K-модуль относительно имеющейся в M операции умножения векторов на скаляры. Для этого необходимо и достаточно, чтобы $xw \in N$ для всех $x \in K$ и $w \in N$. Подмодули $N \subsetneq M$ называются *собственными*. Модуль 0, состоящий из одного нуля, называется *тривиальным*.

Пример 6.1 (кольцо как модуль над собой)
Каждое коммутативное кольцо K является модулем над самим собой: сложение векторов и их умножение на скаляры суть сложение и умножение в K. Если в K имеется единица, K-модуль K является унитальным. K-подмодули $I \subset K$ — это в точности идеалы кольца K. В частности, коммутативное кольцо K с единицей является полем если и только если в K-модуле K нет нетривиальных собственных подмодулей[4].

Пример 6.2 (координатный модуль K^r)
Декартово произведение r экземпляров кольца K обозначается $K^r = K \times \ldots \times K$ и состоит из строк $a = (a_1, \ldots, a_r)$, в которых $a_i \in K$. Сложение таких строк и их умножение их на скаляры $x \in K$ происходит покоординатно: для $a = (a_1, \ldots, a_r)$, $b = (b_1, \ldots, b_r)$ и $x \in K$ мы полагаем

$$a + b \stackrel{\text{def}}{=} (a_1 + b_1, \ldots, a_r + b_r) \quad \text{и} \quad xa \stackrel{\text{def}}{=} (xa_1, \ldots, xa_r)\,.$$

[1] См. n° 2.1.2 на стр. 25.
[2] Где *векторами* называются элементы модуля M, а *скалярами* — элементы кольца K.
[3] См. прим. 2.4 на стр. 25.
[4] См. предл. 5.1 на стр. 85.

Пример 6.3 (модуль матриц $\mathrm{Mat}_{m\times n}(K)$)
Таблицы из m строк и n столбцов, заполненные элементами кольца K, называются *$m\times n$ матрицами с элементами из K*. Множество всех таких матриц обозначается $\mathrm{Mat}_{m\times n}(K)$. Элемент матрицы A, расположенный в i-й строке и j-м столбце, обозначается a_{ij}. Запись $A=(a_{ij})$ означает, что матрица A состоит из таких элементов a_{ij}. Например, матрица $A\in\mathrm{Mat}_{3\times 4}(\mathbb{Z})$ с элементами $a_{ij}=i-j$ имеет вид

$$\begin{pmatrix} 0 & -1 & -2 & -3 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 0 & -1 \end{pmatrix}.$$

Так же как и координатные строки, $m\times n$ матрицы $\mathrm{Mat}_{m\times n}(K)$ образуют K-модуль относительно поэлементного сложения и умножения на скаляры: сумма $S=(s_{ij})$ матриц $A=(a_{ij})$ и $B=(b_{ij})$ имеет $s_{ij}=a_{ij}+b_{ij}$, а произведение $P=\lambda A$ матрицы A на число $\lambda\in K$ имеет $p_{ij}=\lambda a_{ij}$.

Пример 6.4 (абелевы группы как $\mathbb{Z}$-модули)
Каждая аддитивно записываемая абелева группа A может рассматриваться как унитальный $\mathbb{Z}$-модуль, в котором сложение векторов есть сложение в A, а умножение вектора $a\in A$ на скаляр $\pm n$, где $n\in\mathbb{N}$, задаётся правилом

$$\pm na \stackrel{\text{def}}{=} \pm(\underbrace{a+\ldots+a}_{n}).$$

Например, в аддитивной группе вычетов $\mathbb{Z}/(m)$, рассматриваемой как $\mathbb{Z}$-модуль, результатом умножения класса $[k]_m\in\mathbb{Z}/(m)$ на число $z\in\mathbb{Z}$ является класс $[zk]_m$.

6.2. Линейные отображения. Отображение $\varphi\colon M\to N$ между K-модулями M и N называется *K-линейным* или *гомоморфизмом K-модулей*, если оно перестановочно со сложением векторов и умножением векторов на скаляры, т. е. для всех $x\in K$ и $u,w\in M$

$$\varphi(u+w)=\varphi(u)+\varphi(w) \quad\text{и}\quad \varphi(xu)=x\varphi(u). \tag{6-5}$$

Так как K-линейные отображения $\varphi\colon M\to N$ являются гомоморфизмами абелевых групп, они обладают всеми перечисленными в n° 2.5 на стр. 32 свойствами таких гомоморфизмов. В частности, $\varphi(0)=0$ и $\varphi(-w)=-\varphi(w)$ для всех $w\in M$, а каждый непустой слой линейного отображения φ является аддитивным сдвигом его *ядра*

$$\ker\varphi \stackrel{\text{def}}{=} \varphi^{-1}(0)=\{u\in M \mid \varphi(u)=0\},$$

т. е. $\varphi^{-1}(\varphi(w))=w+\ker\varphi$ для всех $w\in M$. В частности, все непустые слои находятся в биекции друг с другом, и инъективность φ равносильна тому, что $\ker\varphi=0$.

Упражнение 6.2. Убедитесь, что ядро и образ K-линейного гомоморфизма $\varphi\colon M\to N$ являются подмодулями в M и в N соответственно.

Биективные гомоморфизмы модулей называются *изоморфизмами*. K-линейное отображение $\varphi\colon M\to N$ является изоморфизмом если и только если $\ker\varphi=0$ и $\operatorname{im}\varphi=N$. Например, выписывание элементов матрицы в строку в произвольном порядке задаёт изоморфизм между модулем матриц $\mathrm{Mat}_{m\times n}(K)$ из прим. 6.3 и координатным K-модулем K^{mn} из прим. 6.2.

Предостережение 6.1. Именуемое в школе «линейной функцией» отображение $\varphi : K \to K$, задаваемое правилом $\varphi(x) = ax + b$, где $a, b \in K$ фиксированы, является K-линейным в смысле предыдущего определения только при $b = 0$. Если же $b \neq 0$, то φ не перестановочно ни со сложением, ни с умножением на числа.

Упражнение 6.3. Убедитесь, что отображение абелевых групп $A \to B$, рассматриваемых как $\mathbb{Z}$-модули согласно прим. 6.4, является гомоморфизмом абелевых групп[1] если и только если оно $\mathbb{Z}$-линейно.

Пример 6.5 (дифференцирование)
Кольцо многочленов $K[x]$ с коэффициентами в коммутативном кольце K можно рассматривать и как K-модуль. Оператор дифференцирования $D = \frac{d}{dx} : K[x] \to K[x]$, $f(x) \mapsto f'(x)$, является гомоморфизмом K-модулей, поскольку перестановочен со сложением многочленов и умножением многочленов на константы, но не является гомоморфизмом колец, так как не перестановочен с умножением многочленов друг на друга.

Упражнение 6.4. Покажите, что композиция K-линейных отображений тоже K-линейна.

6.2.1. Модуль гомоморфизмов. Гомоморфизмы K-модулей $M \to N$ образуют K-модуль относительно операций сложения значений и умножения их на скаляры: отображения $\varphi+\psi$ и $x\varphi$, где $x \in K$, переводят каждый вектор $w \in M$, соответственно, в $\varphi(w) + \psi(w)$ и в $x\varphi(w) = \varphi(xw)$.

Упражнение 6.5. Убедитесь, что для любого $x \in K$ и K-линейных отображений $\varphi, \psi : M \to N$ отображения $\varphi + \psi$ и $x\varphi$ тоже K-линейны.

Модуль K-линейных отображений $M \to N$ называется *модулем гомоморфизмов* из M в N и обозначается $\mathrm{Hom}(M, N)$ или $\mathrm{Hom}_K(M, N)$, если надо явно указать кольцо, над которым рассматриваются модули.

Пример 6.6 (гомоморфизмы между аддитивными группами вычетов)
Вычислим $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n))$. Поскольку в $\mathbb{Z}/(m)$ любой класс $[z]_m = z[1]_m$ является целым кратным класса $[1]_m$, каждое $\mathbb{Z}$-линейное отображение $\varphi : \mathbb{Z}/(m) \to \mathbb{Z}/(n)$ однозначно задаётся своим значением на этом классе: если $\varphi([1]_m) = x \in \mathbb{Z}/(n)$, то для любого $z \in \mathbb{Z}$

$$\varphi([z]_m) = \varphi(z[1]_m) = z\varphi(z[1]_m) = zx\,.$$

Так как $\varphi + \psi : [1]_m \mapsto \varphi([1]_m) + \psi([1]_m)$, отображение вычисления значений гомоморфизмов на элементе $[1]_m$

$$\mathrm{ev}_{[1]_m} : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n)) \hookrightarrow \mathbb{Z}/(n)\,, \quad \varphi \mapsto \varphi([1]_m)\,,$$

является инъективным гомоморфизмом абелевых групп. Чтобы найти его образ, заметим, что $m[1]_m = [m]_m = 0$ в $\mathbb{Z}/(m)$. Поэтому элемент $x = \varphi([1]_m) \in \mathbb{Z}/(n)$ тоже должен удовлетворять соотношению $mx = m\varphi([1]_m) = \varphi(m[1]_m) = \varphi(0) = 0$.

Упражнение 6.6. Убедитесь, что если $mx = 0$ в $\mathbb{Z}/(n)$, то правило $\varphi([z]_m) = zx$ корректно задаёт $\mathbb{Z}$-линейный гомоморфизм $\varphi : \mathbb{Z}/(m) \to \mathbb{Z}/(n)$.

Таким образом, модуль $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n))$ изоморфен подмодулю

$$\mathrm{Ann}(m) = \{x \in \mathbb{Z}/(n) \mid mx = 0\} \subset \mathbb{Z}/(n)\,.$$

[1] См. n° 2.5 на стр. 32.

Упражнение 6.7. Убедитесь, что решения x уравнения $mx = 0$ в $\mathbb{Z}/(n)$ суть целые кратные вычета $[n/\text{нод}(m,n)]_n$, и они образуют в $\mathbb{Z}/(n)$ подмодуль, изоморфный $\mathbb{Z}/(\text{нод}(m,n))$.

Мы заключаем, что $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m),\mathbb{Z}/(n)) \simeq \mathbb{Z}/(\text{нод}(m,n))$, где классу $[k] \in \mathbb{Z}/(\text{нод}(m,n))$ отвечает гомоморфизм $\mathbb{Z}/(m) \to \mathbb{Z}/(n)$, $[z]_m \mapsto [zkn/\text{нод}(n,m)]_n$. В частности, для всех n, m

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n),\mathbb{Z}/(m)) \simeq \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m),\mathbb{Z}/(n))\,,$$

и если m и n взаимно просты, то $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n),\mathbb{Z}/(m)) \simeq \mathbb{Z}/(1) = 0$.

6.3. Прямые произведения и прямые суммы. Из любого семейства K-модулей M_ν, занумерованных элементами ν произвольного множества $\mathcal{N}$, можно образовать прямое произведение $\prod_{\nu\in\mathcal{N}} M_\nu$, состоящее из всевозможных семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ векторов $v_\nu \in M_\nu$, занумерованных элементами $\nu \in \mathcal{N}$, как в n° 2.6 на стр. 36. Такие семейства можно поэлементно складывать и умножать на скаляры точно также, как мы это делали в n° 2.6 в прямых произведениях абелевых групп и коммутативных колец. А именно, сумма $v+w$ семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ и $w = (w_\nu)_{\nu\in\mathcal{N}}$ имеет ν-м членом элемент $v_\nu + w_\nu$, а на ν-тым членом произведения xv семейства $v = (v_\nu)_{\nu\in\mathcal{N}}$ на скаляр $x \in K$ является элемент xv_ν. Модуль $\prod_{\nu\in\mathcal{N}} M_\nu$ называется *прямым произведением* модулей M_ν, а его подмодуль $\bigoplus_{\nu\in\mathcal{N}} M_\nu$, состоящий из всех семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ с конечным числом ненулевых векторов v_ν, называется *прямой суммой* модулей M_ν. Для конечных множеств $\mathcal{N}$ прямые суммы совпадают с прямыми произведениями. Так, координатный модуль K^r из прим. 6.2 и модуль матриц $\operatorname{Mat}_{m\times n}(K)$ из прим. 6.3 являются прямыми суммами (и произведениями), соответственно, r и mn одинаковых экземпляров K-модуля K.

Пример 6.7 (многочлены и степенные ряды)
Обозначим через Kt^n множество одночленов вида at^n, где $a \in K$, а t — переменная. Каждое множество Kt^n является K-модулем, изоморфным модулю K. Прямая сумма $\bigoplus_{n\geqslant 0} Kt^n$ изоморфна модулю многочленов $K[t]$, а прямое произведение $\prod_{n\geqslant 0} Kt^n$ — модулю формальных степенных рядов $K[\![t]\!]$.

Пример 6.8 (модуль функций со значениями в модуле)
Отображения $Z \to M$ из любого множества Z в произвольный K-модуль M можно складывать и умножать на числа из K по тем же правилам, что выше: для $\varphi, \psi : Z \to M$ и $x \in K$ отображения $\varphi + \psi$ и $x\varphi$ переводят $z \in Z$ в $\varphi(z) + \psi(z)$ и $x\varphi(z)$ соответственно. Эти операции задают на множестве M^Z всех отображений $Z \to M$ структуру K-модуля, изоморфного прямому произведению $\prod_{z\in Z} M_z$ одинаковых копий $M_z = M$ модуля M, занумерованных элементами $z \in Z$. Этот изоморфизм сопоставляет отображению $\varphi : Z \to M$ семейство его значений $\big(\varphi(z)\big)_{z\in Z} \in \prod_{z\in X} M_z$. Если Z является K-модулем, то K-линейные отображения $Z \to M$ составляют подмодуль $\operatorname{Hom}_K(Z,N) \subset M^Z$.

Предложение 6.1
Для любого семейства K-модулей M_μ, занумерованных элементами μ произвольного множества $\mathcal{M}$, и любого K-модуля N имеется изоморфизмом K-модулей

$$\prod_{\mu\in\mathcal{M}} \operatorname{Hom}_K(M_\mu, N) \xrightarrow{\sim} \operatorname{Hom}_K\Big(\bigoplus\nolimits_{\mu\in\mathcal{M}} M_\mu,\ N\Big)\,, \tag{6-6}$$

который переводит семейство K-линейных гомоморфизмов $\varphi_\mu : M_\mu \to N$ в гомоморфизм

$$\bigoplus \varphi_\mu :\ \bigoplus\nolimits_{\mu\in\mathcal{M}} M_\mu \to N\,, \tag{6-7}$$

отображающий каждое семейство векторов $(w_\mu)_{\mu\in\mathcal{M}}$ с конечным числом ненулевых членов в сумму $\sum_{\mu\in\mathcal{M}}\varphi_\mu(w_\mu)$ с конечным числом ненулевых слагаемых.

Доказательство. Отображение (6-6) очевидно является K-линейным гомоморфизмом. Обратное к (6-6) отображение переводит каждый K-линейный гомоморфизм $\psi\colon \bigoplus_{\mu\in\mathcal{M}} M_\mu \to N$ в семейство гомоморфизмов $\varphi_\mu\colon M_\mu \to N$, где для каждого $\nu\in\mathcal{M}$ гомоморфизм $\varphi_\nu = \psi\iota_\nu$ является композицией ψ с вложением $\iota_\nu\colon M_\nu \hookrightarrow \bigoplus_{\mu\in\mathcal{M}} M_\mu$, которое отправляет каждый вектор $u\in M_\nu$ в семейство $(w_\mu)_{\mu\in\mathcal{M}}$ с единственным ненулевым элементом $w_\nu = u$. □

Пример 6.9 (продолжение прим. 6.7 на стр. 104)
В прим. 6.7 мы видели, что модуль многочленов $K[t] \simeq \bigoplus_{n\geqslant 0} Kt^n$ можно воспринимать как прямую сумму модулей $Kt^n \simeq K$. Применительно к этому случаю предл. 6.1 утверждает, что каждое K-линейное отображение $\varphi\colon K[t]\to K$ однозначно задаётся последовательностью K-линейных отображений $\varphi_n = \varphi|_{Kt^n}\colon Kt^n\to K$ — ограничениями отображения φ на подмодули $Kt^n\subset K[t]$. Каждое из отображений φ_n в свою очередь однозначно задаётся своим значением на мономе t^n, т. е. числом $f_n = \varphi_n(t^n)\in K$. Последовательность чисел f_n может быть любой, и отвечающее такой последовательности K-линейное отображение $\varphi\colon K[t]\to K$ переводит многочлен $a(t) = a_0 + a_1t + \ldots + a_mt^m$ в число $\varphi(a) = f_0a_0 + f_1a_1 + \ldots + f_ma_m$. Мы заключаем, что модуль $\operatorname{Hom}_K(K[t],K)$ изоморфен прямому произведению счётного множества копий модуля K, т. е. модулю формальных степенных рядов $K[\![x]\!]$. Изоморфизм сопоставляет последовательности (f_n) её *производящую функцию* $F(x) = \sum_{n\geqslant 0} f_nx^n \in K[\![x]\!]$. Например, для любого $\alpha\in K$ *гомоморфизм вычисления* $\operatorname{ev}_\alpha\colon K[t]\to K$, $f\mapsto f(\alpha)$, переводящий многочлены в их значения в точке $\alpha\in K$ и действующий на базисные мономы по правилу $t^n\mapsto\alpha^n$, имеет $f_n = \alpha^n$ и задаётся рядом $\sum_{n\geqslant 0}\alpha^nx^n = (1-\alpha x)^{-1}\in K[\![x]\!]$.

Упражнение 6.8. В условиях предл. 6.1 постройте изоморфизм K-модулей

$$\bigoplus_{\mu\in\mathcal{M}}\operatorname{Hom}_K(N,M_\mu) \xrightarrow{\sim} \operatorname{Hom}_K\Bigl(N,\bigoplus_{\mu\in\mathcal{M}} M_\mu\Bigr) \tag{6-8}$$

$$\prod_{\mu\in\mathcal{M}}\operatorname{Hom}_K(N,M_\mu) \xrightarrow{\sim} \operatorname{Hom}_K\Bigl(N,\prod_{\mu\in\mathcal{M}} M_\mu\Bigr). \tag{6-9}$$

6.4. Пересечения и суммы подмодулей. В произвольном K-модуле M пересечение любого множества подмодулей также является подмодулем в M. Пересечение всех подмодулей, содержащих заданное множество векторов $A\subset M$, называется *K-линейной оболочкой* множества A или K-подмодулем, *порождённым* множеством A, и обозначается $\operatorname{span}(A)$ или $\operatorname{span}_K(A)$, если надо указать, из какого кольца берутся константы. Линейная оболочка является наименьшим по включению K-подмодулем в M, содержащим A, и может быть иначе описана как множество всех конечных линейных комбинаций $x_1a_1 + \ldots + x_na_n$ векторов $a_i\in A$ с коэффициентами $x_i\in K$, ибо все такие линейные комбинации образуют подмодуль в M и содержатся во всех подмодулях, содержащих A. В противоположность пересечениям, объединения подмодулей почти никогда не являются подмодулями.

Упражнение 6.9. Покажите, что объединение двух подгрупп в абелевой группе является подгруппой если и только если одна из подгрупп содержится в другой.

K-линейная оболочка объединения произвольного множества подмодулей $U_\nu\subset M$ называется *суммой* этих подмодулей и обозначается $\sum_\nu U_\nu \stackrel{\text{def}}{=} \operatorname{span}\bigcup_\nu U_\nu$. Таким образом, сумма подмодулей представляет собою множество всевозможных конечных сумм векторов, принадлежащих

этим подмодулям. Например,

$$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1\,,\ u_2 \in U_2\}$$
$$U_1 + U_2 + U_3 = \{u_1 + u_2 + u_3 \mid u_1 \in U_1\,,\ u_2 \in U_2\,,\ u_3 \in U_3\}$$

и т. д. Если подмодули $U_1, \dots, U_m \subset M$ таковы, что гомоморфизм сложения

$$U_1 \oplus \dots \oplus U_n \to U_1 + \dots + U_n \subset M\,, \quad (u_1, \dots, u_n) \mapsto u_1 + \dots + u_n\,, \tag{6-10}$$

является биекцией между $U_1 \oplus \dots \oplus U_n$ и $U_1 + \dots + U_n$, то сумму $U_1 + \dots + U_n$ называют *прямой* и обозначают $U_1 \oplus \dots \oplus U_n$, как в n° 6.3 выше. Биективность отображения (6-10) эквивалентна тому, что каждый вектор $w \in U_1 + \dots + U_n$ имеет *единственное* разложение $w = u_1 + \dots + u_n$, в котором $u_i \in U_i$ при каждом i.

Предложение 6.2
Сумма подмодулей $U_1, \dots, U_n \subset V$ является прямой если и только если каждый из подмодулей имеет нулевое пересечение с суммой всех остальных. В частности, сумма $U+W$ двух подмодулей прямая тогда и только тогда, когда $U \cap W = 0$.

Доказательство. Обозначим через W_i сумму всех подмодулей U_ν за исключением i-того. Если пересечение $U_i \cap W_i$ содержит ненулевой вектор $u_i = u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_n$, где $u_i \in U_i$ при всех i, то у этого вектора имеется два различных представления[1]

$$0 + \dots + 0 + u_i + 0 + \dots + 0 = u_1 + \dots + u_{i-1} + 0 + u_{i+1} + \dots + u_n\,.$$

Поэтому такая сумма не прямая. Наоборот, если $U_i \cap W_i = 0$ при всех i, то переписывая равенство $u_1 + \dots + u_n = w_1 + \dots + w_n$, где $u_\nu, w_\nu \in U_\nu$ при всех i, в виде $u_i - w_i = \sum_{\nu \neq i}(w_\nu - u_\nu)$, заключаем, что этот вектор лежит в $U_i \cap W_i = 0$. Поэтому $u_i = w_i$ для каждого $i = 1, \dots, n$. □

Следствие 6.1
Для того чтобы модуль M распадался в прямую сумму собственных подмодулей $L, N \subset M$ необходимо и достаточно, чтобы $L + N = M$ и $L \cap N = 0$. □

6.5. Фактормодули. Для любых K-модуля M подмодуля $N \subseteq M$ можно образовать *фактормодуль* M/N, состоящий из классов

$$[m]_N = m\,(\mathrm{mod}\ N) \stackrel{\text{def}}{=} m + N = \{m' \in M \mid m' - m \in N\}\,,$$

которые являются аддитивными сдвигами подмодуля N на всевозможные элементы $m \in M$ или, что тоже самое, классами эквивалентности по отношению $m_1 \equiv m_2\ (\mathrm{mod}\ N)$ сравнимости по модулю N, означающему, что $m_1 - m_2 \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами $[m_1]_N + [m_2]_N \stackrel{\text{def}}{=} [m_1 + m_2]_N$ и $x \cdot [m]_N \stackrel{\text{def}}{=} [xm]_N$.

Упражнение 6.10. Проверьте, что отношение сравнимости по модулю N является эквивалентностью, а операции корректно определены и удовлетворяют аксиомам (6-1) – (6-4).

В частности, факторкольцо K/I кольца K по идеалу $I \subset K$ является фактором K-модуля K по его K-подмодулю I, ср. с прим. 6.1 выше.

[1] В левом отлично от нуля только i-е слагаемое, а в правом оно нулевое.

6.5.1. Строение гомоморфизма. Любой гомоморфизм K-модулей $\varphi : M \to N$ является композицией сюръективного гомоморфизма факторизации

$$\pi_\varphi : M \twoheadrightarrow M/\ker\varphi\,, \quad w \mapsto [w]_{\ker\varphi}$$

и отображения

$$\iota_\varphi : M/\ker\varphi \hookrightarrow N\,, \quad [w]_{\ker\varphi} \mapsto \varphi(w)\,,$$

которое корректно определено и инъективно в силу того, что

$$\varphi(u) = \varphi(w) \iff u - w \in \ker\varphi \iff [u]_{\ker\varphi} = [w]_{\ker\varphi}\,,$$

и K-линейно, ибо

$$\iota_\varphi(x[u] + y[w]) = \iota_\varphi([xu + yw]) = \varphi(xu + yw) = x\varphi(u) + y\varphi(w) = x\iota_\varphi([u]) + y\iota_\varphi([w])\,.$$

Мы заключаем, что $\iota_\varphi : M/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$ является изоморфизмом K-модулей, а произвольный гомоморфизм $\varphi : M \to N$ канонически раскладывается в композицию $\varphi = \iota_\varphi\pi_\varphi$ мономорфизма ι_φ и эпиморфизма π_φ. Этот факт известен как *теорема о строении гомоморфизма*.

6.5.2. Фактор модуля по идеалу кольца Для произвольных K-модуля M и идеала $I \subset K$ обозначим через

$$IM \stackrel{\text{def}}{=} \{x_1a_1 + \ldots + x_na_n \in M \mid x_i \in I,\ a_i \in M,\ n \in \mathbb{N}\}$$

K-подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I.

Упражнение 6.11. Проверьте, что IM действительно является K-подмодулем в M.

Фактор модуль M/IM состоит из классов $[w]_{IM} = w + IM = \{v \in M \mid v - w \in IM\}$ и является модулем над факторкольцом K/I: умножение векторов на скаляры задаётся правилом

$$[x]_I \cdot [w]_{IM} = [xw]_{[IM]}\,,$$

корректным, поскольку для $x' = x + y$ и $w' = w + u$, где $y \in I$, $u \in IM$, имеем $[x'w'] = [xw + (xu + yw + xu)] = [xw]$, так как сумма в круглых скобках лежит в IM.

Если $M = N_1 \oplus \ldots \oplus N_m$ раскладывается с прямую сумму своих подмодулей $N_i \subset M$, то возникает аналогичное разложение $IM = IN_1 \oplus \ldots \oplus IN_m$ в сумму подмодулей

$$IN_i = N_i \cap IM\,.$$

В самом деле, подмодули IN_i линейно порождают IM, коль скоро подмодули N_i линейно порождают M, при этом $IN_i \subset N_i \cap IM$, а каждый подмодуль $N_i \cap IM$ имеет нулевое пересечение с суммой остальных подмодулей $N_\nu \cap IM$ с $\nu \neq i$, ибо $N_i \cap \sum_{\nu\neq i} N_\nu = 0$. Мы заключаем, что

$$M/IM = (N_1/IN_1) \oplus \ldots \oplus (N_m/IN_m)\,.$$

В частности, $K^n/IK^n = (K/I)^n$ для любого идеала $I \subset K$.

6.6. Дополнительные подмодули и разложимость. Подмодули $L, N \subset M$ называются *дополнительными*, если $M = L \oplus N$. Согласно сл. 6.1 на стр. 106 для этого необходимо и достаточно, чтобы $L \cap N = 0$ и $L + N = M$. В такой ситуации модуль M называется *разложимым*, а про подмодули L, N говорят, что они *отщепляются* от M прямыми слагаемыми.

Упражнение 6.12. Пусть модуль M является прямой суммой своих подмодулей $L, N \subset M$. Покажите, что $M/N \simeq L$ и $M/L \simeq N$.

Модуль M, не представимый в виде прямой суммы своих собственных подмодулей называется *неразложимым*. Например, $\mathbb{Z}$-модуль $\mathbb{Z}$ неразложим, хотя и имеет собственные $\mathbb{Z}$-подмодули. В самом деле, каждый собственный подмодуль $I \subset \mathbb{Z}$ представляет собою главный идеал $I = (d)$. Согласно упр. 6.12, разложение $\mathbb{Z} = (d) \oplus N$ означает наличие в $\mathbb{Z}$ подмодуля $N \subset \mathbb{Z}$, изоморфного $\mathbb{Z}$-модулю $\mathbb{Z}/(d)$, все элементы которого аннулируются умножением на число $d \in \mathbb{Z}$, тогда как в $\mathbb{Z}$-модуле $\mathbb{Z}$ умножение на число d действует инъективно.

Пример 6.10 (проекции)
С каждым разложением $M = N_1 \oplus N_2$ в прямую сумму дополнительных подмодулей $N_1, N_2 \subset M$ связаны линейные эндоморфизмы

$$\pi_1 : M \to M\,,\ (u_1, u_2) \mapsto (u_1, 0) \quad \text{и} \quad \pi_2 : M \to M\,,\ (u_1, u_2) \mapsto (0, u_2)\,,$$

которые называются *проекциями* модуля M, соответственно, на подмодуль N_1 вдоль подмодуля N_2 и на подмодуль N_2 вдоль подмодуля N_1. Первая из них имеет $\ker \pi_1 = N_2$, $\operatorname{im} \pi_1 = N_1$ и тождественно действует на подмодуле N_1, а вторая имеет $\ker \pi_2 = N_1$, $\operatorname{im} \pi_2 = N_2$ и тождественно действует на подмодуле N_2. Эти эндоморфизмы удовлетворяют соотношениям

$$\pi_1\pi_2 = \pi_2\pi_1 = 0\,, \quad \pi_1 + \pi_2 = \mathrm{Id}_M\,, \quad \pi_1^2 = \pi_1\,, \quad \pi_2^2 = \pi_2\,.$$

Наоборот, если линейный эндоморфизм $\pi : M \to M$ удовлетворяет соотношению $\pi^2 = \pi$, то $\pi(\pi v) = \pi^2 v = \pi v$ для всех $v \in M$. Поэтому π тождественно действует на $\operatorname{im} \pi$ и $v - \pi(v) \in \ker \pi$ для любого $v \in M$. Тем самым, $\ker \pi \cap \operatorname{im} \pi = 0$ и $\operatorname{im} \pi + \ker \pi = M$, откуда $M = \ker \pi \oplus \operatorname{im} \pi$. Так как $\pi(u + w) = w$ для всех $u \in \ker \pi$, $w \in \operatorname{im} \pi$, мы заключаем, что π является проекцией M на $\operatorname{im} \pi$ вдоль $\ker \pi$.

Упражнение 6.13. Пусть эндоморфизм $\pi : V \to V$ удовлетворяет соотношению $\pi^2 = \pi$. Покажите, что $\overline{\pi} = \mathrm{Id}_V - \pi$ удовлетворяет соотношениям $\overline{\pi}^2 = \overline{\pi}$, $\overline{\pi}\pi = \pi\overline{\pi} = 0$ и является проекцией модуля V на $\ker \pi$ вдоль $\operatorname{im} \pi$.

Следствие 6.2
Модуль M разложим если и только если существует эндоморфизм $\pi \in \operatorname{End} M$ с $\pi^2 = \pi$, и в этом случае $M = \ker \pi \oplus \operatorname{im} \pi$. □

Определение 6.1 (проекторы)
Линейный эндоморфизм π со свойством $\pi^2 = \pi$ называется *идемпотентом* или *проектором*.

6.7. Образующие и соотношения. Говорят, что вектор v из K-модуля M *линейно выражается* над K через векторы $w_1, \ldots, w_m$, если $v = x_1 w_1 + \ldots + x_m w_m$ для некоторых $x_1, \ldots, x_m \in K$. Правая часть этой формулы называется *линейной комбинацией* векторов $w_i \in V$ с коэффициентами $x_i \in K$. Линейная комбинация, в которой все коэффициенты $x_i = 0$, называется *тривиальной*.

Множество векторов $Z \subset M$ называется *линейно зависимым*, если некоторая нетривиальная конечная линейная комбинация векторов из Z обращается в нуль, т. е. $x_1u_1 + \ldots + x_ku_k = 0$ для некоторых $u_1, \ldots, u_k \in Z$ и $x_1, \ldots, x_k \in K$, среди которых есть $x_i \neq 0$. Каждая такая линейная комбинация называется *линейным соотношением* на векторы из множества Z. Обратите внимание, что любой набор векторов, содержащий нулевой вектор, линейно зависим, поскольку $1 \cdot 0 + 0 \cdot v = 0$ для произвольного $v \in V$.

Мы говорим, что множество $Z \subset M$ *порождает* модуль M, если любой вектор $v \in M$ является линейной комбинацией конечного числа векторов из Z, т. е. $v = x_1u_1 + \ldots + x_mu_m$ для некоторых $x_i \in K$, $w_i \in G$ и $m \in \mathbb{N}$. Векторы из множества Z называются в этом случае *образующими* или *порождающими* модуля M. Например, $1 \in K$ порождает K-модуль K, а класс $[1]_I$ порождает K-модуль K/I, где $I \subset K$ — любой идеал. Модуль называется *конечно порождённым*, если у него имеется конечное множество образующих. Например, модуль матриц[1] $\mathrm{Mat}_{m\times n}(K)$ линейно порождается mn матрицами E_{ij} с единственным ненулевым элементом 1, стоящим в клетке (i, j), поскольку каждая матрица $A = (a_{ij})$ является линейной комбинацией $A = \sum_{ij} a_{ij}E_{ij}$. Напротив, модуль многочленов $K[t]$ нельзя породить никаким конечным множеством многочленов, поскольку степень линейной комбинации многочленов не превышает максимальной из их степеней этих многочленов.

6.7.1. Свободные модули. Множество $E \subset M$ называется *базисом* модуля M, если каждый вектор $v \in M$ единственным образом линейно выражается через векторы из E, т. е.

$$v = \sum_{e\in E} x_e e\,,$$

где все $x_e \in K$ и только конечное множество из них отлично от нуля, причём равенство двух таких сумм $\sum_{e\in E} x_e e = \sum_{e\in E} y_e e$ равносильно равенству коэффициентов $x_e = y_e$ при каждом векторе $e \in E$. Модуль M, обладающий базисом, называется *свободным*, а коэффициенты x_e единственного линейного выражения вектора v через базисные векторы $e \in E$ какого-либо базиса $E \subset M$ называются *координатами* вектора v в базисе E. Иначе можно сказать, что свободный модуль с базисом E представляет собою прямую сумму $\bigoplus_{e\in E} Ke$ одинаковых копий $Ke = K$ модуля K, занумерованных элементами $e \in E$.

Например, модуль многочленов $K[t]$ свободен, и его базис состоит из мономов t^n, ср. с прим. 6.7 на стр. 104. Координатный модуль K^n из прим. 6.2 на стр. 101 тоже свободен, так как каждый вектор $(x_1, \ldots, x_n) \in K^n$ единственным образом представляется в виде линейной комбинации $x_1e_1 + \ldots + x_ne_n$ стандартных базисных векторов $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ с ровно одной ненулевой координатой, равной 1 и стоящей на i-том месте.

Если K-модуль F свободен с базисом $u_1, \ldots, u_n$, то отображение

$$K^n \xrightarrow{\sim} F\,, \quad (x_1, \ldots, x_n) \mapsto x_1u_1 + \ldots + x_nu_n\,,$$

задаёт линейный изоморфизм координатного модуля K^n с F. Ниже, в сл. 7.3 на стр. 117 мы докажем, что при $n \neq m$ модули K^m и K^n не изоморфны ни для какого коммутативного кольца K с единицей или, что то же самое, что все базисы свободного модуля F состоят из одинакового числа векторов. Это число обозначается $\mathrm{rk}\, F$ и называется *рангом* свободного модуля F.

Предостережение 6.2. Если кольцо скаляров K не является полем, то отнюдь не все K-модули свободны. Например, идеал $I \subset K$ порождается как модуль над K одним элементом если и толь-

[1] См. прим. 6.3 на стр. 102.

ко если он главный, т. е. $I = (d)$ для некоторого $d \in K$. Такой идеал является свободным K-модулем с базисом d если и только если d не делит нуль в K — в противном случае есть линейная зависимость $\lambda d = 0$ с ненулевым $\lambda \in K$. Если идеал $I \subset K$ не главный, то его нельзя линейно породить менее, чем двумя элементами, а любой набор из двух и более элементов кольца линейно зависим, так как $ab - ba = 0$ для любых $a, b \in K$. Поэтому никакой идеал, не являющийся главным, не имеет базиса как модуль над K. Так, идеал $(x, y) \subset \mathbb{Q}[x, y]$, состоящий из всех многочленов с нулевым свободным членом, как модуль над кольцом $K = \mathbb{Q}[x, y]$ линейно порождается векторами $w_1 = x$ и $w_2 = y$, которые линейно зависимы над K, ибо $yw_1 - xw_2 = 0$. Обратите внимание, что ни один из них не выражается $\mathbb{Q}[x, y]$-линейно через другой.

Предложение 6.3
Множество векторов E составляет базис K-модуля M если и только если оно линейно независимо и линейно порождает M над K.

Доказательство. Пусть множество векторов E порождает K-модуль M. Если существует линейное соотношение $x_1e_1 + \ldots + x_ne_n = 0$, в котором $e_i \in E$ и $x_1 \neq 0$, то оно у нулевого вектора $0 \in M$ имеется два различных представления в линейной комбинации векторов из E: первое даётся указанным соотношением, второе имеет вид $0 = 0 \cdot e_1$. Наоборот, если множество E линейно независимо и имеется равенство $\sum_{e\in E} x_e e = \sum_{e\in E} y_e e$, в обоих частях которого имеется лишь конечное число ненулевых коэффициентов, то перенося все ненулевые слагаемые в одну часть, получаем конечное линейное соотношение $\sum_{e\in E}(x_e - y_e)\cdot e = 0$, возможное только если все коэффициенты нулевые, т. е. только когда $x_e = y_e$ при всех e. □

Предложение 6.4
Пусть векторы $e_1, \ldots, e_n$ образуют базис свободного модуля F над коммутативным кольцом K. Тогда для любого K-модуля M и любого набора из n векторов $w_1, \ldots, w_n \in M$ существует единственное такое линейное отображение $f : F \to M$, что $f(e_i) = w_i$ для всех i.

Доказательство. Если такое отображение f существует, то в силу линейности оно действует на произвольный вектор $v = \sum x_i e_i \in F$ по правилу $f(v) = \sum x_i f(e_i) = \sum x_i w_i$ и тем самым единственно. С другой стороны, для любого набора векторов $w_1, \ldots, w_n \in M$ отображение

$$f : F \to M, \quad x_1e_1 + \ldots + x_ne_n \mapsto x_1w_1 + \ldots + x_nw_n,$$

очевидно линейно и при каждом i переводит e_i в w_i. □

6.7.2. Задание модуля образующими и соотношениями. Если K-модуль M линейно порождается над K векторами $w_1, \ldots, w_m$, то имеется K-линейный эпиморфизм

$$\pi_{w_1,\ldots,w_m} : K^m \twoheadrightarrow M, \quad (x_1, \ldots, x_m) \mapsto x_1w_1 + \ldots + x_mw_m. \tag{6-11}$$

Его ядро $R = \ker \pi$ называется *модулем соотношений* между образующими w_i, поскольку оно состоит из всех тех строк $(x_1, \ldots, x_n) \in K^m$, которые являются коэффициентами линейных соотношений $x_1w_1 + \ldots + x_mw_m = 0$ между образующими w_i в модуле M. Таким образом, каждый конечно порождённый K-модуль M имеет вид $M = K^m/R$ для некоторого числа $m \in \mathbb{N}$ и некоторого подмодуля $R \subset K^m$.

Пример 6.11 (аддитивные группы вычетов)
Аддитивная группа вычетов $\mathbb{Z}/(m)$, рассматриваемая как $\mathbb{Z}$-модуль[1], линейно порождается классом $[1]_m$. Отображение (6-11)

$$\pi_{[1]_m}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(m)\,, \quad z \mapsto z[1]_m = [z]_m\,,$$

есть не что иное, как гомоморфизм факторизации по модулю m. Таким образом, аддитивная абелева группа $\mathbb{Z}/(m)$ является фактором свободного модуля $\mathbb{Z}$ по подмодулю соотношений $R = (m) \subset \mathbb{Z}$, который тоже свободен с базисом m.

6.7.3. Соотношения и гомоморфизмы. Для любых K-модулей M, N и подмодуля $L \subset M$ гомоморфизмы $\varphi : M \to N$, переводящие L в нуль, образуют K-подмодуль

$$\operatorname{Ann}^N(L) \stackrel{\text{def}}{=} \{\varphi : M \to N \mid \varphi(L) = 0\}$$

в модуле $\operatorname{Hom}_K(M, N)$ всех гомоморфизмов, ибо если гомоморфизмы $\varphi_1, \varphi_2 : M \to N$ аннулируют L, то любая их линейная комбинация $x_1\varphi_1 + y_1\varphi_2$ тоже аннулирует L. Каждый гомоморфизм $\varphi \in \operatorname{Ann}^N(L)$ корректно задаёт K-линейное отображение

$$\varphi_L : M/L \to M\,, \quad [w]_L \mapsto f(w)\,, \tag{6-12}$$

так как $\varphi(w + u) = \varphi(w) + \varphi(u) = \varphi(w)$ для любого вектора $u \in L$.

Предложение 6.5
Отображение $\operatorname{Ann}^N(L) \to \operatorname{Hom}_K(M/L, N)$, $\varphi \mapsto \varphi_L$, является изоморфизмом K-модулей. Обратный к нему изоморфизм $\operatorname{Hom}_K(M/L, N) \to \operatorname{Ann}^N(L)$, $\psi \mapsto \psi\pi_L$, переводит гомоморфизм $\psi : M/L \to N$ в его композицию с эпиморфизмом факторизации $\pi_L : M \twoheadrightarrow M/L$.

Доказательство. Поскольку отображение (6-12) K-линейно зависит от φ, правило $\varphi \mapsto \varphi_L$ задаёт гомоморфизм K-модулей. Так как для любого гомоморфизма $\psi : M/L \to M$ выполняется равенство $(\psi\pi_L)_L = \psi$, а для любого гомоморфизма $\varphi \in \operatorname{Ann}^N(L)$ — равенство $\varphi_L\pi_L = \varphi$, отображения $\varphi \mapsto \varphi_L$ и $\psi \mapsto \psi\pi_L$ обратны друг другу и тем самым биективны. □

Предложение 6.6
Пусть $M_1 = F_1/R_1$, $M_2 = F_2/R_2$, где модули F_1 и F_2 свободны. Тогда

$$\operatorname{Hom}(M_1, M_2) = \{\varphi \in \operatorname{Hom}(F_1, F_2) \mid \varphi(R_1) \subset R_2\}/\{\varphi \in \operatorname{Hom}(F_1, F_2) \mid \varphi(F_1) \subset R_2\}\,.$$

Доказательство. По предл. 6.5 $\operatorname{Hom}(M_1, M_2) \simeq \operatorname{Ann}^{M_2}(R_1) = \{\varphi \in \operatorname{Hom}(F_1, M_2) \mid \varphi(R_1) = 0\}$. Обозначим через $\pi_2 : F_2 \twoheadrightarrow M_2$ гомоморфизм факторизации по подмодулю $R_2 \subset F_2$. Линейное отображение

$$\varrho : \operatorname{Hom}(F_1, F_2) \to \operatorname{Hom}(F_1, M_2)\,, \quad \varphi \mapsto \pi_2 \circ \varphi\,, \tag{6-13}$$

имеет ядро $\ker \varrho = \{\varphi \in \operatorname{Hom}(F_1, F_2) \mid \varphi(F_1) \subset R_2\}$. Покажем, что это отображение сюръективно. Обозначим через $E \subset F_1$ базис модуля F_1. Пусть $\varphi : F_1 \to M_2$ — произвольный гомоморфизм. Для каждого $e \in E$ выберем такой вектор $w_e \in F_2$, что $\varphi(e) = \pi_2(w_e)$. По предл. 6.4 на стр. 110 существует такой гомоморфизм $\widetilde{\varphi} : F_1 \to F_2$, что $\widetilde{\varphi}(e) = w_e$ для всех $e \in E$. Тогда $\pi_2 \circ \widetilde{\varphi}(e) = \varphi(e)$ для всех $e \in E$.

[1] См. прим. 6.4 на стр. 102.

Упражнение 6.14. Пусть множество векторов Z линейно порождает модуль M, а линейные отображения $\varphi, \psi : M \to N$ таковы, что $\varphi(u) = \psi(u)$ для всех $u \in Z$. Покажите, что $\varphi = \psi$.

Из упражнения вытекает, что $\varrho(\widetilde{\varphi}) = \varphi$. Тем самым, отображение (6-13) эпиморфно. Полным прообразом подмодуля $\mathrm{Ann}^{M_2}(R_1) \subset \mathrm{Hom}(F_1, M_2)$ при эпиморфизме (6-13) является подмодуль

$$\{\varphi \in \mathrm{Hom}(F_1, F_2) \mid \varphi(R_1) \subset R_2\}\,.$$

В силу теоремы о строении гомоморфизма[1], применённой к ограничению отображения ϱ на этот подмодуль, $\{\varphi \in \mathrm{Hom}(F_1, F_2) \mid \varphi(R_1) \subset R_2\}/\ker \varrho \simeq \mathrm{Ann}^{M_2}(R_1)$, что и требовалось. □

Задачи для самостоятельного решения к §6

Задача 6.1. Модуль, порождённый одной образующей, называется *циклическим*. Докажите, что
а) всякий циклический $\mathbb{Z}$-модуль изоморфен либо $\mathbb{Z}$, либо $\mathbb{Z}/(n)$
б) $\mathbb{Z}$-модуль $\mathbb{Z}/(n) \oplus \mathbb{Z}/(m)$ циклический если и только если нод$(m, n) = 1$.

Задача 6.2. Являются ли циклическими $\mathbb{Z}$-модули а) $\mathbb{Z}^2$ б) $\mathbb{Z} \oplus \mathbb{Z}/(n)$?

Задача 6.3. $\mathbb{Z}$-подмодуль $L \subset \mathbb{Z}^2$ порождается векторами $(1, 2)$ и $(2, 1)$. Отщепляется ли он прямым слагаемым[2]?

Задача 6.4. Модуль M называется *полупростым*, если для любой его подмодуль отщепляется прямым слагаемым. Полупросты ли $\mathbb{Z}$-модули: а) $\mathbb{Z}^k$ б) $\big(\mathbb{Z}/(p)\big)^k$ в) $\mathbb{Z}/(p^k)$, где $p \in \mathbb{N}$ простое и $k > 1$?

Задача 6.5. Верно ли, что порождённый вектором $w = (z_1, \ldots, z_m) \in \mathbb{Z}^m$ подмодуль $\mathbb{Z}w \subset \mathbb{Z}^m$ отщепляется прямым слагаемым[3] если и только если нод$(z_1, \ldots, z_m) = 1$?

Задача 6.6. Пусть фактормодуль $L = M/N$ свободен. Верно ли, что $M \simeq N \oplus L$?

Задача 6.7. Являются ли конечно порождёнными $\mathbb{Z}$-модули: а) $\mathbb{Q}$ б) $\mathbb{Q}/\mathbb{Z}$.

Задача 6.8 (целозначные многочлены). Пусть

$$M_n = \{f \in \mathbb{Q}[x] \mid \deg f \leqslant n \text{ и } \forall\, z \in \mathbb{Z}\ f(z) \in \mathbb{Z}\}\,.$$

Докажите, что многочлены $\gamma_0(x) = 1$ и $\gamma_k(x) = \binom{x+k}{k} = (x+1)\ldots(x+k)/k!$, где $1 \leqslant k \leqslant n$, составляют базис модуля M_n над $\mathbb{Z}$ и подсчитайте число элементов в факторе $M_n/(M_n \cap \mathbb{Z}[x])$. Для этого выясните, как действует на многочлены γ_k оператор $\nabla : f(x) \mapsto f(x) - f(x-1)$, и покажите, что любой многочлен $f \in M_n$ единственным образом записывается в виде

$$f = z_0\gamma_0 + z_1\gamma_1 + \ldots + z_n\gamma_n\,,\ \text{где}^4\ z_k \in \mathbb{Z}\,.$$

Задача 6.9*. Пусть $d \in \mathbb{Z}$ свободно от квадратов и $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[t]/(t^2 - d)$. Покажите, что лежащие в $\mathbb{Q}[\sqrt{d}]$ корни приведённых квадратных трёхчленов с целыми коэффициентами образуют свободный $\mathbb{Z}$-модуль ранга 2, и укажите в нём какой-нибудь базис над $\mathbb{Z}$.

[1] См. n° 6.5.1 на стр. 107.
[2] Т. е. существует ли такой $\mathbb{Z}$-подмодуль $N \subset \mathbb{Z}^2$, что $\mathbb{Z}^2 = L \oplus N$, см. n° 6.6 на стр. 108.
[3] Т. е. существует такой $\mathbb{Z}$-подмодуль $N \subset \mathbb{Z}^m$, что $\mathbb{Z}^m = \mathbb{Z}w \oplus N$.
[4] Подсказка: каждый коэффициент z_k равен значению многочлена $\nabla^k f$ при $x = -1$.

Задача 6.10. Для трёх вложенных друг в друга подмодулей $K \subset L \subset M$ произвольного модуля убедитесь, что L/K является подмодулем в M/K и докажите, что $(M/K)/(L/K) \simeq M/L$.

Задача 6.11. Постройте для любых двух подмодулей M, N произвольного модуля изоморфизм

$$(M+N)/N \simeq M/(M \cap N).$$

Задача 6.12. Сколько элементов в факторе $\mathbb{Z}$-модуля $\mathbb{Z}/(9) \oplus \mathbb{Z}/(27)$ по $\mathbb{Z}$-подмодулю, порождённому элементами: а) $\big([3]_9, [9]_{27}\big)$ б) $\big([3]_9, [6]_{27}\big)$ в) $\big([6]_9, [3]_{27}\big)$.

Задача 6.13. Опишите модули гомоморфизмов:
а) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(12), \mathbb{Z}/(20)\big)$ б) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(20), \mathbb{Z}/(12)\big)$ в) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(2) \oplus \mathbb{Z}/(8), \mathbb{Z}/(4)\big)$
г) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(8), \mathbb{Z}/(16) \oplus \mathbb{Z}/(4)\big)$ д) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(2) \oplus \mathbb{Z}/(8), \mathbb{Z}/(4) \oplus \mathbb{Z}/(16)\big)$
е) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(m), \mathbb{Z}\big)$ ж) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(m), \mathbb{Q}\big)$ з) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}\big)$.

Задача 6.14. Существует ли инъективный гомоморфизм а) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(8) \hookrightarrow \mathbb{Z}/(2) \oplus \mathbb{Z}/(16)$ б) $\mathbb{Z}/(4) \oplus \mathbb{Z}/(4) \hookrightarrow \mathbb{Z}/(2) \oplus \mathbb{Z}/(16)$ в) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \hookrightarrow \mathbb{Z}/(2) \oplus \mathbb{Z}/(16)$?

Задача 6.15. Докажите для любых линейных эндоморфизмов $f, g : M \to M$ произвольного модуля M включения а) $\ker(fg) \supset \ker(g)$ б) $\mathrm{im}(fg) \subset \mathrm{im}(f)$ и приведите примеры, в которых оба эти включения строгие.

Задача 6.16. Докажите для любого линейного эндоморфизма $f : M \to M$ произвольного модуля M импликации:
а) $\ker(f^k) = \ker(f^{k+1}) \Rightarrow \forall\, n \in \mathbb{N}\ \ker(f^k) = \ker(f^{k+n})$
б) $\mathrm{im}(f^k) = \mathrm{im}(f^{k+1}) \Rightarrow \forall\, n \in \mathbb{N}\ \mathrm{im}(f^k) = \mathrm{im}(f^{k+n})$.

Задача 6.17. Пусть линейное отображение модулей $f : M \to N$ переводит подмодуль $U \subset N$ в подмодуль $W \subset M$. Покажите, что отображение $\overline{f} : M/U \to M/W, [v]_U \mapsto [f(v)]_W$, корректно определено и линейно.

Задача 6.18 (нётеровы модули). Докажите, что следующие свойства модуля M над произвольным коммутативным кольцом эквивалентны[1]: а) любое множество векторов $X \subset M$ содержит конечное подмножество, линейная оболочка которого совпадает с линейной оболочкой всего X б) каждый подмодуль $N \subseteq M$ конечно порождён в) каждая возрастающая цепочка вложенных подмодулей $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots \subseteq M$ стабилизируется, т. е. существует такое $n \in \mathbb{N}$, что $N_\nu = N_n$ при $\nu \geqslant n$.

Задача 6.19. Покажите, что а) всякий сюръективный эндоморфизм нётерова модуля является изоморфизмом б) если K-модуль M нётеров, то факторкольцо $K/\mathrm{Ann}(M)$ по идеалу

$$\mathrm{Ann}(M) \stackrel{\text{def}}{=} \{x \in K \mid xM = 0\}$$

тоже нётерово.

Задача 6.20. Покажите, что каждый конечно порождённый модуль над нётеровым[2] кольцом а) нётеров б) все его подмодули и фактормодули конечно порождены.

[1] Ср. с лем. 5.1 на стр. 85.
[2] См. n° 5.1.1 на стр. 85.

§7. Векторные пространства

7.1. Базисы и размерность. Пусть $\Bbbk$ — произвольное поле. Унитальные $\Bbbk$-модули[1] называются *векторными пространствами* над полем $\Bbbk$. Таким образом, векторное пространство — это абелева группа векторов V вместе с операцией умножения векторов на скаляры из $\Bbbk$:

$$\Bbbk \times V \to V\,, \quad (x, v) \mapsto xv = vx\,,$$

которая удовлетворяет четырём свойствам (6-1) – (6-4) со стр. 101. Главное отличие векторных пространств от модулей над произвольными кольцами заключается в том, что линейная зависимость векторов над полем означает, что любой вектор, входящий в неё с ненулевым коэффициентом, линейно выражается через остальные. Скажем, если

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = 0 \text{ и } \lambda_m \neq 0\,,$$

то $v_m = -(\lambda_1/\lambda_m)v_1 - \ldots - (\lambda_{m-1}/\lambda_m)v_{m-1}$. Над произвольным кольцом это не так: например, многочлены x и y линейно зависимы над кольцом $\mathbb{Q}[x, y]$, ибо $xy - yx = 0$, но не один из них не выражается $\mathbb{Q}[x, y]$-линейно через другой.

Лемма 7.1 (лемма о замене)
Если векторы $w_1, \ldots, w_m$ линейно порождают векторное пространство V над полем $\Bbbk$, а векторы $u_1, \ldots, u_k \in V$ линейно независимы, то $m \geqslant k$ и векторы w_i можно перенумеровать так, что набор векторов $u_1, \ldots, u_k, w_{k+1}, \ldots, w_m$, полученный заменой первых k из них на векторы u_i, тоже порождает V.

Доказательство. Пусть $u_1 = x_1 w_1 + \ldots + x_m w_m$. Так как u_i линейно независимы, $u_1 \neq 0$, и среди коэффициентов x_i есть ненулевой. Перенумеруем векторы w_i так, чтобы $x_1 \neq 0$. Поскольку вектор w_1 линейно выражается через u_1 и $w_2, \ldots, w_m$:

$$w_1 = \frac{1}{x_1}\,u_1 - \frac{x_2}{x_1}\,w_2 - \ \ldots\ - \frac{x_m}{x_1}\,w_m\,,$$

векторы u_1, w_2, $w_3, \ldots, w_m$ порождают V. Далее действуем по индукции. Пусть для очередного $i < k$ векторы $u_1, \ldots, u_i, w_{i+1}, \ldots, w_m$ порождают V. Тогда

$$u_{i+1} = y_1 u_1 + \ldots + y_i u_i + x_{i+1} w_{i+1} + \ldots + x_m w_m\,.$$

В силу линейной независимости векторов u_ν вектор u_{i+1} нельзя линейно выразить только через векторы $u_1, \ldots, u_i$. Поэтому в написанном разложении присутствует с ненулевым коэффициентом хоть один из оставшихся векторов w_j. Следовательно, $m > i$ и мы можем занумеровать оставшиеся w_j так, чтобы $x_{i+1} \neq 0$. Теперь, как и на первом шаге, вектор w_{i+1} линейно выражается через векторы $u_1, \ldots, u_{i+1}, w_{i+2}, \ldots, w_m$. Тем самым, эти векторы линейно порождают V, что воспроизводит индуктивное предположение. □

Теорема 7.1 (теорема о базисе)
Пусть векторное пространство V линейно порождается конечным множеством векторов. Тогда каждый порождающий V набор векторов содержит в себе некоторый базис, каждый линейно независимый набор векторов можно дополнить до базиса, и все базисы состоят из одинакового количества векторов.

[1] См. n° 6.1 на стр. 101.

Доказательство. Поскольку векторов в любом линейно независимом наборе не больше, чем в любом порождающем, во всех базисах одинаковое число векторов.

Если конечный набор векторов порождает V, то последовательно удаляя из него векторы, линейно выражающиеся через остальные, мы придём к линейно независимому порождающему набору, т. е. к базису.

Если задан линейно независимый набор векторов $u_1, \dots, u_k$, то по лемме о замене в любом базисе $e_1, \dots, e_n$ пространства V можно заменить некоторые k векторов e_i векторами u_i так, что полученный набор из n векторов останется порождающим. Он будет базисом, так как по уже доказанному содержит в себе некоторый базис из n векторов. □

Определение 7.1
Векторное пространство V называется *конечномерным*, если оно линейно порождается конечным множеством векторов. Число векторов в базисе такого пространства V называется его *размерностью* и обозначается $\dim V$ или $\dim_{\mathbb{k}} V$, если важно явно указать поле $\mathbb{k}$, над которым рассматривается векторное пространство.

Следствие 7.1
В n-мерном векторном пространстве V всякий линейно независимый набор из n векторов, а также всякий линейно порождающий пространство V набор из n векторов являются базисами.

Доказательство. По лем. 7.1 при замене любого базиса любыми n линейно независимыми векторами получится порождающий набор, т. е. тоже базис. По теор. 7.1 любой порождающий набор из n векторов содержит в себе некоторый базис. Так как этот базис тоже состоит из n векторов, он совпадает с исходным набором. □

Следствие 7.2
В конечномерном пространстве V каждое векторное подпространство $U \subset V$ тоже конечномерно и $\dim U \leqslant \dim V$, причём равенство размерностей равносильно равенству $U = V$, а при $U \neq V$ всегда существует такое[1] подпространство $W \subset V$, что $V = U \oplus W$.

Доказательство. Если k векторов $u_1, \dots, u_k \in U$ линейно независимы, но не порождают U, то для любого ненулевого вектора $u_{k+1} \in U$, который линейно через них не выражается, набор из $k+1$ векторов $u_1, \dots, u_k, u_{k+1}$ тоже линейно независим. По лемме о замене, линейно независимый набор векторов из подпространства $U \subset V$ не может содержать больше $\dim V$ векторов. Таким образом, начав с произвольного линейно независимого набора в U и добавляя к нему векторы, линейно не выражающиеся через предыдущие, мы через конечное число шагов получим линейно независимый набор, порождающий U, т. е. базис. По теореме о базисе, этот базис можно достроить подходящими векторами $w_1, \dots, w_m$ до базиса в V. Поэтому $\dim U \leqslant \dim V$. Если $\dim U = \dim V$, то по сл. 7.1 всякий базис в U является одновременно базисом в V, откуда $V = U$. Если $\dim U < \dim W$, то линейная оболочка W векторов $w_1, \dots, w_m$ имеет нулевое пересечение с U, откуда $V = U \oplus W$. □

Пример 7.1 (пространство функций, ср. с прим. 6.8 на стр. 104)
Множество $\mathbb{k}^X$ всех функций $f : X \to \mathbb{k}$ на произвольном множестве X со значениями в произвольном поле $\mathbb{k}$ образует векторное пространство, в котором сложение функций и их умножение на числа задаётся обычными правилами: $f_1 + f_2 : x \mapsto f_1(x) + f_2(x)$ и $\lambda f : x \mapsto \lambda \cdot f(x)$.

[1] Вообще говоря, не единственное.

Пространство функций на конечном множестве $X = \{1, \dots, n\}$ изоморфно координатному пространству $\Bbbk^n$. Изоморфизм сопоставляет функции f набор её значений $\big(f(1), \dots, f(n)\big)$ и отождествляет стандартный базис пространства $\Bbbk^n$ с базисом из *δ-функций* $\delta_i : X \to \Bbbk$:

$$\delta_i(j) = \begin{cases} 1 & \text{при } j = i \\ 0 & \text{при } j \neq i\,. \end{cases}$$

Пример 7.2 (пространство подмножеств)
Если в предыдущем примере взять в качестве $\Bbbk$ двухэлементное поле $\mathbb{F}_2$ и сопоставить каждому подмножеству $Z \subset X$ его *характеристическую функцию* $\chi_Z : X \to \mathbb{F}_2$, принимающую значение 1 всюду на Z и значение 0 всюду на $X \smallsetminus Z$, мы получим взаимно однозначное соответствие между пространством функций и множеством всех подмножеств в X. Эта биекция наделяет множество подмножеств структурой векторного пространства над полем $\mathbb{F}_2$, изоморфного пространству функций $X \to \mathbb{F}_2$.

Упражнение 7.1. Укажите в пространстве подмножеств на конечном множестве $X = \{1, \dots, n\}$ какой-нибудь базис. Какое подмножество является нулевым вектором пространства подмножеств?

Пример 7.3 (интерполяционная формула Лагранжа, ср. с прим. 3.5 на стр. 48)
Зафиксируем $n + 1$ различных чисел $a_0, a_1, \dots, a_n \in \Bbbk$ и обозначим через $\Bbbk[x]_{\leqslant n}$ пространство многочленов степени не выше n. По определению многочленов, мономы $1, x, \dots, x^n$ образуют базис в $\Bbbk[x]_{\leqslant n}$, откуда $\dim \Bbbk[x]_{\leqslant n} = n + 1$. Для каждого $i = 0, 1, \dots, n$ обозначим через

$$f_i(x) = \prod\nolimits_{\nu \neq i}(x - a_\nu) \Big/ \prod\nolimits_{\nu \neq i}(a_i - a_\nu)$$

многочлен степени n, зануляющийся во всех точках a_ν кроме точки a_i, а в точке a_i принимающий значение $f_i(a_i) = 1$. Многочлены f_i линейно независимы, ибо подставляя в равенство

$$\lambda_0 f_0(x) + \lambda_1 f_1(x) + \ldots + \lambda_n f_n(x) = 0$$

значение $x = a_i$, мы заключаем, что $\lambda_i = 0$ для каждого i. Тем самым, многочлены f_i тоже образуют базис пространства $\Bbbk[x]_{\leqslant n}$. Подставляя в разложение $g(x) = x_0 f_0(x) + \ldots + x_n f_n(x)$ произвольного многочлена $g \in \Bbbk[x]_{\leqslant n}$ по базису $f_0, \dots, f_n$ значение $x = a_i$, мы заключаем, что $x_i = g(a_i)$, т. е. i-тая координата многочлена g в базисе $f_0, f_1, \dots, f_n$ равна значению этого многочлена в точке a_i. Таким образом, для любого набора значений $b_0, b_1, \dots, b_n \in \Bbbk$ существует единственный такой многочлен $g \in \Bbbk[x]_{\leqslant n}$, что $g(a_i) = b_i$ для всех i, а именно

$$g(x) = b_0 f_0(x) + b_1 f_1(x) + \ldots + b_n f_n(x)\,.$$

Пример 7.4 (конечные поля)
Пусть конечное поле $\mathbb{K}$ содержит подполе $\mathbb{F}_q \subset \mathbb{K}$, состоящее из q элементов. Будучи конечномерным векторным пространством над $\mathbb{F}_q$, поле $\mathbb{K}$ находится в линейной биекции с координатным пространством $\mathbb{F}_q^n$ для некоторого $n \in \mathbb{N}$ и, тем самым, состоит из q^n элементов. Применяя это наблюдение к простому подполю[1] $\mathbb{F}_p \subset \mathbb{K}$, мы заключаем, что число элементов в любом конечном поле является степенью простого числа, равного характеристике этого поля, ср. с упр. 3.21 на стр. 55.

[1] См. n° 2.5.6 на стр. 35.

Следствие 7.3 (равномощность базисов свободного модуля)
Любые два базиса свободного модуля F над произвольным коммутативным кольцом K с единицей равномощны.

Доказательство. Пусть множество векторов $E \subset F$ является базисом модуля F, т. е.

$$F = \bigoplus\nolimits_{e\in E} Ke\,.$$

Рассмотрим произвольный максимальный идеал[1] $\mathfrak{m} \subset K$. В n° 6.5.2 на стр. 107 мы видели, что фактормодуль $F/\mathfrak{m}F$ является векторным пространством над полем $\Bbbk = K/\mathfrak{m}$ и изоморфен

$$\bigoplus\nolimits_{e\in E} \Bbbk \cdot [e]_{\mathfrak{m}F}\,.$$

Таким образом, классы $[e]_{\mathfrak{m}F}$ векторов $e \in E$ составляют базис ничего не знающего про E векторного пространства $F/\mathfrak{m}F$ над полем $\Bbbk = K/\mathfrak{m}$, и число элементов в E равно размерности этого пространства. □

Замечание 7.1. В n° 7.3 на стр. 119 мы покажем, что теорема о базисе верна и без предположения о том, что пространство V линейно порождается конечным набором векторов. Соответственно, и сл. 7.3 тоже справедлива для любых свободных модулей, не обязательно конечно порождённых.

Следствие 7.4
Каждый свободный модуль F ранга n над любым коммутативным кольцом K изоморфен координатному модулю K^n. Линейные изоморфизмы $K^n \xrightarrow{\sim} F$ взаимно однозначно соответствуют базисам в F.

Доказательство. Обозначим через $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ стандартные базисные векторы координатного модуля K^n. По предл. 6.4 на стр. 110 для любых n векторов $v_1, \dots, v_n \in F$ существует единственное такое линейное отображение $f\colon K^n \xrightarrow{\sim} F$, что $f(e_i) = v_i$. Оно переводит каждую строку $(x_1, \dots, x_n) \in K^n$ в вектор $x_1v_1 + \dots + x_nv_n \in F$, и его сюръективность равносильна тому, что векторы v_i порождают V, а инъективность — тому, что они линейно независимы. Тем самым, биективные отображения взаимно однозначно соответствуют базисам в F. □

7.2. Размерности подпространств и факторпространств. По сл. 7.2 на стр. 115 для любого подпространства U конечномерного пространства V выполняется неравенство $\dim U \leqslant \dim V$. Разность $\operatorname{codim}_V U \stackrel{\text{def}}{=} \dim V - \dim U$ называется *коразмерностью* подпространства U в V.

Предложение 7.1
Для любых конечномерных подпространств U_1, U_2 в произвольном[2] векторном пространстве V выполняется равенство $\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

Доказательство. Выберем какой-нибудь базис $u_1, \dots, u_k$ в $U_1 \cap U_2$ и дополним его векторами $v_1, \dots, v_r$ и $w_1, \dots, w_s$ до базисов в подпространствах U_1 и U_2 соответственно. Достаточно показать, что векторы $u_1, \dots, u_k$, $v_1, \dots, v_r$, $w_1, \dots, w_s$ образуют базис пространства $U_1 + U_2$. Ясно,

[1] См. прим. 5.3 на стр. 88.
[2] Не обязательно конечномерном.

что они его порождают. Допустим, что они линейно зависимы. Поскольку каждый из наборов $u_1, \dots, u_k, v_1, \dots, v_r$ и $u_1, \dots, u_k, w_1, \dots, w_s$ в отдельности линейно независим, в равенстве

$$\lambda_1 u_1 + \dots + \lambda_k u_k + \mu_1 v_1 + \dots + \mu_r v_r + \eta_1 w_1 + \dots + \eta_s w_s = 0$$

имеются как векторы v_i, так и векторы w_j. Перенося $w_1, \dots, w_s$ в правую часть, получаем равенство между вектором из U_1 и вектором из U_2, означающее, что этот вектор лежит в пересечении $U_1 \cap U_2$. Но тогда в его разложении по базисам пространств U_1 и U_2 нет векторов v_i и w_j — противоречие. □

Следствие 7.5
Для любых подпространств U_1, U_2 конечномерного векторного пространства V

$$\dim(U_1 \cap U_2) \geqslant \dim(U_1) + \dim(U_2) - \dim(V)\,.$$

В частности, $U_1 \cap U_2 \neq 0$ при $\dim(U_1) + \dim(U_2) > \dim V$.

Доказательство. Это вытекает из предл. 7.1 и неравенства $\dim(U_1 + U_2) \leqslant \dim V$. □

Предложение 7.2
Для любого линейного отображения $f\colon V \to W$ из конечномерного векторного пространства V справедливо равенство $\dim \ker f + \dim \operatorname{im} f = \dim V$.

Доказательство. Выберем в $\ker f$ базис $u_1, \dots, u_k$, дополним его векторами $e_1, \dots, e_m$ до базиса в V и покажем, что векторы $f(e_1), \dots, f(e_m)$ образуют базис в $\operatorname{im} f$. Они порождают образ, поскольку для любого вектора $v = \sum y_i u_i + \sum x_j e_j \in V$

$$f(v) = \sum y_i f(u_i) + \sum x_j f(e_j) = \sum x_j f(e_j)\,.$$

Они линейно независимы, поскольку равенство $0 = \sum \lambda_i f(e_i) = f(\sum \lambda_i e_i)$ означает, что $\sum \lambda_i e_i$ лежит в $\ker f$, т. е. является линейной комбинацией векторов u_i, что возможно только когда все $\lambda_i = 0$. □

Следствие 7.6
Следующие свойства линейного эндоморфизма $f\colon V \to V$ пространства V эквивалентны друг другу: (1) f изоморфизм (2) $\ker f = 0$ (3) $\operatorname{im} f = V$.

Доказательство. Свойства (2) и (3) равносильны друг другу по предл. 7.2, а их одновременное выполнение означает инъективность и сюръективность отображения f (ср. с n° 6.2 на стр. 102). □

Пример 7.5 (интерполяция с кратными узлами, продолжение прим. 7.3)
Зафиксируем, как в прим. 7.3 на стр. 116, несколько различных чисел $a_1, \dots, a_n \in \Bbbk$, однако теперь для каждого a_i зададим m_i+1 произвольных значений $b_{i0}, b_{i1}, \dots, b_{im_i} \in \Bbbk$. Пусть общее число заданных значений $(m_1+1)+\dots+(m_n+1) = m+1$. Покажем, что существует единственный такой многочлен $g \in \Bbbk[x]$ степени не выше m, что при каждом i сам этот многочлен и первые его m_i производных принимают в каждой точке a_i заданные значения

$$g(a_i) = b_{i0},\ g'(a_i) = b_{i1},\ g''(a_i) = b_{i2},\ \dots\ ,\ g^{(m_i)}(a_i) = b_{im_i}\,,$$

где $g^{(k)}(x) = d^k g(x)/dx^k$ означает k-ю производную от многочлена g. Для этого произвольным образом занумеруем $m+1$ пар чисел (i,j) с $1 \leqslant i \leqslant n$, $0 \leqslant j \leqslant m_j$ и выпишем их в одну строчку в порядке возрастания номеров. Рассмотрим отображение $f : \Bbbk[x]_{\leqslant m} \to \Bbbk^{m+1}$, переводящее каждый многочлен g степени $\deg g \leqslant m$ в набор значений[1] $g^{(j)}(a_i)$, записанных в строчку согласно зафиксированному только что порядку на множестве индексов (i,j).

Упражнение 7.2. Убедитесь, что отображение f линейно и $\ker f = 0$.

Так как $\dim \operatorname{im} f = \dim \Bbbk[x]_{\leqslant m} = \dim \Bbbk^{m+1}$, мы заключаем, что отображение f биективно, что и требовалось.

Предложение 7.3
Если векторы $v_1, \dots, v_k$ дополняют некоторый базис $u_1, \dots, u_m$ подпространства $U \subset V$ до базиса во всём пространстве V, то их классы $[v_1]_U, \dots, [v_k]_U$ по модулю U образуют базис факторпространства V/U. В частности, $\dim U + \dim V/U = \dim V$.

Доказательство. Это вытекает из предл. 7.2 на стр. 118 и его доказательства, применённых к линейному отображению факторизации $V \twoheadrightarrow V/U$, но поучительно повторить проведённое там рассуждение на языке вычетов. Классы $[v_i]$ линейно независимы в V/U, поскольку равенство

$$[0] = \lambda_1[v_1] + \dots + \lambda_k[v_k] = [\lambda_1 v_1 + \dots + \lambda_k v_k]$$

в V/U означает, что $\lambda_1 v_1 + \dots + \lambda_k v_k = \mu_1 u_1 + \dots + \mu_m u_m$ в V, а такое возможно только когда все $\lambda_i = 0$ и все $\mu_j = 0$. Классы $[v_i]$ линейно порождают пространство V/U, так как для любого вектора $v = \lambda_1 v_1 + \dots + \lambda_k v_k + \mu_1 u_1 + \dots + \mu_m u_m \in V$ класс $[v] = [\lambda_1 v_1 + \dots + \lambda_k v_k] = \lambda_1[v_1] + \dots + \lambda_k[v_k]$ в V/U. □

Пример 7.6 (линейная оболочка как фактор)
Линейная оболочка $W = \operatorname{span}(w_1, \dots, w_m) \subset V$ произвольного набора из m векторов векторного пространства V является образом линейного отображения $\pi_w : \Bbbk^m \to V$, переводящего стандартный базисный вектор $e_i \in \Bbbk^m$ в вектор $w_i \in W$. Ядро этого отображения $\ker \pi_w \subset \Bbbk^m$ представляет собою *пространство линейных соотношений* между векторами w_i и состоит всех таких $(x_1, \dots, x_m) \in \Bbbk^m$, что $x_1 w_1 + \dots + x_m w_m = 0$ в W, ср. с n° 6.7.2 на стр. 110. Изоморфизм[2] $\operatorname{im} \pi_w \simeq \Bbbk^n/\ker \pi_w$ позволяет трактовать векторы $w \in W$ как элементы факторпространства $\Bbbk^m$ по подпространству линейных соотношений между векторами w_i.

7.3. Бесконечномерные векторные пространства. В этом разделе мы докажем теор. 7.1 на стр. 114 о базисе без предположения о конечной порождённости пространства V. Напомню[3], что подмножество B векторного пространства V называется *порождающим*, если каждый вектор $v \in V$ записывается в виде

$$v = \lambda_1 b_1 + \dots + \lambda_n b_n\,, \quad \text{где} \quad n \in \mathbb{N}\,,\ b_i \in B\,,\ \lambda_i \in \Bbbk\,.$$

Иначе можно сказать, что каждый вектор $v \in V$ допускает линейное разложение

$$v = \sum_{b \in B} \lambda_b b\,, \quad \text{где} \quad \lambda_b \in \Bbbk\,, \tag{7-1}$$

[1] Где для единообразия обозначений мы полагаем $g^{(0)} \stackrel{\text{def}}{=} g$.
[2] См. n° 6.5.1 на стр. 107.
[3] См. n° 6.7 на стр. 108.

в котором лишь конечное число коэффициентов λ_b отлично от нуля. Порождающее подмножество $B \subset V$ называется *базисом* пространства V, если для каждого $v \in V$ разложение (7-1) единственно, то есть равенство $\sum_{b\in B} \lambda_b b = \sum_{b\in B} \mu_b b$, в котором лишь конечное число коэффициентов λ_b, μ_b отлично от нуля, равносильно тому, что $\lambda_b = \mu_b$ при всех $b \in B$. Непустое множество $A \subset V$ называется *линейно независимым* если равенство

$$\lambda_1 a_1 + \ldots + \lambda_n a_n = 0\,, \quad \text{где} \quad n \in \mathbb{N}\,,\ a_i \in A\,,\ \lambda_i \in \Bbbk\,,$$

возможно только когда все $\lambda_i = 0$.

Теорема 7.2 (существование базиса)
В каждом отличном от нуля векторном пространстве V для любого[1] линейно независимого множества $A \subset V$ и любого[2] порождающего V множества векторов $B \supset A$ существует базис E, содержащий A и содержащийся в B.

Доказательство. Линейно независимые множества векторов $X \subseteq V$ со свойством $A \subseteq X \subseteq B$ образуют частично упорядоченное отношением включения множество, удовлетворяющее лемме Цорна[3]. В качестве верхней грани линейно упорядоченной цепи вложенных друг в друга линейно независимых наборов векторов можно взять их объединение. Оно линейно независимо, поскольку любой конечный набор его векторов лежит в одном из множеств цепи, а оно линейно независимо. По лемме Цорна существует такое линейно независимое множество E, что $A \subseteq E \subseteq B$ и для любого линейно независимого множества X со свойством $A \subseteq X \subseteq B$ включение $E \subseteq X$ влечёт равенство $E = X$. Покажем, что E линейно порождает V. Достаточно убедиться, что каждый вектор $b \in B \smallsetminus E$ линейно выражается через E. Так как множество $E \cup \{b\}$ строго больше E, оно линейно зависимо. Поскольку само множество E линейно независимо, любое линейное соотношение между векторами из $E \cup \{b\}$ содержит с ненулевым коэффициентом вектор b. Тем самым, он линейно выражается через E. □

Следствие 7.7
Каждое ненулевое векторное пространство имеет базис, и любой базис любого подпространства можно дополнить до базиса во всём пространстве. □

Теорема 7.3 (равномощность базисов)
Все базисы любого векторного пространства равномощны.

Доказательство. Пусть базис B строго мощнее базиса E. Поскольку в конечномерном пространстве это невозможно по теор. 7.1 на стр. 114, оба базиса бесконечны. Каждый вектор $e \in E$ является линейной комбинацией конечного множества векторов $B_e \subset B$. Так как множество E бесконечно, объединение $B_E = \bigcup_{e\in E} B_e$ всех этих конечных множеств равномощно E.

Упражнение 7.3. Убедитесь в этом.

Стало быть, существует вектор $b \in B$, не лежащий в B_E. Линейно выражая b через векторы базиса E, а каждый из входящих в это выражение векторов $e \in E$ — через векторы из B_E, мы получим линейное выражение вектора $b \in B \smallsetminus B_E$ через векторы из B_E. Тем самым, множество B линейно зависимо. Противоречие. □

[1] В том числе, пустого.
[2] В том числе, совпадающего с V.
[3] См. сл. 1.1 на стр. 20.

Следствие 7.8
Всякое более мощное, чем базис, множество векторов линейно зависимо. □

Теорема 7.4 (продолжение линейных отображений)
Для каждого линейного отображения $F : U \to W$, заданного на подпространстве U векторного пространства V, существует такое[1] линейное отображение $G : V \to W$, что $G|_U = F$.

Доказательство. Каждое линейное отображение $G : V \to W$ однозначно задаётся своими значениями на векторах любого базиса E пространства V, и для любого отображения множеств $g : E \to W$ существует единственное такое линейное отображение $G : V \to W$, что $G(e) = g(e)$ для всех $e \in E$.

Упражнение 7.4. Убедитесь в этом.

Рассмотрим произвольный базис B в U, дополним его до базиса $E = B \sqcup C$ в V и рассмотрим любое отображение множеств $g : E \to W$, переводящее каждый вектор $b \in B$ в $F(b)$. Отвечающее этому отображению линейное отображение $G : V \to W$ обладает нужным свойством. □

7.4. Двойственность. Линейные отображения $V \to \Bbbk$ принято называть *линейными функционалами*[2] или *ковекторами*. Они образуют векторное пространство, которое обозначается

$$V^* \stackrel{\text{def}}{=} \operatorname{Hom}_{\Bbbk}(V, \Bbbk)$$

и называется *двойственным* или *сопряжённым* к пространству V.

Пример 7.7 (линейные функционалы на координатном пространстве)
Каждый линейный функционал $\xi : \Bbbk^n \to \Bbbk$ однозначно задаётся набором своих значений

$$\xi_i = \xi(e_i) \in \Bbbk$$

на стандартных базисных векторах e_i пространства $\Bbbk^n$. Значение функционала ξ на произвольном векторе $v = e_1 x_1 + \cdots + e_n x_n$ при этом равно

$$\xi(v) = \xi(e_1 \cdot x_1 + \cdots + e_n \cdot x_n) = \xi(e_1) \cdot x_1 + \cdots + \xi(e_n) \cdot x_n = \xi_1 x_1 + \cdots + \xi_n x_n \,.$$

Наоборот, для любого набора из n констант $\xi_1, \ldots, \xi_n \in \Bbbk$ эта формула задаёт линейный функционал $\xi : \Bbbk^n \to \Bbbk$.

Пример 7.8 (функционалы вычисления функций на множестве)
Пусть X — любое множество, и $V = \Bbbk^X$ — пространство всех функций $X \to \Bbbk$, как в прим. 7.1 на стр. 115. С каждой точкой $x \in X$ связан *функционал вычисления* $\operatorname{ev}_x : \Bbbk^X \to \Bbbk$, $f \mapsto f(x)$, переводящий функцию $f : X \to \Bbbk$ в её значение $f(x) \in \Bbbk$ в точке x. Функционалы вычисления линейно независимы, поскольку вычисляя обе части равенства $\lambda_1 \operatorname{ev}_{x_1} + \cdots + \lambda_m \operatorname{ev}_{x_m} = 0$ на дельта-функции $\delta_{x_i} : X \to \Bbbk$, равной нулю во всех точках множества X кроме точки x_i, где она равна единице, мы заключаем, что $\lambda_i = 0$ для каждого $i = 1, \ldots, m$.

[1] Вообще говоря, не единственное.
[2] А также *линейными формами*.

7.4.1. Двойственные базисы. С каждым базисом $\boldsymbol{e} = (e_1, \dots, e_n)$ конечномерного векторного пространства V связан набор *координатных функционалов* $\boldsymbol{e}^* = (e_1^*, \dots, e_n^*)$, лежащих в двойственном пространстве V^*. По определению, функционал $e_i^* : V \to \Bbbk$ сопоставляет каждому вектору пространства V его i-ю координату в базисе $\boldsymbol{e}$, т. е. $e_i^*(x_1e_1 + \dots + x_ne_n) \stackrel{\text{def}}{=} x_i$. Таким образом, значения функционала e_i^* на базисных векторах e_j суть

$$e_i^*(e_j) = \begin{cases} 1 & \text{при } j = i \\ 0 & \text{при } j \neq i. \end{cases} \tag{7-2}$$

Упражнение 7.5. Убедитесь, что все отображения $e_i^* : V \to \Bbbk$ линейны.

Из формулы (7-2) вытекает, что ковекторы $e_1^*, \dots, e_n^*$ линейно независимы: вычисляя обе части равенства $\lambda_1e_1^* + \dots + \lambda_ne_n^* = 0$ на базисном векторе e_i, мы заключаем, что $\lambda_i = 0$ для каждого $i = 1, \dots, n$. С другой стороны, каждый линейный функционал $\varphi : V \to \Bbbk$ линейно выражается через координатные функционалы e_i^* — коэффициентами этого линейного выражения являются значения функционала φ на соответствующих базисных векторах пространства V, поскольку для любого вектора $v = x_1e_1 + \dots + x_ne_n$ выполняется равенство

$$\varphi(v) = \varphi(x_1e_1 + \dots + x_ne_n) = x_1\varphi(e_1) + \dots + x_n\varphi(e_n) = e_1^*(v)\varphi(e_1) + \dots + e_n^*(v)\varphi(e_n), \tag{7-3}$$

как раз и означающее, что $\varphi = e_1^* \cdot \varphi(e_1) + \dots + e_n^* \cdot \varphi(e_n)$ в пространстве V^*. Таким образом, координатные функционалы e_i^* образуют базис векторного пространства V^*. Этот базис называется *двойственным* к базису из векторов e_i в V. В частности, для конечномерного пространства V выполняется равенство $\dim V^* = \dim V$.

Упражнение 7.6. Пусть $\dim V = n$, а векторы $v_1, \dots, v_n \in V$ и ковекторы $\varphi_1, \dots, \varphi_n \in V^*$ таковы, что $\varphi_i(v_i) = 1$ и $\varphi_i(v_j) = 0$ при $i \neq j$. Покажите, что векторы v_i образуют базис в V, а ковекторы φ_i — двойственный базис в V^*.

Пример 7.9 (формула Тейлора)
Пусть поле $\Bbbk$ имеет характеристику нуль[1]. Зафиксируем число $a \in \Bbbk$ и для каждого $i = 0, 1, \dots, n$ рассмотрим на пространстве $\Bbbk[x]_{\leqslant n}$ многочленов степени не выше n функционал

$$\varphi_i : \Bbbk[x]_{\leqslant n} \to \Bbbk, \quad f \mapsto f^{(i)}(a),$$

сопоставляющий многочлену значение его i-й производной в точке a. При $i = 0$ мы полагаем $\varphi_0(f) = \mathrm{ev}_a(f) = f(a)$. Функционалы $\varphi_0, \varphi_1, \dots, \varphi_n$ и многочлены $f_k(x) = (x-a)^k / k!$, где $k = 0, 1, \dots, n$ и $0! \stackrel{\text{def}}{=} 1$, удовлетворяют условиям упр. 7.6, т. е. $\varphi_i(f_i) = 1$ и $\varphi_i(f_j) = 0$ при $i \neq j$. Следовательно, многочлены f_i образуют в $\Bbbk[x]_{\leqslant n}$ базис, в котором координатами каждого многочлена служат его значение и значения первых n его производных в точке a. Поэтому для любого многочлена g степени не выше n имеет место *формула Тэйлора*

$$g(x) = g(a) + g'(a) \cdot (x-a) + g''(a) \cdot \frac{(x-a)^2}{2} + \dots + g^{(n)}(a) \cdot \frac{(x-a)^n}{n!}, \tag{7-4}$$

и для любого набора чисел $b_0, b_1, \dots, b_n \in \Bbbk$ существует единственный такой многочлен g степени не выше n, что $g^{(i)}(a) = b_i$ при всех $i = 0, 1, \dots, n$, причём g задаётся явной формулой

$$g(x) = \sum_{k=0}^{n} b_k(x-a)^k / k!.$$

[1] Т. е. сумма любого числа единиц поля $\Bbbk$ отлична от нуля.

7.4.2. Свёртки. Каждый вектор $v \in V$ задаёт на двойственном к V пространстве V^* *функционал вычисления* $\mathrm{ev}_v : V^* \to \Bbbk$, $\varphi \mapsto \varphi(v)$. Поскольку число $\varphi(v) \in \Bbbk$ линейно зависит как от $v \in V$, так и от $\varphi \in V^*$, сопоставление вектору v функционала вычисления ev_v задаёт *каноническое*[1] линейное вложение

$$\mathrm{ev} : V \hookrightarrow V^{**}, \quad v \mapsto \mathrm{ev}_v \,. \tag{7-5}$$

Упражнение 7.7. Убедитесь, что отображение (7-5) инъективно[2].

Если пространство V конечномерно, то согласно упр. 7.6 каждый базис $e_1, \dots, e_n$ пространства V переводится отображением (7-5) в двойственный к базису $e_1^*, \dots, e_n^*$ пространства V^* базис пространства V^{**}. Тем самым, для конечномерного пространства V отображение (7-5) канонически отождествляет V^{**} с V, т. е. каждая линейная форма $V^* \to \Bbbk$ представляет собою функционал вычисления значений ковекторов из V^* на однозначно задаваемом этой формой векторе $v \in V$, и любой базис $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n)$ пространства V^* состоит из координатных функционалов для однозначно задаваемого этим базисом базиса $\boldsymbol{\varepsilon}^* = (\varepsilon_1^*, \dots, \varepsilon_n^*)$ в V. Таким образом, двойственные конечномерные пространства V и V^* играют по отношению друг к другу совершенно симметричные роли: *каждое* из них является пространством линейных функционалов на другом. Дабы подчеркнуть симметрию между векторами и ковекторами, мы будем называть число

$$\langle\, \varphi\,,\, v\,\rangle \stackrel{\text{def}}{=} \varphi(v) = \mathrm{ev}_v(\varphi) \in \Bbbk \tag{7-6}$$

свёрткой ковектора φ с вектором v. Свёртка является билинейным отображением

$$V^* \times V \to \Bbbk\,, \quad (\varphi, v) \mapsto \langle\, \varphi\,,\, v\,\rangle\,.$$

Для координатного пространства $V = \Bbbk^n$ в обозначениях из прим. 7.7 на стр. 121 свёртка ковектора-строки $\xi = (\xi_1, \dots, \xi_n) \in \Bbbk^{n*}$ с вектором-столбцом $x = (x_1, \dots, x_n)^t \in \Bbbk^n$ задаётся матричным произведением $\langle\, \xi\,,\, x\,\rangle = \xi x = \xi_1 x_1 + \cdots + \xi_n x_n$. Обратите внимание, что правая часть этого равенства абсолютно симметрична по буквам ξ и x.

Более общим образом, будем называть *спариванием* или *свёрткой* между векторными пространствами U и W отображение $U \times W \to \Bbbk$, сопоставляющее каждой паре векторов $u \in U$, $w \in W$ число $\langle\, u\,,\, w\,\rangle \in \Bbbk$, которое линейно зависит от u при фиксированном w и линейно зависит от w при фиксированном u, т. е. для любых векторов $u_1, u_2 \in U$, $w_1, w_2 \in W$ и любых чисел $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \Bbbk$ выполняется равенство[3]

$$\langle\, \lambda_1 u_1 + \lambda_2 u_2\,,\, \mu_1 w_1 + \mu_2 w_2\,\rangle = \\ = \lambda_1\mu_1\langle\, u_1\,,\, w_1\,\rangle + \lambda_1\mu_2\langle\, u_1\,,\, w_2\,\rangle + \lambda_2\mu_1\langle\, u_2\,,\, w_1\,\rangle + \lambda_2\mu_2\langle\, u_2\,,\, w_2\,\rangle\,.$$

Спаривание называется *невырожденным*, если оно удовлетворяет условиям следующей леммы:

Лемма 7.2

Следующие свойства спаривания между конечномерными пространствами U и W эквивалентны друг другу:

1) для каждого ненулевого $u \in U$ найдётся $w \in W$, а для каждого ненулевого $w \in W$ найдётся $u \in U$, такие, что $\langle\, u\,,\, w\,\rangle \neq 0$.

[1] Т. е. не требующее выбора базиса.

[2] Для любого, в том числе и бесконечномерного векторного пространства V.

[3] Обладающие этим свойством функции двух переменных называются *билинейными*).

2) отображение $U \to W^*$, сопоставляющее вектору u линейную форму $w \mapsto \langle u, w \rangle$ на W, является изоморфизмом

3) отображение $W \to U^*$, сопоставляющее вектору w линейную форму $u \mapsto \langle u, w \rangle$ на U, является изоморфизмом

Доказательство. В силу линейности $\langle u, w \rangle$ по u и по w, оба отображения, о которых идёт речь в (2) и (3), корректно определены и линейны. Условие (1) утверждает, что оба они инъективны, откуда $\dim U \leqslant \dim W^*$ и $\dim W \leqslant \dim U^*$. Так как $\dim U = \dim U^*$ и $\dim W = \dim W^*$, оба неравенства являются равенствами, а вложения (2) и (3) — изоморфизмами. Тем самым, условие (1) влечёт за собою (2) и (3). Покажем, что условия (2), (3), равносильны. Пусть отображение $U \xrightarrow{\sim} W^*$ из (2) является изоморфизмом. Тогда $\dim U = \dim W$, а отображение $W \hookrightarrow U^*$ из (3) инъективно, поскольку каждый лежащий в его ядре вектор w таков, что $\langle u, w \rangle = 0$ для всех $u \in U$, а это в силу (2) означает, что $\varphi(w) = 0$ для всех $\varphi \in W^*$, откуда $w = 0$. Тем самым, отображение из (3) тоже изоморфизм. Обратная импликация доказывается дословно также. При одновременном выполнении условий (2), (3) условие (1) очевидно тоже выполняется. □

Пример 7.10
Пусть $U = \mathbb{Q}[x]_{\leqslant n}$ — пространство многочленов степени не выше n, а $W = \mathbb{Q}[D]/(D^{n+1})$ — фактор кольца многочленов от дифференциального оператора

$$D = d/dx : \mathbb{Q}[x] \to \mathbb{Q}[x], \quad f(x) \mapsto f'(x).$$

Положим $\langle f, [g] \rangle \stackrel{\text{def}}{=} g(D)f(0)$, где $g(D)f \in \mathbb{Q}[x]$ — результат применения к f дифференциального оператора[1] $g(D)$, а $g(D)f(0)$ — значение получившегося многочлена при $x = 0$, т. е. его свободный член.

Упражнение 7.8. Убедитесь, что это спаривание корректно определено, билинейно и невырождено. Найдите базис пространства W, двойственный к базису из мономов x^k в U, а также базис пространства U, двойственный к базису из классов мономов $[D^k]$ в W.

Предостережение 7.1. Бесконечномерное пространство V, вообще говоря, не изоморфно V^{**}. Так, в прим. 6.9 на стр. 105 мы видели, что двойственное к $\Bbbk[x]$ пространство векторное пространство $\Bbbk[x]^*$ изоморфно пространству формальных степенных рядов $\Bbbk[\![x]\!]$.

Упражнение 7.9 (по теории множеств). Убедитесь, что множество $\mathbb{Q}[x]$ счётно, а $\mathbb{Q}[\![]\!]$ нет.

Упражнение 7.10. Убедитесь, что над любым полем $\Bbbk$ функционалы $\mathrm{ev}_\alpha : \Bbbk[x] \to \Bbbk$, $f \mapsto f(\alpha)$, вычисляющие значения многочленов в точках $\alpha \in \Bbbk$, линейно независимы.

Из последней задачи вытекает, что в $\mathbb{R}[x]^*$ (соотв. в $\mathbb{R}[\![x]\!]$) имеется несчётное линейно независимое множество функционалов ev_α (соответственно, рядов $(x-\alpha)^{-1}$) с $\alpha \in \mathbb{R}$, поэтому размерность этого пространства как минимум континуум, тогда как пространство $\mathbb{R}[x]$ счётномерно.

[1] См. формулу (4-21) на стр. 71.

7.4.3. Двойственность между подпространствами. Каждое множество $M \subset V^*$ задаёт систему однородных линейных уравнений $\langle\, \xi\,,\, x\,\rangle = 0$, где ξ пробегает M, на неизвестный вектор $x \in V$. Множество всех решений этой системы обозначается $\operatorname{Ann}(M) \stackrel{\text{def}}{=} \{v \in V \mid \langle\, \xi\,,\, v\,\rangle = 0\ \forall\, \xi \in M\}$ и называется *аннулятором* множества $M \subset V^*$. Будучи пересечением ядер линейных отображений $\xi : V \to \Bbbk$ по всем $\xi \in M$, аннулятор $\operatorname{Ann}(M)$ любого множества $M \subset V^*$ является векторным подпространством в V. Двойственным образом, для любого множества векторов $N \subset V$ положим $\operatorname{Ann}(N) \stackrel{\text{def}}{=} \{\varphi \in V^* \mid \langle\, \varphi\,,\, v\,\rangle = 0\ \forall\, v \in N\}$. Это множество всех линейных функционалов, ядро которых содержит N, или — на двойственном языке — пространство решений системы однородных линейных уравнений $\langle\, y\,,\, v\,\rangle = 0$, где v пробегает N, на неизвестный ковектор $y \in V^*$. В частности, аннулятор любого множества векторов является векторным подпространством в V^*.

Упражнение 7.11. Убедитесь, что аннулятор любого множества X векторов или ковекторов совпадает с аннулятором их линейной оболочки $\operatorname{span}(X)$.

Предложение 7.4
Для любых[1] векторного пространства V и подпространства $U \subset V$ имеются канонические изоморфизмы $(V/U)^* \simeq \operatorname{Ann} U$ и $V^*/\operatorname{Ann} U \simeq U^*$.

Доказательство. Первый изоморфизм является частным случаем предл. 6.5 на стр. 111. Чтобы задать второй изоморфизм, рассмотрим линейное отображение $G : V^* \to U^*, \xi \mapsto \xi|_U$, которое сопоставляет линейному функционалу $\xi : V \to \Bbbk$ его ограничение на подпространство $U \subset V$. По построению, $\ker G = \operatorname{Ann} U$. Отображение G сюръективно, поскольку по теор. 7.4 на стр. 121 каждый функционал $\psi : U \to \Bbbk$ можно продолжить до функционала $\varphi : V \to \Bbbk$ с ограничением $\varphi|_U = \psi$. Изоморфизм $V^*/\operatorname{Ann} U \xrightarrow{\sim} U^*$ есть не что иное, как изоморфизм $V^*/\ker G \xrightarrow{\sim} \operatorname{im} G$ из n° 6.5.1 на стр. 107. □

Следствие 7.9
Для конечномерного пространства V и любого подпространства $U \subset V$ выполняется равенство $\dim U + \dim \operatorname{Ann} U = \dim V$.

Доказательство. В силу предл. 7.4 $\dim \operatorname{Ann} U = \dim(V/U)^* = \dim(V/U)$, а по предл. 7.3 на стр. 119 $\dim(V/U) = \dim V - \dim U$. □

Упражнение 7.12. Пусть векторы $u_1, \dots, u_k$ составляют базис в U, а векторы $w_1, \dots, w_m$ дополняют их до базиса в V. Обозначим через $u_1^*, \dots, u_k^*, w_1^*, \dots, w_m^*$ двойственный базис[2] в V^*. Покажите, что ковекторы $w_1^*, \dots, w_m^*$ образуют базис в $\operatorname{Ann} U$.

Следствие 7.10
Для любого векторного подпространства $U \subset V$ выполняется равенство $\operatorname{Ann}\operatorname{Ann} U = U$.

Доказательство. По определению аннуляторов, $U \subset \operatorname{Ann}\operatorname{Ann} U$. С другой стороны, по сл. 7.9 $\dim \operatorname{Ann}\operatorname{Ann} U = \dim V^* - \dim \operatorname{Ann} U = \dim V^* - \dim V + \dim U = \dim U$. □

[1] В том числе бесконечномерных.
[2] См. n° 7.4.1 на стр. 122.

Замечание 7.2. Если в сл. 7.9 и сл. 7.10 взять в качестве V двойственное пространство V^* и отождествить двойственное к V^* пространство V^{**} с исходным пространством V при помощи канонического изоморфизма из n° 7.4.2, то мы получим для любого подпространства $U \subset V^*$ равенства $\dim U + \dim \operatorname{Ann} U = \dim V$ и $\operatorname{Ann}\operatorname{Ann} U = U$.

Упражнение 7.13. Покажите, что $\operatorname{Ann}\operatorname{Ann} N = \operatorname{span} N$ для любого подмножества $N \subset V$.

Пример 7.11 (ранг матрицы)
Столбцы $a_1, \ldots, a_n$ произвольной матрицы $A \in \operatorname{Mat}_{m\times n}(\Bbbk)$ являются векторами координатного пространства $\Bbbk^m$. Обозначим через $U \subset \Bbbk^m$ их линейную оболочку. Каждый максимальный по включению линейно независимый набор столбцов матрицы A является базисом в U и состоит ровно из $\dim U$ векторов. В i-й строке матрицы A стоят вычисленные на векторах $a_1, \ldots, a_n$ значения базисного ковектора $e_i^* \in \Bbbk^{m*}$ из двойственного к стандартному базису в $\Bbbk^m$ базиса в $\Bbbk^{m*}$. Согласно предл. 7.4, ограничения функционалов $e_1^*, \ldots, e_n^*$ на подпространство U линейно порождают двойственное к U пространство U^*. Поэтому любой максимальный по включению линейно независимый набор функционалов $e_i^*|_U$ составляет базис в U^* и тоже состоит из $\dim U^* = \dim U$ векторов. Но каждый линейный функционал $e_i^*|_U$ однозначно определяется набором своих значений на порождающих пространство U векторах $a_1, \ldots, a_n$. В частности, ограничения функционалов $e_{i_1}^*, \ldots, e_{i_k}^*$ на подпространство U линейно зависимы если и только если линейно зависимы наборы этих значений, т. е. соответствующие строки матрицы A. Поэтому максимальный по включению линейно независимый набор строк матрицы A также состоит из $\dim U^* = \dim U$ векторов. Мы заключаем, что для любой матрицы $A \in \operatorname{Mat}_{m\times n}(\Bbbk)$ линейная оболочка её строк в координатном пространстве $\Bbbk^n$ и линейная оболочка её столбцов в координатном пространстве $\Bbbk^m$ имеют равные размерности. Эта размерность называется *рангом* матрицы A и обозначается $\operatorname{rk} A$. Равенство размерностей линейных оболочек строк и столбцов известно как *теорема о ранге матрицы* и обычно записывается мнемонической формулой $\operatorname{rk} A = \operatorname{rk} A^t$, где A^t — *транспонированная* к A матрица, строки которой являются столбцами матрицы A.

Теорема 7.5
Соответствие $U \leftrightarrow \operatorname{Ann} U$ задаёт биекцию между подпространствами дополнительных размерностей в двойственных пространствах V и V^*. Эта биекция оборачивает включения:

$$U \subset W \iff \operatorname{Ann} U \supset \operatorname{Ann} W\,,$$

и переводит суммы подпространств в пересечения, а пересечения — в суммы.

Доказательство. Обозначим через $\mathcal{S}(V)$ множество всех подпространств векторного пространства V. Равенство $\operatorname{Ann}\operatorname{Ann} U = U$ означает, что отображения, сопоставляющие подпространству его аннулятор в двойственном пространстве

$$\mathcal{S}(V) \underset{\operatorname{Ann} W \mapsto W}{\overset{U\mapsto \operatorname{Ann} U}{\rightleftarrows}} \mathcal{S}(V^*)$$

обратны друг другу, и следовательно, биективны. Импликация $U \subset W \Rightarrow \operatorname{Ann} U \supset \operatorname{Ann} W$ очевидна. Если взять в ней в качестве U и W, соответственно, подпространства $\operatorname{Ann} W$ и $\operatorname{Ann} U$ и

воспользоваться равенствами $\operatorname{Ann}\operatorname{Ann} W = W$ и $\operatorname{Ann}\operatorname{Ann} U = U$, получим обратную импликацию $\operatorname{Ann} U \supset \operatorname{Ann} W \Rightarrow U \subset W$. Равенство

$$\bigcap_\nu \operatorname{Ann} U_\nu = \operatorname{Ann}\Big(\sum_\nu U_\nu\Big) \tag{7-7}$$

тоже очевидно: любая линейная форма, зануляющаяся на каждом из подпространств U_ν, зануляется и на их линейной оболочке, а форма, зануляющаяся на сумме подпространств, зануляется и на каждом подпространстве в отдельности. Если взять в (7-7) в качестве подпространств U_ν пространства $\operatorname{Ann} U_\nu$, получаем равенство $\bigcap_\nu U_\nu = \operatorname{Ann}\Big(\sum_\nu \operatorname{Ann} U_\nu\Big)$. Беря в нём аннуляторы обеих частей, приходим к равенству $\operatorname{Ann}\big(\bigcap_\nu W_\nu\big) = \sum_\nu \operatorname{Ann} W_\nu$. □

7.4.4. Двойственные линейные отображения. С каждым линейным отображением векторных пространств $F : U \to W$ канонически связано *двойственное отображение*

$$F^* : W^* \to U^*, \quad \xi \mapsto \xi \circ F, \tag{7-8}$$

действующее между двойственными пространствами в противоположном к F направлении и переводящее линейную форму $\xi : W \to \Bbbk$ в линейную форму $F^*\xi$, значение которой на векторе $v \in U$ равно $F^*\xi(v) \stackrel{\text{def}}{=} \xi(Fv)$.

Упражнение 7.14. Убедитесь, что композиция $F \circ \xi$ является линейной формой на U и что отображение F^* линейно.

На языке свёрток между векторами и ковекторами[1] связь между двойственными операторами описывается равенством

$$\langle F^*\xi\,,\, v\rangle = \langle \xi\,,\, Fv\rangle \quad \text{для всех } v \in W \text{ и } \xi \in U^*, \tag{7-9}$$

из которого видно, что операторы F и F^* играют симметричные роли по отношению друг к другу: двойственный к оператору $F^* : W^* \to U^*$ оператор $F^{**} : U^{**} \to W^{**}$ превращается в оператор $F : U \to W$ при канонических отождествлениях $U^{**} \simeq U$ и $W^{**} \simeq W$ из n° 7.4.2 на стр. 123.

Упражнение 7.15. Убедитесь в этом.

Предложение 7.5
Для двойственных операторов $F : U \to W$ и $F^* : W^* \to U^*$ имеют место равенства

$$\begin{aligned} &(1)\ \ker F = \operatorname{Ann}\operatorname{im}(F^*) && (2)\ \ker(F^*) = \operatorname{Ann}\operatorname{im} F \\ &(3)\ \operatorname{im}(F^*) = \operatorname{Ann}\ker F && (4)\ \operatorname{im} F = \operatorname{Ann}\ker(F^*)\,. \end{aligned}$$

Доказательство. Вектор $F(v) \in W$ нулевой если и только если все линейные функционалы $\xi : W \to \Bbbk$ принимают на нём нулевое значение, т. е. $\langle \xi\,,\, Fv\rangle = 0$ для всех $\xi \in W^*$. В силу (7-9) это требование равносильно требованию $\langle F^*\xi\,,\, v\rangle = 0$ для всех $\xi \in W^*$, которое означает, что $v \in \operatorname{Ann}\operatorname{im} F^*$. Это доказывает равенство (1). Равенство (2) представляет собою равенство (1), написанное для оператора F^* в роли F и оператора $F^{**} = F$ в роли F^*. Равенства (3) и (4) получаются из равенства (1) и (2) взятием аннуляторов обеих частей. □

[1] См. формулу (7-6) на стр. 123.

Задачи для самостоятельного решения к §7

Задача 7.1. Является ли векторным пространством над $\mathbb{R}$ множество
а) всех вещественных последовательностей[1] $\mathbb{N} \to \mathbb{R}$
б) ограниченных сверху вещественных последовательностей $\mathbb{N} \to \mathbb{R}$
в) приведённых[2] многочленов в $\mathbb{R}[x]$
г) $\{f \in \mathbb{R}[x] \mid \deg f \leqslant m \text{ и } x^m f(1/x) = f(x)\}$?

Задача 7.2. Укажите базис и найдите размерность векторного пространства
а) однородных многочленов степени d от m переменных
б) всех многочленов степени $\leqslant d$ от m переменных.
в) симметрических[3] многочленов степени $\leqslant 6$ от x, y, z.

Задача 7.3. Какова размерность над полем $\mathbb{R}$ пространства многочленов $f \in \mathbb{R}[x]$ степени $\leqslant n$, обращающихся в нуль в точке $(3-2i) \in \mathbb{C}$?

Задача 7.4. Являются ли линейно зависимыми в пространстве функций $\mathbb{R} \to \mathbb{R}$ над полем $\mathbb{R}$ функции: а) $1, \sin x, \cos x, \dots, \cos nx$ б) $1, \sin x, \sin^2 x, \dots, \sin^m x$ в) $e^{\lambda_1 x}, \dots, e^{\lambda_m x}$, где $\lambda_i \in \mathbb{R}$ все различны г) $x^{\lambda_1}, \dots, x^{\lambda_m}$, где $\lambda_i \in \mathbb{R}$ все различны.

Задача 7.5. Образуют ли базис в пространстве $\mathbb{Q}[x]_{\leqslant n}$ многочленов степени не выше n с рациональными коэффициентами многочлены
а) $\binom{x+k}{k} = (x+1)\cdots(x+k)/k!$, где $0 \leqslant k \leqslant n$ и $\binom{x}{0} \stackrel{\text{def}}{=} 1$,
б) $(x-k)^n$, где $0 \leqslant k \leqslant n$.

Задача 7.6. Являются ли линейно зависимыми в пространстве функций $\mathbb{F}_p \to \mathbb{F}_p$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$ функции а) $1, x, x^2, \dots, x^{p-1}$ б) $x, x^2, \dots, x^p$?

Задача 7.7. Может ли поле из 27 элементов содержать подполе из 9 элементов?

Задача 7.8. Сколько k-мерных подпространств в n-мерном векторном пространстве над полем из q элементов? При фиксированных n, k найдите предел этого количества при $q \to 1$.

Задача 7.9. Сколько различных разложений в прямую сумму имеет $\mathbb{Z}$-модуль $\mathbb{Z}/(5) \oplus \mathbb{Z}/(5)$?

Задача 7.10. Пусть $\Bbbk \subset \mathbb{F}$ — два поля, и $\mathbb{F}$ конечномерно как векторное пространство над $\Bbbk$. Покажите, что любой элемент $a \in \mathbb{F}$ является корнем некоторого неприводимого многочлена $f \in \Bbbk[x]$ и размерность наименьшего по включению подполя в $\mathbb{F}$, содержащего $\Bbbk$ и α, равна $\deg f$.

Задача 7.11. Конечномерно ли $\mathbb{R}$ как векторное пространство над $\mathbb{Q}$?

Задача 7.12. Являются ли линейно зависимыми над $\mathbb{Q}$ вещественные числа: а) $\sqrt{2}$, $\sqrt{3}$ и $\sqrt{5}$ б*) $\sqrt[n_1]{p_1^{m_1}}, \dots, \sqrt[n_s]{p_s^{m_s}}$, где $p_i \in \mathbb{N}$ различные простые и все дроби $m_i/n_i \in \mathbb{Q} \smallsetminus \mathbb{Z}$.

Задача 7.13. Приведите пример конечномерного векторного пространства W и трёх таких ненулевых подпространств $U, V, T \subset W$ с суммой размерностей $\dim W$, что любые два из них имеют нулевое пересечение, но $W \neq U \oplus V \oplus T$.

Задача 7.14. Верно ли, что в каждом векторном пространстве для любых трёх векторных подпространств U, V, W выполняются соотношения:
а) $(U+V) \cap (V+W) \cap (W+U) = (U+W) \cap V + (U+V) \cap W$

[1] Сложение последовательностей и умножение их на константы происходит поэлементно.
[2] Т. е. со старшим коэффициентом 1.
[3] Т. е. не меняющихся при перестановках переменных: $f(x,y,z) = f(x,z,y) = f(y,x,z)$.

б) $(U+V)\cap(V+W)\cap(W+U)\subseteq(U\cap V)+(V\cap W)+(W\cap U)$
в) $(U+V)\cap(V+W)\cap(W+U)\supseteq(U\cap V)+(V\cap W)+(W\cap U)$?
Покажите, что для конечномерных U, V, W разность размерностей левой и правой частей в предыдущих двух включениях в любом случае чётна.

Задача 7.15. Может ли векторное пространство над бесконечным полем оказаться объединением конечного числа подпространств меньшей размерности?

Задача 7.16. Пусть $\dim(U+V)=\dim(U\cap V)+1$ для некоторых подпространств $U, V\subset V$. Обязательно ли $U+V$ равно одному из подпространств U, V, а $U\cap V$ — другому?

Задача 7.17. Пусть k-мерные подпространства $W_1,\dots,W_m$ таковы, что $\dim W_i\cap W_j=k-1$ при всех $i\neq j$. Покажите, что существует либо $(k-1)$-мерное подпространство $U\subset V$, содержащееся во всех W_i, либо $(k+1)$-мерное подпространство $W\subset V$, содержащее все W_i.

Задача 7.18. Векторы $v_0, v_1,\dots,v_n\in\mathbb{R}^n$ имеют нулевую сумму, но некоторые n из них образуют в $\mathbb{R}^n$ базис. Докажите, что а) каждый вектор $w\in\mathbb{R}^n$ имеет единственное представление

$$w=x_0v_0+x_1v_1+\ldots+x_nv_n\,,$$

в котором $x_i\in\mathbb{R}$ и $\sum x_i=0$ б) любые n векторов v_i образуют базис в $\mathbb{R}^n$ в) для любого вектора $w\in\mathbb{R}^n$ найдётся составленный из векторов v_i базис, в котором все координаты вектора w неотрицательны.

Задача 7.19. Подсчитайте количество 3×3 матриц ранга 2 над полем из q элементов.

Задача 7.20. Докажите, что любую матрицу ранга r можно представить в виде суммы r матриц ранга 1, но нельзя представить в виде суммы меньшего числа таких матриц.

Задача 7.21. Пусть $\alpha_1,\alpha_2,\alpha_3\in\Bbbk$ различны, $f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\in\Bbbk[x]$ и $V=\Bbbk[x]/(f)$.
а) Покажите, что функционалы вычисления $\varepsilon_i\colon V\to\Bbbk$, $[g]\mapsto g(\alpha_i)$, корректно определены и образуют базис в V^*. б) Найдите двойственный к нему базис в V.

Задача 7.22. Покажите, что ограничения линейных функционалов $\xi_1,\dots,\xi_m$ на линейную оболочку векторов $u_1,\dots,u_n$ линейно независимы тогда и только тогда, когда линейно независимы строки матрицы $\big(\langle\,\xi_i\,,\,u_j\,\rangle\big)\in\mathrm{Mat}_{m\times n}(\Bbbk)$ и выведите из этого теорему о ранге матрицы.

Задача 7.23 (теневой анализ). Обозначим через $D\colon\mathbb{Q}[x]\to\mathbb{Q}[x]$, $f\mapsto f'$, оператор дифференцирования и сопоставим каждому степенному ряду $\varphi(t)=\sum_{k\geqslant0}\varphi_kt^k\in\mathbb{Q}[\![t]\!]$ линейный оператор $\varphi(D)\colon\mathbb{Q}[x]\to\mathbb{Q}[x]$, $f\mapsto\sum_{k\geqslant0}\varphi_kD^kf=\varphi_0f+\varphi_1f'+\varphi_2f''+\ldots$, а также ковектор $\varphi\in\mathbb{Q}[x]^*$, переводящий многочлен $f(x)$ в число[1] $\langle\,\varphi\,,\,f\,\rangle\stackrel{\text{def}}{=}\mathrm{ev}_0(\varphi(D)f)$, равное значению многочлена $\varphi(D)f$ при $x=0$.
а) Как действуют на $\mathbb{Q}[x]$ линейные операторы $e^{\alpha D}=\sum_{k\geqslant0}\frac{\alpha^k}{k!}D^k$, где $\alpha\in\mathbb{Q}$?
б) Убедитесь, что сопоставление степенным рядам ковекторов задаёт линейный изоморфизм векторных пространств $\mathbb{Q}[\![t]\!]\xrightarrow{\sim}\mathbb{Q}[x]^*$ и для каждого $\alpha\in\mathbb{Q}$ укажите ряд, соответствующий функционалу вычисления $\mathrm{ev}_\alpha\colon\mathbb{Q}[x]\to\mathbb{Q}$, $f\mapsto f(\alpha)$.
в) Опишите линейные операторы $\mathbb{Q}[\![t]\!]\to\mathbb{Q}[\![t]\!]$, двойственные к действующим на $\mathbb{Q}[x]$ операторам умножения на $x\colon f(x)\mapsto x\cdot f(x)$, дифференцирования $D\colon f(x)\mapsto f'(x)$, сдвига $T_\alpha\colon f(x)\mapsto f(x+\alpha)$, где $\alpha\in\mathbb{Q}$, и разностным операторам $\Delta\colon f(x)\mapsto f(x+1)-f(x)$ и $\nabla\colon f(x)\mapsto f(x)-f(x-1)$.

[1] Обратите внимание, что указанное здесь сопоставление степенному ряду линейной формы на пространстве многочленов отличается от того, что использовалось в прим. 6.9 на стр. 105.

г) Убедитесь, что отображение $\mathbb{Q}[\![t]\!] \to \mathrm{End}\big(\mathbb{Q}[x]\big)$, $\varphi \mapsto \varphi(D)$, $\mathbb{Q}$-линейно, инъективно и переводит умножение рядов в композицию операторов, а его образ состоит из всех линейных операторов $F : \mathbb{Q}[x] \to \mathbb{Q}[x]$, которые удовлетворяют условиям зад. 4.25 на стр. 83.

д) Докажите равенства $\langle\, \varphi\psi\,,\, x^n \,\rangle = \langle\, \varphi\,,\, \psi(D)\, x^n \,\rangle = \sum_{k=0}^{n} \binom{n}{k} \langle\, \varphi\,,\, x^{n-k} \,\rangle \langle\, \psi\,,\, x^k \,\rangle$.

е) Пусть ряд $\varphi(t) \in \mathbb{Q}[\![t]\!]$ имеет $\varphi_0 = 0$ и $\varphi_1 \neq 0$. Покажите, что существует единственный такой ряд $\overline{\varphi}(t) \in \mathbb{Q}[\![t]\!]$, что $\overline{\varphi}(\varphi(t)) = t$.

ж) Определим многочлены $p_k(x) \in \mathbb{Q}[x]$ равенством $e^{x\overline{\varphi}(t)} = \sum_{k\geqslant 0} p_k(x)\, t^k/k!$. Докажите для любых $\psi \in \mathbb{Q}[\![t]\!]$ и $q \in \mathbb{Q}[x]$ равенства $\psi = \sum_{k\geqslant 0} \langle\, \psi\,,\, p_k \,\rangle \cdot \varphi^k/k!$ и $q = \sum_{k\geqslant 0} \langle\, \varphi^k\,,\, q \,\rangle \cdot p_k/k!$.

Задача 7.24. Покажите, что в счётномерном[1] пространстве всякое подпространство конечномерно или счётномерно, а всякое несчётное множество векторов линейно зависимо.

Задача 7.25. Покажите, что спаривание из прим. 7.10 на стр. 124 корректно задаёт $\mathbb{Z}$-билинейное отображение $\mathbb{Z}[\nabla]/(\nabla^{n+1}) \times M_n \to \mathbb{Z}$, где $\mathbb{Z}[\nabla]/(\nabla^{n+1}) \subset \mathbb{Q}[D]/(D^{n+1})$ — $\mathbb{Z}$-подмодуль, порождённый разностным оператором[2] $\nabla = \mathrm{Id} - e^{-D} : f(x) \mapsto f(x) - f(x-1)$, а $M_n \subset \mathbb{Q}[x]_{\leqslant n}$ — $\mathbb{Z}$-подмодуль *целозначных многочленов*[3], причём оба отображения

$$M_n \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\nabla]/(\nabla^{n+1}), \mathbb{Z}) \quad \text{и} \quad \mathbb{Z}[\nabla]/(\nabla^{n+1}) \to \mathrm{Hom}_{\mathbb{Z}}(M_n, \mathbb{Z}),$$

сопоставляющие классу $[g] \in \mathbb{Z}[\nabla]/(\nabla^{n+1})$ и многочлену $f \in M_n$ $\mathbb{Z}$-линейные функционалы

$$\mathbb{Z}[\nabla]/(\nabla^{n+1}) \to \mathbb{Z},\ [h] \mapsto \langle\, [h]\,,\, f \,\rangle \quad \text{и} \quad M_n \to \mathbb{Z},\ p \mapsto \langle\, [g]\,,\, p \,\rangle$$

соответственно, являются изоморфизмами $\mathbb{Z}$-модулей.

[1] Т. е. в пространстве со счётным базисом. Например, пространство многочленов $\Bbbk[x]$ счётномерно.

[2] См. 4-24 на стр. 72.

[3] См. зад. 6.8 на стр. 112.

§8. Матрицы

В этом параграфе мы обозначаем через K произвольное коммутативное кольцо с единицей, а через $\Bbbk$ — произвольное поле.

8.1. Алгебры над коммутативными кольцами. Модуль A над коммутативным кольцом K называется *K-алгеброй* или *алгеброй над K*, если на нём задана операция умножения

$$A \times A \to A\,, \quad (a,b) \mapsto ab\,,$$

которая K-линейна по a при фиксированном b и K-линейна по b при фиксированном[1] a, т. е.

$$(x_1a_1 + x_2a_2)\,b = x_1a_1b + x_2a_2b \quad \text{и} \quad a\,(y_1b_1 + y_2b_2) = y_1ab_1 + y_2ab_2$$

для всех $a, b, a_i, b_j \in A$ и всех $x_i, y_j \in K$. Поскольку для любого $a \in A$ выполняются равенства $0 \cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$ и $a \cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$, мы заключаем, что $0 \cdot a = 0 = a \cdot 0$ в любой K-алгебре A.

Алгебра A называется *ассоциативной*, если $(ab)c = a(bc)$ для всех $a, b, c \in A$, и *коммутативной* — если $ab = ba$ для всех $a, b \in A$. Алгебра A называется *алгеброй с единицей*, если в ней есть нейтральный элемент по отношению к умножению, т. е. такой $e \in A$, что $ea = ae = a$ для всех $a \in A$. Так как для любых элементов e', e'' с этим свойством выполняются равенства $e' = e' \cdot e'' = e''$, единица в алгебре единственна, если существует.

Отображение $\varphi\colon A \to B$ между K-алгебрами A и B называется *гомоморфизмом K-алгебр*, если оно K-линейно и перестановочно с умножением, т. е. $\varphi(a_1a_2) = \varphi(a_1)\varphi(a_2)$. Будучи гомоморфизмами K-модулей, гомоморфизмы K-алгебр обладают всеми свойствами из n° 6.2 на стр. 102. Примерами коммутативных ассоциативных K-алгебр с единицами являются алгебра многочленов $K[x_1, \ldots, x_n]$ и другие конечно порождённые коммутативные K-алгебры из прим. 5.5 на стр. 89. Ключевыми примерами некоммутативных K-алгебр являются алгебры эндоморфизмов и алгебры матриц, обсуждаемые ниже.

Пример 8.1 (алгебра линейных эндоморфизмов модуля)
Рассмотрим любой модуль M над произвольным коммутативным кольцом K и обозначим через $\operatorname{End} M = \operatorname{Hom}_K(M, M)$ модуль всех K-линейных отображений[2] $M \to M$. Операция композиции[3] $\operatorname{End}(M) \times \operatorname{End}(M) \to \operatorname{End}(M)$, сопоставляющая паре отображений $(\varphi, \psi) \in \operatorname{End}(M) \times \operatorname{End}(M)$ их композицию $\varphi\circ\psi\colon M \to M, w \mapsto \varphi(\psi(w))$, задаёт на $\operatorname{End} M$ структуру ассоциативной K-алгебры с единицей, в роли которой выступает тождественный эндоморфизм $\mathrm{Id}_M\colon w \mapsto w$. Эта алгебра называется *алгеброй эндоморфизмов K-модуля M*.

Упражнение 8.1. Убедитесь, что композиция линейных отображений ассоциативна и линейно зависит от каждого из компонуемых отображений.

8.1.1. Алгебра квадратных матриц $\mathbf{Mat}_n(K)$. Рассмотрим координатный модуль K^n с базисом $e_1, \ldots, e_n$. Согласно предл. 6.4 на стр. 110, K-линейные эндоморфизмы $\varphi\colon K^n \to K^n$ находятся в биекции с упорядоченными наборами векторов

$$\boldsymbol{w} = (w_1, \ldots, w_n) \in K^n \times \ldots \times K^n \simeq K^{n^2}\,.$$

[1] Такие функции от двух аргументов называются *билинейными*.

[2] Такие отображения обычно называют *эндоморфизмами* модуля M, см. стр. 7.

[3] См. n° 1.5 на стр. 14.

Каждому набору $\boldsymbol{w}$ отвечает эндоморфизм $\varphi\colon K^n \to K^n$, действующий на базисные векторы e_i по правилу $\varphi(e_i) = w_i$, а на произвольный вектор $u = x_1e_1 + \ldots + x_ie_i$ — по правилу

$$\varphi(u) = \varphi(x_1e_1 + \ldots + x_ne_n) = x_1\varphi(e_1) + \ldots + x_n\varphi(w_n) = x_1w_1 + \ldots + x_nw_n\,,$$

и наоборот, каждому эндоморфизму $\varphi\colon K^n \to K^n$ отвечает набор векторов $w_i = \varphi(e_i)$.

Упражнение 8.2. Убедитесь в том, что эта биекция K-линейна, т. е. является изоморфизмом K-модулей $\operatorname{End} K^n \simeq K^n \times \ldots \times K^n$.

Набор векторов $w_i = \varphi(e_i)$, задающих эндоморфизм $\varphi\colon K^n \to K^n$, принято записывать в виде квадратной таблицы Φ размера $n\times n$, помещая координаты j-го вектора w_j относительно базиса $e_1, \ldots, e_n$ в j-й столбец этой таблицы:

$$w_1, \ldots, w_n = \begin{pmatrix}\varphi_{11}\\ \vdots \\ \varphi_{n1}\end{pmatrix}, \begin{pmatrix}\varphi_{12}\\ \vdots \\ \varphi_{n2}\end{pmatrix}, \ \ldots\ , \begin{pmatrix}\varphi_{1n}\\ \vdots \\ \varphi_{nn}\end{pmatrix} \dashrightarrow \Phi = \begin{pmatrix}\varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n}\\ \vdots & \vdots & \ldots & \vdots \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn}\end{pmatrix}.$$

Матрица $\Phi = \big(\varphi_{ij}\big)$ в i-й строке и j-м столбце которой находится i-я координата вектора $\varphi(e_j)$, называется *матрицей* отображения $\varphi\colon K^n \to K^n$ в базисе $e_1, \ldots, e_n$. Таким образом, сопоставляя эндоморфизму φ его матрицу Φ, мы получаем изоморфизм K-модулей

$$\operatorname{End}(K^n) \xrightarrow{\sim} \operatorname{Mat}_{n\times n}(K)\,, \quad \varphi \mapsto \Phi\,, \tag{8-1}$$

где $\operatorname{Mat}_n(K) \stackrel{\text{def}}{=} \operatorname{Mat}_{n\times n}(K)$ — модуль $n \times n$ матриц[1] с элементами из K. Изоморфизм (8-1) позволяет перенести на матрицы ассоциативное умножение из прим. 8.1, которое имеется в алгебре $\operatorname{End}(K^n)$ и задаётся композицией отображений. В результате возникает билинейное ассоциативное произведение

$$\operatorname{Mat}_{n\times n}(K) \times \operatorname{Mat}_{n\times n}(K) \to \operatorname{Mat}_{n\times n}(K)\,, \quad (\Phi, \Psi) \mapsto \Phi\Psi\,,$$

сопоставляющее матрицам Φ, Ψ линейных отображений $\varphi, \psi\colon K^n \to K^n$, матрицу $\Phi\Psi$ их композиции $\varphi\psi\colon K^n \to K^n, w \mapsto \varphi(\psi(w))$. Оно называется *произведением матриц*. Элемент $p_{ij} \in K$ произведения $P = \Phi\Psi = (p_{ij})$ является i-й координатой вектора

$$\varphi(\psi(e_j)) = \varphi(\psi_{1j}e_1 + \ldots + \psi_{nj}e_n) = \psi_{1j}\varphi(e_1) + \ldots + \psi_{nj}\varphi(e_n)\,,$$

которая равна $\psi_{1j}\varphi_{i1} + \ldots + \psi_{nj}\varphi_{in}$. Мы заключаем, что произведение $C = AB$ матриц $A = \big(a_{ij}\big)$ и $B = \big(b_{ij}\big)$ имеет в i-й строке и j-м столбце элемент

$$c_{ij} = \sum_k a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}\,. \tag{8-2}$$

Единицей алгебры $\operatorname{Mat}_{n\times n}(K)$ является матрица тождественного отображения $\mathrm{Id}\colon K^n \to K^n$

$$E = \begin{pmatrix}1 & 0 & \ldots & 0\\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0\\ 0 & \ldots & 0 & 1\end{pmatrix} \in \operatorname{Mat}_{n\times n}(K)\,, \tag{8-3}$$

[1] См. прим. 6.3 на стр. 102.

(по диагонали стоят единицы, в остальных местах — нули). Как и композиция отображений, умножение матриц не коммутативно. Например,

$$\begin{pmatrix}1&2\\0&3\end{pmatrix}\cdot\begin{pmatrix}3&0\\4&5\end{pmatrix}=\begin{pmatrix}11&10\\12&15\end{pmatrix}$$
$$\begin{pmatrix}3&0\\4&5\end{pmatrix}\cdot\begin{pmatrix}1&2\\0&3\end{pmatrix}=\begin{pmatrix}3&6\\4&23\end{pmatrix}.$$

Как K-модуль, алгебра $\mathrm{Mat}_n(K)$ изоморфна свободному координатному модулю K^{n^2}. Стандартный базис в $\mathrm{Mat}_n(K)$ состоит из матриц E_{ij}, единственным ненулевым элементом которых является единица, стоящая в i-й строке и j-м столбце. Произвольная матрица $A=(a_{ij})$ линейно выражается через этот базис по формуле $A=\sum_{i,j}a_{ij}E_{ij}$. Прообразами базисных матриц E_{ij} при изоморфизме (8-1) являются K-линейные отображения $E_{ij}:K^n\to K^n$, которые мы обозначаем также, как и базисные матрицы, и которые действуют на базисные векторы e_k координатного модуля K^n по правилам

$$E_{ij}(e_k)=\begin{cases}e_i & \text{при } k=j\\ 0 & \text{при } k\neq j.\end{cases}$$

Отсюда немедленно получается таблица умножения базисных матриц E_{ij}:

$$E_{ik}E_{\ell j}=\begin{cases}E_{ij} & \text{при } k=\ell\\ 0 & \text{при } k\neq\ell,\end{cases}\tag{8-4}$$

которая ещё раз показывает, что умножение матриц не коммутативно: $E_{12}E_{21}\neq E_{21}E_{12}$.

Упражнение 8.3. Составьте таблицу *коммутаторов* $[E_{ik},E_{\ell j}]\stackrel{\text{def}}{=}E_{ik}E_{\ell j}-E_{\ell j}E_{ik}$.

Пример 8.2
Вычислим F^{2020} для матрицы $F=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. Поскольку $F=E+E_{12}$ и матрицы E и E_{12} коммутируют, вычислить $(E+E_{12})^{2020}$ можно по формуле для раскрытия бинома[1], а так как $E_{12}^n=0$ при $n>1$, на ответ влияют только первые два члена:

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}^{2020}=(E+E_{12})^{2020}=E+2020\,E_{12}=\begin{pmatrix}1&2020\\0&1\end{pmatrix}.$$

Упражнение 8.4. Покажите, что $\begin{pmatrix}1&1\\0&1\end{pmatrix}^n=\begin{pmatrix}1&n\\0&1\end{pmatrix}$ при всех $n\in\mathbb{Z}$.

8.1.2. Алгебраические и трансцендентные элементы. Пусть $\Bbbk$ — произвольное поле. Каждый элемент ξ любой ассоциативной $\Bbbk$-алгебры A с единицей определяет гомоморфизм вычисления

$$\mathrm{ev}_\xi:\Bbbk[t]\to A,\quad f(t)\mapsto f(\xi)\in A,\tag{8-5}$$

сопоставляющий многочлену $f(x)=a_0x^m+\ldots+a_{m-1}x+a_m$ его значение на элементе ξ:

$$f(\xi)=a_0\xi^m+\ldots+a_{m-1}\xi+a_m\xi^0\in A,$$

[1] См. формулу (1-8) на стр. 10.

где мы полагаем $\xi^0 \stackrel{\text{def}}{=} e$ равным единице алгебры A. Если гомоморфизм (8-5) инъективен, то элемент ξ называется *трансцендентным* над $\Bbbk$. Отметим, что в этом случае алгебра A обязательно бесконечномерна как векторное пространство над $\Bbbk$, поскольку все степени элемента ξ линейно независимы.

Если гомоморфизм (8-5) имеет ненулевое ядро, то элемент ξ называется *алгебраическим* над $\Bbbk$. Так как $\Bbbk[x]$ является областью главных идеалов, идеал $\ker \mathrm{ev}_\xi = \big(\mu_\xi\big)$ главный, а его образующая $\mu_\xi \in \Bbbk[t]$ — это единственный приведённый многочлен наименьшей степени, аннулирующий ξ и являющийся наибольшим общим делителем всех многочленов, аннулирующих ξ. Он называется *минимальным многочленом* элемента $\xi \in A$ над полем $\Bbbk$.

Пример 8.3 (алгебраичность квадратных матриц)
Алгебра $n \times n$ матриц над полем $\Bbbk$ является векторным пространством размерности n^2. Поэтому целые неотрицательные степени F^k любой матрицы $F \in \mathrm{Mat}_n(\Bbbk)$ линейно зависимы и тем самым каждая квадратная матрица алгебраична над $\Bbbk$. В n° 11.4.5 на стр. 200 мы укажем для каждой $n \times n$ матрицы над любым коммутативным кольцом с единицей аннулирующий эту матрицу многочлен степени n.

Пример 8.4 (аннулирующий многочлен 2×2-матрицы)
Покажем, что каждая 2×2-матрица F над произвольным коммутативным кольцом K удовлетворяет приведённому квадратному уравнению. Имеем

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\Rightarrow\; F^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ca+dc & cb+d^2 \end{pmatrix} = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & cb+d^2 \end{pmatrix},$$

откуда

$$F^2 - (a+d)\cdot F = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & cb+d^2 \end{pmatrix} - \begin{pmatrix} a(a+d) & b(a+d) \\ c(a+d) & d(a+d) \end{pmatrix} = \\ = \begin{pmatrix} (bc-ad) & 0 \\ 0 & (bc-ad) \end{pmatrix} = (bc-ad)\cdot E\,.$$

Тем самым, $F^2 - (a+b)F + (ad-bc)E = 0$. Числа $\det F \stackrel{\text{def}}{=} ad-bc$ и $\operatorname{tr} F \stackrel{\text{def}}{=} a+b$ называются, соответственно, *определителем* и *следом* 2×2 матрицы F. В этих обозначениях квадратное уравнение на матрицу F имеет вид

$$F^2 - \operatorname{tr}(F)\cdot F + \det(F)\cdot E = 0\,. \tag{8-6}$$

8.1.3. Обратимые элементы. Элемент a алгебры A с единицей $e \in A$ называется *обратимым*, если существует такой элемент $a^{-1} \in A$, что $aa^{-1} = a^{-1}a = e$. В ассоциативной алгебре A это требование можно ослабить до существования таких $a', a'' \in A$, что $a'a = aa'' = e$. В самом деле, из равенств $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$ вытекает, во-первых, что любые два таких элемента a', a'' равны, а во-вторых, что обратный к a элемент a^{-1}, если он существует, однозначно определяется по a равенствами $a^{-1}a = aa^{-1} = e$.

Пример 8.5 (обратимые 2×2-матрицы, продолжение прим. 8.4)
Покажем, что 2×2-матрица F обратима в алгебре $\mathrm{Mat}_{2\times 2}(K)$ если и только если её определитель $\det F$ обратим в K. Перепишем равенство (8-6) как

$$\det(F)E = F(\operatorname{tr}(F)E - F) = (\operatorname{tr}(F)E - F)F\,. \tag{8-7}$$

Матрица $F^\vee \stackrel{\text{def}}{=} \operatorname{tr}(F)E - F$ называется *присоединённой* к 2×2 матрице F. В явном виде

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\vee = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tag{8-8}$$

Упражнение 8.5. Убедитесь, что $(AB)^\vee = B^\vee A^\vee$ для любых $A, B \in \operatorname{Mat}_{2\times 2}(K)$.

Из формулы (8-7) вытекает, что если $\det(F)$ обратим в K, то матрица F тоже обратима и

$$F^{-1} = \det{}^{-1}(F)F^\vee\,. \tag{8-9}$$

С другой стороны, согласно упр. 8.5 для всех $A, B \in \operatorname{Mat}_{2\times 2}(K)$

$$\det(AB)E = AB(AB)^\vee = ABB^\vee A^\vee = A\det(B)EA^\vee = \det(B)AA^\vee = \det(A)\det(B)E\,,$$

откуда $\det(AB) = \det(A)\det(B)$. Если F обратима, то $1 = \det E = \det(F^{-1}F) = \det(F^{-1})\det(F)$, и $\det F$ обратим в K.

Пример 8.6 (обращение унитреугольной матрицы)
Диагональ, идущая из левого верхнего угла квадратной матрицы в правый нижний, называется *главной*. Если все стоящие под (соотв. над) главной диагональю элементы нулевые, матрица называется *верхней* (соотв. *нижней*) *треугольной*.

Упражнение 8.6. Проверьте, что верхние и нижние треугольные матрицы являются подалгебрами[1] в $\operatorname{Mat}_n(K)$.

Треугольные матрицы с единицами на главной диагонали называются *унитреугольными*. Покажем, что каждая верхняя унитреугольная матрица $A = \left(a_{ij}\right)$ обратима[2] и обратная к ней матрица $B = A^{-1}$ тоже верхняя унитреугольная с наддиагональными элементами

$$\begin{aligned} b_{ij} = \sum_{s=0}^{j-i-1}(-1)^{s+1} \sum_{i<\nu_1<\ldots<\nu_s<j} a_{i\nu_1}a_{\nu_1\nu_2}a_{\nu_2\nu_3}\,\ldots\,a_{\nu_{s-1}\nu_s}a_{\nu_s j} = \\ = -a_{ij} + \sum_{i<k<j} a_{ik}a_{kj} - \sum_{i<k<\ell<j} a_{ik}a_{k\ell}a_{\ell j} + \sum_{i<k<\ell<m<j} a_{ik}a_{k\ell}a_{\ell m}a_{mj} - \ldots\,. \end{aligned} \tag{8-10}$$

Для этого запишем матрицу A в виде линейной комбинации базисных матриц E_{ij}:

$$A = E + \sum_{i<j} a_{ij}E_{ij} = E + N\,,$$

где матрица $N = \sum_{i<j} a_{ij}E_{ij}$ представляет собою наддиагональную часть матрицы A. Согласно форм. (8-4) на стр. 133 коэффициент при[3] E_{ij} в матрице N^k равен нулю при $j - i < k$, а при

[1] Т. е. являются подмодулями, замкнутыми относительно умножения.

[2] Причём этот факт, как и приводимое здесь доказательство, остаётся в силе для матриц с элементами в произвольном (даже некоммутативном) ассоциативном кольце с единицей.

[3] Продуктивно представлять себе E_{ij} как стрелку, ведущую из числа j в число i на числовой прямой. Произведение k сомножителей E_{ij} отлично от нуля если и только если конец каждой стрелки совпадает с началом предыдущей, и в этом случае такое произведение равно сумме всех перемножаемых стрелок, рассматриваемых как целочисленные векторы на числовой прямой. Таким образом, каждое ненулевое произведение k стрелок имеет длину как минимум k, а разложения элемента E_{ij} в произведение k таких элементов находятся в биекции со всевозможными способами пройти из j в i за k шагов.

$j - i \geqslant k$ представляет собою сумму всевозможных произведений

$$\underbrace{a_{iv_1}a_{v_1v_2}\dots a_{v_{k-2}v_{k-1}}a_{v_{k-1}j}}_{k \text{ сомножителей}}, \quad \text{где} \quad i < v_1 < \dots < v_{k-1} < j\,.$$

В частности, он заведомо зануляется, когда k превышает размер матрицы A. Полагая $x = E$, $y = N$ в равенстве[1] $(x+y)(x^{m-1} - x^{m-2}y + \dots + (-1)^{m-1}y^{m-1}) = x^m - y^m$, при достаточно большом m мы получим матричное равенство $A(E - N + N^2 - N^3 + \dots) = E$, откуда

$$A^{-1} = E - N + N^2 - N^3 + \dots\,,$$

что и утверждалось.

8.1.4. Отступление о группах. Множество G с одной операцией $G \times G \to G, (g_1, g_2) \mapsto g_1g_2$, называется *группой*, если эта операция ассоциативна: $(fg)h = f(gh)$ для всех $f, g, h \in G$, и существует единица $e \in G$ со свойством $eg = g$ для всех $g \in G$, а у каждого элемента $g \in G$ есть обратный элемент $g^{-1} \in G$ со свойством $g^{-1}g = e$. Состоящая из одной единицы группа $G = \{e\}$ называется *тривиальной*.

В каждой группе элемент g^{-1} автоматически удовлетворяет соотношению $gg^{-1} = e$, которое получается умножением правой и левой части равенства $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$ слева на обратный к g^{-1} элемент. Поэтому для всех $g \in G$ также выполняется соотношение

$$ge = g(g^{-1}g) = (gg^{-1})g = eg = g\,.$$

Упражнение 8.7. Убедитесь, что единичный элемент $e \in G$ единствен, а g^{-1} однозначно определяется элементом g, и $\bigl(g_1 \dots g_k\bigr)^{-1} = g_k^{-1} \dots g_1^{-1}$.

Подмножество $H \subset G$ называется *подгруппой*, если оно образует группу относительно имеющейся в G операции. Для этого достаточно, чтобы вместе с каждым элементом $h \in H$ в H лежал и обратный к нему элемент h^{-1}, а вместе с каждой парой элементов $h_1, h_2 \in H$ — их произведение h_1h_2. При этом $e \in G$ автоматически окажется в H, ибо $e = hh^{-1}$ для любого $h \in H$.

Упражнение 8.8. Проверьте, что пересечение любого множества подгрупп является подгруппой.

Группа, в которой любые два элемента $f, g \in G$ перестановочны: $fg = gf$, называется *коммутативной* или *абелевой*. Отображение групп $\varphi : G \to H$ называется *гомоморфизмом*, если $\varphi(ab) = \varphi(a)\varphi(b)$ для всех $a, b \in G$. Группы *изоморфны*, если между ними имеется биективный гомоморфизм.

Обратимые элементы любой K-алгебры A с единицей образуют мультипликативную группу $A^\times \subset A$. Группа обратимых элементов алгебры $\mathrm{End}_K(M)$ эндоморфизмов K-модуля M состоит из K-линейных биекций $M \xrightarrow{\sim} M$. Она называется *группой автоморфизмов* или *полной линейной группой* модуля M и обозначается $\mathrm{Aut}(M)$ или $\mathrm{GL}(M)$. Группа обратимых элементов алгебры матриц $\mathrm{Mat}_n(K)$, где K — коммутативное кольцо с единицей, обозначается $\mathrm{GL}_n(K)$ и называется *полной линейной группой* ранга n над K.

Упражнение 8.9. Убедитесь, что верхние унитреугольные матрицы образуют в $\mathrm{GL}_n(K)$ подгруппу.

[1] Поскольку матрицы E и N коммутируют друг с другом, в результате этой подстановки мы получим верное матричное равенство.

Если модуль M свободен с базисом $e_1, \dots, e_n$, то сопоставляя автоморфизму $\varphi : M \to M$ его матрицу Φ в этом базисе, как это объяснялось в n° 8.1.1 на стр. 131, мы задаём изоморфизм групп $\mathrm{GL}(M) \xrightarrow{\sim} \mathrm{GL}_n(K)$.

8.2. Умножение матриц. Матрица из m строк и n столбцов, заполненная элементами какого-нибудь K-модуля R, называется $m \times n$ *матрицей* с элементами из R. Множество всех таких матриц обозначается $\mathrm{Mat}_{m\times n}(R)$ и является K-модулем, изоморфным R^{mn} — прямому произведению mn копий модуля R. Пусть элементы K-модулей L и M можно билинейно перемножать со значениями в K-модуле N, т. е. задано такое отображение $L \times M \to N$, $(u, w) \to uw$, что

$$(x_1u_1 + x_2u_2)(y_1w_1 + y_2w_2) = x_1y_1u_1w_1 + x_1y_2u_1w_2 + x_2y_1u_2w_1 + x_2y_2u_2w_2$$

для всех $u_i \in L$, $w_j \in M$ и $x_i, y_j \in K$. В этой ситуации для всех $m, s, n \in \mathbb{N}$ определено *произведение матриц*

$$\mathrm{Mat}_{m\times s}(L) \times \mathrm{Mat}_{s\times n}(M) \to \mathrm{Mat}_{m\times n}(N), \quad (A, B) \mapsto AB\,.$$

Обратите внимание, что в этом произведении ширина левой матрицы A должна быть равна высоте правой матрицы B, а само произведение имеет столько же строк, сколько левый сомножитель, и столько же столбцов, сколько правый. При $m = n = 1$ результатом умножения строки ширины s на столбец высоты s является матрица размера 1×1, т. е. один элемент, который определяется по форм. (8-2) на стр. 132:

$$(a_1, \dots, a_s)\begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix} \stackrel{\text{def}}{=} a_1b_1 + \dots + a_sb_s = \sum_{k=1}^{s} a_kb_k\,. \tag{8-11}$$

Для произвольных m и n элемент c_{ij} матрицы $C = AB$ равен произведению i-й строки из A на j-й столбец из B:

$$c_{ij} = \begin{pmatrix} a_{i1}, \dots\ a_{is} \end{pmatrix} \cdot \begin{pmatrix} b_{1j} \\ \vdots \\ b_{sj} \end{pmatrix} = \sum_{k=1}^{s} a_{ik}b_{kj}\,. \tag{8-12}$$

Иначе можно сказать, что в j-том столбце матрицы AB стоит линейная комбинация s столбцов матрицы A с коэффициентами из j-го столбца матрицы B. Это описание получается, если подставить в формулу (8-11) в качестве элементов b_i числа из j-го столбца матрицы B, а в качестве элементов a_j — столбцы матрицы A, интерпретируемые как элементы K-модуля L^m, записанные в виде координатных столбцов.

Упражнение 8.10. Удостоверьтесь, что это описание согласуется с формулой (8-12).

Например, для того, чтобы превратить матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \tag{8-13}$$

в матрицу из четырёх столбцов, равных, соответственно, сумме 1-го столбца матрицы A со 2-м, умноженным на λ, сумме 1-го и 3-го столбцов матрицы A, сумме 3-го столбца матрицы A со 2-м, умноженным на μ, и сумме всех трёх столбцов матрицы A, умноженных на их номера, надо умножить матрицу A справа на матрицу

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ \lambda & 0 & \mu & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Упражнение 8.11. Проверьте это прямым вычислением по формуле (8-12).

Симметричным образом, если в формуле (8-11) взять в в качестве элементов a_j те, что стоят в i-й строке матрицы A, а в качестве b_i — строки матрицы B, интерпретируемые как элементы K-модуля M^n, записанные в виде координатных строк, то можно сказать, что i-й строкой матрицы AB является линейная комбинация строк матрицы B с коэффициентами, стоящими в i-й строке матрицы A. Например, если в той же матрице (8-13) хочется поставить вторую строку на место первой, а вместо второй написать её сумму с первой строкой, умноженной на λ, то это достигается умножением слева на матрицу

$$\begin{pmatrix} 0 & 1 \\ \lambda & 1 \end{pmatrix}$$

Упражнение 8.12. Проверьте это прямым вычислением по формуле (8-12).

Предыдущие два описания произведения AB получаются друг из друга одновременной перестановкой букв A, B и заменой слов «столбец» и «строка» друг на друга. Матрица $C^t = (c^t_{ij})$ размера $n \times m$, по строкам которой записаны столбцы $m \times n$ матрицы $C = (c_{ij})$, называется *транспонированной* к матрице C. Её элементы $c^t_{ij} = c_{ji}$ получаются отражением элементов матрицы C относительно биссектрисы левого верхнего угла матрицы.

Предложение 8.1
Для матриц с элементами из коммутативного кольца выполняется равенство $(AB)^t = B^t A^t$, т. е. транспонирование обращает порядок сомножителей в произведениях матриц, элементы которых коммутируют друг с другом.

Доказательство. Пусть $AB = C$, $B^t A^t = D$, тогда $c_{ij} = \sum\limits_k a_{ik} b_{kj} = \sum\limits_k a^t_{ki} b^t_{jk} = \sum\limits_k b^t_{jk} a^t_{ki} = d_{ji}$. □

Упражнение 8.13. Убедитесь, что если операция умножения $L \times M \to N$ билинейна, то произведение матриц $\mathrm{Mat}_{m\times s}(L) \times \mathrm{Mat}_{s\times n}(M) \to \mathrm{Mat}_{m\times n}(N)$ тоже билинейно, т. е.

$$(x_1 A_1 + x_2 A_2)B = x_1 A_1 B + x_2 A_2 B \quad \text{и} \quad A(y_1 B_1 + y_2 B_2) = y_1 AB_1 + y_2 AB_2$$

для всех $A, A_1, A_2 \in \mathrm{Mat}_{m\times s}(L)$, $B, B_1, B_2 \in \mathrm{Mat}_{m\times s}(M)$ и $x_i, y_j \in K$.

Предложение 8.2
Если на абелевых группах $L_1, L_2, L_3, L_{12}, L_{23}, L_{123}$ заданы дистрибутивные[1] и ассоциативные[2] умножения $L_1 \times L_2 \to L_{12}$, $L_{12} \times L_3 \to L_{123}$, $L_2 \times L_3 \to L_{23}$, $L_1 \times L_{23} \to L_{123}$, то при всех $m, k, \ell, n \in \mathbb{N}$ умножения матриц

$$\mathrm{Mat}_{m\times k}(L_1) \times \mathrm{Mat}_{k\times \ell}(L_2) \to \mathrm{Mat}_{m\times \ell}(L_{12}), \quad \mathrm{Mat}_{m\times \ell}(L_{12}) \times \mathrm{Mat}_{\ell\times n}(L_3) \to \mathrm{Mat}_{m\times n}(L_{123}),$$
$$\mathrm{Mat}_{k\times \ell}(L_2) \times \mathrm{Mat}_{\ell\times n}(L_3) \to \mathrm{Mat}_{k\times n}(L_{23}), \quad \mathrm{Mat}_{m\times k}(L_1) \times \mathrm{Mat}_{k\times n}(L_{23}) \to \mathrm{Mat}_{m\times n}(L_{123}).$$

тоже дистрибутивны и ассоциативны, т. е. $A(B + C) = AB + AC$, $(A + B)C = AC + BC$ и $(AB)C = A(BC)$ для всех матриц A, B, C, на которых эти операции определены.

[1] Т. е. $(a + b)c = ac + bc$ и $a(b + c) = ab + ac$

[2] Т. е. $(ab)c = a(bc)$.

Доказательство. Дистрибутивность вытекает из упр. 8.13. Докажем ассоциативность. Полагаем $AB = P$, $BC = Q$ и проверяем, что (i, j)-е элементы произведений PC и AQ равны друг другу:

$$\sum_k p_{ik}c_{kj} = \sum_k \Big(\sum_\ell a_{i\ell}b_{\ell k}\Big)c_{kj} = \sum_{k\ell}(a_{i\ell}b_{\ell k})c_{kj} = \\ = \sum_{k\ell} a_{i\ell}(b_{\ell k}c_{kj}) = \sum_\ell a_{i\ell}\Big(\sum_k b_{\ell k}c_{kj}\Big) = \sum_\ell a_{i\ell}q_{\ell j}\,.$$

Обратите внимание, что второе и четвёртое равенство используют дистрибутивность умножений между абелевыми группами. □

8.3. Матрицы перехода. Пусть в K-модуле M заданы два набора векторов:

$$\boldsymbol{u} = (u_1, \dots, u_n) \quad \text{и} \quad \boldsymbol{w} = (w_1, \dots, w_m)\,,$$

причём первый из них содержится в линейной оболочке второго, т. е. каждый вектор u_j имеет вид $u_j = w_1c_{1j} + w_2c_{2j} + \dots + w_mc_{mj}$, где $c_{ij} \in K$. Эти n равенств собираются в одну матричную формулу $\boldsymbol{u} = \boldsymbol{w}\,C_{\boldsymbol{wu}}$, где $\boldsymbol{u} = (u_1, \dots, u_n)$ и $\boldsymbol{w} = (w_1, \dots, w_m)$ суть матрицы-строки с элементами из M, а матрица $C_{\boldsymbol{wu}} = \big(c_{ij}\big)$ получается подстановкой в матрицу $\boldsymbol{u}$ вместо каждого из векторов u_j столбца коэффициентов его линейного выражения через векторы w_i. Матрица $C_{\boldsymbol{wu}}$ называется *матрицей перехода* от векторов $\boldsymbol{u}$ к векторам $\boldsymbol{w}$. Название объясняется тем, что если имеется набор векторов $\boldsymbol{v} = (v_1, \dots, v_k)$, линейно выражающихся через векторы $\boldsymbol{u}$ по формулам $\boldsymbol{v} = \boldsymbol{u}C_{\boldsymbol{uv}}$, то выражение векторов $\boldsymbol{v}$ через векторы $\boldsymbol{w}$ задаётся матрицей

$$C_{\boldsymbol{wv}} = C_{\boldsymbol{wu}}C_{\boldsymbol{uv}}\,, \tag{8-14}$$

которая возникает при подстановке $\boldsymbol{u} = \boldsymbol{w}C_{\boldsymbol{wu}}$ в разложение $\boldsymbol{v} = \boldsymbol{u}C_{\boldsymbol{uv}}$. Таким образом, если записывать линейные выражения $v = u_1x_1 + \dots + u_nx_n = w_1y_1 + \dots + w_my_m$ произвольного вектора $v \in \operatorname{span}(u_1, \dots, u_n)$ через векторы $\boldsymbol{u}$ и $\boldsymbol{w}$ в виде $v = \boldsymbol{u}\boldsymbol{x} = \boldsymbol{w}\boldsymbol{y}$, где $\boldsymbol{x} = (x_1, \dots, x_n)^t$ и $\boldsymbol{y} = (y_1, \dots, y_m)^t$ суть столбцы коэффициентов, то эти столбцы будут связаны соотношением

$$\boldsymbol{y} = C_{\boldsymbol{wu}}\boldsymbol{x}\,.$$

Подчеркнём, что когда набор векторов $\boldsymbol{w} = (w_1, \dots, w_m)$ линейно зависим, у каждого вектора v из их линейной оболочки бывают *разные* линейные выражения через векторы w_j. Поэтому обозначение $C_{\boldsymbol{wv}}$ не корректно в том смысле, что элементы матрицы $C_{\boldsymbol{wv}}$ определяются наборами векторов $\boldsymbol{w}$ и $\boldsymbol{v}$ не однозначно. Тем не менее, равенство (8-14) вполне осмысленно и означает, что имея какие-либо линейные выражения $C_{\boldsymbol{wu}}$ и $C_{\boldsymbol{uv}}$ векторов $\boldsymbol{u}$ через $\boldsymbol{w}$ и векторов $\boldsymbol{v}$ через $\boldsymbol{u}$, мы можем явно предъявить одно из линейных выражений $C_{\boldsymbol{wv}}$ векторов $\boldsymbol{v}$ через векторы $\boldsymbol{w}$, перемножив матрицы $C_{\boldsymbol{wu}}$ и $C_{\boldsymbol{uv}}$.

Если набор векторов $\boldsymbol{e} = (e_1, \dots, e_n)$ является базисом своей линейной оболочки, то матрица перехода $C_{\boldsymbol{ew}}$, выражающая произвольный набор векторов $\boldsymbol{w} = (w_1, \dots, w_m)$ через $\boldsymbol{e}$ однозначно определяется наборами $\boldsymbol{e}$ и $\boldsymbol{w}$, т. е. $\boldsymbol{u} = \boldsymbol{w}$ если и только если $C_{\boldsymbol{eu}} = C_{\boldsymbol{ew}}$. Отсюда получается следующий критерий обратимости матрицы с элементами из коммутативного кольца.

Предложение 8.3
Следующие условия на квадратную матрицу $C \in \operatorname{Mat}_n(K)$ эквивалентны:

1) матрица C обратима в $\operatorname{Mat}_n(K)$

2) столбцы матрицы C образуют базис свободного модуля K^n

3) строки матрицы C образуют базис свободного модуля K^n.

Доказательство. По предл. 8.1 на стр. 138 равенства $BC = CB = E$ при транспонировании превращаются в равенства $C^tB^t = B^tC^t = E$. Поэтому обратимость матрицы C влечёт обратимость транспонированной матрицы C^t и наоборот. Это доказывает равносильность последних двух условий. Чтобы установить равносильность двух первых, обозначим через $u_1, \dots, u_n$ столбцы матрицы C, рассматриваемые как векторы координатного модуля K^n. Тогда $C = C_{\boldsymbol{ue}}$ является матрицей перехода от них к стандартному базису $\boldsymbol{e} = (e_1, \dots, e_n)$ в K^n. Если набор векторов $\boldsymbol{u} = (u_1, \dots, u_n)$ является базисом в K^n, набор векторов $\boldsymbol{e}$ линейно выражается через $\boldsymbol{u}$ как $\boldsymbol{e} = \boldsymbol{u}\,C_{\boldsymbol{eu}}$, где $C_{\boldsymbol{eu}} \in \mathrm{Mat}_n(K)$. Из формулы (8-14) вытекают равенства $C_{\boldsymbol{ee}} = C_{\boldsymbol{eu}}C_{\boldsymbol{ue}}$ и $C_{\boldsymbol{uu}} = C_{\boldsymbol{ue}}C_{\boldsymbol{eu}}$. Так как оба набора являются базисами, $C_{\boldsymbol{ee}} = C_{\boldsymbol{uu}} = E$, т. е. матрицы $C_{\boldsymbol{ue}}$ и $C_{\boldsymbol{eu}}$ обратны друг другу. Наоборот, если матрица $C_{\boldsymbol{eu}}$ обратима, то умножая обе части равенства $\boldsymbol{u} = \boldsymbol{e}C_{\boldsymbol{eu}}$ справа на $C_{\boldsymbol{eu}}^{-1}$, получаем линейное выражение $\boldsymbol{e} = \boldsymbol{u}\,C_{\boldsymbol{eu}}^{-1}$ векторов $\boldsymbol{e}$ через векторы $\boldsymbol{u}$. Поэтому последние линейно порождают модуль K^n. Если столбец $\boldsymbol{x}$ коэффициентов $x_i \in K$ таков, что $0 = \boldsymbol{ux} = \boldsymbol{e}\,C_{\boldsymbol{eu}}\boldsymbol{x}$, то столбец $C_{\boldsymbol{eu}}\boldsymbol{x} \in K^n$ нулевой, ибо векторы $\boldsymbol{e}$ составляют базис в K^n. Умножая его слева на $C_{\boldsymbol{eu}}^{-1}$, заключаем, что и столбец $\boldsymbol{x}$ нулевой. Поэтому векторы $\boldsymbol{u}$ линейно независимы. □

Пример 8.7 (теорема об элементарных симметрических функциях)
Многочлен $f \in \mathbb{Z}[x_1, \dots, x_n]$ называется *симметрическим*, если он не меняется при перестановках номеров переменных, т. е. когда $f(x_1, \dots, x_n) = f(x_{g(1)}, \dots, x_{g(n)})$ для всех биекций

$$g : \{1, \dots, n\} \xrightarrow{\sim} \{1, \dots, n\}.$$

Иначе говоря, многочлен f симметрический если и только если вместе с каждым входящим в f мономом $x_1^{m_1}\dots x_n^{m_n}$ с тем же самым коэффициентом в f входят и все мономы $x_1^{m_{g(1)}}\dots x_n^{m_{g(n)}}$, которые получаются из него перестановками степеней. Так как среди них есть ровно один моном $x_1^{\lambda_1}\dots x_n^{\lambda_n}$ с невозрастающими показателями $\lambda_1 \geqslant \dots \geqslant \lambda_n$, мы заключаем, что однородные симметрические многочлены степени d образуют свободный $\mathbb{Z}$-модуль с базисом из многочленов

$$m_\lambda = (\text{сумма всех различных мономов вида } x_1^{\lambda_{g(1)}}\dots x_n^{\lambda_{g(n)}}), \tag{8-15}$$

где $\lambda = (\lambda_1, \dots, \lambda_n)$ пробегает диаграммы Юнга[1] из d клеток и n строк, часть из которых может быть нулевой длины. Многочлен (8-15) называется *мономиальным симметрическим*.

Упражнение 8.14. Сколько слагаемых в правой части (8-15)?

Симметрические многочлены $e_0 = 1$ и $e_k(x_1, \dots, x_n) = \sum_{i_1<\dots<i_k} x_{i_1}\dots x_{i_k}$, равный сумме всех произведений из k различных переменных, где $1 \leqslant k \leqslant n$, называются *элементарными*. Они появляются в *формулах Виета*: если $\alpha_1, \dots, \alpha_n$ — корни приведённого многочлена

$$t^n + a_1t^{n-1} + \dots + a_n = \prod_{i=1}^{n}(x - \alpha_i), \tag{8-16}$$

то $a_i = (-1)^i e_i(\alpha_1, \dots, \alpha_n)$.

[1] См. прим. 1.3 на стр. 10.

Упражнение 8.15. Убедитесь в этом.

Для каждой диаграммы Юнга $\mu = (\mu_1, \dots, \mu_n)$ положим $e_\mu \stackrel{\text{def}}{=} e_{\mu_1} \dots e_{\mu_n}$. Это лишь другое обозначение для монома $e_1^{m_1} \dots e_n^{m_n}$, каждый показатель m_i в котором равен количеству строк длины i в диаграмме μ.

Упражнение 8.16. Убедитесь, что диаграмма Юнга μ и набор $(m_1, \dots, m_n) \in \mathbb{Z}^n_{\geqslant 0}$ взаимно однозначно определяют друг друга из равенства $e_{\mu_1} \dots e_{\mu_n} = e_1^{m_1} \dots e_n^{m_n}$.

Многочлен e_μ однороден степени $m_1 + 2m_2 + \dots + nm_n$, а его лексикографически старший по переменным $x_1, \dots, x_n$ мономом является произведением старших мономов $x_1 \dots x_{\mu_1}$ из e_{μ_1}, $x_1 \dots x_{\mu_2}$ из e_{μ_2} и т. д. вплоть до $x_1 \dots x_{\mu_n}$ из e_{μ_n}. Это произведение является результатом перемножения переменных x_i, вписанных в клетки диаграммы Юнга μ так, что номер переменной совпадает с номером столбца, в котором она стоит, и равно $x_1^{\mu_1^t} \dots x_n^{\mu_n^t}$, где $\mu^t = (\mu_1^t, \dots, \mu_n^t)$ — транспонированная к μ диаграмма Юнга[1]. Таким образом, разложение многочлена e_μ по базису (8-15) имеет вид:

$$e_\mu = m_{\mu^t} + (\text{лексикографически младшие члены}). \tag{8-17}$$

Если выписать все диаграммы λ из d клеток в одну строку в порядке лексикографического возрастания наборов чисел $(\lambda_1, \dots, \lambda_n)$, а все диаграммы μ из d клеток — в порядке лексикографического возрастания транспонированных диаграмм μ^t, то согласно формуле (8-17) матрица перехода от многочленов e_μ к многочленам m_λ является верхней унитреугольной. В прим. 8.6 на стр. 135 мы видели, что такая матрица обратима в алгебре целочисленных матриц. Тем самым, по предл. 8.3 многочлены $e_\mu = e_1^{m_1} \dots e_n^{m_n}$, где $m_1 + 2m_2 + \dots + nm_n = d$, тоже составляют базис модуля однородных симметрических многочленов степени d над $\mathbb{Z}$. Это означает, что любой симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических многочленов $e_1, \dots, e_n$. Иначе говоря, алгебра симметрических многочленов совпадает с алгеброй многочленов $\mathbb{Z}[e_1, \dots, e_n]$.

Пример 8.8 (дискриминант)
Дискриминантом приведённого многочлена $f(x) = t^n + a_1 t^{n-1} + \dots + a_n = \prod_{i=1}^n (x - \alpha_i)$ называется произведение $\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2$ квадратов разностей его корней, вычисленное в любом кольце, над которым f полностью раскладывается на линейные множители. Будучи симметрическим многочленом от корней, Δ_f является многочленом от $e_i(\alpha_1, \dots, \alpha_n) = (-1)^i a_i$, т. е. многочленом от коэффициентов уравнения. При этом $\Delta_f = 0$ если и только если f не сепарабелен. Так, дискриминант квадратного трёхчлена $f(x) = x^2 + px + q = (x - \alpha_1)(x - \alpha_2)$ равен $(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = p^2 - 4q$. Он зануляется если и только если f является полным квадратом линейного двучлена, и если $\Delta_f = \delta^2$ сам является квадратом, то корни f находятся из равенств $\alpha_1 + \alpha_2 = -p$, $\alpha_1 - \alpha_2 = \pm\delta$.

Упражнение 8.17. Вычислите дискриминант кубического трёхчлена $x^3 + px + q$.

8.4. Матрицы линейных отображений. Пусть K-модули N и M линейно порождаются наборами векторов $\boldsymbol{u} = (u_1, \dots, u_n)$ и $\boldsymbol{w} = (w_1, \dots, w_m)$ соответственно. Всякое K-линейное отображение $\varphi : N \to M$ однозначно задаётся набором $\varphi(\boldsymbol{u}) \stackrel{\text{def}}{=} \big(\varphi(u_1), \dots, \varphi(u_n)\big)$ своих значений на

[1] Её строками являются столбцы диаграммы μ также, как при транспонировании матриц.

порождающих векторах и действует на произвольный вектор $v = \boldsymbol{ux}$, где $\boldsymbol{x} \in K^n$ — столбец коэффициентов линейного выражения вектора v через образующие $\boldsymbol{u}$, по правилу

$$\varphi(\boldsymbol{ux}) = \varphi\Big(\sum_{i=1}^{n} u_i x_i\Big) = \sum_{i=1}^{n} \varphi(u_i)\, x_i = \varphi(\boldsymbol{u})\boldsymbol{x}\,. \tag{8-18}$$

Матрица перехода от векторов $\varphi(\boldsymbol{u})$ к образующим $\boldsymbol{w}$ модуля M обозначается $\Phi_{\boldsymbol{wu}} \in \mathrm{Mat}_{m\times n}(K)$ и называется *матрицей отображения*[1] φ в образующих $\boldsymbol{w}$ и $\boldsymbol{u}$. Её j-й столбец состоит из коэффициентов линейного выражения вектора $\varphi(u_j)$ через векторы $\boldsymbol{w}$. Если $N = K^n$, а $M = K^n$, и в качестве $\boldsymbol{u}$ и $\boldsymbol{w}$ берутся стандартные базисы этих координатных модулей, мы получаем в точности то же сопоставление линейному отображению $\varphi : K^n \to K^m$ его матрицы Φ, с которого мы начинали в n° 8.1.1 на стр. 131.

Согласно (8-18) линейное отображение $\varphi : N \to M$ с матрицей $\Phi_{\boldsymbol{wu}}$ в образующих $\boldsymbol{w}$, $\boldsymbol{u}$ переводит произвольный вектор $v = \boldsymbol{ux} \in N$, где $\boldsymbol{x} = (x_1, \dots, x_n)^t \in K^n$ — столбец коэффициентов, в вектор $\varphi(v) = \boldsymbol{w}\Phi_{\boldsymbol{wu}}\boldsymbol{x} \in M$, имеющий в образующих $\boldsymbol{w}$ столбец коэффициентов $F_{\boldsymbol{wu}}\boldsymbol{x} \in K^m$. Таким образом в терминах коэффициентов линейных выражений векторов через образующие отображение φ действует по правилу

$$\phi : \boldsymbol{x} \mapsto \Phi\,\boldsymbol{x}\,. \tag{8-19}$$

Вычисление (8-18) также показывает, что для любого набора векторов $\boldsymbol{v} = (v_1, \dots, v_k)$ в N, любой матрицы $A \in \mathrm{Mat}_{\ell\times k}(K)$ и любого K-линейного отображения $\varphi : N \to M$ выполняется равенство

$$\varphi(\boldsymbol{v}A) = \varphi(\boldsymbol{v})A\,. \tag{8-20}$$

Поэтому матрица композиции линейных отображений равна произведению их матриц (в том же порядке). А именно, если имеется ещё один K-модуль L с образующими $\boldsymbol{v} = (v_1, \dots, v_k)$, и линейные отображения $\psi : M \to L$ и $\varphi : L \to N$ имеют, соответственно, матрицу $\Psi_{\boldsymbol{vw}}$ в образующих $\boldsymbol{w}$, $\boldsymbol{v}$ и матрицу $\Phi_{\boldsymbol{uv}}$ в образующих $\boldsymbol{v}$, $\boldsymbol{u}$, то их композиция $\eta = \varphi\psi : N \to M$ имеет в образующих $\boldsymbol{w}$, $\boldsymbol{u}$ матрицу $H_{\boldsymbol{uw}} = \Phi_{\boldsymbol{uv}}\Psi_{\boldsymbol{vw}}$, так как

$$\eta(\boldsymbol{w}) = \varphi\big(\psi(\boldsymbol{w})\big) = \varphi\big(\boldsymbol{v}\Psi_{\boldsymbol{vw}}\big) = \varphi(\boldsymbol{v})\Psi_{\boldsymbol{vw}} = \boldsymbol{u}\Phi_{\boldsymbol{uv}}\Psi_{\boldsymbol{vu}}\,.$$

Предостережение 8.1. (некорректность обозначения $F_{\boldsymbol{wu}}$) Если образующие $\boldsymbol{w}$ модуля M линейно зависимы, то, как и другие матрицы перехода[2], матрица $\Phi_{\boldsymbol{wu}}$ линейного отображения $\varphi : N \to M$ определяется отображением φ не однозначно, поскольку набор векторов $F(\boldsymbol{u})$ имеет различные линейные выражения через образующие $\boldsymbol{w}$, отличающиеся на линейные соотношения между этими образующими. Формулы (8-19) и (8-20) в этом случае означают, что если известно какое-либо выражение $v = \boldsymbol{ux}$ вектора v через образующие $\boldsymbol{u}$, то столбец коэффициентов $\boldsymbol{y} = \Phi_{\boldsymbol{wu}}\boldsymbol{x}$ даёт одно из возможных линейных выражений $\varphi(v) = \boldsymbol{wy}$ вектора $\varphi(v)$ через образующие $\boldsymbol{w}$, а произведение каких-либо матриц, которыми записываются отображения φ и ψ, является одной из матриц, которыми записывается композиция $\varphi\psi$.

Предостережение 8.2. (не все матрицы являются матрицами гомоморфизмов) Если образующие $\boldsymbol{u}$ линейно зависимы, то матрица $\Phi_{\boldsymbol{wu}}$ линейного отображения $\varphi : N \to M$ отнюдь не не

[1] Ср. с n° 8.1.1 на стр. 131.
[2] Ср. с n° 8.3 на стр. 139

произвольна: для каждого имеющегося в модуле N линейного соотношения $\boldsymbol{ux} = 0$ между векторами $\boldsymbol{u}$ в модуле M должно выполняться соотношение $0 = F(0) = F(\boldsymbol{ux}) = \boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x}$, т. е. задаваемое умножением на матрицу $\Phi_{\boldsymbol{wu}}$ отображение

$$\Phi_{\boldsymbol{wu}} : K^n \to K^m, \quad \boldsymbol{x} \mapsto \Phi_{\boldsymbol{wu}}\boldsymbol{x}$$

переводит коэффициенты любого линейного соотношения между образующими $\boldsymbol{u}$ в коэффициенты линейного соотношения между образующими $\boldsymbol{w}$. Наоборот, если матрица $A \in \mathrm{Mat}_{m\times n}(K)$ обладает этим свойством, то правило $\boldsymbol{ux} \mapsto \boldsymbol{w}\,A\boldsymbol{x}$ корректно задаёт K-линейное отображение $N \to M$, поскольку равенство $\boldsymbol{ux_1} = \boldsymbol{ux_2}$ означает, что $\boldsymbol{u}(\boldsymbol{x_1} - \boldsymbol{x_2}) = 0$, откуда $\boldsymbol{w}F_{\boldsymbol{wu}}(\boldsymbol{x_1} - \boldsymbol{x_2}) = 0$, и тем самым $\boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x_1} = \boldsymbol{w}F_{\boldsymbol{wu}}\boldsymbol{x_2}$. При этом две матрицы A и B задают одинаковые отображения $N \to M$ если и только если для любого $\boldsymbol{x} \in K^n$ столбцы $A\boldsymbol{x}, B\boldsymbol{x} \in K^m$ являются наборами коэффициентов одного и того же вектора из M, т. е. столбец $(A - B)\boldsymbol{x} \in K^m$ является линейным соотношением между образующими $\boldsymbol{w}$ модуля M. Обратите внимание, что мы получили новое доказательство предл. 6.6 на стр. 111, которое на языке матриц формулируется следующим образом:

Предложение 8.4
Пусть модули $N = K^n / R_N$ и $M = K^m / R_M$ заданы образующими и соотношениями, как в предл. 6.6 на стр. 111. Матрица $A \in \mathrm{Mat}_{m\times n}(K)$ тогда и только тогда является матрицей некоторого линейного отображения $F : N \to M$, когда для любого столбца $x \in R_N$ столбец $Ax \in R_M$. Две такие матрицы A и B задают одинаковые отображения $N \to M$ если и только если $(A-B)x \in R_M$ для всех $x \in K^n$. □

8.4.1. Матрицы гомоморфизмов свободных модулей. Если оба модуля N и M свободны и наборы векторов $\boldsymbol{u}$ и $\boldsymbol{w}$ являются их базисами, то, как мы видели в n° 8.1.1 на стр. 131, сопоставление K-линейному отображению $F : N \to M$ его матрицы $F_{\boldsymbol{wu}}$ в этих базисах задаёт K-линейный изоморфизм $\mathrm{Hom}_K(N, M) \xrightarrow{\sim} \mathrm{Mat}_{m\times n}(K)$, $F \mapsto F_{\boldsymbol{wu}}$.

Пример 8.9 (как меняется матрица отображения при замене базисов)
Пусть модули M и N свободны с базисами $\boldsymbol{w}$ и $\boldsymbol{u}$, и линейное отображение $F : M \to N$ имеет в этих базисах матрицу $F_{\boldsymbol{uw}}$. В других базисах $\boldsymbol{e} = \boldsymbol{w}\,C_{\boldsymbol{we}}$ и $\boldsymbol{f} = \boldsymbol{u}\,C_{\boldsymbol{uf}}$ матрица отображения F имеет вид

$$F_{\boldsymbol{fe}} = C_{\boldsymbol{fu}}F_{\boldsymbol{uw}}C_{\boldsymbol{we}} = C_{\boldsymbol{uf}}^{-1}F_{\boldsymbol{u}}C_{\boldsymbol{we}} = C_{\boldsymbol{fu}}F_{\boldsymbol{u}}C_{\boldsymbol{ew}}^{-1}, \tag{8-21}$$

поскольку $F(\boldsymbol{e}) = F(\boldsymbol{w}\,C_{\boldsymbol{we}}) = F(\boldsymbol{w})\,C_{\boldsymbol{we}} = \boldsymbol{u}\,F_{\boldsymbol{uw}}C_{\boldsymbol{uw}} = \boldsymbol{f}\,C_{\boldsymbol{fu}}F_{\boldsymbol{uw}}C_{\boldsymbol{uw}}$.

Упражнение 8.18. Убедитесь, что матрица $F_{\boldsymbol{wu}}$ линейного отображения $f : U \to W$ векторных пространств, написанная в базисах $\boldsymbol{u} \subset U$, $\boldsymbol{w} \subset W$, и матрица $F_{\boldsymbol{u^*w^*}}$ двойственного отображения[1] $f^* : W^* \to U^*$, написанная в двойственных базисах[2] $\boldsymbol{w}^* \subset W^*$, $\boldsymbol{u}^* \subset U^*$, получаются друг из друга транспонированием: $F_{\boldsymbol{u^*w^*}} = F_{\boldsymbol{wu}}^t$.

Пример 8.10 (матрицы эндоморфизмов)
Пусть модуль M свободен и набор векторов $\boldsymbol{u}$ составляет его базис. Матрица $F_{\boldsymbol{uu}}$ линейного эндоморфизма $F : M \to M$ в базисах $\boldsymbol{u}$ и $\boldsymbol{u}$ обозначается просто $F_{\boldsymbol{u}}$ и называется *матрицей эндоморфизма* F в базисе $\boldsymbol{u}$. По формуле (8-21) любом другом базисе $\boldsymbol{w} = \boldsymbol{u}\,C_{\boldsymbol{uw}}$ матрица оператора F

[1] См. n° 7.4.4 на стр. 127.
[2] См. n° 7.4.1 на стр. 122.

имеет вид

$$F_w = C_{wu}F_uC_{uw} = C_{uw}^{-1}F_uC_{uw} = C_{wu}F_uC_{wu}^{-1}. \tag{8-22}$$

8.5. Матрицы систем линейных уравнений. Система неоднородных линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{8-23}$$

на неизвестные $x_1, \ldots, x_n$, в которой все a_{ij} и b_i являются заданными элементами из некоторого коммутативного кольца K, в матричных обозначениях записывается одним равенством $Ax = b$, в котором $A = \left(a_{ij}\right) \in \mathrm{Mat}_{m\times n}$, а x и b обозначают матрицы-столбцы, состоящие из неизвестных и правых частей уравнений (8-23). Матрица A, называется *матрицей системы* (8-23). Обозначим через $F_A : K^n \to K^m$, $x \mapsto Ax$, линейное отображение, переводящее стандартные базисные векторы $e_1, \ldots, e_n \in K^n$ в столбцы матрицы A. Множество решений уравнения $Ax = b$ и системы (8-23) состоит из всех таких векторов $x \in K^n$, что $F_A(x) = b$, т. е. представляет собою полный прообраз $F_A^{-1}(b)$ вектора b при отображении F_A. Если $b \notin \operatorname{im} F_A$, то этот прообраз пуст и система (8-23) несовместна. Если $b = F_A(p) \in \operatorname{im} F_A$, то[1] $F_A^{-1}(b) = p + \ker F_A$. Мы заключаем, что множество решений системы (8-23) либо пусто, либо является сдвигом подмодуля $\ker F_A \subset K^n$ в какую-нибудь точку $p \in K^n$, являющуюся решением системы (8-23). На языке уравнений ядро $\ker F_A$ представляет собою множество решений системы однородных линейных уравнений $Ax = 0$ с теми же самыми левыми частями, что у системы (8-23). В развёрнутом виде она выглядит так:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0\,. \end{cases} \tag{8-24}$$

Наличие у такой системы ненулевого решения означает, что $\ker F_A \neq 0$, и в этом случае любая система (8-23) либо несовместна, либо имеет более одного решения. Это наблюдение известно как *альтернатива Фредгольма*: либо у однородной системы (8-24) есть ненулевое решение, либо у каждой системы (8-23) имеется не более одного решения.

8.5.1. Системы линейных уравнений над полем. Если система линейных уравнений (8-23) задана над полем $\Bbbk$, решения однородной системы (8-24) образуют в $\Bbbk^n$ векторное подпространство размерности

$$\dim \ker F_A = n - \dim \operatorname{im} F_A = n - \operatorname{rk} A\,,$$

где $\operatorname{rk} A$ — ранг матрицы[2] A. В частности, $\dim \ker F_A \geqslant n - m$, и если число уравнений m строго меньше числа неизвестных n, то система (8-24) обязательно имеет ненулевое решение.

Если рассматривать строки матрицы A как ковекторы из двойственного к $\Bbbk^n$ пространства $\Bbbk^{n*}$, то пространство решений однородной системы (8-24) является их аннулятором[3]. Из

[1] См. формулу (n° 6.2) на стр. 102.

[2] Т. е. размерность линейной оболочки столбцов, которая совпадает с $\operatorname{im} F_A$. Напомню, размерность линейной оболочки столбцов равна размерности линейной оболочки строк, см. прим. 7.11 на стр. 126.

[3] См. n° 7.4.3 на стр. 125.

сл. 7.10 на стр. 125 вытекает, что каждая линейная форма, которая зануляется на всех решениях системы (8-24), является линейной комбинацией левых частей этой системы, а сл. 7.9 на стр. 125 утверждает, что каждое векторное подпространство коразмерности m в $\Bbbk^n$ можно задать системой из m линейно независимых линейных уравнений.

Пример 8.11 (критерий совместности Кронекера – Капелли)
Матрица $\left[\begin{array}{c|c} A & b \end{array}\right] \in \mathrm{Mat}_{m\times(n+1)}(\Bbbk)$, которая получается приписыванием справа к матрице A левых частей системы (8-23) столбца b её правых частей, называется *расширенной матрицей* системы (8-23). Система (8-23) совместна если и только если вектор b лежит в линейной оболочке столбцов матрицы A, что в свою очередь равносильно равенству рангов $\operatorname{rk} A = \operatorname{rk}\left[\begin{array}{c|c} A & b \end{array}\right]$. Это наблюдение известно как *критерий Кронекера – Капелли*.

Пример 8.12 (системы с квадратной матрицей левых частей)
Если количество уравнений в системе (8-23) равно количеству неизвестных, линейное отображение $F_A : \Bbbk^n \to \Bbbk^n$ является эндоморфизмом n-мерного векторного пространства, и по сл. 7.6 на стр. 118 равенство $\ker F_A = 0$ равносильно сюръективности оператора F_A. Это позволяет уточнить альтернативу Фредгольма: при $m = n$ либо все неоднородные системы (8-23) имеют единственное решение, либо у однородной системы (8-24) есть ненулевое решение. В первом случае матрица A обратима по предл. 8.3, и знание обратной матрицы A^{-1} позволяет решить систему $Ax = b$ при любой правой части b по формуле $x = A^{-1}b$.

Задачи для самостоятельного решения к §8

Задача 8.1. Пусть матрица A имеет столбцы (слева направо) c_1, c_2, c_3 и строки (сверху вниз) r_1, r_2, r_3, r_4. На какую матрицу и с какой стороны надлежит умножить матрицу A, чтобы получилась матрица а) со строками (сверху вниз) $r_3 + 2r_4, 3r_1 + r_2, r_2 + r_3$ б) со столбцами (слева направо) $c_1 + 2c_2, 2c_2 + 3c_3, 3c_3 + 4c_1, 5c_1 + 6c_2, c_1 + c_2 + c_3$?

Задача 8.2. Центром алгебры A называется подалгебра $Z(A) = \{c \in A \mid \forall a \in A\ ca = ac\}$. Опишите центр алгебры матриц $\mathrm{Mat}_n(\Bbbk)$ над полем $\Bbbk$.

Задача 8.3. Укажите в $\mathrm{Mat}_3(\mathbb{Q})$ какую-нибудь матрицу X с $X^3 = \begin{pmatrix} 8 & 16 & 32 \\ 0 & 8 & 16 \\ 0 & 0 & 8 \end{pmatrix}$.

Задача 8.4. Найдите: а) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}^{2023}$ б) $\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1}$.

Задача 8.5. Пусть квадратная матрица A такова, что $A^m = 0$ для некоторого $m \in \mathbb{N}$. Обязательно ли матрица $E + A$ обратима?

Задача 8.6. На побочной диагонали матрицы $A \in \mathrm{Mat}_n(\mathbb{C})$ стоят числа $e^{2\pi i/a_k}$, где $a_1, \ldots, a_n \in \mathbb{N}$, а в остальных местах — нули. Найдите наименьшее такое m, что $A^m = E$.

Задача 8.7 (коммутаторы). Разность $[A, B] = AB - BA$ называется *коммутатором* квадратных матриц $A, B \in \mathrm{Mat}_n(K)$. Докажите, что для любых A, B, C имеют место следующие два *правила Лейбница*: а) $[A, BC] = [A, B]C + B[A, C]$ б) $[A, [B, C]] = [[A, B], C] + [B, [A, C]]$.

Задача 8.8. Выразите $(A + B)^n$ через $A^i B^j$, если: а) $[A, B] = 0$ б*) $[A, B] = B$ в*) $[A, B] = A$.

Задача 8.9 (след). Сумма $\operatorname{tr} A = \sum a_{ii}$ стоящих на главной диагонали элементов квадратной матрицы A называется *следом* этой матрицы. Покажите, что над любым коммутативным кольцом K а) $\operatorname{tr}[A,B] = 0$ для всех $A, B \in \mathrm{Mat}_n(K)$ б) $\operatorname{tr}(C^{-1}AC) = \operatorname{tr}(A)$ для всех $A \in \mathrm{Mat}_n(K)$ и обратимых $C \in \mathrm{Mat}_n(K)$

Задача 8.10. Пусть $\Bbbk$ — произвольное поле, и матрица $A \in \mathrm{Mat}_n(\Bbbk)$ такова, что $\operatorname{tr}(AX) = 0$ для всех матриц X с нулевым следом. Покажите, что $A = \lambda E$ для некоторого $\lambda \in \Bbbk$.

Задача 8.11 (нильпотентные матрицы). Матрица $A \in \mathrm{Mat}_n(K)$ называется *нильпотентной*, если $A^n = 0$ для некоторого $n \in \mathbb{N}$. Пусть матрицы A и B нильпотентны. Покажите, что

а) обе матрицы $E \pm A$ обратимы

б) матрицы вида $f(A)$, где f пробегает формальные степенные ряды без свободного члена, образуют абелеву группу с операцией $f(A) * g(A) \stackrel{\text{def}}{=} f(A) + g(A) - f(A)g(A)$

в) матрица $A + B$ может не быть нильпотентна

г) если $[A,B] = 0$, то матрица $A + B$ нильпотентна

д) если $[A,[A,B]] = [B,[B,A]] = 0$, то матрица $A + B$ нильпотентна.

Задача 8.12 (унипотентные матрицы). Матрица $A \in \mathrm{Mat}_n(\Bbbk)$, где $\Bbbk$ — поле, называется *унипотентной*, если $A = E + N$, где N нильпотентна. Покажите, что а) если $\operatorname{char}\Bbbk > 0$, то для любой унипотентной матрицы A найдётся такое $n \in \mathbb{N}$, что $A^n = E$ б) если $\operatorname{char}\Bbbk = 0$, то матрица A унипотентна, если и только если $A = e^B$ для некоторой нильпотентной матрицы B.

Задача 8.13 (обращение Мёбиуса в чуме). Пусть в чуме[1] P с отношением $x \leqslant y$ существует такой $m \in P$, что $m \leqslant x$ для всех $x \in P$, и для всех $x < y$ множество $\{z \in P \mid x \leqslant z \leqslant y\}$ конечно. Обозначим через $A = A(P)$ множество всех таких функций $\varrho : P \times P \to \mathbb{C}$, что $\varrho(x,y) = 0$, если отношение $x \leqslant y$ не выполнено. Покажите, что а) сумма и произведение

$$\varrho_1 + \varrho_2 : (x,y) \mapsto \varrho_1(x,y) + \varrho_2(x,y) \quad \text{и}^2 \quad \varrho_1\varrho_2 : (x,y) \mapsto \sum\nolimits_{x \leqslant z \leqslant y} \varrho_1(x,z)\varrho_2(z,y)$$

задают на A структуру ассоциативной $\mathbb{C}$-алгебры с единицей б) функция $\varrho \in A$ обратима если и только если $\varrho(x,x) \neq 0$ для всех $x \in P$ в) существует функция[3] $\mu \in A$, обратная к функции $\zeta \in A$, равной 1 для всех $x \leqslant y$, причём $\mu(x,x) = 1$ для всех $x \in P$ и $\mu(x,y) = -\sum_{x \leqslant z < y} \mu(x,z) = -\sum_{x < z \leqslant y} \mu(z,y)$ для всех $x < y$ г) если для функции $g : P \to \mathbb{C}$ известны значения всех сумм $\sigma_g(x) = \sum_{y \leqslant x} g(y)$, то g однозначно восстанавливается из них по *формуле обращения Мёбиуса*: $g(x) = \sum_{y \leqslant x} \sigma_g(y)\,\mu(y,x)$.

Задача 8.14. Убедитесь, что условия зад. 8.13 выполнены для а) множества $\mathbb{N}$ с отношением $n | m$ б) множества всех конечных подмножеств произвольного множества X с отношением $N \subseteq M$ и явно опишите для них функции Мёбиуса и формулы обращения[4].

Задача 8.15. Найдите ранг $\mathbb{Z}$-модуля симметрических многочленов степени n от m переменных с коэффициентами в $\mathbb{Z}$ для всех $2 \leqslant m, n \leqslant 5$.

Задача 8.16. Найдите все комплексные решения системы уравнений

$$x_1 + x_2 + x_3 = x_1^2 + x_2^2 + x_3^2 = 0\,,\ x_1^3 + x_2^3 + x_3^3 = 24\,.$$

Задача 8.17. Найдите сумму:

[1] Т. е. в частично упорядоченном множестве.

[2] Поучительно сравнить это умножение с умножением комплексных верхнетреугольных матриц.

[3] Она называется *функцией Мебиуса* чума P.

[4] Ответы в (б) поучительно сравнить с комбинаторными формулами включения-исключения.

а) 4-х степеней комплексных корней многочлена $x^3 - 3x - 1$
б) обратных кубов комплексных корней многочлена $x^4 - x - 2$.

Задача 8.18. Пользуясь тем, что каждая 2×2 матрица удовлетворяет приведённому квадратному уравнению, решите в $\mathrm{Mat}_2(\mathbb{Q})$ уравнения а) $X^2 = 0$ б) $X^3 = 0$ в) $X^2 = X$ г) $X^2 = E$ д) $X^2 = -E$.

Задача 8.19. При каких $t \in \mathbb{Q}$ векторы $(1, 2, 3)$, $(2, 5, 7)$ и $(3, 7, 10 + t)$ образуют базис в $\mathbb{Q}^3$?

Задача 8.20. Векторы v_1, v_2, v_3 линейно независимы над $\mathbb{Q}$. Перечислите все $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Q}^3$, для которых векторы $v_1 + \lambda_2 v_2$, $v_2 + \lambda_3 v_3$, $v_3 + \lambda_1 v_1$ линейно зависимы.

Задача 8.21. Рассмотрим разностный оператор $\nabla\colon f(x) \mapsto f(x) - f(x-1)$ на пространстве $\mathbb{Q}[x]_{\leqslant 3}$ многочленов степени $\leqslant 3$ с коэффициентами в $\mathbb{Q}$. Напишите его матрицу в стандартном базисе x^i, где $0 \leqslant i \leqslant 3$ и $x^0 \stackrel{\text{def}}{=} 1$, а также в базисе $\binom{x+k}{k} = (x+1)\cdots(x+k)/k!$, где $0 \leqslant k \leqslant 3$ и $\binom{x}{0} = 1$. Напишите матрицы переходов между этими базисами. Найдите $\ker \nabla$ и $\operatorname{im} \nabla$.

Задача 8.22. Рассмотрим оператор умножения на $x\colon f \mapsto xf$ в кольце вычетов $\mathbb{Q}[x]/\big((x-2)^4\big)$. Напишите его матрицу в базисе x^i, $0 \leqslant i \leqslant 3$, и в базисе $(x-2)^i$, $0 \leqslant i \leqslant 3$, а также матрицы переходов между этими базисами. Найдите $\ker x$ и $\operatorname{im} x$.

Задача 8.23. Для векторных пространств U, W размерностей $\dim U = n$, $\dim W = m$ и их подпространств $U_0 \subset U$ и $W_0 \subset W$ размерностей n_0 и m_0 покажите, что множество линейных отображений $\{f\colon U \to W \mid \ker f \subset U_0 \text{ и } \operatorname{im} f \subset W_0\}$ является векторным подпространством в $\mathrm{Hom}(U, W)$ и найдите его размерность.

Задача 8.24. Покажите, что следующие свойства матрицы над полем эквивалентны: а) все столбцы пропорциональны б) все строки пропорциональны в) матрица является произведением столбца и строки, и если квадратная матрица A имеет эти свойства, то она пропорциональна A^2.

Задача 8.25. Пусть элементы матрицы $A = \big(a_{ij}\big) \in \mathrm{Mat}_{m\times n}(\Bbbk)$ имеют вид $a_{ij} = x_i + y_j$ для некоторых $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \Bbbk$. Верно ли, что $\operatorname{rk} A \leqslant 2$?

Задача 8.26. Обозначим через $U_1, U_2 \subset \Bbbk^n$ и $W_1, W_2 \subset \Bbbk^m$ линейные оболочки строк и столбцов матриц $A_1, A_2 \in \mathrm{Mat}_{m\times n}(\Bbbk)$. Какие импликации имеются между условиями
а) $\operatorname{rk}(A_1 + A_2) = \operatorname{rk}(A_1) + \operatorname{rk}(A_2)$ б) $U_1 \cap U_2 = 0$ в) $W_1 \cap W_2 = 0$?

Задача 8.27 (неравенство Фробениуса). Для любых трёх линейных операторов $A, B, C\colon V \to V$ докажите соотношения
а) $\dim \operatorname{im} A = \dim \operatorname{im}(BA) + \dim(\operatorname{im} A \cap \ker B)$
б) $\dim \operatorname{im}(BA) + \dim \operatorname{im}(AC) \leqslant \dim \operatorname{im} A + \dim \operatorname{im}(BAC)$

Задача 8.28. Верно ли, что в $\mathrm{Mat}_n(\Bbbk)$ каждая матрица, перестановочная с заданной диагональной матрицей A, все диагональные элементы которой попарно различны, имеет вид $f(A)$ для некоторого многочлена $f(x) \in \Bbbk[x]$?

Задача 8.29. Пусть $n \times n$-матрицы A, B, C, D обратимы. Явно вычислите $\begin{pmatrix} A & B \\ C & D \end{pmatrix}^{-1}$ в предположении, что матрицы $A - BD^{-1}C$, $C - DB^{-1}A$, $B - AC^{-1}D$, $D - CA^{-1}B$ тоже обратимы.

Задача 8.30. На клетчатой бумаге нарисован по линиям сетки прямоугольник и во все внешние клетки, имеющие общую сторону с его контуром, записаны числа. Всегда ли возможно написать в каждую клетку прямоугольника по числу так, чтобы любое из них равнялось среднему арифметическому чисел из четырёх клеток, имеющих общую сторону с рассматриваемой? Если да, то сколько имеется способов это сделать?

Задача 8.31. Вершины куба надписаны числами $b_1, \dots, b_8$. При каких условиях на эти числа можно написать ещё шесть чисел на грани так, чтобы число в каждой из вершин оказалось равно сумме чисел на трёх сходящихся в этой вершине гранях? Найдите все наборы $b_1, \dots, b_8$, для которых задача имеет решение, и для каждого из них найдите все решения задачи.

§9. Метод Гаусса

Всюду в этом параграфе K означает произвольную область главных идеалов, а $\Bbbk$ — произвольное поле.

9.1. Метод Гаусса над областью главных идеалов. Будем называть *элементарным преобразованием строк* прямоугольной матрицы $A \in \mathrm{Mat}_{m\times n}(K)$ замену каких-нибудь двух строк r_i и r_j их линейными комбинациями

$$r_i' = \alpha r_i + \beta r_j \quad \text{и} \quad r_j' = \gamma r_i + \delta r_j\,, \quad \text{где} \quad \alpha,\beta,\gamma,\delta \in K$$

и определитель $\Delta = \alpha\delta - \beta\gamma$ обратимым в K. В этом случае матрица преобразования

$$\begin{pmatrix} r_i \\ r_j \end{pmatrix} \mapsto \begin{pmatrix} r_i' \\ r_j' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} r_i \\ r_j \end{pmatrix}$$

обратима[1], и исходные строки r_i и r_j восстанавливаются из преобразованных строк r_i' и r_j' по формулам $r_i' = (\delta r_i - \beta r_j)/\Delta$ и $r_j' = (-\gamma r_i + \alpha r_j)/\Delta$.

Упражнение 9.1. Убедитесь в этом.

Например, прибавление к одной строке другой строки, умноженной на любое число $x \in K$, а также перестановка двух строк местами и умножение строк на обратимые элементы $s_1, s_2 \in K$ являются элементарными преобразованиями, задаваемыми 2×2 матрицами

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} s_1 & 0 \\ 0 & s_2 \end{pmatrix}.$$

Элементарное преобразование не меняет линейной оболочки строк матрицы A и заключается в умножении A слева на обратимую $m\times m$ матрицу L, которая получается из единичной $m\times m$ матрицы тем же самым элементарным преобразованием строк, что происходит в матрице A.

Симметричным образом, *элементарным преобразованием столбцов* матрицы A мы называем замену каких-нибудь двух столбцов c_i и c_j их линейными комбинациями $c_i' = \alpha c_i + \beta c_j$ и $c_j' = \gamma c_i + \delta c_j$ с обратимым в K определителем $\alpha\delta - \beta\gamma$. Такое преобразование не меняет линейной оболочки столбцов матрицы A и достигается умножением A справа на обратимую $n\times n$ матрицу R, которая получается из единичной $n\times n$ матрицы тем же самым элементарным преобразованием столбцов, что производится в матрице A. Прибавление к одному из столбцов другого, умноженного на произвольное число $x \in K$, а также перестановка столбцов местами и умножение столбцов на обратимые элементы из K являются частными примерами элементарных преобразований.

Лемма 9.1
В области главных идеалов K любую пару ненулевых элементов (a, b), стоящих в одной строке (соотв. в одном столбце) матрицы $A \in \mathrm{Mat}_{m\times n}(K)$, можно подходящим элементарным преобразованием содержащих их столбцов (соотв. строк) заменить парой $(d, 0)$, где $d = \text{нод}(a, b)$.

Доказательство. Запишем $d = \text{нод}(a, b)$ как $d = ax + by$ и пусть $a = da'$, $b = db'$. Тогда $a'x + b'y = 1$ и $a'b - b'a = 0$. Поэтому

$$(a, b) \cdot \begin{pmatrix} x & -b' \\ y & a' \end{pmatrix} = (d, 0) \quad \text{и} \quad \begin{pmatrix} x & y \\ -b' & a' \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix},$$

[1] См. прим. 8.5 на стр. 134.

где $\det\begin{pmatrix} x & -b' \\ y & a' \end{pmatrix} = \det\begin{pmatrix} x & y \\ -b' & a' \end{pmatrix} = 1$. □

Теорема 9.1
В области главных идеалов K любая матрица $A \in \mathrm{Mat}_{m\times n}(K)$ конечным числом элементарных преобразований строк и столбцов преобразуется в матрицу $D_A = (d_{ij})$, у которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, где мы считаем, что $d \mid 0$ для всех $d \in K$, но $0 \nmid d$ при $d \neq 0$.

Доказательство. Если $A = 0$, то доказывать нечего. Если $A \neq 0$, то перестановками строк и столбцов добьёмся, чтобы $a_{11} \neq 0$. Если все элементы матрицы A делятся на a_{11}, то вычитая из всех строк подходящие кратные первой строки, а из всех столбцов — подходящие кратные первого столбца, добьёмся того, чтобы все элементы за исключением a_{11} в первом столбце и первой строке занулились. При этом все элементы матрицы останутся делящимися на a_{11}, и можно заменить A на матрицу размера $(m-1)\times(n-1)$, дополнительную к первой строке и первому столбцу матрицы A, после чего повторить процедуру.

Пусть в матрице A есть элемент a, не делящиеся на a_{11}, и $d = \text{нод}(a, a_{11})$. Ниже мы покажем, что в этом случае можно элементарными преобразованиями перейти к новой матрице A' с $a'_{11} = d$. Так как $(a_{11}) \subsetneq (d)$, главный идеал, порождённый левым верхним угловым элементом матрицы, при таком переходе строго увеличится. Поскольку в области главных идеалов не существует бесконечно возрастающих цепочек строго вложенных друг в друга идеалов, после конечного числа таких переходов мы получим матрицу, все элементы которой делятся на a_{11}, и к этой матрице будут применимы предыдущие рассуждения.

Если не делящийся на a_{11} элемент a стоит в первой строке или первом столбце, достаточно заменить пару (a_{11}, a) на $(d, 0)$ по лем. 9.1. Если все элементы первой строки и первого столбца делятся на a_{11}, а не делящийся на a_{11} элемент a стоит строго ниже и правее a_{11}, то мы, как и выше, сначала занулим все элементы первой строки и первого столбца за исключением самого a_{11}, вычитая из всех строк подходящие кратные первой строки, а из всех столбцов — подходящие кратные первого столбца. К элементу a при этом будут добавляться числа, кратные a_{11}, и $\text{нод}(a, a_{11})$ не изменится. Далее, прибавим ту строку, где стоит a, к первой строке и получим в первой строке копию элемента a. Наконец, заменим пару (a_{11}, a) на $(d, 0)$ по лем. 9.1. □

9.1.1. Инвариантные множители и нормальная форма Смита. Ниже, в n° 10.2.4 на стр. 177 мы покажем, что «диагональная» матрица D_A, в которой $d_{ij} = 0$ при $i \neq j$ и $d_{ii} \mid d_{jj}$ при $i < j$, с точностью до умножения её элементов на обратимые элементы из K не зависит от выбора последовательности элементарных преобразований, приводящих матрицу A к такому виду. По этой причине диагональные элементы d_{ii} матрицы D_A называются *инвариантными множителями* матрицы A, а сама диагональная матрица D_A — *нормальной формой Смита* матрицы A.

Так как каждое элементарное преобразование строк (соотв. столбцов) матрицы A является результатом умножения матрицы A слева (соотв. справа) на квадратную обратимую матрицу, которая получается из единичной матрицы E ровно тем же преобразованием, что совершается в матрице A, мы заключаем, что $D_A = LAR$, где $L = L_\ell \dots L_2 L_1$ и $R = R_1 R_2 \dots R_r$ — обратимые матрицы размеров $m\times m$ и $n\times n$, являющиеся произведениями обратимых матриц L_i и R_j, осуществляющих последовательные элементарные преобразования строк и столбцов матрицы A. Мы будем называть L и R *матрицами перехода* от матрицы A к её нормальной форме Смита. Так как $L = L_\ell \dots L_1 E$ и $R = E R_1 \dots R_r$, матрицы L и R получаются из единичных матриц размеров $m\times m$ и $n\times n$ теми же цепочками элементарных преобразований строк и соответственно столбцов, которые производились с матрицей A. Поэтому для явного отыскания матриц L

и R следует приписать к матрице $A \in \mathrm{Mat}_{m\times n}(K)$ справа и снизу единичные матрицы размеров $m \times m$ и $n \times n$ так, что получится Г-образная таблица вида

$$\begin{array}{|c|c|}\hline A & E \\ \hline E & \\ \hline \end{array},$$

и в процессе приведения матрицы A к диагональному виду осуществлять элементарные преобразования строк и столбцов сразу во всей Г-образной таблице. В результате на выходе получится Г-образная таблица

$$\begin{array}{|c|c|}\hline D_A & L \\ \hline R & \\ \hline \end{array}.$$

Пример 9.1
Вычислим нормальную форму Смита и матрицы перехода к ней для целочисленной матрицы

$$A = \begin{pmatrix} -9 & -18 & 15 & -24 & 24 \\ 15 & 30 & -27 & 42 & -36 \\ -6 & -12 & 6 & -12 & 24 \\ 31 & 62 & -51 & 81 & -87 \end{pmatrix} \in \mathrm{Mat}_{4x5}(\mathbb{Z}).$$

Составляем Г-образную матрицу

$$\begin{array}{|c|c|}\hline A & E \\ \hline E & \\ \hline \end{array} = \begin{array}{|rrrrr|cccc|}\hline -9 & -18 & 15 & -24 & 24 & 1 & 0 & 0 & 0 \\ 15 & 30 & -27 & 42 & -36 & 0 & 1 & 0 & 0 \\ -6 & -12 & 6 & -12 & 24 & 0 & 0 & 1 & 0 \\ 31 & 62 & -51 & 81 & -87 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ \hline \end{array}.$$

Прибавим к 4-й строке третью, умноженную на 5 и переставим полученную строку наверх:

$$\begin{array}{|rrrrr|cccc|}\hline 1 & 2 & -21 & 21 & 33 & 0 & 0 & 5 & 1 \\ -9 & -18 & 15 & -24 & 24 & 1 & 0 & 0 & 0 \\ 15 & 30 & -27 & 42 & -36 & 0 & 1 & 0 & 0 \\ -6 & -12 & 6 & -12 & 24 & 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ \hline \end{array}.$$

Теперь обнулим 1-ю строку и 1-й столбец левой матрицы вне левого верхнего угла, прибавив

ко всем строкам и столбцам надлежащие кратные 1-й строки и 1-го столбца:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & 0 & -174 & 165 & 321 & 1 & 0 & 45 & 9 \\ 0 & 0 & 288 & -273 & -531 & 0 & 1 & -75 & -15 \\ 0 & 0 & -120 & 114 & 222 & 0 & 0 & 31 & 6 \\ \hline 1 & -2 & 21 & -21 & -33 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 0 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \end{array}\right).$$

Делаем второй столбец пятым, а к 3-му столбцу прибавляем 4-й:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -9 & 165 & 321 & 0 & 1 & 0 & 45 & 9 \\ 0 & 15 & -273 & -531 & 0 & 0 & 1 & -75 & -15 \\ 0 & -6 & 114 & 222 & 0 & 0 & 0 & 31 & 6 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Вычитаем из 2-й строки 4-ю:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 51 & 99 & 0 & 1 & 0 & 14 & 3 \\ 0 & 15 & -273 & -531 & 0 & 0 & 1 & -75 & -15 \\ 0 & -6 & 114 & 222 & 0 & 0 & 0 & 31 & 6 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 0 & 0 & 0 & & & & \\ 0 & 1 & 1 & 0 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Все элементы 3×4 матрицы, стоящей в строках со 2-й по 4-ю и столбцах со 2-го по 5-й, делятся на 3. Поэтому мы обнуляем в этой матрице верхнюю строку и левый столбец, вычитая из 3-й и 4-й строк подходящие кратные 2-й строки, а потом из 3-го и 4-го столбцов — подходящие кратные 2-го:

$$\left(\begin{array}{ccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 0 & 0 & 0 & 1 & 0 & 14 & 3 \\ 0 & 0 & -18 & -36 & 0 & 5 & 1 & -5 & 0 \\ 0 & 0 & 12 & 24 & 0 & -2 & 0 & 3 & 0 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 17 & 33 & 0 & & & & \\ 0 & 1 & 18 & 33 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Теперь прибавляем к 3-й строке 4-ю:

$$\left(\begin{array}{rrrrr|rrrr} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 0 & 0 & 0 & 1 & 0 & 14 & 3 \\ 0 & 0 & -6 & -12 & 0 & 3 & 1 & -2 & 0 \\ 0 & 0 & 12 & 24 & 0 & -2 & 0 & 3 & 0 \\ \hline 1 & 0 & -21 & -33 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 17 & 33 & 0 & & & & \\ 0 & 1 & 18 & 33 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right)$$

и видим, что можно занулить все недиагональные элементы исходной матрицы, прибавляя к 4-й строке удвоенную 3-ю и вычитая из 4-го столбца удвоенный 3-й:

$$\left(\begin{array}{rrrrr|rrrr} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 1 \\ 0 & -3 & 0 & 0 & 0 & 1 & 0 & 14 & 3 \\ 0 & 0 & -6 & 0 & 0 & 3 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 2 & -1 & 0 \\ \hline 1 & 0 & -21 & 9 & -2 & & & & \\ 0 & 0 & 0 & 0 & 1 & & & & \\ 0 & 1 & 17 & -1 & 0 & & & & \\ 0 & 1 & 18 & -3 & 0 & & & & \\ 0 & 0 & 0 & 1 & 0 & & & & \end{array}\right).$$

Таким образом, инвариантные множители матрицы A суть $1, -3, -6, 0$ и

$$L = \begin{pmatrix} 0 & 0 & 5 & 1 \\ 1 & 0 & 14 & 3 \\ 3 & 1 & -2 & 0 \\ 4 & 2 & -1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 & -21 & 9 & -2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 17 & -1 & 0 \\ 0 & 1 & 18 & -3 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad D_A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & -6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Упражнение 9.2. Проверьте равенство $LAR = D_A$ прямым вычислением.

9.1.2. Отыскание обратной матрицы. Пусть квадратная матрица $A \in \mathrm{Mat}_n(K)$ обратима. Тогда и любая матрица вида $B = LAR$, где $L, R \in \mathrm{Mat}_n(K)$ обратимы, тоже обратима, ибо матрица $R^{-1}A^{-1}L^{-1}$ обратна к B. В частности, обратимы все матрицы, которые получаются из A элементарными преобразованиями строк и столбцов, включая нормальную форму Смита D_A.

Упражнение 9.3. Убедитесь, что диагональная матрица обратима если и только если обратимы все её диагональные элементы.

Таким образом, матрица A обратима если и только если обратимы все её инвариантные множители, и в этом случае существуют такие обратимые матрицы $L = L_\ell \dots L_1$ и $R = R_1 \dots R_r$,

что $LAR = E$, а каждая из матриц L_ν, R_μ имеет вид

$$\begin{pmatrix} \ddots & & & & & & & \\ & 1 & & & & & & \\ & & \alpha & & & & \beta & \\ & & & 1 & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & \gamma & & & & \delta & \\ & & & & & & & 1 \\ & & & & & & & & \ddots \end{pmatrix},$$

где на обозначенных многоточиями местах главной диагонали стоят единицы, в остальных местах — нули, а определитель $\alpha\beta - \beta\gamma \in K$ обратим. В этом случае $A = L^{-1}ER^{-1} = L^{-1}R^{-1}$, откуда $A^{-1} = RL = RLE$, а $E = RLA$, т. е. умножение слева на матрицу $RL = R_1 \dots R_r L_\ell \dots L_1$ задаёт цепочку элементарных преобразований строк, превращающую матрицу A в матрицу E, а матрицу E — в матрицу A^{-1}.

Упражнение 9.4. Покажите, что элементарными преобразованиями строк матрицы A можно превратить любой её ненулевой столбец в столбец, единственным ненулевым элементом которого является нод элементов исходного столбца матрицы A, и если этот элемент необратим, то и матрица A необратима.

Таким образом, чтобы выяснить, обратима ли $n \times n$ матрица A, и найти A^{-1}, если A обратима, следует элементарными преобразованиями строк и столбцов $n \times 2n$ матрицы $\left(\begin{array}{c|c} A & E \end{array}\right)$ попытаться получить в левой половине матрицу E, последовательно слева направо обнуляя в каждом столбце все элементы, кроме одного. Если в ходе вычислений матрица A превратится в заведомо необратимую матрицу, то и сама матрица A необратима. Ну а если удастся превратить матрицу A в матрицу E, то на выходе получится матрица $\left(\begin{array}{c|c} E & B \end{array}\right)$, в которой $B = A^{-1}$.

Пример 9.2

Выясним, обратима ли в $\mathrm{Mat}_4(\mathbb{Z})$ матрица

$$A = \begin{pmatrix} 1 & -3 & 2 & 2 \\ -3 & 9 & -6 & -5 \\ -1 & 4 & 0 & 2 \\ 3 & -7 & 11 & 12 \end{pmatrix}.$$

Приписываем к ней справа единичную матрицу:

$$\left(\begin{array}{rrrr|cccc} 1 & -3 & 2 & 2 & 1 & 0 & 0 & 0 \\ -3 & 9 & -6 & -5 & 0 & 1 & 0 & 0 \\ -1 & 4 & 0 & 2 & 0 & 0 & 1 & 0 \\ 3 & -7 & 11 & 12 & 0 & 0 & 0 & 1 \end{array}\right).$$

Обнуляем 1-й столбец вне левого верхнего угла, прибавляя ко всем строкам надлежащие кратные 1-й строки:

$$\left(\begin{array}{cccc|cccc} 1 & -3 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 4 & 1 & 0 & 1 & 0 \\ 0 & 2 & 5 & 6 & -3 & 0 & 0 & 1 \end{array}\right).$$

Теперь обнуляем верхний и нижний элементы 2-го столбца, прибавляя к верхней и нижней строкам надлежащие кратные 3-й строки, после чего переставляем 2-ю строку вниз:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 8 & 14 & 4 & 0 & 3 & 0 \\ 0 & 1 & 2 & 4 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & -2 & -5 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right).$$

Обнуляем верхние два элемента 3-го столбца, прибавляя к верхним двум строкам надлежащие кратные 3-й строки:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 30 & 44 & 0 & 19 & -8 \\ 0 & 1 & 0 & 8 & 11 & 0 & 5 & -2 \\ 0 & 0 & 1 & -2 & -5 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right).$$

Наконец, обнуляем 4-й столбец над нижней единицей, прибавляя к верхним трём строкам надлежащие кратные 4-й строки:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -46 & -30 & 19 & -8 \\ 0 & 1 & 0 & 0 & -13 & -8 & 5 & -2 \\ 0 & 0 & 1 & 0 & 1 & 2 & -2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right).$$

Таким образом, матрица A обратима и

$$A^{-1} = \begin{pmatrix} -46 & -30 & 19 & -8 \\ -13 & -8 & 5 & -2 \\ 1 & 2 & -2 & 1 \\ 3 & 1 & 0 & 0 \end{pmatrix}.$$

Упражнение 9.5. Проверьте прямым умножением двух матриц, что $AA^{-1} = E$.

9.1.3. Решение систем линейных уравнений. Как мы видели в n° 8.5 на стр. 144, система линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ a_{31}x_1 + a_{32}x_2 + \ldots + a_{3n}x_n = b_3 \\ \qquad \ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} \tag{9-1}$$

на неизвестные $x_1, \ldots, x_n$ равносильна одному матричному равенству $Ax = b$, в котором $A = \left(a_{ij}\right) \in \mathrm{Mat}_{m\times n}(K)$, а x и b обозначают столбцы высоты n и m, состоящие из неизвестных и правых частей уравнений (8-23). Как и выше, обозначим через $D_A = LAR$ нормальную форму Смита матрицы A. Умножая равенство $Ax = b$ слева на L и полагая $x = Ry$, где $y = R^{-1}x$ — новые переменные, получаем систему уравнений $D_A y = c$ на неизвестные y, в которой $c = Lb$ и матрица коэффициентов D_A диагональна, и которая равносильна (8-23) в том смысле, что между решениями обеих систем имеется K-линейная биекция $x = Ry$. В частности, система $D_A y = c$ совместна если и только если совместна исходная система (8-23).

Уравнения системы $D_A y = c$ имеют вид $d_{ii} y_i = c_i$. Такое уравнение не имеет решений, если и только если $d_{ii} \nmid c_i$. Если же $d_{ii} \mid c_i$, то при $d_{ii} = c_i = 0$ решениями уравнения являются все числа $y_i \in K$, а при $d_{ii} \neq 0$ уравнение имеет единственное решение $y_i = c_i / d_{ii}$.

Пусть $d_{ii} \neq 0$ при $i \leqslant r$ и $d_{jj} = 0$ при $j > r$. Мы заключаем, что система $D_A y = c$ несовместна если и только если $d_{ii} \nmid c_i$ хотя бы при одном $i \leqslant r$ или $c_j \neq 0$ хотя бы при одном $j > r$, и в этом случае исходная система (8-23) тоже несовместна. Если же система $D_A y = c$ совместна, то её решения имеют вид $y = w_0 + w$, где $w_0 = (c_1 / d_{11}, \ldots, c_r / d_{rr}, 0, \ldots, 0)^t$, а вектор $w \in K^n$ пробегает свободный подмодуль ранга $\min(m, n) - r$ с базисом из векторов

$$w_k = (0, \ldots, 0, 1, 0, \ldots, 0)^t, \text{ где 1 стоит на } (r+k)\text{-м месте,}$$

и в этом случае все решения исходной системы (8-23) имеют вид $x = u_0 + u$, где $u_0 = R w_0$, а $u \in K^n$ пробегает свободный подмодуль ранга $\min(m, n) - r$ с базисом из векторов $u_k = R w_k$.

Отметим, что столбец $c = Lb$ правых частей системы $D_A y = c$ получается из столбца b правых частей исходной системы (8-23) теми же преобразованиями строк, что производятся с матрицей A в процессе её приведения к виду D_A, а матрица R получается из единичной матрицы E теми же преобразованиями столбцов, что производятся с матрицей A в том же процессе. Поэтому для отыскания c и R можно составить Г-образную матрицу вида

$$\begin{array}{|c|c|}\hline A & b \\ \hline E & \\ \cline{1-1}\end{array},$$

привести A к нормальной форме Смита и получить на выходе

$$\begin{array}{|c|c|}\hline D_A & c \\ \hline R & \\ \cline{1-1}\end{array}.$$

Пример 9.3
Найдём все целые решения системы уравнений

$$\begin{cases} -65x_1 - 156x_2 + 169x_3 + 104x_4 = 117 \\ -143x_1 - 351x_2 + 364x_3 + 221x_4 = 195 \\ 52x_1 + 117x_2 - 143x_3 - 91x_4 = -156 \end{cases} \tag{9-2}$$

Для этого составим Г-образную таблицу из матрицы коэффициентов при неизвестных, к которой справа приписана матрица правых частей уравнений, а снизу — единичная матрица:

$$\begin{array}{|rrrr|r|}\hline -65 & -156 & 169 & 104 & 117 \\ -143 & -351 & 364 & 221 & 195 \\ 52 & 117 & -143 & -91 & -156 \\ \hline 1 & 0 & 0 & 0 & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 1 & \\ \cline{1-4}\end{array}.$$

Вычтем из 2-й строки 1-ю, умноженную на 2, и поменяем две верхние строки местами:

$$\left(\begin{array}{cccc|c} -13 & -39 & 26 & 13 & -39 \\ -65 & -156 & 169 & 104 & 117 \\ 52 & 117 & -143 & -91 & -156 \end{array}\right) \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Поскольку все элементы матрицы коэффициентов делятся на 13, зануляем в ней верхнюю строку и левый столбец, за исключением верхнего левого углового элемента, прибавляя ко 2-й и 3-й строкам надлежащие кратные 1-й строки, а ко 2-му, 3-му и 4-му столбцам — надлежащие кратные 1-го столбца:

$$\left(\begin{array}{cccc|c} -13 & 0 & 0 & 0 & -39 \\ 0 & 39 & 39 & 39 & 312 \\ 0 & -39 & -39 & -39 & -312 \end{array}\right) \left(\begin{array}{cccc} 1 & -3 & 2 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Прибавляем к 3-й строке 2-ю, после чего вычитаем 2-й столбец из 3-го и 4-го:

$$\left(\begin{array}{cccc|c} -13 & 0 & 0 & 0 & -39 \\ 0 & 39 & 0 & 0 & 312 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \left(\begin{array}{cccc} 1 & -3 & 5 & 4 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Мы заключаем, что система (9-2) равносильна системе

$$\begin{cases} -13y_1 = -39 \\ 39y_2 = 312 \end{cases} \tag{9-3}$$

на *четыре* неизвестные $y_1, \dots, y_4$, через которые исходные неизвестные $x_1, \dots, x_4$ выражаются по формуле:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 5 & 4 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}. \tag{9-4}$$

Все решения системы (9-3) описываются формулой:

$$(y_1, y_2, y_3, y_4) = (3, 8, z_1, z_2), \quad \text{где} \quad z_1, z_2 \in \mathbb{Z} \text{ — любые.}$$

Решения исходной системы получаются из них по формуле (9-4):

$$(x_1, x_2, x_3, x_4) = (5z_1 + 4z_2 - 21, 8 - z_1 - z_2, z_1, z_2), \quad \text{где} \quad z_1, z_2 \in \mathbb{Z} \text{ — любые.}$$

9.2. Метод Гаусса над полем. Пусть $\Bbbk$ — произвольное поле. Матрица $R \in \mathrm{Mat}_{m\times n}(\Bbbk)$ называется *приведённой ступенчатой*, если в каждой её строке самый левый ненулевой элемент равен единице, располагается строго правее, чем в предыдущей строке и является единственным ненулевым элементом своего столбца. Такова, например, матрица

$$\begin{pmatrix} 0 & 1 & * & 0 & * & * & 0 & * & 0 & * \\ 0 & 0 & 0 & 1 & * & * & 0 & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{9-5}$$

Упражнение 9.6. Убедитесь, что ненулевые строки любой приведённой ступенчатой матрицы линейно независимы и, тем самым, образуют базис своей линейной оболочки.

Столбцы, содержащие самые левые единицы каждой строки, принято называть *базисными*. Их номера $j_1, \ldots, j_r$ строго возрастают, и в пересечениях базисных столбцов с верхними r строками стоит единичная матрица размера $r \times r$. В матрице (9-5) базисными являются столбцы с номерами 2, 4, 7 и 9.

Упражнение 9.7. Убедитесь, что базисные столбцы линейно независимы и образуют базис в линейной оболочке столбцов приведённой ступенчатой матрицы.

Классический метод Гаусса преобразует произвольную матрицу в приведённую ступенчатую при помощи простейших элементарных преобразований строк следующих трёх типов:

1) к одной из строк прибавляется другая строка, умноженная на число
2) две строки меняются местами (9-6)
3) одна из строк умножается на ненулевое число.

Теорема 9.2 (о преобразовании к приведённому ступенчатому виду)
Каждая матрица $A \in \mathrm{Mat}_{m\times n}(\Bbbk)$ элементарными преобразованиями строк может быть превращена в приведённую ступенчатую матрицу A_{red}. Ненулевые строки матрицы A_{red} образуют базис в линейной оболочке строк матрицы A.

Доказательство. Удобно разбить процесс на последовательные шаги, соответствующие столбцам матрицы A. Будем предполагать, что после выполнения $(k-1)$-го шага та часть матрицы, что находится слева от k-ого столбца, имеет приведённый ступенчатый вид и s ненулевых строк. При $k = 1$ это требование означает, что $s = 0$, и не накладывает никаких ограничений на матрицу. При $k > 1$ ненулевые s строк слева от k-ого столбца суть верхние s строк и $0 \leqslant s \leqslant k-1$. Очередной k-тый шаг вычисления состоит в следующем. Если все элементы k-го столбца, расположенные строго ниже s-й строки, нулевые, то можно переходить к $(k+1)$-му шагу. Если же в k-том столбце имеется ненулевой элемент a, расположенный строго ниже s-той строки, то мы умножаем содержащую его строку на a^{-1}, а затем меняем её местами с $(s+1)$-ой строкой. При этом левые $(k-1)$ столбцов матрицы не изменятся, а $(s+1)$-я строка примет вид

$$\underbrace{0\,0\,\ldots\,0\,0}_{k-1}\;1\;\underbrace{*\;*\;\ldots\;*\;*}_{n-k}.$$

Теперь для каждого $i \neq s+1$ вычтем из i-й строки полученной матрицы $(s+1)$-ую строку, умноженную на элемент, стоящий в пересечении i-й строки и k-го столбца. Это не изменит левые $(k-1)$ столбцов матрицы и обнулит все элементы k-того столбца за исключением стоящей

$(s+1)$-ой строке единицы. В результате мы попадаем в исходное положение для $(k+1)$-го шага. Последнее утверждение предложения вытекает из упр. 9.6 и сделанного выше замечания, что элементарные преобразования строк не меняют линейной оболочки строк матрицы. □

9.2.1. Построение базиса в подпространстве. Рассмотрим n-мерное координатное векторное пространство $\Bbbk^n$, векторы которого будем записывать в виде строк $(x_1, \dots, x_n)$. Сопоставим каждому набору векторов $w_1, \dots, w_m \in \Bbbk^n$ матрицу размера $m \times n$, по строкам которой выписаны координаты этих векторов и которую мы будем называть *матрицей координат* векторов w_i. Поскольку элементарные преобразования строк не меняют их линейной оболочки, ненулевые строки приведённой ступенчатой матрицы, в которую матрица координат векторов w_i преобразуется методом Гаусса, составят по упр. 9.6 базис в линейной оболочке этих векторов.

Пример 9.4
Построим в координатном пространстве $\mathbb{Q}^5$ базис линейной оболочки строк матрицы

$$\begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix}. \tag{9-7}$$

Для этого умножим последнюю строку на -1 и поменяем местами с первой:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ 2 & -4 & -8 & 2 & -4 \end{pmatrix}.$$

Теперь обнулим первый столбец ниже первой строки, прибавляя надлежащие кратные первой строки ко второй, третьей и четвёртой строкам:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & -1 & -1 & 1 & -2 \\ 0 & -4 & -4 & 4 & -2 \end{pmatrix}.$$

Далее обнулим второй столбец ниже второй строки, добавив подходящие её кратные к нижним двум строкам:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & -1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}.$$

Наконец, делим третью строку на -2 и зануляем последний столбец вне третьей строки, добавляя к первой и четвёртой строкам подходящие кратные третьей:

$$\begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{9-8}$$

Верхние три строки этой приведённой ступенчатой матрицы составляют базис в линейной оболочке $U \subset \mathbb{Q}^5$ строк исходной матрицы (9-7). В частности, $\dim U = 3$.

9.2.2. Решение систем линейных уравнений. В n° 8.5 на стр. 144 мы сопоставили системе линейных уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{9-9}$$

её расширенную матрицу $C = \left[\begin{array}{c|c} A & b \end{array}\right]$ размера $m \times (n+1)$, которая получается приписыванием столбца $b = \left(b_i\right)$ правых частей системы (9-9) к $m \times n$ матрице $A = \left(a_{ij}\right)$, составленной из коэффициентов левых частей уравнений (9-9). Элементарным преобразованиям (9-6) строк матрицы C на языке уравнений отвечают следующие три типа преобразований системы (9-9):

1) почленное сложение одного из уравнений с другим, умноженным на константу
2) перестановка двух уравнений друг с другом (9-10)
3) умножение обеих частей некоторого уравнения на ненулевую константу.

Так как исходная система может быть получена из преобразованной системы аналогичным элементарным преобразованием, обратным к проделанному, исходная и преобразованная система имеют одно и то же пространство решений. Таким образом, метод Гаусса преобразует систему уравнений (9-9) с матрицей $C = \left[\begin{array}{c|c} A & b \end{array}\right]$ в эквивалентную ей систему уравнений с приведённой ступенчатой матрицей C_{red}. Пусть базисные столбцы[1] матрицы C_{red} имеют номера $j_1 < j_2 < \ldots < j_r$. Если $j_r = n+1$, то r-тое уравнение системы имеет вид $0 = 1$, и система несовместна. Если же $j_r \leqslant n$, то систему можно переписать в виде

$$\begin{aligned} x_{j_1} &= \beta_1 - \alpha_{1i_1}x_{i_1} - \alpha_{1i_2}x_{i_2} - \cdots - \alpha_{1i_{n-r}}x_{i_{n-r}} \\ x_{j_2} &= \beta_2 - \alpha_{2i_1}x_{i_1} - \alpha_{2i_2}x_{i_2} - \cdots - \alpha_{2i_{n-r}}x_{i_{n-r}} \\ &\cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ x_{j_r} &= \beta_r - \alpha_{ri_1}x_{i_1} - \alpha_{ri_2}x_{i_2} - \cdots - \alpha_{ri_{n-r}}x_{i_{n-r}}, \end{aligned} \tag{9-11}$$

где $\{i_1, \ldots, i_{n-r}\} = \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$. Переменные $x_{i_1}, \ldots, x_{i_{n-r}}$, находящиеся вне базисных столбцов приведённой ступенчатой матрицы, называются *свободными*, так как могут принимать любые значения. Стоящие в базисных столбцах переменные $x_{j_1}, \ldots, x_{j_r}$ называются *связанными*, поскольку для любого набора значений свободных переменных есть ровно один набор значений связанных переменных, дополняющий указанные значения свободных переменных до решения системы (9-9). Эти единственные значения задаются формулами (9-11), которые, таким образом, доставляют параметрическое описание всех решений системы (9-9).

Это описание согласуется с качественным описанием пространства решений из n° 8.5.1 на стр. 144. А именно, подставляя в правую часть (9-11) нулевые значения $x_{i_1} = \cdots = x_{i_r} = 0$, мы получаем точку $p \in \Bbbk^n$ с координатами $\beta_1, \ldots, \beta_r$ на местах с номерами $j_1, \ldots, j_r$ и нулевыми остальными координатами. Она удовлетворяет уравнениям (9-9), и каждое решение системы (9-9) имеет вид $p + v$, где вектор v пробегает векторное подпространство $\ker F_A \subset \Bbbk^n$

[1] Т. е. столбцы, в которых расположены самые левые ненулевые элементы строк матрицы C_{red}, см. стр. 158.

решений однородной системы $Ax = 0$, которая в развёрнутом виде выглядит как

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0\,, \end{cases} \tag{9-12}$$

и эквивалентна системе $A_{\text{red}}x = 0$, которую тоже можно переписать в виде

$$\begin{aligned} x_{j_1} &= -\alpha_{1i_1}x_{i_1} - \alpha_{1i_2}x_{i_2} - \cdots - \alpha_{1i_{n-r}}x_{i_{n-r}} \\ x_{j_2} &= -\alpha_{2i_1}x_{i_1} - \alpha_{2i_2}x_{i_2} - \cdots - \alpha_{2i_{n-r}}x_{i_{n-r}} \\ &\cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ x_{j_r} &= -\alpha_{ri_1}x_{i_1} - \alpha_{ri_2}x_{i_2} - \cdots - \alpha_{ri_{n-r}}x_{i_{n-r}}\,. \end{aligned} \tag{9-13}$$

Базис в векторном пространстве решений системы (9-13) составляют векторы $u_1, \ldots, u_{n-r}$, которые получаются следующим образом. Для каждого $k = 1, \ldots, (n-r)$ подставим в правую часть (9-13) значения $x_{i_k} = 1$ и $x_{i_\nu} = 0$ при $\nu \neq k$. Получим вектор с координатами $-\alpha_{1i_k}, \ldots, -\alpha_{ri_k}$ на местах с номерами $j_1, \ldots, j_r$, координатой 1 на i_k-м месте, и остальными $n-r-1$ координатами равными нулю. Это и есть k-й базисный вектор u_k.

Пример 9.5
Решим методом Гаусса следующую систему уравнений над полем $\mathbb{Q}$:

$$\begin{cases} x_1 + 2x_2 + 2x_3 + x_4 + 5x_5 + 3x_6 = 6 \\ -2x_1 - 4x_2 - 3x_3 - 9x_5 - 5x_6 = -10 \\ 3x_1 + 6x_2 + 4x_3 - x_4 + 13x_5 + 7x_6 = 14 \\ -x_1 - 2x_2 - 5x_3 - 7x_4 - 8x_5 - 6x_6 = -12 \\ -3x_1 - 6x_2 - 7x_3 - 5x_4 - 16x_5 - 9x_6 - 2x_7 = -17 \end{cases} \tag{9-14}$$

Расширенная матрица этой системы вид

$$\left(\begin{array}{ccccccc|c} 1 & 2 & 2 & 1 & 5 & 3 & 0 & 6 \\ -2 & -4 & -3 & 0 & -9 & -5 & 0 & -10 \\ 3 & 6 & 4 & -1 & 13 & 7 & 0 & 14 \\ -1 & -2 & -5 & -7 & -8 & -6 & 0 & -12 \\ -3 & -6 & -7 & -5 & -16 & -9 & -2 & -17 \end{array}\right).$$

Обнуляем первый столбец вне первой строки, прибавляя ко всем строкам надлежащие кратные первой:

$$\left(\begin{array}{ccccccc|c} 1 & 2 & 2 & 1 & 5 & 3 & 0 & 6 \\ 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 \\ 0 & 0 & -2 & -4 & -2 & -2 & 0 & -4 \\ 0 & 0 & -3 & -6 & -3 & -3 & 0 & -6 \\ 0 & 0 & -1 & -2 & -1 & 0 & -2 & 1 \end{array}\right).$$

Обнуляем третий столбец вне второй строки, прибавляя ко всем строкам надлежащие кратные второй:

$$\left(\begin{array}{ccccccc|c} 1 & 2 & 0 & -3 & 3 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 & 3 \end{array}\right).$$

Удаляем нулевые строки и обнуляем шестой столбец вне нижней строки, прибавляя ко второй и тртьей строкам надлежащие кратные нижней строки:

$$\left(\begin{array}{ccccccc|c} 1 & 2 & 0 & -3 & 3 & 0 & 2 & -1 \\ 0 & 0 & 1 & 2 & 1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 & 3 \end{array}\right).$$

Система уравнений, отвечающая этой приведённой ступенчатой матрице может быть записана в виде

$$\begin{cases} x_1 = -1 - 2x_2 + 3x_4 - 3x_5 - 2x_7 \\ x_3 = -1 - 2x_4 - x_5 - 2x_7 \\ x_6 = 3 + 2x_7\,. \end{cases} \tag{9-15}$$

Придавая свободным переменным x_2, x_4, x_5, x_7 произвольные значения и вычисляя соответствующие значения связанных переменных x_1, x_3, x_6 по формулам (9-15) получаем параметрическое описание всех решений исходной системы (9-14).

На геометрическом языке эти решения заметают в $\mathbb{Q}^7$ аффинное пространство $p + U$, где точка $p = (-1, 0, -1, 0, 0, 3, 0)$ получается подстановкой $x_2 = x_4 = x_5 = x_7 = 0$ в (9-15), а векторное подпространство $U \subset \mathbb{Q}^7$ имеет базис из векторов

$$u_1 = (-2, 1, 0, 0, 0, 0, 0)\,, \qquad u_2 = (3, 0, -2, 1, 0, 0, 0)\,,$$
$$u_3 = (-3, 0, -1, 0, 1, 0, 0)\,, \quad u_4 = (-2, 0, -2, 0, 0, 1, 2)\,,$$

координаты которых получаются подстановкой в однородные версии формул (9-15)

$$\begin{cases} x_1 = -2x_2 + 3x_4 - 3x_5 - 2x_7 \\ x_3 = -2x_4 - x_5 - 2x_7 \\ x_6 = 2x_7\,. \end{cases}$$

значений $(x_2, x_4, x_5, x_7) = (1, 0, 0, 0),\ (0, 1, 0, 0),\ (0, 0, 1, 0),\ (0, 0, 0, 1)$.

9.2.3. Построение базиса в ядре и образе линейного отображения. Пусть линейное отображение $F : U \to W$ имеет матрицу $A = F_{\boldsymbol{wu}} \in \mathrm{Mat}_{m\times n}(\Bbbk)$ в некоторых базисах $\boldsymbol{u} = (u_1, \ldots, u_n)$ и $\boldsymbol{w} = (w_1, \ldots, w_m)$ пространств U и W. Тогда образ вектора $v = \boldsymbol{u}x$ со столбцом координат $x = (x_1, \ldots, x_n)^t$ в базисе $\boldsymbol{u}$ равен $F(\boldsymbol{u}x) = F(\boldsymbol{u})x = \boldsymbol{w}F_{\boldsymbol{wu}}x$ и имеет в базисе $\boldsymbol{w}$ столбец координат $F_{\boldsymbol{wu}}x = Ax$. Тем самым ядро $\ker F$ состоит из всех таких векторов $\boldsymbol{u}x$, координатный столбец x которых в базисе $\boldsymbol{u}$ является решением системы однородных уравнений $Ax = 0$. Для описания этих решений матрицу A следует преобразовать к приведённому ступенчатому виду A_{red}, после чего базис в пространстве решений находится описанным выше способом.

Поскольку матрица $A_{\mathrm{red}} = SA$ получается умножением матрицы A слева на некоторую обратимую $m \times m$-матрицу S, матрица $A_{\mathrm{red}} = F_{\boldsymbol{eu}}$ является матрицей отображения F в прежнем

базисе $\boldsymbol{u}$ пространства U, но в другом базисе $\boldsymbol{e} = \boldsymbol{w}S^{-1}$ пространства W. В самом деле, матрица перехода[1] $C_{\boldsymbol{ew}} = C_{\boldsymbol{we}}^{-1} = S$ и по форм. (8-21) на стр. 143 $F_{\boldsymbol{eu}} = C_{\boldsymbol{ew}} F_{\boldsymbol{wu}} = SA = A_{\text{red}}$. Тем самым, образ оператора F состоит из векторов $\boldsymbol{e}y$, столбец координат y которых в новом базисе $\boldsymbol{e}$ пространства W лежит в линейной оболочке столбцов матрицы A_{red}. Как мы видели в упр. 9.7 на стр. 158, базисные столбцы матрицы A_{red} образуют базис в линейной оболочке её столбцов. Это означает, что образы $F(u_{j_1}), \dots, F(u_{j_r})$ тех базисных векторов пространства U, номера которых совпадают с номерами базисных столбцов приведённой ступенчатой матрицы A_{red}, составляют базис в $\operatorname{im} F$.

Пример 9.6 (вариация прим. 9.4 на стр. 159)
Пусть линейное отображение $F : \mathbb{Q}^5 \to \mathbb{Q}^4$ имеет в стандартных базисах матрицу

$$A = \begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix}$$

из прим. 9.4 на стр. 159. Методом Гаусса мы преобразуем её к приведённому ступенчатому виду

$$A_{\text{red}} = \begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

и заключаем, что базис в образе оператора F составляют векторы $F(e_1)$, $F(e_2)$, $F(e_5)$, координаты которых в стандартном базисе пространства $\mathbb{Q}^4$ суть первый, второй и пятый столбцы исходной матрицы A. Ядро оператора F составляют векторы, столбец координат x которых в стандартном базисе пространства $\mathbb{Q}^5$ решает систему $A_{\text{red}}x = 0$. Параметрическое представление решений задаётся формулами

$$\begin{cases} x_1 = 2x_3 + x_4 \\ x_2 = -x_3 + x_4 \\ x_5 = 0\,. \end{cases}$$

а базис в пространстве решений составляют векторы $(2, -1, 1, 0, 0)$, $(1, 1, 0, 1, 0)$, координаты которых получаются подстановкой в предыдущие формулы значений $(x_3, x_4) = (1, 0)\,,\ (0, 1)$.

9.2.4. Построение базиса в факторпространстве. Пусть r-мерное векторное подпространство $U \subset \Bbbk^n$ порождается строками матрицы A и пусть базисные столбцы приведённой ступенчатой матрицы A_{red}, полученной из A элементарными преобразованиями строк, имеют номера $j_1, \dots, j_r$. Покажем, что классы $[e_{i_1}], \dots, [e_{i_{n-r}}]$ стандартных базисных векторов пространства $\Bbbk^n$ с дополнительными к $j_1, \dots, j_r$ номерами $i_1, \dots, i_{n-r}$ образуют базис факторпространства $\Bbbk^n/U$. Для этого обозначим через E_I и E_J координатные подпространства, натянутые на дополнительные наборы базисных векторов $e_{i_1}, \dots, e_{i_{n-r}}$ и $e_{j_1}, \dots, e_{j_r}$. Проекция $\pi_J : \Bbbk^n \twoheadrightarrow E_J$ пространства $\Bbbk^n$ на подпространство E_J вдоль подпространства E_I переводит строки приведённой ступенчатой матрицы A_{red} в точности в базисные векторы $e_{j_1}, \dots, e_{j_r}$. Следовательно, ограничение этой проекции на подпространство $U \subset \Bbbk^n$ является изоморфизмом между U и E_J и, в частности, имеет нулевое ядро $U \cap \ker \pi_J = U \cap E_I = 0$. Но тогда и ограничение отображения факторизации $\pi_U : \Bbbk^n \twoheadrightarrow \Bbbk^n/U$ на подпространство $E_I \subset \Bbbk^n$ тоже имеет нулевое ядро, ибо последнее

[1] См. n° 8.3 на стр. 139.

также равно $E_I \cap \ker \pi_U = E_I \cap U$. Поскольку $\dim E_I = n - r = \dim \Bbbk^n / U$, отображение факторизации изоморфно отображает подпространство E_I на фактор $\Bbbk^n / U$. Поэтому образы $[e_i]$ базисных векторов e_i составят базис в $\Bbbk^n / U$.

Пример 9.7 (ещё одна вариация прим. 9.4 на стр. 159)
Пусть подпространство $U \subset \mathbb{Q}^5$ порождено строками матрицы

$$A = \begin{pmatrix} 2 & -4 & -8 & 2 & -4 \\ -1 & 1 & 3 & 0 & 1 \\ -1 & -1 & 1 & 2 & -1 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix}$$

из прим. 9.4 на стр. 159. Базисные столбцы приведённой ступенчатой матрицы

$$A_{\text{red}} = \begin{pmatrix} 1 & 0 & -2 & -1 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

имеют номера 1, 2, 5, а базис в факторе $\mathbb{Q}^5/U$ составляют классы $[e_3]_U$ и $[e_4]_U$ базисных векторов e_3, e_4 с дополнительными к 1, 2, 5 номерами.

9.3. Расположение подпространства относительно базиса. В этом разделе мы покажем, что в каждом подпространстве $U \subset \Bbbk^n$ существует единственный базис с приведённой ступенчатой матрицей координат[1]. Отсюда вытекает, в частности, что приведённая ступенчатая матрица A_{red}, полученная из матрицы A элементарными преобразованиями строк, не зависит от выбора цепочки преобразований и даже собственно от матрицы A, а зависит только от линейной оболочки строк матрицы A.

Предложение 9.1
Для каждого векторного подпространства $U \subset \Bbbk^n$ размерности r множество $\{1, \dots, n\}$ можно[2] так разбить в объединение двух непересекающихся дополнительных подмножеств

$$I = \{i_1, \dots, i_{n-r}\} \quad \text{и} \quad J = \{j_1, \dots, j_r\} = \{1, \dots, n\} \smallsetminus I,$$

чтобы линейные оболочки $E_I = \operatorname{span}(e_{i_1}, \dots, e_{i_{n-r}})$ и $E_J = \operatorname{span}(e_{j_1}, \dots, e_{j_r})$ стандартных базисных векторов $e_\nu \in \Bbbk^n$ удовлетворяли следующим эквивалентным условиям:

1) подпространства U и E_I имеют нулевое пересечение $U \cap E_I = 0$

2) ограничение на подпространство U проекции $p : V \twoheadrightarrow E_J$, $(x_1, \dots, x_n) \mapsto (x_{j_1}, \dots, x_{j_r})$, пространства V на подпространство E_J вдоль подпространства E_I является изоморфизмом между U и E_J

3) ограничение на подпространство E_I отображения факторизации $\pi : V \twoheadrightarrow V/U$, $v \mapsto [v]_U$, является изоморфизмом между E_I и V/U

4) в подпространстве U найдутся r таких векторов $u_1, \dots, u_r$, что $u_\nu - e_{j_\nu} \in E_I$ при всех $1 \leqslant \nu \leqslant r$.

[1] См. n° 9.2.1 на стр. 159.
[2] Как правило, многими способами.

При выполнении этих условий векторы $u_1, \dots, u_r$ из условия (4) автоматически образуют базис подпространства U и однозначно определяются подпространством U и выбором разложения $\{1, \dots, n\} = I \sqcup J$ обладающего свойствами (1) – (4).

Доказательство. Пусть векторы $v_1, \dots, v_r \in U$ образуют базис подпространства U. По лемме о замене[1] некоторые r векторов $e_{j_1}, \dots, e_{j_r}$ стандартного базиса в $\Bbbk^n$ можно заменить векторами v_j так, чтобы полученный в результате набор $v_1, \dots, v_r, e_{i_1}, \dots, e_{i_{n-r}}$ остался базисом в $\Bbbk^n$. В таком случае линейная оболочка $E_I = \operatorname{span}(e_{i_1}, \dots, e_{i_{n-r}})$ оставшихся базисных векторов обладает свойством (1) и, тем самым, существует. Покажем теперь, что условия (1) – (4) эквивалентны друг другу. В n° 9.2.4 выше мы видели, что ядро ограничения отображения p на подпространство U и ядро ограничения отображения π на подпространство E_I оба равны $U \cap E_I$. Из условия (1) вытекает, что $\ker p|_U = \ker \pi|_{E_I} = U \cap E_I = 0$. Поэтому оба ограничения $p|_U : U \to E_J$ и $\pi|_{E_I} : E_I \to V/U$ инъективны. Так как $\dim U = r = \dim E_J$ и $\dim E_I = n - r = \dim V/U$, оба ограничения — изоморфизмы. Таким образом, (1) влечёт (2) и (3). Наоборот, каждое из условий (2), (3) влечёт равенство $0 = \ker p|_U = \ker \pi|_{E_I} = U \cap E_I$, т. е. условие (1). Условие (4) утверждает, что r векторов $u_1, \dots, u_r$ из r-мерного подпространства U переводятся проекцией p в стандартные базисные векторы r-мерного координатного подпространства E_J, что равносильно условию (2). Наконец, если условия (1)-(4) выполняются, то ограничение $p|_U : U \to E_J$ является изоморфизмом, и в U есть единственный базис $u_1, \dots, u_r$, переводимый эти изоморфизмом в стандартный базис $e_{j_1}, \dots, e_{j_r}$ пространства E_J. □

Замечание 9.1. Векторное подпространство $U \subset \Bbbk^n$ размерности r может иметь нулевое пересечение сразу с несколькими и даже со всеми[2] $(n-r)$-мерными координатными подпространствами E_I. На координатном языке условие (4) в предл. 9.1 означает, что матрица координат векторов $u_1, \dots, u_r$ содержит в столбцах с номерами $j_1, \dots, j_r$ единичную подматрицу размера $r \times r$. Ниже мы увидим, что метод Гаусса строит в подпространстве U удовлетворяющий этому условию базис с лексикографически минимальным[3] возможным набором номеров $j_1, \dots, j_r$.

9.3.1. Комбинаторный тип подпространства. Лексикографически минимальный набор индексов $j_1, \dots, j_r$, для которого выполняются условия предл. 9.1, называется *комбинаторным типом* подпространства $U \subset \Bbbk^n$. Комбинаторный тип имеет следующее альтернативное описание. Для каждого $k = 0, 1, \dots, n$ обозначим через $V_{>k}$ линейную оболочку стандартных базисных векторов $e_{k+1}, \dots, e_n$. Получаем убывающую цепочку вложенных подпространств[4]:

$$V = V_{>0} \supset V_{>1} \supset \dots \supset V_{>(n-1)} \supset V_{>n} = 0\,.$$

Положим $W_{\leqslant k} = V/V_{>k}$ и обозначим через $\pi_k : \Bbbk^n \twoheadrightarrow W_{\leqslant k}$, $v \mapsto [v]$, отображение факторизации. Базис пространства $W_{\leqslant k}$ составляют классы $[e_1], \dots, [e_k]$ первых k стандартных базисных векторов по модулю последних $n-k$ базисных векторов, и проекция π_k переводит вектор

[1] См. лем. 7.1 на стр. 114.

[2] Над бесконечным полем $\Bbbk$ «случайное» r-мерное подпространство $U \subset V$ почти наверняка будет именно таким.

[3] Напомню, что *лексикографический порядок* на множестве r-буквенных слов $x_1 \dots x_r$, составленных из букв некоего упорядоченного алфавита X, представляет собою стандартное упорядочение всех этих слов по алфавиту, при котором слово w_1 меньше слова w_2 если первая слева различающаяся буква этих слов в слове w_1 меньше, чем в слове w_2.

[4] Такая цепочка называется *полным флагом*.

$(x_1, \dots, x_n) \in \Bbbk^n$ в вектор с координатами $(x_1, \dots, x_k)$ в базисе $[e_1], \dots, [e_k]$, т. е. попросту стирает последние $n - k$ координат. При $k = 0$ мы имеем нулевое отображение $\pi_0 : \Bbbk^n \to 0$, а при $k = n$ — тождественное отображение $\pi_n = \mathrm{Id}_{\Bbbk^n} : \Bbbk^n \xrightarrow{\sim} \Bbbk^n$. При $k \geqslant 1$ фактор $W_{\geqslant k} / \Bbbk [e_k]$ пространства $W_{\geqslant k}$ по одномерному подпространству, порождённому базисным классом $[e_k]$, равен $W_{\leqslant (k-1)}$, и проекция $\pi_{k-1} : \Bbbk^n \twoheadrightarrow W_{\leqslant (k-1)}$ является композицией проекции $\pi_k : \Bbbk^n \twoheadrightarrow W_{\leqslant k}$ с последующей проекцией $W_{\leqslant k} \twoheadrightarrow W_{\leqslant (k-1)}$, ядро которой одномерно. Поэтому для каждого r-мерного подпространства $U \subset \Bbbk^n$ размерности $d_k = \dim \pi_k(U)$ образуют нестрого возрастающую последовательность $d_0, d_1, \dots, d_n$ с $d_0 = 0$, $d_n = r$ и приращениями $d_k - d_{k-1} \leqslant 1$. Последнее вытекает из того, что подпространство $\pi_{k-1}(U)$ является образом подпространства $\pi_k(U)$ при линейном отображении $W_{\geqslant k} \twoheadrightarrow W_{\geqslant (k-1)}$ с одномерным ядром, пересечение которого с $\pi_k(U)$ либо нулевое, либо одномерное.

Предложение 9.2
Для данного подпространства $U \subset \Bbbk^n$ размерности r следующие три набора из r возрастающих натуральных чисел совпадают друг с другом:

1) набор $k_1, \dots, k_r$ тех значений $k \geqslant 1$, для которых $d_k > d_{k-1}$ в последовательности размерностей $d_k = \dim \pi_k(U)$.

2) набор номеров $j_1, \dots, j_r$ базисных столбцов приведённой ступенчатой матрицы, полученной методом Гаусса из матрицы координат[1] любого конечного набора векторов, порождающего подпространство U

3) лексикографически наименьший набор индексов $j_1^{\min}, \dots, j_r^{\min}$, для которого в пространстве U существует базис с матрицей координат, содержащей единичную $r \times r$ подматрицу[2] в столбцах с номерами $j_1^{\min}, \dots, j_r^{\min}$.

Доказательство. Ненулевые строки $u_1, \dots, u_r$ приведённой ступенчатой матрицы из (2) составляют в пространстве U базис, удовлетворяющий условиям предл. 9.1 для $J = \{j_1, \dots, j_r\}$. Так как проекции $\pi_k(u_\nu)$ векторов u_ν с $j_\nu \leqslant k$ линейно независимы в силу ступенчатости матрицы их координат, а векторы u_μ с $j_\mu > k$ лежат в $\ker \pi_k$, первые векторы составляют базис в $\pi_k(U)$, а последние — базис в $\ker \pi_k\big|_U = U \cap V_{>k}$. Поэтому $j_1, \dots, j_r$ суть в точности те номера k, для которых $d_k > d_{k-1}$. Это доказывает совпадение последовательностей (1) и (2). Докажем теперь совпадение последовательностей (2) и (3). Пусть матрица координат базисных векторов $w_1, \dots, w_r$ пространства U содержит единичную подматрицу в столбцах с номерами $j_1^{\min}, \dots, j_r^{\min}$. Так как проекции $\pi_k(w_\nu)$ векторов w_ν с $j_\nu^{\min} \leqslant k$ линейно независимы, количество таких векторов при каждом k не превышает размерности $\dim \pi_k(U)$, которая по уже доказанному равна количеству векторов u_ν с $j_\nu \leqslant k$. Иными словами, при каждом $k = 1, \dots, n$ количество чисел $j_\nu^{\min}$, не превышающих k, не больше количества чисел j_ν, не превышающих k. Тем самым, набор $j_1^{\min}, \dots, j_r^{\min}$ не может быть лексикографически меньше набора $j_1, \dots, j_r$. □

Следствие 9.1
В каждом подпространстве $U \subset \Bbbk^n$ существует единственный базис с приведённой ступенчатой матрицей координат M_U, и сопоставление подпространству U этой матрицы M_U устанавливает биекцию между приведёнными ступенчатыми матрицами, имеющими r ненулевых строк, и r-мерными подпространствами в $\Bbbk^n$. □

[1] Напомню, что в этом разделе мы записываем координаты векторов как строки.

[2] См. предл. 9.1 на стр. 164.

Упражнение 9.8. Убедитесь, что приведённые ступенчатые матрицы из r ненулевых строк с номерами базисных столбцов $j_1, \dots, j_r$ образуют в пространстве $\mathrm{Mat}_{r\times n}(\Bbbk)$ аффинное подпространство размерности $r(n-r) - \sum_{\nu=1}^{r}(j_\nu - \nu + 1)$ и докажите тождество

$$\frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)} = \sum_{\lambda\subseteq\Pi} q^{|\Pi\smallsetminus\lambda|},$$

где суммирование происходит по всем различным диаграммам Юнга[1] λ, умещающимся в прямоугольник Π размера $r\times(n-r)$, а показатель $|\Pi\smallsetminus\lambda|$ равен количеству клеток в дополнении диаграммы до прямоугольника (пустая диаграмма $\lambda=\varnothing$ и весь прямоугольник $\lambda=\Pi$ при этом тоже учитываются).

Следствие 9.2
Две системы однородных линейных уравнений $Ax=0$ и $Bx=0$ на переменный вектор-столбец $x\in\Bbbk^n$ имеют одно и то же пространство решений если и только если приведённые ступенчатые матрицы A_{red} и B_{red} этих систем совпадают друг с другом с точностью до добавления или удаления нулевых строк.

Доказательство. Обозначим через U и W линейные оболочки строк матриц A и B в пространстве $\Bbbk^{n*}$ ковекторов-строк ширины n. Согласно упр. 7.13 пространства решений систем уравнений $Ax=0$ и $Bx=0$ суть не что иное как лежащие в пространстве векторов-столбцов $\Bbbk^n$ высоты n аннуляторы $\operatorname{Ann}U$ и $\operatorname{Ann}W$ пространств U и W. По теор. 7.5 равенство $\operatorname{Ann}U=\operatorname{Ann}W$ пространств решений равносильно равенству $U=W$ линейных оболочек строк матриц A и B. По сл. 9.1 эти линейные оболочки совпадают если и только если совпадают их базисы с приведёнными ступенчатыми матрицами координат. □

Задачи для самостоятельного решения к §9

Задача 9.1. Найдите нормальную форму Смита D_A и такие обратимые над $\mathbb{Z}$ квадратные матрицы L_A и R_A, что $D_A = L_A A R_A$ для следующих целочисленных матриц A:

а) $\begin{pmatrix} 24 & -9 & 0 & -3\\ -33 & 9 & 6 & 6\\ -10 & 1 & 4 & 3\end{pmatrix}$ б) $\begin{pmatrix} -42 & 42 & 28 & -56\\ -98 & 56 & 28 & -42\\ 91 & -70 & -42 & 77\end{pmatrix}$ в) $\begin{pmatrix} -48 & 39 & -42 & 51\\ -15 & -6 & -6 & 27\\ -6 & 15 & -9 & 0\end{pmatrix}$

г) $\begin{pmatrix} -34 & -15 & 24 & 36\\ 12 & 12 & -19 & -23\\ -14 & -3 & 5 & 10\end{pmatrix}$ д) $\begin{pmatrix} 50 & -34 & 20 & 8\\ -30 & 35 & -15 & -13\\ -36 & 32 & -16 & -10\end{pmatrix}$ е) $\begin{pmatrix} -56 & 62 & -7 & -23\\ -28 & 14 & 5 & -3\\ 7 & 22 & -14 & -12\end{pmatrix}$.

Задача 9.2. Найдите все целые решения систем уравнений:

а) $\begin{cases} 35x_1 + 63x_2 - 77x_3 = -231\\ -35x_1 - 28x_2 + 42x_3 = 126\end{cases}$ б) $\begin{cases} -371x_1 + 105x_2 - 252x_3 = -357\\ 133x_1 - 35x_2 + 91x_3 = 126\end{cases}$

в) $\begin{cases} 56x_1 + 28x_2 + 7x_3 = 83\\ 196x_1 + 28x_2 - 63x_3 = 10\\ -133x_1 - 14x_2 + 49x_3 = 14\end{cases}$ г) $\begin{cases} -455x_1 - 189x_2 + 336x_3 = 133\\ 196x_1 + 84x_2 - 147x_3 = -56\\ 189x_1 + 63x_2 - 126x_3 = -63\end{cases}$

[1] См. 1-10 на стр. 10.

д) $\begin{cases} -196x_1 + 294x_2 + 427x_3 = -378 \\ 399x_1 - 588x_2 - 840x_3 = 651 \\ 56x_1 - 84x_2 - 119x_3 = 84 \end{cases}$ е) $\begin{cases} 26x_1 - 494x_2 - 169x_3 + 26x_4 = 390 \\ -312x_1 - 390x_2 - 78x_3 + 39x_4 = -117 \\ 234x_1 + 468x_2 + 117x_3 - 39x_4 = -39 \end{cases}$

Задача 9.3. Выясните, обратимы ли над $\mathbb{Z}$ матрицы, и если да, найдите обратные:

а) $\begin{pmatrix} 341 & -10 \\ 989 & -29 \end{pmatrix}$ б) $\begin{pmatrix} 240 & 81 \\ 196 & 66 \end{pmatrix}$ в) $\begin{pmatrix} 1073 & -236 \\ 341 & -75 \end{pmatrix}$ г) $\begin{pmatrix} -19 & 5 & -5 \\ 14 & 13 & 10 \\ 9 & 2 & 4 \end{pmatrix}$ д) $\begin{pmatrix} 31 & -17 & 3 \\ 5 & -2 & 0 \\ 21 & -10 & 1 \end{pmatrix}$

е) $\begin{pmatrix} 81 & 20 & -11 & 6 \\ 52 & 13 & -7 & 4 \\ 0 & -2 & -1 & 1 \\ 2 & 1 & 0 & 0 \end{pmatrix}$ ж) $\begin{pmatrix} -6 & -72 & -6 & 29 \\ 41 & 56 & 16 & -17 \\ -18 & -43 & -8 & 15 \\ -6 & -19 & -3 & 7 \end{pmatrix}$ з) $\begin{pmatrix} 4 & -43 & -17 \\ 1 & -10 & -4 \\ 1 & -8 & -3 \end{pmatrix}$ и) $\begin{pmatrix} -47 & 17 & -6 \\ -12 & 4 & -1 \\ 27 & -10 & 4 \end{pmatrix}$.

Задача 9.4 (теорема о ранге). Докажите, что столбцы и строки любой матрицы $A \in \mathrm{Mat}_{m\times n}(K)$ над областью главных идеалов K порождают в K^m и в K^n свободные подмодули одинакового ранга, равного числу ненулевых элементов нормальной формы Смита матрицы A.

Задача 9.5. Верно ли, что в свободном модуле ранга n над областью главных идеалов любой набор из $m > n$ векторов линейно зависим?

Задача 9.6. Докажите, что каждая обратимая матрица $A \in \mathrm{Mat}_n(\Bbbk)$, где $\Bbbk$ — поле, представляется в виде $A = U_1 P U_2$, где $U_1, U_2 \in \mathrm{Mat}_n(\Bbbk)$ — обратимые верхнетреугольные матрицы, а P — *матрица перестановки*[1].

Задача 9.7. Имеется 7 одинаковых банок, каждая из которых на $9/10$ заполнена краской одного из семи цветов радуги, в разных банках — разные цвета. Можно ли, переливая краску из банки в банку и равномерно размешивая содержимое после каждого переливания, получить хотя бы в одной из банок колер, где все семь цветов представлены в равной пропорции?

Задача 9.8. Найдите размерности и приведённые ступенчатые базисы $\mathbb{Q}$-линейных оболочек строк матриц

а) $\begin{pmatrix} 1 & 1 & 2 & -5 & 3 \\ 1 & 1 & 2 & -5 & 4 \\ -1 & -1 & -1 & 2 & -9 \\ -3 & -3 & -8 & 21 & -4 \end{pmatrix}$ б) $\begin{pmatrix} 1 & -2 & 3 & 6 & 3 \\ 3 & -5 & 7 & 16 & 7 \\ 1 & 1 & -3 & 0 & -3 \\ 3 & -3 & 3 & 12 & 3 \end{pmatrix}$

в) $\begin{pmatrix} 1 & -3 & 1 & 2 & 2 \\ 3 & -9 & 4 & 3 & 7 \\ 1 & -3 & -1 & 8 & 1 \\ -1 & 3 & -2 & 2 & -3 \end{pmatrix}$ г) $\begin{pmatrix} 1 & 2 & -6 & -2 & -1 \\ 3 & 7 & -20 & -3 & -6 \\ 1 & -1 & 0 & -11 & 9 \\ -2 & -1 & 6 & 14 & -6 \end{pmatrix}$

Задача 9.9. Укажите базис над $\mathbb{Q}$ в пространстве решений системы уравнений

а) $\begin{cases} x_1 - 3x_2 - x_3 + 3x_4 - 4x_5 + 8x_6 = 0 \\ 3x_1 - 9x_2 - 3x_3 + 10x_4 - 15x_5 + 27x_6 = 0 \\ 3x_1 - 9x_2 - 2x_3 + 15x_4 - 33x_5 + 40x_6 = 0 \\ 3x_1 - 9x_2 - 4x_3 + 3x_4 + 9x_5 + 8x_6 = 0 \end{cases}$

[1] Т. е. матрица линейного автоморфизма $\Bbbk^n \xrightarrow{\sim} \Bbbk^n$, задающего перестановку базисных векторов, или — что то же самое — матрица, содержащая в каждой строке и каждом столбце ровно один ненулевой элемент, равный 1.

б) $\begin{cases} x_1 - 3x_2 + 3x_3 - 3x_4 + 9x_5 + 12x_6 = 0 \\ -3x_1 + 9x_2 - 9x_3 + 10x_4 - 29x_5 - 39x_6 = 0 \\ -3x_1 + 9x_2 - 9x_3 + 11x_4 - 31x_5 - 42x_6 = 0 \\ 3x_1 - 9x_2 + 9x_3 - 7x_4 + 23x_5 + 30x_6 = 0 \end{cases}$

в) $\begin{cases} x_1 + 2x_2 - 3x_3 + x_4 + x_5 + 9x_6 = 0 \\ x_1 + 3x_2 - 4x_3 - x_4 - x_5 + 2x_6 = 0 \\ x_1 + 5x_2 - 6x_3 - 5x_4 - 4x_5 - 10x_6 = 0 \\ -x_1 - 5x_2 + 6x_3 + 6x_4 + 11x_5 + 27x_6 = 0 \end{cases}$

г) $\begin{cases} x_1 - x_2 + 2x_3 + 2x_4 + 2x_5 + x_6 = 0 \\ 3x_1 - 3x_2 + 6x_3 + 7x_4 + 5x_5 + 3x_6 = 0 \\ 3x_1 - 3x_2 + 6x_3 + 3x_4 + 10x_5 + x_6 = 0 \\ 2x_1 - 2x_2 + 5x_3 + 4x_4 + 11x_5 - 9x_6 = 0 \end{cases}$

Задача 9.10. Напишите систему из минимально возможного числа линейных уравнений, пространство решений которой совпадает с линейной оболочкой векторов

а) $(1, 2, -1, -3)$, $(-3, -6, 3, 10)$, $(2, 4, -2, -7)$, $(1, 2, -1, -1)$, $(2, 5, -1, -9)$ в $\mathbb{Q}^4$

б) $(1, -1, -3, 0, 3)$, $(-2, 2, 6, 0, -6)$, $(2, -1, -4, -2, 4)$, $(-3, 4, 11, -2, -10)$ в $\mathbb{Q}^5$

в) $(1, -1, -2, -7, 0, -3)$, $(-2, 2, 5, 17, -1, 5)$, $(-1, 1, 1, 4, 1, 4)$, $(-2, 2, 6, 20, -2, 5)$ в $\mathbb{Q}^6$.

Задача 9.11. Решите в поле $\mathbb{Q}$ систему уравнений

а) $\begin{cases} x_1 - 3x_2 - 11x_3 + 3x_5 = 5 \\ x_1 - 2x_2 - 8x_3 - x_4 = -6 \\ -x_1 + 3x_2 + 11x_3 - x_5 = -7 \\ 2x_1 - 5x_2 - 19x_3 - x_4 + 2x_5 = 11 \end{cases}$ б) $\begin{cases} x_1 + 2x_2 + 2x_3 - 6x_4 - 6x_5 = -3 \\ -3x_1 - 5x_2 - 3x_3 + 18x_4 + 12x_5 = 8 \\ -2x_1 - 5x_2 - 6x_3 + 13x_4 + 17x_5 = 5 \\ x_1 - x_2 - 10x_3 - 9x_4 + 15x_5 = 7 \end{cases}$

в) $\begin{cases} x_1 + 2x_2 + 2x_3 - 2x_4 + 10x_5 = -5 \\ -2x_1 - 4x_2 - 3x_3 + 5x_4 - 20x_5 = -4 \\ -x_1 - 2x_2 - 2x_3 + 4x_4 - 14x_5 = 7 \\ -3x_1 - 6x_2 - 5x_3 + 6x_4 - 28x_5 = 13 \\ -x_1 - 2x_2 + x_3 - 4x_4 + 8x_5 = -7 \end{cases}$ г) $\begin{cases} x_1 - 2x_2 + x_3 - x_4 + x_5 = 7 \\ x_1 - 2x_2 + 2x_3 - 3x_4 - x_5 = 5 \\ 2x_1 - 4x_2 - x_3 + 4x_4 + 9x_5 = 23 \\ 2x_1 - 3x_2 - 2x_3 + x_4 + 5x_5 = 19 \\ 2x_1 - 2x_2 - 5x_3 + 3x_4 + 10x_5 = 31 \end{cases}$

Задача 9.12. Линейный оператор $F\colon \mathbb{Q}^4 \to \mathbb{Q}^4$ имеет в стандартном базисе матрицу

а) $\begin{pmatrix} 1 & 2 & 3 & -2 \\ 2 & 5 & 9 & -3 \\ -1 & -3 & -6 & 1 \\ -2 & -6 & -12 & 3 \end{pmatrix}$ б) $\begin{pmatrix} 1 & 2 & -1 & -3 \\ -1 & -1 & 4 & 5 \\ -1 & -5 & -8 & -2 \\ 1 & 5 & 9 & 5 \end{pmatrix}$.

Выясните, биективен ли он, и если да — напишите матрицу обратного оператора F^{-1}, а если нет — укажите какие-нибудь базисы в образе и в ядре оператора F.

Задача 9.13. Вычислите размерности факторов пространства $\mathbb{Q}^4$ по подпространствам, линейно порождённым а) строками б) столбцами каждой из двух матриц предыдущей задачи, и укажите какие-нибудь базисы этих факторпространств.

Задача 9.14. Рассмотрим 12-мерное координатное пространство $\mathbb{F}_q^{12}$ над q-элементным полем $\mathbb{F}_q$ и обозначим через $E_{\geqslant k} \subset \mathbb{F}_q^{12}$ линейную оболочку стандартных базисных векторов $e_k, \ldots, e_{12}$. Подсчитайте количество таких трёхмерных подпространств $U \subset \mathbb{F}_q^{12}$, что $\dim U \cap E_{\geqslant 2} = 2$, $\dim U \cap E_{\geqslant 9} = 1$, а $U \cap E_{\geqslant 10} = 0$.

§10. Конечно порождённые модули над областью главных идеалов

Всюду в этом параграфе K означает произвольную область главных идеалов. Все рассматриваемые нами K-модули по умолчанию предполагаются конечно порождёнными.

10.1. Взаимные базисы и инвариантные множители. Как мы видели в n° 6.7.2 на стр. 110, произвольный K-модуль M, линейно порождённый над K конечным набором векторов

$$\boldsymbol{w} = (w_1, \ldots, w_m),$$

представляет собою фактор $M \simeq K^m / R_{\boldsymbol{w}}$ свободного координатного модуля K^m по подмодулю $R_{\boldsymbol{w}} \subset K^m$ линейных соотношений между порождающими векторами $\boldsymbol{w}$. Подмодуль $R_{\boldsymbol{w}}$ состоит из всех таких строк $(x_1, \ldots, x_m) \in K^m$, что $x_1 w_1 + \ldots + x_m w_m = 0$ в M, и является ядром эпиморфизма

$$\pi_{\boldsymbol{w}} : K^m \twoheadrightarrow M, \quad (x_1, \ldots, x_m) \mapsto x_1 w_1 + \ldots + x_m w_m . \tag{10-1}$$

Теорема 10.1
Каждый подмодуль N в свободном модуле F конечного ранга над областью главных идеалов K тоже свободен, и $\operatorname{rk} N \leqslant \operatorname{rk} F$.

Доказательство. Индукция по $m = \operatorname{rk} F$. Пусть $m = 1$. Тогда $F \simeq K$ и каждый ненулевой подмодуль $N \subset K$ представляет собою главный идеал $(d) \subset K$, который является свободным K-модулем ранга 1 с базисом d. Пусть теперь $m > 1$. Зафиксируем в F базис $e_1, \ldots, e_m$ и будем записывать векторы из N строками их координат в этом базисе. Первые координаты всевозможных векторов $v \in N$ образуют идеал $(d) \subset K$. Если $d = 0$, подмодуль N содержится в свободном модуле ранга $m-1$ с базисом $e_2, \ldots, e_m$. По индукции, такой модуль N свободен и $\operatorname{rk} N \leqslant (m-1)$. Если $d \neq 0$, обозначим через $u \in N$ какой-нибудь вектор с первой координатой d. Порождённый вектором u модуль Ku свободен ранга 1, поскольку равенство $xu = 0$ влечёт равенство $xd = 0$, возможное в целостном кольце K только при $x = 0$. Покажем, что $N = Ku \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Очевидно, что $Ku \cap N' = 0$. Если первая координата вектора $v \in N$ равна xd, то $v = xu + w$, где $w = v - xu \in N'$. Поэтому $N = Ku + N'$, и по предл. 6.2 на стр. 106 $N = Ku \oplus N'$ по предл. 6.2 на стр. 106. Модуль N' содержится в свободном модуле ранга $m-1$ с базисом $e_2, \ldots, e_m$. По индукции он свободен и $\operatorname{rk} N' \leqslant (m-1)$. Поэтому $N = Ku \oplus N'$ тоже свободен и $\operatorname{rk} N = 1 + \operatorname{rk} N' \leqslant m$. □

Пример 10.1 (качественный анализ систем линейных уравнений, уточнение n° 8.5)
Если система линейных уравнений $Ax = b$, где $A \in \operatorname{Mat}_{m\times n}(K)$, $b \in K^m$, над областью главных идеалов K совместна, т. е. существует такой вектор $w \in K^n$, что $Aw = b$, то множество её решений[1] $F_A^{-1}(b) = w + \ker F_A$ представляет собою сдвиг свободного модуля $\ker F_A \subset K^n$ на вектор w. Ядро $\ker F_A$ является множеством решений системы однородных линейных уравнений $Ax = 0$. Наличие у такой системы ненулевого решения означает, что $\ker F_A \neq 0$. В этом случае либо система $Ax = b$ несовместна, либо множество её решений является сдвигом свободного модуля положительного ранга, что согласуется с явными формулами из n° 9.1.3 на стр. 155.

[1] Напомню, что $F_A : K^m \to K^n$, $x \mapsto Ax$, — это линейное отображение, задаваемое матрицей A, см. n° 8.5 на стр. 144

Теорема 10.2 (теорема о взаимном базисе)
Пусть F — свободный модуль ранга m над областью главных идеалов K, и $N \subset F$ — произвольный его подмодуль. Тогда в модуле F существует такой базис $\boldsymbol{e} = (e_1, \dots, e_m)$, что подходящие кратности $\lambda_1 e_1, \dots, \lambda_n e_n$ первых $n = \operatorname{rk} N$ его базисных векторов составляют базис в N и $\lambda_i \mid \lambda_j$ при $i < j$.

Доказательство. Зафиксируем произвольные базисы $\boldsymbol{w} = (w_1, \dots, w_m)$ в F и $\boldsymbol{u} = \boldsymbol{w}\, C_{\boldsymbol{wu}}$ в N. Последний существует по теор. 10.1 и состоит из $n \leqslant m$ векторов. Обозначим через $D = LC_{\boldsymbol{wu}}R$ нормальную форму Смита матрицы перехода $C_{\boldsymbol{wu}}$. Поскольку матрицы L и R обратимы, набор векторов $\boldsymbol{e} = \boldsymbol{w}\, L^{-1}$ является базисом в F, а набор векторов $\boldsymbol{v} = \boldsymbol{u}\, R$ — базисом в N. Так как

$$\boldsymbol{v} = \boldsymbol{u}\, R = \boldsymbol{w}\, C_{\boldsymbol{wu}} R = \boldsymbol{e}\, L C_{\boldsymbol{wu}} R = \boldsymbol{e}\, D$$

векторы $v_i = d_{ii} e_i$ базиса $\boldsymbol{v}$ имеют предписанный теоремой вид, в котором $\lambda_i = d_{ii}$ суть инвариантные множители матрицы $C_{\boldsymbol{wu}}$. □

Определение 10.1
Множители $\lambda_1, \dots, \lambda_n$ из теор. 10.2 называются *инвариантными множителями* подмодуля N в свободном модуле F, а построенные в теор. 10.2 базисы $e_1, \dots, e_m$ в F и $\lambda_1 e_1, \dots, \lambda_n e_n$ в N называются *взаимными базисами* свободного модуля F и его подмодуля N. В n° 10.2.4 на стр. 177 ниже мы покажем, что множители λ_i не зависят от выбора взаимных базисов, что оправдывает эпитет «инвариантные» в их названии.

Пример 10.2
Построим взаимные базисы целочисленной решётки $\mathbb{Z}^3$ и её подрешётки $L \subset \mathbb{Z}^3$, порождённой столбцами матрицы

$$A = \begin{pmatrix} 126 & 51 & 72 & 33 \\ 30 & 15 & 18 & 9 \\ 60 & 30 & 36 & 18 \end{pmatrix}. \tag{10-2}$$

Обозначим через $\boldsymbol{e} = (e_1, e_2, e_3)$ стандартный базис в $\mathbb{Z}^3$. По условию, столбцы матрицы A, т. е. векторы $\boldsymbol{a} = (a_1, a_2, a_3, a_4) = \boldsymbol{e}\, A$ порождают решётку L. Пусть $D_A = LAR$ — нормальная форма Смита матрицы A. Тогда векторы $\boldsymbol{w} = \boldsymbol{a}\, R = \boldsymbol{e}\, AR$ тоже порождают L, поскольку образующие $\boldsymbol{a} = \boldsymbol{w}\, R^{-1}$ линейно через них выражаются. По предл. 8.3 на стр. 139 векторы $\boldsymbol{u} = \boldsymbol{e}\, L^{-1}$ составляют базис в $\mathbb{Z}^3$, так как матрица перехода от них к стандартному базису обратима. При этом $\boldsymbol{e} = \boldsymbol{u}\, L$. В силу равенств $\boldsymbol{w} = \boldsymbol{e}\, AR = \boldsymbol{u}\, LAR = \boldsymbol{u}\, D_A$, образующие $w_i = d_{ii} u_i$ пропорциональны базисным векторам u_i. Поэтому взаимные базисы в $\mathbb{Z}^3$ и L состоят из векторов $\boldsymbol{u}$, т. е. столбцов матрицы L^{-1}, и векторов $w_i = d_{ii} u_i$ с ненулевыми d_{ii}. Для их отыскания приведём матрицу A к нормальной форме Смита. Так как матрица R нас сейчас не интересует, в вычислении из прим. 9.1 на стр. 151 можно ограничиться только верхней частью Г-образной таблицы:

$$\left[\begin{array}{c|c} A & E \end{array}\right] = \left[\begin{array}{cccc|ccc} 126 & 51 & 72 & 33 & 1 & 0 & 0 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \end{array}\right].$$

Отнимаем из первой строки удвоенную третью:

$$\left[\begin{array}{cccc|ccc} 6 & -9 & 0 & -3 & 1 & 0 & -2 \\ 30 & 15 & 18 & 9 & 0 & 1 & 0 \\ 60 & 30 & 36 & 18 & 0 & 0 & 1 \end{array}\right]$$

и делаем четвёртый столбец первым:

$$\left(\begin{array}{cccc|ccc} -3 & 6 & -9 & 0 & 1 & 0 & -2 \\ 9 & 30 & 15 & 18 & 0 & 1 & 0 \\ 18 & 60 & 30 & 36 & 0 & 0 & 1 \end{array}\right).$$

Так как все элементы левой матрицы делятся на 3, зануляем в ней 1-ю строку и 1-й столбец вне левого верхнего угла:

$$\left(\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 48 & -12 & 18 & 3 & 1 & -6 \\ 0 & 96 & -24 & 36 & 6 & 0 & -11 \end{array}\right).$$

Теперь зануляем 3-ю строку, отнимая из неё удвоенную 2-ю:

$$\left(\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 48 & -12 & 18 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

Прибавляем к 3-му столбцу 4-й и переставляем результат во 2-й столбец:

$$\left(\begin{array}{cccc|ccc} -3 & 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 6 & 48 & 18 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

Отнимаем из 3-го и 4-го столбцов 2-й, умноженный на 8 и на 3, меняем знак в первой строке и получаем окончательно:

$$\left(\begin{array}{c|c} D_A & L \end{array}\right) = \left(\begin{array}{cccc|ccc} 3 & 0 & 0 & 0 & -1 & 0 & 2 \\ 0 & 6 & 0 & 0 & 3 & 1 & -6 \\ 0 & 0 & 0 & 0 & 0 & -2 & 1 \end{array}\right).$$

Из проделанного вычисления уже видно, что $L \simeq \mathbb{Z}^2$, а $\mathbb{Z}^3/L \simeq \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}$. Для отыскания матрицы L^{-1} действуем как в прим. 9.2 на стр. 154: записываем рядом

$$L = \begin{pmatrix} -1 & 0 & 2 \\ 3 & 1 & -6 \\ 0 & -2 & 1 \end{pmatrix} \quad \text{и} \quad E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

прибавляем в обеих матрицах ко 2-й строке утроенную первую:

$$\begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

затем прибавляем к 3-й строке удвоенную вторую:

$$\begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix},$$

наконец, отнимаем из 1-й строки удвоенную третью, меняем в ней знак и получаем

$$L^{-1} = \begin{pmatrix} 11 & 4 & 2 \\ 3 & 1 & 0 \\ 6 & 2 & 1 \end{pmatrix}.$$

Таким образом, взаимные базисы решётки $\mathbb{Z}^3$ и её подрешётки L состоят из векторов

$$u_1 = (11, 3, 6), \quad u_2 = (4, 1, 2), \quad u_3 = (2, 0, 1)$$

и векторов $w_1 = 3u_1 = (33, 9, 18)$, $w_2 = 6u_2 = (24, 6, 12)$.

Упражнение 10.1. Выразите последние два вектора через столбцы матрицы (10-2).

10.2. Теорема об элементарных делителях. Зафиксируем в каждом классе ассоциированных[1] простых элементов[2] кольца K какого-нибудь представителя и обозначим множество всех этих попарно неассоциированных представителей через $P(K)$. Обозначим[3] через $\nu_p(m)$ показатель, с которым $p \in P(K)$ входит в разложение элемента $m \in K$ на простые множители. Сопоставим каждому упорядоченному набору чисел

$$\lambda_1, \dots, \lambda_n \in K, \quad \text{где} \quad \lambda_i \mid \lambda_j \text{ при } i < j, \tag{10-3}$$

неупорядоченное дизъюнктное объединение по всем $i = 1, \dots, n$ степеней $p^{\nu_p(\lambda_i)}$, имеющих ненулевой показатель $\nu_p(\lambda_i)$. Иначе говоря, рассмотрим для каждого $i = 1, \dots, n$ разложение на простые множители $\lambda_i = \prod_{p \in P(K)} p^{\nu_p(\lambda_i)}$ и соберём все участвующие в этих разложениях сомножители p^ν с $\nu > 0$ в одно неупорядоченное множество, где каждая степень p^ν, присутствующая в разложении ровно k чисел λ_i, тоже присутствует ровно k раз. Получающееся таким образом неупорядоченное множество (возможно повторяющихся) степеней p^ν называется *набором элементарных делителей* упорядоченного набора (10-3).

Лемма 10.1
Описанная выше процедура устанавливает биекцию между рассматриваемыми с точностью до умножения каждого элемента на обратимое число из K упорядоченными наборами чисел $\lambda_1, \dots, \lambda_n \in K$, в которых $\lambda_i \mid \lambda_j$ при $i < j$, и всевозможными неупорядоченными наборами степеней p^ν, где $p \in P(K)$, $n \in \mathbb{N}$, элементы в которых могут повторяться.

Доказательство. Набор $\lambda_1, \dots, \lambda_n$ однозначно восстанавливается по своему набору элементарных делителей следующим образом. Расставим элементарные делители в клетки диаграммы Юнга так, чтобы в первой строке шли в порядке нестрого убывания степени того $p \in P(K)$, степеней которого в наборе элементарных делителей имеется больше всего. Во вторую строку поместим в порядке нестрого убывания степени простого числа, следующего за p по общему количеству вхождений его степеней в набор элементарных делителей и т. д. Поскольку λ_n делится на все остальные λ_i, в его разложение на простые множители входят все встречающиеся среди элементарных делителей простые основания, причём каждое из них — с максимально

[1] См. n° 5.4 на стр. 91.
[2] См. n° 5.4.2 на стр. 93.
[3] Ср. с n° 5.4.3 на стр. 94.

возможным показателем. Таким образом, λ_n является произведением всех элементарных делителей, стоящих в первом столбце построенной диаграммы Юнга. По индукции мы заключаем, что произведения элементарных делителей по столбцам диаграммы, перебираемым слева направо, суть $\lambda_n, \dots, \lambda_1$, т. е. прочитанный справа налево набор (10-3). □

Пример 10.3
Набор элементарных делителей

$$\begin{array}{ccccc} 3^2 & 3^2 & 3 & 3 & 3 \\ 2^3 & 2^3 & 2^2 & 2 & \\ 7^2 & 7 & 7 & & \\ 5 & 5 & & & \end{array}$$

возникает из множителей $\lambda_1 = 3$, $\lambda_2 = 3 \cdot 2$, $\lambda_3 = 3 \cdot 2^2 \cdot 7$, $\lambda_4 = 3^2 \cdot 2^3 \cdot 7 \cdot 5$, $\lambda_5 = 3^2 \cdot 2^3 \cdot 7^2 \cdot 5$.

Теорема 10.3 (теорема об элементарных делителях)
Всякий конечно порождённый модуль над областью главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \dots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \tag{10-4}$$

где $m_\nu \in \mathbb{N}$, все $p_\nu \in K$ просты, и слагаемые в прямой сумме могут повторяться. Два модуля

$$K^{n_0} \oplus \frac{K}{\left(p_1^{n_1}\right)} \oplus \dots \oplus \frac{K}{\left(p_\alpha^{n_\alpha}\right)} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{\left(q_1^{m_1}\right)} \oplus \dots \oplus \frac{K}{\left(q_\beta^{m_\beta}\right)}$$

изоморфны если и только если $n_0 = m_0$, $\alpha = \beta$ и слагаемые можно перенумеровать так, чтобы $n_\nu = m_\nu$ и $p_\nu = s_\nu q_\nu$, где все $s_\nu \in K$ обратимы.

Определение 10.2
Набор (возможно повторяющихся) степеней $p_i^{n_i}$, по которым происходит факторизация в (10-4), называется *набором элементарных делителей* модуля (10-4).

Доказательство существования разложения (10-4). Пусть K-модуль M порождается векторами

$$w_1, \dots, w_m .$$

Тогда $M = K^m / R$, где R — ядро эпиморфизма $K^m \twoheadrightarrow M$, переводящего стандартные базисные векторы $e_i \in K^m$ в образующие $w_i \in M$, как в форм. (10-1) на стр. 170. По теор. 10.2 в K^m существует такой базис $u_1, \dots, u_m$, что некоторые кратности $\lambda_1 u_1, \dots, \lambda_k u_k$ первых K базисных векторов составляют базис в R. Таким образом, $M = K^m / R = K/(\lambda_1) \oplus \dots \oplus K/(\lambda_k) \oplus K^{m-k}$. Пусть i-й инвариантный множитель $\lambda_i = p_1^{m_1} \dots p_s^{m_s}$, где $p_j \in K$ — попарно неассоциированные простые элементы. Тогда по китайской теореме об остатках $K/(\lambda_i) = K/(p_1^{m_1}) \oplus \dots \oplus K/(p_s^{m_s})$, что и даёт разложение (10-4). □

Чтобы установить единственность разложения (10-4) для заданного K-модуля M, мы дадим инвариантное описание его ингредиентов во внутренних терминах модуля M. Этому посвящены идущие ниже разделы n° 10.2.1 – n° 10.2.3. Далее, в n° 10.2.4 мы установим обещанные ранее независимость инвариантных множителей матрицы A от способа её приведения к нормальной форме Смита D_A и независимость инвариантных множителей подмодуля $N \subset F$ в свободном модуле F от выбора взаимных базисов в F и N.

10.2.1. Отщепление кручения. Вектор w из модуля M над целостным[1] кольцом K называется *элементом кручения*, если $xw = 0$ для какого-нибудь ненулевого $x \in K$. Например, любой класс $[k]_n \in \mathbb{Z}/(n)$ является элементом кручения в $\mathbb{Z}$-модуле $\mathbb{Z}/(n)$, так как $n[k]_n = [nk]_n = [0]_n$. В общем случае элементы кручения составляют подмодуль в M, который обозначается

$$\operatorname{Tors} M \stackrel{\text{def}}{=} \{w \in M \mid \exists\, x \neq 0 :\ xm = 0\} \tag{10-5}$$

и называется *подмодулем кручения* в M.

Упражнение 10.2. Убедитесь в том, что $\operatorname{Tors} M$ действительно является подмодулем в M.

Если $\operatorname{Tors} M = 0$, то говорят, что модуль M *не имеет кручения*. Например, любой идеал целостного кольца K и любой подмодуль в координатном модуле K^n над таким кольцом не имеют кручения. Если $\operatorname{Tors} M = M$, то M называется *модулем кручения*. Например, фактор K/I по любому ненулевому идеалу $I \subset K$ является K-модулем кручения, поскольку для любого класса $[a] \in K/I$ и любого ненулегого $x \in I$ класс $x[a] = [xa] = [0]$, так как $xa \in I$.

Предложение 10.1
Для любого модуля M над целостным кольцом K фактор модуль $M/\operatorname{Tors}(M)$ не имеет кручения. Если подмодуль $N \subset M$ таков, что $\operatorname{Tors}(M/N) = 0$, то $\operatorname{Tors}(M) \subset N$.

Доказательство. При ненулевом $x \in K$ равенство $x[w] = [xw] = [0]$ в $M/\operatorname{Tors}(M)$ означает, что $xw \in \operatorname{Tors}(M)$, т. е. $yxw = 0$ для некоторого ненулевого $y \in K$. Так как в K нет делителей нуля, $xy \neq 0$ и $w \in \operatorname{Tors}(M)$, т. е. $[w] = [0]$. Это доказывает первое утверждение. Для доказательства второго заметим, что если $w \in \operatorname{Tors}(M) \smallsetminus N$, то класс $[w] \in M/N$ является ненулевым элементом кручения. □

Теорема 10.4
Всякий конечно порождённый модуль M над областью главных идеалов K является прямой суммой свободного модуля и подмодуля кручения. В частности, любой модуль без кручения автоматически свободен.

Доказательство. По уже доказанному $M \simeq K^{n_0} \oplus K/\left(p_1^{n_1}\right) \oplus \ldots \oplus K/\left(p_\alpha^{n_\alpha}\right)$, где первое слагаемое свободно от кручения, а сумма остальных $N = K/(p_1^{n_1}) \oplus \ldots \oplus K/(p_\alpha^{n_\alpha})$ является модулем кручения, и тем самым содержится в $\operatorname{Tors}(M)$. Так как $M/N \simeq K^{n_0}$ не имеет кручения, $\operatorname{Tors}(M) \subset N$ по предл. 10.1. Тем самым, $\operatorname{Tors}(M) = N$, $M = K^{n_0} \oplus \operatorname{Tors}(M)$ и $M/\operatorname{Tors}(M) \simeq K^{n_0}$. □

Следствие 10.1 (из доказательства теор. 10.4)
В форм. (10-4) на стр. 174 сумма $K/\left(p_1^{n_1}\right) \oplus \ldots \oplus K/\left(p_\alpha^{n_\alpha}\right) = \operatorname{Tors}(M)$ и число n_0, равное рангу свободного модуля $M/\operatorname{Tors}(M)$, не зависят от выбора разложения (10-4). □

10.2.2. Отщепление p-кручения. Для каждого простого $p \in P(K)$ назовём подмодуль

$$\operatorname{Tors}_p(M) \stackrel{\text{def}}{=} \{w \in M \mid \exists\, k \in \mathbb{N} :\ p^k w = 0\}.$$

подмодулем p-кручения в M, а его элементы — *элементами p-кручения*.

Упражнение 10.3. Убедитесь, что $\operatorname{Tors}_p(M)$ действительно является подмодулем в M и докажите для него аналог предл. 10.1: фактор $M/\operatorname{Tors}_p(M)$ не имеет p-кручения, и если подмодуль $N \subset M$ таков, что $\operatorname{Tors}_p(M/N) = 0$, то $\operatorname{Tors}_p(M) \subset N$.

[1] См. n° 2.4.1 на стр. 30.

Теорема 10.5
Всякий конечно порождённый модуль кручения $M = \mathrm{Tors}(M)$ над областью главных идеалов K является прямой суммой своих подмодулей p-кручения: $M = \bigoplus_p \mathrm{Tors}_p(M)$, где сумма берётся по всем таким $p \in P(K)$, что $\mathrm{Tors}_p(M) \neq 0$. При этом каждый конечно порождённый модуль p-кручения имеет вид $K/(p^{\nu_1}) \oplus \ldots \oplus K/(p^{\nu_k})$, где $\nu_1, \ldots, \nu_k \in \mathbb{N}$.

Доказательство. Если простое $q \in K$ не ассоциировано с p, то класс $[p^k]$ обратим в фактор кольце $K/\left(q^m\right)$ и гомоморфизм умножения на p^k:

$$K/\left(q^m\right) \to K/\left(q^m\right), \quad x \mapsto p^k x,$$

биективен и имеет нулевое ядро. Напротив, модуль $K/(p^\nu)$ аннулируется умножением на p^ν. Тем самым, в разложении из форм. (10-4) на стр. 174

$$M = \mathrm{Tors}(M) = \left(\tfrac{K}{(p^{\nu_1})} \oplus \ldots \oplus \tfrac{K}{(p^{\nu_k})}\right) \oplus \left(\bigoplus\nolimits_{q \neq p} \left(\tfrac{K}{(q^{\mu_{q,1}})} \oplus \ldots \oplus \tfrac{K}{(q^{\mu_{q,m_q}})}\right)\right)$$

слагаемое в левых скобках содержится в $\mathrm{Tors}_p(M)$, а фактор по нему, изоморфный сумме в правых скобках, не имеет p-кручения. Поэтому $\mathrm{Tors}_p(M)$ совпадает с левым слагаемым, $M/\mathrm{Tors}_p(M)$ изоморфен правому слагаемому, и $M \simeq \mathrm{Tors}_p(M) \oplus \big(M/\mathrm{Tors}_p(M)\big)$. □

Следствие 10.2 (из доказательства теор. 10.5)
В форм. (10-4) на стр. 174 сумма всех подмодулей $K/(p^\nu)$ с заданным $p \in P(K)$ является подмодулем p-кручения в M и не зависит от выбора разложения (10-4). □

10.2.3. Инвариантность показателей p-кручения. Согласно теор. 10.5 каждый конечно порождённый модуль p-кручения M над областью главных идеалов K имеет вид

$$M = \frac{K}{(p^{\nu_1})} \oplus \ldots \oplus \frac{K}{(p^{\nu_n})}. \tag{10-6}$$

Упорядоченные по нестрогому убыванию натуральные числа $\nu_1 \geqslant \nu_2 \geqslant \ldots \geqslant \nu_n$ называются *показателями p-кручения* модуля M. Они образуют диаграмму Юнга $\nu = \nu(M) = (\nu_1, \ldots, \nu_n)$, которая называется *цикловым типом* модуля p-кручения M. Для завершения доказательства теор. 10.3 остаётся проверить, что цикловой тип зависит только от модуля M, а не от выбора конкретного разложения (10-6). Для этого рассмотрим гомоморфизм умножения на p

$$\varphi : M \to M, \quad w \mapsto pw$$

и обозначим через $\varphi^k = \varphi \circ \ldots \circ \varphi : w \mapsto p^k w$ его k-кратную итерацию, считая, что $\varphi^0 = \mathrm{Id}_M$. Очевидно, что $\ker \varphi^k \subseteq \ker \varphi^{k+1}$ при всех k, и $\ker \varphi^{\nu_1} = M$, а $\ker \varphi^{\nu_1 - 1} \neq M$. Таким образом, мы имеем конечную цепочку возрастающих подмодулей

$$0 = \ker \varphi^0 \subseteq \ker \varphi^1 \subseteq \ldots \subseteq \ker \varphi^{\nu_1 - 1} \subsetneq \ker \varphi^{\nu_1} = M, \tag{10-7}$$

которая зависит только от модуля M.

Лемма 10.2
Для каждого $k \in \mathbb{N}$ фактор модуль $\ker \varphi^k / \ker \varphi^{k-1}$ является векторным пространством над полем $\Bbbk = K/(p)$ размерности, равной высоте k-го столбца диаграммы Юнга $\nu(M)$.

Доказательство. Зададим умножение класса $[x] \in K/(p)$ на класс $[w] \in \ker\varphi^k/\ker\varphi^{k-1}$ правилом $[x][z] \stackrel{\text{def}}{=} [xz]$. Оно корректно, поскольку для $x' = x + py$ и $w' = w + u$, где $p^{k-1}u = 0$, имеем $x'w' = xw + (x + py)u + pyw$ и $p^{k-1}\big((x + py)\,u + pyw\big) = 0$, так как $p^{k-1}u = 0$ и $p^k w = 0$. Аксиомы дистрибутивности и ассоциативности очевидно выполняются. Это доказывает первое утверждение. Для доказательства второго допустим, что модуль M раскладывается по формуле (10-6). Так как оператор φ переводит каждое слагаемое этого разложения в себя, $\ker\varphi^k/\ker\varphi^{k-1}$ является прямой суммой модулей $\ker\varphi_i^k/\ker\varphi_i^{k-1}$, где $\varphi_i = \varphi|_{K/(p^{\nu_i})}$ — ограничение отображения φ на i-е слагаемое разложения (10-6).

Упражнение 10.4. Убедитесь, что для модуля $M = K/(p^m)$ при каждом $k = 1, \dots, m$ отображение $K/(p) \to \ker\varphi^k/\ker\varphi^{k-1}$, $x \pmod p \mapsto p^{m-k}x \pmod{\ker\varphi^{k-1}}$, корректно определено, $\Bbbk$-линейно и биективно.

Мы заключаем, что для каждого слагаемого $K/(p_i^{\nu_i})$ в разложении (10-6) цепочка ядер (10-7) имеет вид $0 = \ker\varphi_i^0 \subsetneq \ker\varphi_i^1 \subsetneq \dots \subsetneq \ker\varphi_i^{\nu_i - 1} \subsetneq \ker\varphi^{\nu_i} = K/(p_i^{\nu_i})$, и при каждом $k = 1, \dots, \nu_i$ фактор $\ker\varphi_i^k/\ker\varphi_i^{k-1}$ является одномерным векторным пространством над полем $\Bbbk = K/(p)$. Таким образом во всём модуле (10-6) пространство $\ker\varphi^k/\ker\varphi^{k-1}$ является прямой суммой одномерных пространств $\Bbbk$ в количестве, равном числу строк диаграммы ν, длина которых не меньше k, т. е. высоте k-го столбца диаграммы ν. □

На этом доказательство теор. 10.3 об элементарных делителях заканчивается. В силу лем. 10.1 на стр. 173 эта теорема допускает следующую эквивалентную переформулировку.

Следствие 10.3 (теорема об инвариантных множителях)
Всякий конечно порождённый модуль над областью главных идеалов K изоморфен

$$K^{n_0} \oplus \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_g)} \tag{10-8}$$

где n_0, g — целые неотрицательные, а $\lambda_1, \dots, \lambda_g \in K$ — такие ненулевые необратимые элементы, что $\lambda_i \mid \lambda_j$ при $i < j$. Два таких модуля

$$K^{n_0} \oplus \frac{K}{(\lambda_1)} \oplus \dots \oplus \frac{K}{(\lambda_g)} \quad \text{и} \quad K^{m_0} \oplus \frac{K}{(\mu_1)} \oplus \dots \oplus \frac{K}{(\mu_h)}$$

изоморфны если и только если $n_0 = m_0$, $g = h$ и $\lambda_i = s_i\mu_i$, где все $s_i \in K$ обратимы. □

10.2.4. Единственность инвариантных множителей. Пусть F — свободный модуль конечного ранга m над областью главных идеалов K и $N \subset F$ — его подмодуль. Покажем, что множители $\lambda_1, \dots, \lambda_n$ из теоремы о взаимном базисе[1] не зависят от выбора взаимных базисов. В самом деле, фактор модуль $M = F/N$ ничего не знает о взаимных базисах, и по теореме об элементарных делителях[2] он имеет вид

$$M \simeq K^{m_0} \oplus \frac{K}{(p_1^{m_1})} \oplus \dots \oplus \frac{K}{(p_\alpha^{m_\alpha})} \tag{10-9}$$

С другой стороны, если базис $e_1, \dots, e_m$ модуля F таков, что векторы $\lambda_1 e_1, \dots, \lambda_n e_n$ составляют базис в N и $\lambda_i \mid \lambda_j$ при $i < j$, то $M = F/N \simeq K^{m-n} \oplus K/(\lambda_1) \oplus \dots \oplus K/(\lambda_n)$, а каждый фактор $K/(\lambda)$

[1] См. теор. 10.2 на стр. 171.
[2] См. теор. 10.3 на стр. 174.

по китайской теореме об остатках является прямой суммой модулей вида $K/(p^{\nu_p(\lambda)})$, где $p^{\nu_p(\lambda)}$ берутся из разложения $\lambda = \prod_{p\in P(K)} p^{\nu_p(\lambda)}$ на простые множители. По теореме об элементарных делителях $n = m - \mathrm{rk}(M/\mathrm{Tors}(M))$, а набор степеней $p^{\nu_p(\lambda)}$ точно такой же, как в (10-9), т. е. представляет собою набор элементарных делителей модуля M, зависящий только от M в силу предыдущих теорем. Согласно лем. 10.1 на стр. 173 набор чисел $\lambda_1, \dots, \lambda_n$, в котором $\lambda_i \mid \lambda_j$ при $i < j$, однозначно восстанавливается по дизъюнктному объединению своих делителей $p^{\nu_p(\lambda_i)}$, что доказывает независимость инвариантных множителей от выбора базиса.

Применительно к модулю $F = K^m$ и его подмодулю $N \subset K^m$, порождённому столбцами матрицы $A \in \mathrm{Mat}_{m\times n}(K)$, это утверждение означает, что элементы d_{ii} нормальной формы Смита матрицы A не зависят от способа приведения матрицы к нормальной форме и даже от собственно матрицы, а зависят лишь от подмодуля N. В самом деле, обозначим через $\boldsymbol{a} = (a_1, \dots, a_n)$ набор столбцов матрицы A, а через $D = LAR$ — какую-нибудь нормальную форма Смита матрицы A. Из равенства $\boldsymbol{a} = \boldsymbol{e}A$ вытекает равенство $\boldsymbol{a}R = \boldsymbol{e}L^{-1}LAR = \boldsymbol{e}L^{-1}D$. В силу обратимости матриц R и L векторы $\boldsymbol{u} = \boldsymbol{e}\,L^{-1}$ тоже составляют базис в K^m, а векторы $\boldsymbol{w} = \boldsymbol{a}R$ линейно порождают N. Так как $\boldsymbol{w} = \boldsymbol{u}\,D$, векторы $\boldsymbol{u} = (u_1, \dots, u_m)$ и векторы $w_i = d_{ii}u_i$ с ненулевыми d_{ii} образуют взаимные базисы модуля K^n и его подмодуля N, а ненулевые диагональные элементы d_{ii} являются инвариантными множителями этого подмодуля.

10.3. Конечно порождённые абелевы группы. При $K = \mathbb{Z}$ теорема об инвариантных множителях[1] и теорема об элементарных делителях[2] дают две альтернативных полных классификации конечно порождённых абелевых групп.

Теорема 10.6 (теорема об инвариантных множителях)
Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(n_g)}, \tag{10-10}$$

где r — целое неотрицательное, а натуральные $n_1, \dots, n_g \geqslant 2$ таковы, что $n_i \mid n_j$ при $i < j$. Две такие группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(n_g)} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(m_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(m_h)}$$

изоморфны если и только если $r = s$, $g = h$ и $n_i = m_i$ при всех i. □

Теорема 10.7 (теорема об элементарных делителях)
Всякая конечно порождённая абелева группа изоморфна прямой сумме аддитивных групп

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}, \tag{10-11}$$

где $p_\nu \in \mathbb{N}$ — простые числа (не обязательно различные). Две такие группы

$$\mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})} \quad \text{и} \quad \mathbb{Z}^s \oplus \frac{\mathbb{Z}}{(q_1^{m_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(q_\beta^{m_\beta})}$$

изоморфны если и только если $r = s$, $\alpha = \beta$ и после надлежащей перестановки слагаемых будут выполняться равенства $n_\nu = m_\nu$ и $p_\nu = q_\nu$ при всех ν. □

[1] См. сл. 10.3 на стр. 177.
[2] См. теор. 10.3 на стр. 174.

При этом в разложениях (10-10) и (10-11) данной абелевой группы A целые неотрицательные r одинаковы, а упорядоченный набор натуральных чисел $n_1 \mid \ldots \mid n_g$ из разложения (10-10) и неупорядоченное множество возможно повторяющихся степеней p^ν из разложения (10-11) однозначно определяют друг друга по лем. 10.1 на стр. 173: множество элементарных делителей является дизъюнктным объединением степеней $p^{\nu_p(n_i)}$ с $\nu_p(m_i) > 0$ по всем $1 \leqslant i \leqslant g$ и всем простым $p \in \mathbb{N}$, а набор инвариантных множителей $n_1, \ldots, n_g$ является прочитанным справа налево набором произведений, взятых по столбцам диаграммы Юнга, в первую строку которой выписаны в порядке нестрого убывания показателей все степени того числа p, степеней которого больше всего, во вторую — все степени следующего по общему количеству степеней числа p и т. д. Единственная с точностью до перестановки прямых слагаемых аддитивная группа (10-11), изоморфная заданной конечно порождённой абелевой группе A, называется *стандартным* (или *жордановым*) *представлением* группы A или разложением группы A в прямую сумму неразложимых циклических подгрупп, а прямая сумма (10-10) — *фробенусовым представлением* группы A.

Пример 10.4 (абелевы группы порядка $\leqslant 10$)
Абелевы группы из двух, трёх, пяти, шести, семи и десяти элементов с точностью до изоморфизма единственны и их стандартные представления (10-11) имеют, соответственно, вид:

$$\mathbb{Z}/(2)\,,\ \mathbb{Z}/(3)\,,\ \mathbb{Z}/(5)\,,\ \mathbb{Z}/(3)\oplus\mathbb{Z}/(2)\,,\ \mathbb{Z}/(7)\,,\ \mathbb{Z}/(5)\oplus\mathbb{Z}/(2)\,.$$

Групп из четырёх элементов с точностью до изоморфизма две: $\mathbb{Z}/(4)$ и $\mathbb{Z}/(2)\oplus\mathbb{Z}/(2)$.

Упражнение 10.5. Убедитесь явным образом, что эти две группы не изоморфны.

Групп из девяти элементов с точностью до изоморфизма тоже две: $\mathbb{Z}/(9)$ и $\mathbb{Z}/(3)\oplus\mathbb{Z}/(3)$. Группы из восьми элементов с точностью до изоморфизма исчерпываются тремя попарно не изоморфными группами $\mathbb{Z}/(8)$, $\mathbb{Z}/(4)\oplus\mathbb{Z}/(2)$ и $\mathbb{Z}/(2)\oplus\mathbb{Z}/(2)\oplus\mathbb{Z}/(2)$.

10.3.1. Канонические и не канонические слагаемые стандартного представления. Для каждого простого p, участвующего в стандартном представлении данной группы A, в A имеется единственная подгруппа, изоморфная прямой сумме всех прямых слагаемых вида $\mathbb{Z}/(p^m)$ в разложении (10-11) — это подгруппа p-кручения $\mathrm{Tors}_p(A) \subset A$. Прямая сумма этих подгрупп, т. е. подгруппа кручения $\mathrm{Tors}(A) = \bigoplus_p \mathrm{Tors}_p(A)$ — это единственная подгруппа в A, изоморфная сумме всех отличных от $\mathbb{Z}^r$ элементов разложения (10-11). В противоположность этому, дополнительная к $\mathrm{Tors}(A)$ свободная подгруппа $B \subset A$, изоморфная $\mathbb{Z}^r \simeq A/\mathrm{Tors}(A)$ может быть выбрана в A разными способами. Например, группа $A = \mathbb{Z}\oplus\mathbb{Z}/(3)$ иначе раскладывается как $B \oplus \mathbb{Z}/(3)$, где подгруппа $B \subset A$ порождена элементом $(1, [1]_3) \in A$.

Упражнение 10.6. Убедитесь в этом и перечислите для группы $A = \mathbb{Z}\oplus\mathbb{Z}/(3)$ все изоморфные $\mathbb{Z}$ подгруппы $B \subset A$, дополнительные к $\mathrm{Tors}(A)$.

Разложение подгруппы p-кручения в сумму неразложимых циклических подгрупп

$$\mathrm{Tors}_p(A) = \frac{\mathbb{Z}}{(p^{\nu_1})} \oplus \ldots \oplus \frac{\mathbb{Z}}{(p^{\nu_n})}$$

тоже не единственно: для каждого показателя ν_i изоморфная $\mathbb{Z}/(p^{\nu_i})$ подгруппа в A может выбираться разными способами. Например, группа $A = \mathbb{Z}/(4)\oplus\mathbb{Z}(2)$ иначе раскладывается в сумму $B \oplus C$ подгрупп $B \simeq \mathbb{Z}/(4)$ и $C \simeq \mathbb{Z}/(4)$, порождённых элементами $([1]_4, [1]_2)$ и $([2]_4, [1]_2)$ соответственно. Но цикловой тип группы A, т. е. набор $(\nu_1, \ldots, \nu_n)$ показателей p-кручения, от выбора разложения не зависит.

10.3.2. Циклические группы и минимальные наборы образующих. Пусть абелева группа A порождается как $\mathbb{Z}$-модуль элементами $a_1, \dots, a_m$. Наборы образующих с наименьшим возможным m называется *минимальными*. Группа (10-10)

$$A = \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(n_1)} \oplus \dots \oplus \frac{\mathbb{Z}}{(n_g)},$$

где $n_i \mid n_j$ при $i < j$, порождается $r + g$ элементами вида $(0, \dots, 0, 1, 0, \dots, 0)$. Покажем, что это минимальный набор образующих. Пусть A порождается m элементами $a_1, \dots, a_m$. Тогда

$$A \simeq \mathbb{Z}^m / R,$$

где $R \subset \mathbb{Z}^m$ — ядро сюръективного гомоморфизма $\mathbb{Z} \twoheadrightarrow A$, переводящего стандартные базисные векторы $e_1, \dots, e_m \in \mathbb{Z}^m$ в $a_1, \dots, a_m \in A$. Пусть векторы $f_1, \dots, f_m$ и $\lambda_1 f_1, \dots, \lambda_k f_k$ образуют взаимные базисы в $\mathbb{Z}^m$ и R, и пусть $\lambda_1 = \dots = \lambda_s = 1$, а $\lambda_{s+1} \mid \dots \mid \lambda_k$ строго больше 1. Тогда фробениусово представление группы $A = \mathbb{Z}^m / R$ имеет вид

$$\frac{\mathbb{Z}}{(\lambda_{s+1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(\lambda_k)} \oplus \mathbb{Z}^{m-k},$$

и в силу единственности фробениусова представления $r = (m - k)$, $g = k - s$ и $n_i = \lambda_{s+i}$ при всех $i = 1, \dots, g$. В частности $r + g = m - s \leqslant m$, что и утверждалось.

В терминах разложения (10-11) в прямую сумму неразложимых циклических подгрупп число g конечных слагаемых фробениусова разложения абелевой группы A равно максимальному числу элементарных делителей с одним и тем же простым основанием, т. е. длине верхней строки диаграммы Юнга, составленной из элементарных делителей группы A.

Абелевы группы, которые можно породить одним элементом, называются *циклическими*. Фробениусово разложение такой группы имеет ровно одно слагаемое. Тем самым, циклические абелевы группы исчерпываются группами $\mathbb{Z}$ и $\mathbb{Z}/(n)$. В терминах элементарных делителей абелева группа A циклическая если и только если все простые числа в слагаемых $\mathbb{Z}/(p^m)$ её стандартного представления (10-11) попарно различны. Например, группа $\mathbb{Z}/(125) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}/(16)$ циклическая, а группа $\mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(4) \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(12)$ — нет.

10.3.3. Неразложимые группы. Абелева группа A называется *разложимой*, если она является прямой суммой $A = B \oplus C$ двух ненулевых собственных подгрупп $B, C \subsetneq A$. Из теор. 10.7 на стр. 178 вытекает, что каждая неразложимая абелева группа изоморфна $\mathbb{Z}$ или $\mathbb{Z}/(p^m)$, где $p \in \mathbb{N}$ — простое, причём эти неразложимые группы попарно не изоморфны, а произвольная конечно порождённая абелева группа является прямой суммой неразложимых.

10.3.4. Простые и полупростые группы. Абелева группа A называется *простой*[1], если в ней нет ненулевых собственных подгрупп. Каждая простая группа автоматически неразложима. Обратное неверно: группы $\mathbb{Z}$ и $\mathbb{Z}/(p^m)$, где $m \geqslant 2$ неразложимы, но не просты, поскольку содержат ненулевые собственные подгруппы.

Упражнение 10.7. Опишите все ненулевые собственные подгруппы в $\mathbb{Z}$ и в $\mathbb{Z}/(p^m)$, где $m \geqslant 2$.

Поскольку порядок любой подгруппы в конечной группе A делит порядок A, все конечные группы простого порядка просты. Мы заключаем, что конечно порождённые простые абелевы группы с точностью до изоморфизма исчерпываются группами $\mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое, и при разных p такие группы не изоморфны.

[1] В другой терминологии — *неприводимой*.

Абелева группа называется *полупростой*, если она является прямой суммой простых подгрупп. Таким образом, конечно порождённые полупростые абелевы группы исчерпываются конечными прямыми суммами групп вида $\mathbb{Z}/(p)$, где $p \in \mathbb{N}$ — простое.

Предложение 10.2
Следующие свойства конечно порождённой абелевой группы A эквивалентны:

(1) A полупроста

(2) A порождается своими простыми подгруппами

(3) каждая ненулевая собственная подгруппа $B \subsetneq A$ отщепляется прямым слагаемым, т. е. найдётся такая подгруппа $C \subset A$, что $A = B \oplus C$.

Доказательство. Импликация (1) $\Rightarrow$ (2) очевидна. Докажем импликацию (2) $\Rightarrow$ (3). Так как все простые абелевы группы являются группами кручения, группа A, удовлетворяющая условию (2), тоже является группой кручения и по теор. 10.7 на стр. 178 конечна. Пересечение любой простой подгруппы $U \subset A$ с любой подгруппой $W \subsetneq A$, будучи подгруппой в U, либо нулевое, либо совпадает с U. Так как линейная оболочка простых подгрупп совпадает с A, для любой собственной подгруппы $B \subsetneq A$ найдётся простая подгруппа $U_1 \subsetneq B$. Сумма подгрупп B и U_1 прямая. Если $B \oplus U_1 \neq A$, заменяем B на $B \oplus U_1$ и повторяем рассуждение, до тех пор пока не получим равенство $A = B \oplus U_1 \oplus \ldots \oplus U_k$, где все U_k просты. Остаётся положить $C = U_1 \oplus \ldots \oplus U_k$.

Чтобы установить импликацию (3) $\Rightarrow$ (1), докажем сначала, что если группа A обладает свойством (3), то им обладает и каждая подгруппа $B \subset A$. Пусть $V \subset B$ — любая подгруппа. Тогда в A существуют такие подгруппы C, U, что $A = B \oplus C = V \oplus C \oplus U$. Обозначим через

$$\pi : A \twoheadrightarrow B, \quad b + c \mapsto b,$$

проекцию A на B вдоль C и положим $W = \pi(U)$.

Упражнение 10.8. Проверьте, что $B = V \oplus W$.

Поскольку группы $\mathbb{Z}^n$ и $\mathbb{Z}/(p^m)$ с $m \geqslant 2$ не просты и неразложимы, они не обладают свойством (3) и по доказанному не могут входить в стандартное представление группы, которая обладает свойством (3). Тем самым, каждая группа, обладающая свойством (3) является прямой суммой простых групп. □

Упражнение 10.9. Убедитесь непосредственно, что группы $\mathbb{Z}$ и $\mathbb{Z}/(p^m)$ с $m \geqslant 2$ не порождаются своими простыми подгруппами.

10.3.5. Группы, заданные образующими и соотношениями. На практике конечно порождённые абелевы группы часто задаются образующими и соотношениями, т. е. как факторы $A = \mathbb{Z}^m / L_R$ координатного $\mathbb{Z}$-модуля по подмодулю $L_R = \operatorname{span}_{\mathbb{Z}}(R) \subset \mathbb{Z}^m$, заданному как $\mathbb{Z}$-линейная оболочка некоторого множества векторов $R \subset \mathbb{Z}^m$. Векторы из множества R называются *порождающими соотношениями*. В просторечии подобное описание обычно звучит так: рассмотрим абелеву группу A, порождённую элементами $a_1, \ldots, a_m$, которые связаны соотношениями

$$\begin{cases} a_1 r_{11} + a_2 r_{21} + \ldots + a_m r_{m1} = 0 \\ a_1 r_{12} + a_2 r_{22} + \ldots + a_m r_{m2} = 0 \\ \qquad \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ a_1 r_{1n} + a_2 r_{2n} + \ldots + a_m r_{mn} = 0, \end{cases} \tag{10-12}$$

где $R = (r_{ij}) \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$. В предыдущих терминах это означает, что $A = \mathbb{Z}^m / L_R$, где подмодуль $L_R \subset \mathbb{Z}^m$ порождается над $\mathbb{Z}$ столбцами матрицы R, а образующие $a_j = [e_j]_{L_R} \in A$ суть классы стандартных базисных векторов $e_j \in \mathbb{Z}^m$ по модулю решётки $L_R \subset \mathbb{Z}^m$.

Рассмотрим векторное пространство $\mathbb{Q}^m \supset \mathbb{Z}^m$, в которое координатный модуль $\mathbb{Z}^m$ естественным образом вложен, и обозначим через $\mathbb{Q} \otimes L_R = \mathrm{span}_{\mathbb{Q}}(L_R) \subset \mathbb{Q}^m$ векторное подпространство, порождённое решёткой L_R в $\mathbb{Q}^m$, или, что то же самое, $\mathbb{Q}$-линейную оболочку столбцов матрицы R. Его размерность $\dim_{\mathbb{Q}}(\mathbb{Q} \otimes L_R) = \mathrm{rk}\, R = \mathrm{rk}\, L_R$ совпадает с рангом матрицы R, рассматриваемой как матрица над полем $\mathbb{Q}$, и равна рангу свободного $\mathbb{Z}$-модуля $L_R \subset \mathbb{Z}^n$, так как любой базис решётки L_R над $\mathbb{Z}$ одновременно является базисом пространства $\mathbb{Q} \otimes L_R$ над $\mathbb{Q}$.

Упражнение 10.10. Докажите, что набор векторов $v_1, \ldots, v_k \in \mathbb{Z}^m \subset \mathbb{Q}^m$ линейно независим над $\mathbb{Z}$ если и только если он линейно независим над $\mathbb{Q}$.

Мы заключаем, что $\mathrm{rk}(A / \mathrm{Tors}(A)) = m - \mathrm{rk}\, R$, т. е. ранг свободного слагаемого в стандартном представлении (10-4) группы $A = \mathbb{Z}^m / L_R$ равен $m - \mathrm{rk}\, R$. Обратите внимание, что ранг матрицы R можно вычислить методом Гаусса над полем $\mathbb{Q}$, как в прим. 9.4 на стр. 159. Для вычисления остальных слагаемых стандартного представления необходимо найти все ненулевые инвариантные множители[1] $\lambda_1, \ldots, \lambda_r$, где $r = \mathrm{rk}\, R$, подмодуля $L_R \subset \mathbb{Z}^m$. Они совпадают с инвариантными множителями матрицы[2] R, и $A = \mathbb{Z}^{m-r} \oplus \mathbb{Z}/(\lambda_1) \oplus \ldots \oplus \mathbb{Z}/(\lambda_r)$. Стандартное представление группы A получается отсюда разложением каждого фактора $\mathbb{Z}/(\lambda_i)$ по китайской теореме об остатках[3].

Пример 10.5

Найдём стандартное представление абелевой группы, порождённой элементами a_1, a_2, a_3, которые связаны соотношениями

$$\begin{cases} -57a_1 + 58a_2 - 55a_3 = 0 \\ -34a_1 + 40a_2 - 22a_3 = 0 \\ 5a_1 - 10a_2 - 5a_3 = 0 \\ 9a_1 - 11a_2 + 5a_3 = 0\,. \end{cases}$$

Для этого методом Гаусса найдём инвариантные множители матрицы

$$R = \begin{pmatrix} -57 & -34 & 5 & 9 \\ 58 & 40 & -10 & -11 \\ -55 & -22 & -5 & 5 \end{pmatrix}$$

Прибавим к 1-й строке 2-ю:

$$\begin{pmatrix} 1 & 6 & -5 & -2 \\ 58 & 40 & -10 & -11 \\ -55 & -22 & -5 & 5 \end{pmatrix}$$

Зануляем верхнюю строку и левый столбец вне левого верхнего угла:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -308 & 280 & 105 \\ 0 & 308 & -280 & -105 \end{pmatrix}$$

[1] См. опр. 10.1 на стр. 171.
[2] См. n° 9.1.1 на стр. 150.
[3] См. n° 2.7 на стр. 37.

Так как 3-я строка кратна 2-й, и наибольший общий делитель второй строки равен 7, ненулевые множители матрицы R суть 1 и 7, а её ранг равен 2. Мы заключаем, что

$$A = \mathbb{Z}^3 / L_R \simeq \mathbb{Z} \oplus \mathbb{Z}/(7)\,.$$

Пример 10.6 (порядки элементов)
Пусть абелева группа $A = \mathbb{Z}^m/L_R$ порождается элементами $a_1, \dots, a_m$ и $w = k_1a_1 + \dots + k_ma_m$. Как узнать, отличен ли элемент w от нуля, и если да, то каков его порядок[1]? Если известен какой-нибудь базис $r_1, \dots, r_n$ решётки L_R над $\mathbb{Z}$, то ответить на эти вопросы можно при помощи вычислений над полем $\mathbb{Q}$, т. е. в векторном пространстве $\mathbb{Q}^m \supset \mathbb{Z}^m$. Возьмём в качестве матрицы соотношений $R \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$ набор столбцов координат базисных векторов $r_1, \dots, r_n$. Если столбец $\widetilde{w} = (k_1, \dots, k_n)^t \in \mathbb{Z}^n$ не лежит в $\mathbb{Q}$-линейной оболочке столбцов матрицы R, то никакое целое кратное $z\widetilde{w}$ не лежит в L_R, и в этом случае $w \neq 0$ в A и $\operatorname{ord} w = \infty$. Если же

$$\widetilde{w} = \frac{p_1}{q_1}r_1 + \dots + \frac{p_n}{q_n}r_n \in \mathbb{Q} \otimes L_R$$

где $\operatorname{нод}(p_i, q_i) = 1$ при всех i, то $\operatorname{ord}(w) = \ \dots(q_1, \dots, q_n)$. В частности, $w = 0$ если и только если все $q_i = 1$. Мы заключаем, что w является ненулевым элементом бесконечного порядка если и только если система уравнений $Rx = \widetilde{w}$ не имеет решений в поле $\mathbb{Q}$, если же система имеет решение $u = (\mu_1, \dots, \mu_n) \in \mathbb{Q}^n$, то это решение единственно в силу линейной независимости n столбцов матрицы R, и $\operatorname{ord}(w) = \min(z \in \mathbb{N} \mid zu \in \mathbb{Z}^n)$. В частности, $w = 0$ если и только если система $Rx = \widetilde{w}$ имеет целое решение.

10.3.6. Подрешётки в $\mathbb{Z}^m$. Абелевы подгруппы $L \subset \mathbb{Z}^m$ обычно называют *подрешётками* в $\mathbb{Z}^m$. Согласно теор. 10.1 на стр. 170 каждая подрешётка $L \subset \mathbb{Z}^m$ является свободным $\mathbb{Z}$-модулем ранга $\operatorname{rk} L \leqslant m$. Если $\operatorname{rk} L = m$, подрешётка L называется *соизмеримой* с $\mathbb{Z}^m$. Из сказанного выше вытекает

Предложение 10.3 (соизмеримые подрешётки)
Следующие свойства подрешётки $L_A \subset \mathbb{Z}^m$, порождённой столбцами матрицы $A \in \mathrm{Mat}_{m\times n}(\mathbb{Z})$, эквивалентны друг другу:

(1) $\operatorname{rk} L = m$

(2) фактор группа $\mathbb{Z}^m / L$ конечна

(3) ранг матрицы A над полем $\mathbb{Q}$ равен m. □

Решётка $L \subset \mathbb{Z}^m$ называются *отщепимой*, если она удовлетворят следующему предложению.

Предложение 10.4 (отщепимые подрешётки)
Следующие свойства подрешётки $L \subset \mathbb{Z}^m$ эквивалентны друг другу:

(1) все ненулевые инвариантные множители подрешётки L равны единице

(2) фактор группа $\mathbb{Z}^m / L$ не имеет кручения

(3) существует такая подрешётка $N \subset \mathbb{Z}^m$, что $\mathbb{Z}^m = L \oplus N$

[1] Напомню, что *порядком* $\operatorname{ord}(w)$ элемента w в аддитивной абелевой группе называется наименьшее такое $n \in \mathbb{N}$, что $nw = 0$, а если такого n нет, то $\operatorname{ord}(w) = \infty$, см. n° 3.5.1 на стр. 56.

(4) решётка L является множеством всех целых решений системы однородных линейных уравнений $Ax = 0$ с целочисленной матрицей A высоты m.

Доказательство. Равносильность условий (1), (2) и импликации (1) ⇒ (3), (4) вытекают из теоремы о взаимном базисе: если первые r базисных векторов базиса $u_1, \dots, u_m$ в $\mathbb{Z}^m$ образуют базис в L, то дополнительная к L подрешётка N является линейной оболочкой последних $m-r$ базисных векторов, а решётка L является ядром линейного отображения $\mathbb{Z}^m \to \mathbb{Z}^{m-r}$, переводящего вектор $w \in \mathbb{Z}^m$ в набор его последних $m-r$ координат в базисе $u_1, \dots, u_m$. Импликация (3) ⇒ (2) очевидна, так как $(L \oplus N)/L \simeq N$. Докажем импликацию (4) ⇒ (2). Пусть $A \in \mathrm{Mat}_{k\times m}(\mathbb{Z})$ и подрешётка $L \subset \mathbb{Z}^m$ является ядром линейного отображения $\alpha\colon \mathbb{Z}^m \to \mathbb{Z}^k$, $x \mapsto Ax$. Тогда отображение $\overline{\alpha}\colon \mathbb{Z}^m/L \hookrightarrow \mathbb{Z}^k$, $[x] \mapsto Ax$, корректно определено и инъективно.

Упражнение 10.11. Убедитесь в этом.

Тем самым, $\mathbb{Z}$-модуль $\mathbb{Z}^m/L$ изоморфен подмодулю модуля без кручения. □

Задачи для самостоятельного решения к §10

Задача 10.1. Найдите взаимные базисы в $\mathbb{Z}^3$ и его подмодуле, порождённом столбцами матриц

а) $\begin{pmatrix} -70 & 59 \\ 8 & -6 \\ -25 & 22 \end{pmatrix}$ б) $\begin{pmatrix} 91 & 49 \\ -21 & -21 \\ 28 & 7 \end{pmatrix}$ в) $\begin{pmatrix} -46 & -16 & 15 \\ -30 & -14 & 5 \\ -20 & -2 & 13 \end{pmatrix}$ г) $\begin{pmatrix} 78 & -13 & 65 \\ -78 & -13 & -39 \\ 78 & 0 & 52 \end{pmatrix}$

д) $\begin{pmatrix} 28 & -35 & 100 & -33 \\ -15 & -2 & -10 & 5 \\ 10 & 23 & -39 & 10 \end{pmatrix}$ е) $\begin{pmatrix} 68 & -20 & 40 & -1 \\ -17 & 10 & -20 & 9 \\ -51 & 22 & -44 & 13 \end{pmatrix}$ ж) $\begin{pmatrix} 76 & -95 & 57 & 19 & -19 \\ 26 & -6 & -10 & -4 & 12 \\ 37 & -86 & 72 & 25 & -37 \end{pmatrix}$.

Задача 10.2. Выясните, отщепляется ли решётка, порождённая столбцами матрицы

а) $\begin{pmatrix} 107 & 60 & 19 & -13 \\ -50 & -28 & -9 & 6 \\ -7 & -4 & -1 & 1 \end{pmatrix}$ б) $\begin{pmatrix} 466 & -170 & -96 & -81 \\ -164 & 60 & 34 & 29 \\ 252 & -92 & -52 & -44 \end{pmatrix}$.

в) $\begin{pmatrix} 146 & -34 & -50 & -15 \\ 22 & -6 & -6 & -1 \\ -41 & 9 & 15 & 5 \end{pmatrix}$ г) $\begin{pmatrix} -32 & 679 & 413 & 78 \\ -18 & 383 & 233 & 44 \\ 4 & -87 & -53 & -10 \end{pmatrix}$.

прямым слагаемым в $\mathbb{Z}^3$, и если да, укажите какую-нибудь дополнительную решётку.

Задача 10.3. Пусть конечно порождённые модули A, B, C над областью главных идеалов таковы, что $A \oplus C \simeq B \oplus C$. Покажите, что $A \simeq B$.

Задача 10.4. Напишите жорданово представление[1] аддитивных абелевых групп

а) $\mathbb{Z}/(6)$, $\mathbb{Z}/(12)$, $\mathbb{Z}/(24)$ и $\mathbb{Z}/(60)$ б) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(15), \mathbb{Z}/(48)\big)$ и $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(81), \mathbb{Z}/(9)\big)$

в) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(12) \oplus \mathbb{Z}(16), \mathbb{Z}/(24)\big)$ г) $\mathrm{Hom}_{\mathbb{Z}}\big(\mathbb{Z}/(6) \oplus \mathbb{Z}/(15), \mathbb{Z}/(20) \oplus \mathbb{Z}/(12)\big)$

Задача 10.5. Изоморфны ли абелевы группы $\mathbb{Z}/(6) \oplus \mathbb{Z}/(36)$ и $\mathbb{Z}/(12) \oplus \mathbb{Z}/(18)$?

Задача 10.6. Сколько подгрупп порядков 2 и 6 в нециклической абелевой группе порядка 12?

Задача 10.7. Есть ли в абелевой группе $\mathbb{Z}/(12) \oplus \mathbb{Z}/(81)$ подгруппа, изоморфная а) $\mathbb{Z}/(6) \oplus \mathbb{Z}/(6)$ б) $\mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$ в) $\mathbb{Z}/(9) \oplus \mathbb{Z}/(9)$ г) $\mathbb{Z}/(3) \oplus \mathbb{Z}/(27)$ д) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(9) \oplus \mathbb{Z}/(18)$?

[1] См. формулу (??) на стр. ??.

Задача 10.8. Напишите жорданово представление всех абелевых групп порядков
а) 4 б) 6 в) 8 г) 12 д) 16 е) 24 ж) 36 з) 48.

Задача 10.9. Обозначим через $g(A)$ минимальное число порождающих абелевой группы A. Найдите $\max g(A)$ по всем абелевым группам A порядка 315000, укажите, на скольких группах он достигается, и приведите пример такой группы.

Задача 10.10. Напишите жорданово представление фактора решётки $\mathbb{Z}^3$ по подрешётке, порождённой векторами: а) $(7,2,3)$, $(21,8,9)$, $(5,-4,3)$ б) $(2,-4,6)$, $(6,-6,10)$, $(2,5,8)$, $(6,0,5)$
в) $(4,5,3)$, $(5,6,5)$, $(8,7,9)$ г) $(-81,-6,-33)$, $(60,6,24)$, $(-3,6,-3)$, $(18,6,6)$
д) $(-62,-8,-26)$, $(40,10,16)$, $(22,-8,10)$, $(20,2,8)$.

Задача 10.11. Напишите жорданово представление фактора решётки $\mathbb{Z}^4$ по подрешётке, порождённой столбцами матрицы

а) $\begin{pmatrix} -2 & 87 & -86 \\ 41 & -51 & 69 \\ 32 & -69 & 81 \\ 24 & -71 & 80 \end{pmatrix}$ б) $\begin{pmatrix} 29 & 22 & -17 \\ 50 & 7 & -19 \\ -83 & -28 & 37 \\ -53 & -16 & 23 \end{pmatrix}$ в) $\begin{pmatrix} -45 & -72 & 19 & 14 \\ 1 & 16 & 15 & 4 \\ 9 & 18 & 3 & 0 \\ 8 & 26 & 8 & 0 \end{pmatrix}$ г) $\begin{pmatrix} 76 & 60 & -34 & -2 \\ 100 & 78 & -42 & -6 \\ -28 & -24 & 10 & 2 \\ 86 & 66 & -36 & -6 \end{pmatrix}$

д) $\begin{pmatrix} -31 & -52 & -47 & 13 & 11 \\ -7 & -4 & -5 & 1 & 1 \\ -62 & 66 & 24 & -6 & -10 \\ -100 & 10 & -28 & 8 & 2 \end{pmatrix}$ е) $\begin{pmatrix} 36 & 20 & -12 & -16 & 20 \\ 18 & 10 & -6 & -8 & 10 \\ 24 & 56 & -12 & -16 & 32 \\ -6 & -46 & 6 & 8 & -22 \end{pmatrix}$.

Задача 10.12. Напишите жорданово представление фактора решётки $\mathbb{Z}^3$ по подрешётке, задаваемой уравнениями:

а) $\begin{cases} 686x_1 - 240x_2 + 122x_3 = 0 \\ 65x_1 - 24x_2 + 11x_3 = 0 \\ -159x_1 + 54x_2 - 29x_3 = 0 \\ -17x_1 + 6x_2 - 3x_3 = 0 \end{cases}$ б) $\begin{cases} -143x_1 - 40x_2 + 36x_3 = 0 \\ -24x_1 - 6x_2 + 9x_3 = 0 \\ 48x_1 + 15x_2 - 6x_3 = 0 \end{cases}$

в) $\begin{cases} 140x_1 - 175x_2 + 42x_3 = 0 \\ 43x_1 - 54x_2 + 13x_3 = 0 \end{cases}$.

Задача 10.13. В абелевой группе, порождённой элементами a_1, a_2, a_3, найдите порядок элемента
а) $a_1 + 2a_3$, если $a_1 + a_2 + 4a_3 = 2a_1 - a_2 + 2a_3 = 0$
б) $32a_1 + 31a_3$, если $2a_1 + a_2 - 50a_3 = 4a_1 + 5a_2 + 60a_3 = 0$.

Задача 10.14. Напишите жорданово представление для фактора группы $A = \mathbb{Z}/(9) \oplus \mathbb{Z}/(27)$ по подгруппе, порождённой элементами: а) $\big([3]_9, [9]_{27}\big)$ б) $\big([3]_9, [6]_{27}\big)$ в) $\big([6]_9, [3]_{27}\big)$.

Задача 10.15. Пусть порядки[1] конечных подгрупп $A_1, \ldots, A_n$ абелевой группы A попарно взаимно просты. Докажите ли, что их сумма в A является прямой.

Задача 10.16. Пусть $n = 2^\mu p_1^{\nu_1} \ldots p_m^{\nu_m}$, где все $p_i > 2$ просты и попарно различны. Докажите, что:
а) $(\mathbb{Z}/(n))^\times = \big(\mathbb{Z}/(2^\mu)\big)^\times \times \big(\mathbb{Z}/(p_1^{\nu_1})\big)^\times \times \ldots \times \big(\mathbb{Z}/(p_m^{\nu_m})\big)^\times$
б*) все группы $\big(\mathbb{Z}/(p_i^{\nu_i})\big)^\times$ циклические порядка $p_i^{\nu_i} - p_i^{\nu_i - 1}$
в*) $(\mathbb{Z}/(4))^\times \simeq \mathbb{Z}/(2)$ и $\big(\mathbb{Z}/(2^\mu)\big)^\times \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2^{\mu-2})$ при $\mu > 2$.

Задача 10.17. Верно ли, что для любого натурального m, делящего порядок конечной абелевой группы, в этой группе найдётся подгруппа порядка m?

[1] *Порядком* конечной группы называется количество элементов в ней.

Задача 10.18. Пусть для любого $m \in \mathbb{N}$ число элементов порядка m в двух конечных абелевых группах A и B одинаково. Докажите, что $A \simeq B$.

Задача 10.19. Для каждого $\mathbb{Z}$-модуля M положим $M^* \stackrel{\text{def}}{=} \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$.

а) Приведите пример ненулевого $\mathbb{Z}$-модуля M с $M^* = 0$.

б) Для каждого гомоморфизма $\varphi : M \to N$ постройте гомоморфизм $\varphi^* : N^* \to M^*$. Верно ли, что: (1) если φ сюръективен, то φ^* инъективен? (2) если φ инъективен, то φ^* сюръективен?

в) Пусть конечно порождённый $\mathbb{Z}$-модуль N свободен, и его подмодуль $L \subset N$ таков, что фактор N/L конечен. Покажите, что L^* свободен и конечно порождён, $N^* \subset L^*$ является его подмодулем, а фактор L^*/N^* конечен, и имеются канонические изоморфизмы:

$$\operatorname{Hom}_{\mathbb{Z}}(N/L, \mathbb{Q}/\mathbb{Z}) \simeq \{\varphi \in \operatorname{Hom}_{\mathbb{Z}}(N, \mathbb{Q}) \mid \varphi(L) \subset \mathbb{Z}\}/N^* \simeq L^*/N^* .$$

Задача 10.20. Опишите с точностью до изоморфизма[1] все пары (A, f), где A — конечная аддитивная абелева группа, а $f \in \operatorname{End} A$ имеет $f^2 = -\mathrm{Id}_A$.

Задача 10.21. Классифицируйте все конечно порождённые модули над кольцом $\mathbb{C}[\varepsilon]/(\varepsilon^2)$.

Задача 10.22 (диаграмный поиск). Цепочка гомоморфизмов абелевых групп $\ldots \xrightarrow{\alpha} C \xrightarrow{\beta} \ldots$ называется *точной* в C, если $\ker\beta = \operatorname{im}\alpha$. Фактор группа $\operatorname{coker}\alpha \stackrel{\text{def}}{=} C/\operatorname{im}\alpha$ называется *коядром* стрелки α. Точность диаграммы

$$0 \to A \xrightarrow{\alpha} C \xrightarrow{\beta} B \to 0 \tag{10-13}$$

означает, что $A = \ker\beta$ и $B = \operatorname{coker}\alpha$. Такие диаграммы называются *точными тройками*. Диаграмма гомоморфизмов абелевых групп называется *коммутативной*, если для любых групп A, B в ней композиция стрелок, ведущих из A в B, зависит только от A и B, но не от пути, вдоль которого вычисляется композиция.

а) Для абелевой группы X и гомоморфизма абелевых групп $\varphi : A \to B$ положим

$$\varphi_* : \operatorname{Hom}(X, A) \to \operatorname{Hom}(X, B),\ \alpha \mapsto \varphi\alpha,$$
$$\varphi^* : \operatorname{Hom}(B, X) \to \operatorname{Hom}(A, X),\ \beta \mapsto \beta\varphi.$$

Убедитесь, что $(\varphi\psi)_* = \varphi_*\psi_*$, а $(\varphi\psi)^* = \psi^*\varphi^*$, и покажите, что если тройка (10-13) точна, то последовательности

$$0 \to \operatorname{Hom}(X, A) \xrightarrow{\alpha_*} \operatorname{Hom}(X, C) \xrightarrow{\beta_*} \operatorname{Hom}(X, B) \tag{10-14}$$
$$0 \to \operatorname{Hom}(B, X) \xrightarrow{\beta^*} \operatorname{Hom}(C, X) \xrightarrow{\alpha^*} \operatorname{Hom}(A, X)$$

тоже точны, причём самые правые стрелки в них не обязательно сюръективны.

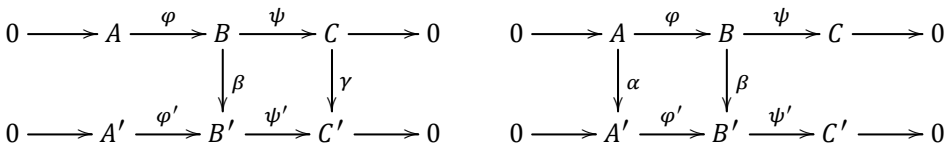
б) Покажите, что если для любой абелевой группы X последовательность (10-14) точна и правая стрелка в ней сюръективна, то тройка (10-13), из которой она получается, тоже точна.

в) Постройте для любой композиции гомоморфизмов $\beta\alpha$ точную последовательность

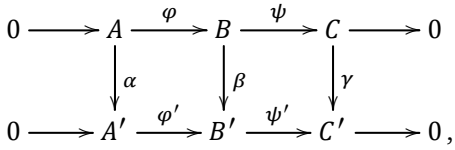
$$0 \to \ker\alpha \to \ker\beta\alpha \to \ker\beta \to \operatorname{coker}\alpha \to \operatorname{coker}\beta\alpha \to \operatorname{coker}\beta \to 0 .$$

[1] Пары (A, f) и (B, g) называются изоморфными, если существует такой изоморфизм абелевых групп $h : A \xrightarrow{\sim} B$, что $g = hfh^{-1}$.

г) (лемма о змее) Покажите, что коммутативные диаграммы с точными строками



однозначно достраиваются до коммутативной диаграммы

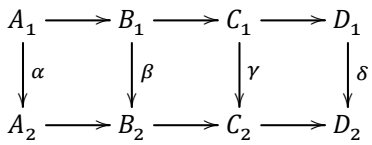


постройте гомоморфизм $\delta\colon\ \ker\gamma \to \operatorname{coker}\alpha$, включающийся в точную последовательность

$$0\longrightarrow\ker\alpha\xrightarrow{\varphi}\ker\beta\xrightarrow{\psi}\ker\gamma\xrightarrow{\delta}\operatorname{coker}\alpha\xrightarrow{[\varphi']}\operatorname{coker}\beta\xrightarrow{[\psi']}\operatorname{coker}\gamma\longrightarrow 0\,,$$

и выясните, влечёт ли обратимость стрелки β инъективность α и сюръективность γ, а обратимость стрелок α и γ — обратимость β.

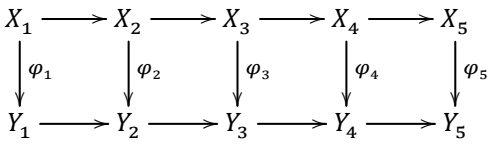
д) Для коммутативной диаграммы с точными строками



постройте точные в среднем члене последовательности:

$$\ker\beta \to \ker\gamma \to \ker\delta\,, \quad \text{если } \operatorname{coker}\alpha = 0$$
$$\operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma\,, \quad \text{если } \ker\delta = 0$$

е) (лемма о пяти гомоморфизмах) Пусть в коммутативной диаграмме



строки точны, φ_1 сюръективен, φ_5 инъективен, а φ_2 и φ_4 обратимы. Покажите, что φ_3 тоже обратим.

§11. Грассмановы многочлены и определители

11.1. Длина, знак и чётность перестановки. Биективные отображения

$$g\colon \{1,\dots,n\} \to \{1,\dots,n\}, \quad i \mapsto g_i,$$

называются *перестановками n элементов*. Перестановки образуют группу преобразований множества $\{1,\dots,n\}$ в смысле прим. 1.7 на стр. 16. Эта группа обозначается $S_n = \mathrm{Aut}\big(\{1,\dots,n\}\big)$ и называется *n-той симметрической группой*. Перестановку $g \in S_n$ принято записывать словом

$$g = (g_1,\dots,g_n),$$

i-тая буква которого равна значению $g_i = g(i)$ отображения g на элементе i. Например, слово

$$(2,4,3,5,1) \in S_5$$

задаёт отображение $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 5$, $5 \mapsto 1$. Композиция fg перестановок f, g действует по правилу $fg\colon i \mapsto f\big(g(i)\big)$. Например, в группе S_5 две возможных композиции перестановок $f = (2,4,3,5,1)$ и $g = (3,2,1,5,4)$ суть $fg = (3,4,2,1,5)$ и $gf = (2,5,1,4,3)$.

Назовём пару возрастающих чисел $i < j$ *инверсной* для перестановки g, если $g_i > g_j$. Таким образом, каждая перестановка $g \in S_n$ разбивает множество всех $n(n-1)/2$ возрастающих пар $1 \leqslant i < j \leqslant n$ на два непересекающихся подмножества — инверсные пары и неинверсные пары. Количество инверсных пар перестановки g называется *числом инверсий* или *длиной* перестановки g и обозначается $\ell(g)$.

Упражнение 11.1. Найдите $\max \ell(g)$ по всем $g \in S_n$ и укажите все перестановки на которых он достигается.

Число $\mathrm{sgn}(g) \stackrel{\text{def}}{=} (-1)^{\ell(g)}$ называется *знаком* перестановки g. Перестановка g называется *чётной*, если $\mathrm{sgn}(g) = 1$ и *нечётной*, если $\mathrm{sgn}(g) = -1$.

Перестановка, меняющая местами какие-либо два элемента i, j и оставляющая все остальные элементы на месте, обозначается σ_{ij} и называется *транспозицией* i-го и j-го элементов.

Упражнение 11.2. Убедитесь, что каждая перестановка $g \in S_n$ является композицией транспозиций.

Разложение перестановки в композицию транспозиций не единственно: например, транспозицию $\sigma_{13} = (3,2,1) \in S_3$ иначе можно записать как $\sigma_{12}\sigma_{23}\sigma_{12}$ или как $\sigma_{23}\sigma_{12}\sigma_{23}$. Тем не менее чётность количества транспозиций, в композицию которых раскладывается данная перестановка g, не зависит от способа разложения и совпадает с чётностью числа инверсных пар перестановки g, т. е. все чётные перестановки являются композициями чётного числа транспозиций, а нечётные — нечётного. Это вытекает из следующей леммы.

Лемма 11.1
$\mathrm{sgn}(g\sigma_{ij}) = -\mathrm{sgn}(g)$ для любой перестановки $g \in S_n$ и любой транспозиции $\sigma_{ij} \in S_n$.

Доказательство. Перестановки

$$\begin{aligned} g &= \big(g_1,\dots,g_{i-1},\, \boldsymbol{g_i},\, g_{i+1},\dots,g_{i-1},\, \boldsymbol{g_j},\, g_{j+1},\dots,g_n\big) \\ g\sigma_{ij} &= \big(g_1,\dots,g_{i-1},\, \boldsymbol{g_j},\, g_{i+1},\dots,g_{i-1},\, \boldsymbol{g_i},\, g_{j+1},\dots,g_n\big) \end{aligned} \tag{11-1}$$

отличаются друг от друга транспозицией элементов g_i и g_j, стоящих на i-том и j-том местах перестановки g. В этих двух перестановках пара (i, j), а также $2(j-i-1)$ пар вида (i, m) и (m, j) с произвольным m из промежутка $i < m < j$ имеют противоположную инверсность, а инверсность всех остальных пар одинакова. □

Следствие 11.1
Если перестановка g является композицией m транспозиций, то $\operatorname{sgn}(g) = (-1)^m$ и чётность перестановки совпадает с чётностью числа m.

Доказательство. Тождественная перестановка не имеет инверсных пар и, стало быть, чётна. В силу леммы, перестановка получающаяся из тождественной умножением на m транспозиций, имеет чётность $(-1)^m$. □

Следствие 11.2 (знаковый гомоморфизм)
Отображение $\operatorname{sgn}: S_n \twoheadrightarrow \{+1, -1\}$, $g \mapsto (-1)^{\ell(g)}$, является мультипликативным гомоморфизмом, т. е. $\operatorname{sgn}(gh) = \operatorname{sgn}(g)\operatorname{sgn}(h)$ для всех $g, h \in S_n$, и множества чётных и нечётных перестановок суть полные прообразы элементов 1 и -1 при этом гомоморфизме. □

Пример 11.1 (правило ниточек)
Напишем исходные числа и их перестановку друг под другом, как на рис. 11⋄1, и соединим одинаковые числа нитями так, чтобы ни одна из нитей не вылезала за пределы прямоугольника, образованного четырьмя угловыми числами, и чтобы все точки пересечения нитей были простыми двойными[1]. Тогда чётность числа инверсных пар будет равна чётности числа точек пересечения нитей.

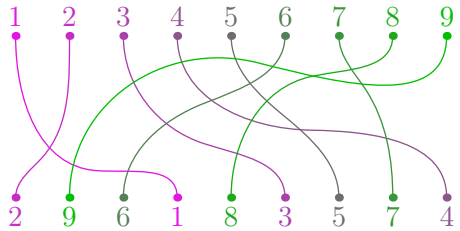


Рис. 11⋄1. $\operatorname{sgn}(2, 9, 6, 1, 8, 3, 5, 7, 4) = +1$ (всего 18 пересечений).

Упражнение 11.3. Докажите это и убедитесь при помощи правила ниточек, что знак *тасующей перестановки* $(i_1, \dots, i_k, j_1, \dots, j_m)$, где оба набора номеров $i_1, \dots, i_k$ и $j_1, \dots, j_m$ возрастают слева направо, равен $\operatorname{sgn}(i_1, \dots, i_k, j_1, \dots, j_m) = (-1)^{|I|+k(k+1)/2}$, где $|I| \stackrel{\text{def}}{=} i_1 + \dots + i_k$.

11.2. Определитель. Рассмотрим квадратную матрицу $C = (c_{ij}) \in \operatorname{Mat}_n(K)$ с элементами из произвольного коммутативного кольца K с единицей и обозначим через $v_1, \dots, v_n \in K^n$ её столбцы. Многочлен

$$\det C = \det(v_1, \dots, v_n) \stackrel{\text{def}}{=} \sum\nolimits_{g \in S_n} \operatorname{sgn}(g) \cdot c_{g_1 1} c_{g_2 2} \dots c_{g_n n} \tag{11-2}$$

называется *определителем* матрицы C или набора векторов $v_1, \dots, v_n$. Формула (11-2) предписывает всеми возможными способами выбирать в матрице n элементов так, чтобы в каждой

[1] Это означает, что в каждой точке пересечения встречается ровно две нити, причём пересечение происходит трансверсально:), а не по касательной:).

строке и в каждом столбце выбирался ровно один элемент. Каждые такие n элементов надо перемножить, а полученные $n!$ произведений сложить с надлежащими знаками, определяемыми так: множество клеток, где стоят выбранные n элементов, представляет собою график биективного отображения $j \mapsto g_j$ из множества номеров столбцов в множество номеров строк, т. е. перестановки n номеров $\{1, \dots, n\}$, и знак равен знаку этой перестановки. Например, определители матриц размеров 2×2 и 3×3 имеют вид

$$\det \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = c_{11}c_{22} - c_{12}c_{21} \tag{11-3}$$

$$\det \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = c_{11}c_{22}c_{33} + c_{13}c_{21}c_{32} + c_{12}c_{23}c_{31} - \\ - c_{11}c_{23}c_{32} - c_{13}c_{22}c_{31} - c_{12}c_{21}c_{33} \tag{11-4}$$

(во втором равенстве сначала выписаны тождественная и две циклических перестановки, потом — три транспозиции).

Предложение 11.1
Определитель $\det C = \det(v_1, \dots, v_n)$ линеен по каждому столбцу v_i матрицы C, кососимметричен (т. е. $\det(v_1, \dots, v_n) = 0$ если $v_i = v_j$ для некоторых $i \neq j$) и не меняется при транспонировании матрицы[1] (т. е. $\det C^t = \det C$, где $C^t = \left(c^t_{ij}\right)$ имеет $c^t_{ij} = c_{ji}$).

Доказательство. Так как каждое из $n!$ произведений, которые складываются в формуле (11-2), содержит ровно по одному сомножителю из каждого столбца, оно линейно по каждому столбцу, а значит линейна и их сумма. Если i-тый столбец матрицы C совпадает с j-тым, то $c_{g_i i} = c_{g_i j}$ и $c_{g_j j} = c_{g_j i}$ для любой перестановки $g \in S_n$. Множество всех перестановок разбиваются на не пересекающиеся пары вида $(g, g\sigma_{ij})$, поскольку композиция с транспозицией $\sigma_{ij} \colon S_n \xrightarrow{\sim} S_n$, $g \mapsto g\sigma_{ij}$, является инволютивной[2] биекцией без неподвижных точек[3]. В сумме (11-2) слагаемые, отвечающие каждой паре g и $g\sigma_{ij}$ имеют вид

$$\operatorname{sgn}(g) \cdot c_{g_1 1} \dots c_{g_i i} \dots c_{g_j j} \dots c_{g_n n} \quad \text{и} \quad \operatorname{sgn}(g\sigma_{ij}) \cdot c_{g_1 1} \dots c_{g_j i} \dots c_{g_i j} \dots c_{g_n n}$$

и различаются только знаком, сокращая друг друга. Поэтому сумма получится нулевая. Наконец, равенство $\det C^t = \det C$ вытекает из того, что набор произведений n-ок матричных элементов в разложениях $\det C$ и $\det C^t$ одинаков, а знаки, с которыми каждое произведение входит в $\det C$ и $\det C^t$, суть знаки обратных друг другу перестановок.

Упражнение 11.4. Покажите, что знаки обратных друг другу перестановок совпадают.

Тем самым, разложения (11-2) для $\det C$ и $\det C^t$ состоят из одних и тех же слагаемых с одними и теми же знаками. □

Следствие 11.3
Определитель является полилинейной кососимметричной функцией от строк матрицы. □

Следствие 11.4
Определитель меняет знак при любой транспозиции строк или столбцов матрицы[4].

[1] См. обсуждение перед предл. 8.1 на стр. 138.
[2] Т. е. обратной самой себе.
[3] Равенство $g = g\sigma_{ij}$ невозможно, так как умножая на g^{-1} слева, получаем $\mathrm{Id} = \sigma_{ij}$, что не так.
[4] Функции с таким свойством называются *знакопеременными*.

Доказательство. В силу кососимметричности и полилинейности

$$0 = \det(\dots, (v_i + v_j), \dots, (v_i + v_j), \dots) = \det(\dots, v_i, \dots, v_j, \dots) + \det(\dots, v_j, \dots, v_i, \dots),$$

что и утверждается. □

Упражнение 11.5. Убедитесь, что если $1 + 1 \neq 0$ в K, то каждая знакопеременная функция от n векторов кососимметрична.

Пример 11.2 (знакопеременные многочлены, определитель Вандермонда и базис Шура) Многочлен $f \in \mathbb{Z}[x_1, \dots, x_n]$ называется *знакопеременным* если для всех перестановок $g \in S^n$

$$f(x_{g_1}, \dots, x_{g_n}) = \operatorname{sgn}(g) \cdot f(x_1, \dots, x_n).$$

Так как при транспозиции любой пары переменных знакопеременный многочлен f меняет знак, в каждом мономе $x_1^{\nu_1} \dots x_n^{\nu_n}$ многочлена f все степени ν_i попарно различны, и вместе с таким мономом в f входят $n!$ мономов $x_{g_1}^{\nu_1} \dots x_{g_n}^{\nu_n}$, где $g \in S_n$, причём коэффициенты при мономах $x_1^{\nu_1} \dots x_n^{\nu_n}$ и $x_{g_1}^{\nu_1} \dots x_{g_n}^{\nu_n}$ получаются друг из друга умножением на знак $\operatorname{sgn}(g)$. Мы заключаем, что знакопеременные многочлены образуют свободный $\mathbb{Z}$ модуль с базисом из многочленов

$$\Delta_\nu \stackrel{\text{def}}{=} \sum_{g \in S_n} \operatorname{sgn}(g)\, x_{g_1}^{\nu_1} \dots x_{g_n}^{\nu_n} = \det(x_j^{\nu_i}) = \det \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix}, \tag{11-5}$$

которые нумеруются диаграммами Юнга ν из n строк попарно разных длин $\nu_1 > \dots > \nu_n \geqslant 0$. Минимальной такой диаграмме $\delta = \big((n-1), \dots, 0\big)$ отвечает *определитель Вандермонда*

$$\Delta_\delta = \det(x_j^{n-i}) = \det \begin{pmatrix} x_1^{n-1} & \dots & x_n^{n-1} \\ \vdots & \vdots & \vdots \\ x_1 & \dots & x_n \\ 1 & \dots & 1 \end{pmatrix} = \prod_{i<j} (x_i - x_j). \tag{11-6}$$

Последнее равенство вытекает из того, что при подстановке $x_i = x_j$ с $j \neq i$ определитель Вандермонда, как и всякий знакопеременный многочлен, обращается в нуль, и поэтому делится в $\mathbb{Z}[x_1, \dots, x_n]$ на $x_i - x_j$. Так все такие разности неприводимы, а кольцо $\mathbb{Z}[x_1, \dots, x_n]$ факториально, определитель Вандермонда делится на $\prod_{i<j}(x_i - x_j)$, а поскольку лексикографически старшие мономы определителя и произведения равны $x_1^{n-1} x_2^{n-2} \dots x_{n-1}$ и имеют коэффициент 1, частное от деления равно 1. Это рассуждение показывает, что любой знакопеременный многочлен f делится в $\mathbb{Z}[x_1, \dots, x_n]$ на определитель Вандермонда, и частное является симметрическим многочленом. Мы заключаем, что знакопеременные многочлены образуют свободный модуль ранга 1 с базисом Δ_δ над кольцом симметрических многочленов, а симметрические *многочлены Шура* $\sigma_\lambda = \Delta_{\lambda+\delta}/\Delta_\delta$, где $\lambda = (\lambda_1, \dots, \lambda_n)$ пробегает произвольные диаграммы Юнга из n строк, а $\lambda + \delta = (\lambda_1 + (n-1), \lambda_2 + (n-2), \dots, \lambda_n)$, образуют базис $\mathbb{Z}$-модуля симметрических многочленов.

11.3. Грассмановы многочлены. Алгебра *грассмановых многочленов* $K\langle\xi_1,\dots,\xi_n\rangle$ от переменных $\xi_1,\dots,\xi_n$ с коэффициентами в произвольном коммутативном кольце K с единицей определяется точно также, как алгебра обычных многочленов, но только грассмановы переменные ξ_i, в отличие от обычных, не коммутируют, а *антикоммутируют* друг с другом, т. е. подчиняются соотношениям[1]

$$\forall\, i,j \quad \xi_i\wedge\xi_j = -\xi_j\wedge\xi_i \quad \text{и} \quad \forall\, i \quad \xi_i\wedge\xi_i = 0\,. \tag{11-7}$$

Символ «$\wedge$» здесь и далее используется для обозначения грассманова (антикоммутативного) умножения, чтобы отличать его от обычного (коммутативного). Константы из K по определению перестановочны с грассмановыми переменными, и умножение переменных на константы записывается обычным образом: $a\xi_i = \xi_i a$, для всех i и всех $a\in K$. Для каждой строго возрастающей слева направо последовательности номеров $I=(i_1,\dots,i_m)$, где $i_1<\dots<i_m$, положим

$$\xi_I \stackrel{\text{def}}{=} \xi_{i_1}\wedge\dots\wedge\xi_{i_m}\,. \tag{11-8}$$

Каждая перестановка $g=(g_1,\dots,g_m)\in S_m$ переменных в этом мономе меняет его знак по правилу

$$\xi_{i_{g(1)}}\wedge\dots\wedge\xi_{i_{g(m)}} = \operatorname{sgn}(g)\cdot\xi_{i_1}\wedge\dots\wedge\xi_{i_m}\,. \tag{11-9}$$

Поскольку квадраты грассмановых переменных равны нулю, мономы (11-9) исчерпывают всё множество грассмановых мономов, т. е. однородные грассмановы многочлены степени m от n переменных $\xi_1,\dots,\xi_n$ по-определению образуют свободный K-модуль ранга $\binom{n}{m}$ с базисом из мономов (11-8). Этот модуль обозначается Λ^m. Вся грассманова алгебра как модуль над K является конечной прямой суммой $K\langle\xi_1,\dots,\xi_n\rangle = \Lambda^0\oplus\Lambda^1\oplus\Lambda^2\oplus\dots\oplus\Lambda^n$, где младшее слагаемое $\Lambda^0\simeq K$ состоит из констант и имеет в качестве базиса моном $\xi_\varnothing\stackrel{\text{def}}{=}1$, отвечающий пустому набору $I=\varnothing$ и служащий единицей грассмановой алгебры, а старшее слагаемое $\Lambda^0\simeq K$ имеет в качестве базиса $\xi_{(1,\dots,n)}=\xi_1\wedge\dots\wedge\xi_n$ — единственный моном степени n, отвечающий набору $I=(1,\dots,n)$. Обратите внимание, что этот моном аннулируется умножением на любой грассманов многочлен с нулевым свободным членом. Умножение базисных мономов $\xi_I=\xi_{i_1}\wedge\dots\wedge\xi_{i_k}$ и $\xi_J=\xi_{j_1}\wedge\dots\wedge\xi_{j_m}$ происходит по правилу

$$\xi_I\wedge\xi_J = \begin{cases}\operatorname{sgn}(I,J)\,\xi_{I\sqcup J} & \text{если } I\cap J=\varnothing\\ 0 & \text{если } I\cap J\neq\varnothing\,,\end{cases} \tag{11-10}$$

где $\operatorname{sgn}(I,J)$ — знак тасующей перестановки, упорядочивающей набор $(i_1,\dots,i_k,\,j_1,\dots,j_m)$ по возрастанию[2]. Так как для базисных грассмановых мономов выполняется равенство[3]

$$(\xi_{i_1}\wedge\dots\wedge\xi_{i_k})\wedge(\xi_{j_1}\wedge\dots\wedge\xi_{j_m}) = (-1)^{km}(\xi_{j_1}\wedge\dots\wedge\xi_{j_m})\wedge(\xi_{i_1}\wedge\dots\wedge\xi_{i_k})\,,$$

однородные грассмановы многочлены коммутируют друг с другом по правилу

$$\omega\wedge\eta = (-1)^{\deg\omega\deg\eta}\eta\wedge\omega\,, \tag{11-11}$$

[1] Если $1+1$ не делит нуль в K, то соотношения $\xi_i\wedge\xi_i=0$ могут быть опущены, поскольку они вытекают из соотношений $\xi_i\wedge\xi_j=-\xi_j\wedge\xi_i$, если положить в них $i=j$. Если же $-1=1$, то антикоммутирование $\xi_i\wedge\xi_j=-\xi_j\wedge\xi_i$ не отличается от коммутирования $\xi_i\wedge\xi_j=\xi_j\wedge\xi_i$, и в этой ситуации именно соотношение $\xi_i\wedge\xi_i=0$ отличает грассмановы переменные от обычных.

[2] Если $I\sqcup J=\{1,\dots,n\}$, то $\operatorname{sgn}(i_1,\dots,i_k,\,j_1,\dots,j_m)=(-1)^{|I|+k(k+1)/2}$ по упр. 11.3 на стр. 189.

[3] Для проноса каждой из m переменных ξ_j влево через k переменных ξ_i нужно совершить k транспозиций.

которое называется *кошулевым правилом знаков*. В частности, любой однородный многочлен чётной степени коммутирует со всеми грассмановыми многочленами.

Упражнение 11.6. Опишите *центр* грассмановой алгебры

$$Z(K\langle\xi_1,\dots,\xi_n\rangle) \stackrel{\text{def}}{=} \{\tau\in K\langle\xi_1,\dots,\xi_n\rangle \mid \forall\,\omega\in K\langle\xi_1,\dots,\xi_n\rangle\ \ \tau\wedge\omega=\omega\wedge\tau\}\,.$$

11.3.1. Грассманова алгебра свободного модуля. Обозначим через V свободный K-модуль ранга r. Если векторы $e_1,\dots,e_r\in V$ образуют базис модуля V, то алгебра грассмановых многочленов $K\langle e_1,\dots,e_r\rangle$ от переменных $e_1,\dots,e_r$ обозначается ΛV и называется *грассмановой* (или *внешней*) алгеброй свободного модуля V, а подмодуль однородных грассмановых многочленов степени d обозначается $\Lambda^d V\subset\Lambda V$ и называется d-й *внешней степенью* свободного модуля V. Эти не апеллирующие к выбору базиса названия и обозначения связаны с тем, что при каждом $d=0,1,\dots,n$ подмодуль $\Lambda^d=\Lambda^d V\subset K\langle e_1,\dots,e_r\rangle$ однородных многочленов степени d не зависит от выбора базиса в V. В самом деле, подмодуль констант $\Lambda^0 V\simeq K$ порождается единицей грассмановой алгебры, подмодуль $\Lambda^1 V$ однородных грассмановых многочленов степени 1, т. е. множество всевозможных K-линейных комбинаций базисных векторов $e_1,\dots,e_r$, канонически отождествляется с модулем V и тоже не зависит от выбора базиса, а для прочих d подмодуль $\Lambda^d V\subset K\langle e_1,\dots,e_r\rangle$ является линейной оболочкой всевозможных произведений $v_1\wedge\ldots\wedge v_d$, составленных из d произвольных векторов $v_i\in V$ и опять таки не зависит от выбора базиса. Таким образом, вся алгебра $\Lambda V=\bigoplus_{d=0}^n\Lambda^d V$ является прямой суммой модулей, не зависящих от выбора базиса в V.

Упражнение 11.7. Убедитесь, что $v\wedge v=0$ и $u\wedge w=-w\wedge u$ для всех $u,v,w\in V$.

11.3.2. Линейные замены переменных и миноры. Пусть в обозначениях их предыдущего раздела n однородных грассмановых линейных форм $\eta_1,\dots,\eta_n\in\Lambda^1 V$ линейно выражается через m однородных грассмановых форм $\xi_1,\dots,\xi_m\in\Lambda^1 V$ по формуле

$$(\eta_1,\dots,\eta_n)=(\xi_1,\dots,\xi_m)\cdot C\,,$$

где $C\in\mathrm{Mat}_{n\times k}(K)$. Тогда при каждом $d=1,\dots,\min(m,n)$ набор мономов $\eta_J=\eta_{j_1}\wedge\ldots\wedge\eta_{j_d}$ степени d линейно выражается через набор мономов $\xi_I=\xi_{i_1}\wedge\ldots\wedge\xi_{i_d}$ степени d по формуле

$$\begin{aligned}\eta_J=\eta_{j_1}\wedge\ldots\wedge\eta_{j_d}&=\Big(\sum_{i_1}\xi_{i_1}c_{i_1j_1}\Big)\wedge\Big(\sum_{i_2}\xi_{i_2}c_{i_2j_2}\Big)\wedge\ldots\wedge\Big(\sum_{i_d}\xi_{i_d}c_{i_dj_d}\Big)=\\&=\sum_{1\leqslant i_1<\ldots<i_d\leqslant m}\xi_{i_1}\wedge\ldots\wedge\xi_{i_d}\cdot\sum_{g\in S_d}\operatorname{sgn}(g)\,c_{i_{g(1)}j_1}\ldots c_{i_{g(d)}j_d}=\sum_I\xi_I\cdot c_{IJ}\,,\end{aligned}\tag{11-12}$$

где $I=(i_1,\dots,i_d)$ пробегает наборы из d возрастающих номеров, а $c_{IJ}=\det C_{IJ}$ обозначает определитель $d\times d$-подматрицы $C_{IJ}\subset C$, сосредоточенной в пересечениях столбцов с номерами из J и строк с номерами из I. Определитель $c_{IJ}\stackrel{\text{def}}{=}\det C_{IJ}$ называется IJ-тым *минором* d-того порядка в матрице C. Таким образом, IJ-тый элемент матрицы, выражающей грассманов моном η_J через грассмановы мономы ξ_I равен IJ-тому минору d-того порядка в матрицы выражающей переменные η через переменные ξ. Матрица размера $\binom{n}{d}\times\binom{n}{d}$, клетки которой нумеруются лексикографически упорядоченными наборами I из d возрастающих номеров и которая имеет в клетке (IJ) минор c_{IJ} матрицы C, обозначается $\Lambda^d C$ и называется d-*й внешней степенью* матрицы C.

Предложение 11.2 (мультипликативность внешних степеней)
Для любых матриц $A \in \mathrm{Mat}_{m\times k}(K)$, $B \in \mathrm{Mat}_{k\times n}(K)$ над произвольным коммутативным кольцом K при всех $1 \leqslant d \leqslant \min(m,n,k)$ выполняется равенство $\Lambda^d(A\cdot B) = \Lambda^d A \cdot \Lambda^d B$. В частности, для квадратных матриц A и B одинакового размера $\det(AB) = \det(A)\det(B)$.

Доказательство. Рассмотрим в свободном K-модуле V с базисом $\boldsymbol{e} = (e_1,\dots,e_m)$ наборы векторов $\boldsymbol{a} = (a_1,\dots,a_k) = \boldsymbol{e}\,A$ и $\boldsymbol{b} = (b_1,\dots,b_n) = \boldsymbol{a}\,B = \boldsymbol{e}\,AB$. Обозначим через $\boldsymbol{e_d} \subset \Lambda^d V$ набор из $\binom{m}{d}$ грассмановых мономов $e_I = e_{i_1}\wedge\ldots\wedge e_{i_d}$, а через $\boldsymbol{b_d}, \boldsymbol{a_d} \subset \Lambda^d V$ — наборы из $\binom{n}{d}$ и $\binom{k}{d}$ грассмановых многочленов $b_J = b_{j_1}\wedge\ldots\wedge b_{j_d}$ и $a_L = a_{\ell_1}\wedge\ldots\wedge a_{\ell_d}$ соответственно. Набор мономов $\boldsymbol{e_d}$ является базисом в $\Lambda^d V$, а набор многочленов $\boldsymbol{b_d}$ выражается через него, с одной стороны, как $\boldsymbol{b_d} = \boldsymbol{e_d}\,\Lambda^d(AB)$, а с другой стороны — как $\boldsymbol{b_d} = \boldsymbol{a_d}\,\Lambda^d B = \boldsymbol{e_d}\,\Lambda^d A\,\Lambda^d B$. Поскольку матрица перехода от произвольного набора векторов к базису однозначно определяется этим набором, мы заключаем, что $\Lambda^d(A\cdot B) = \Lambda^d A\cdot\Lambda^d B$. □

Пример 11.3 (детерминантная формула для инвариантных множителей)
Из предл. 11.2 вытекает, что столбцы матрицы $\Lambda^k(AB)$ являются линейными комбинациями столбцов матрицы $\Lambda^k A$. Поэтому любое число $x \in K$, делящее все $k\times k$ миноры матрицы A, делит и все $k\times k$ миноры матрицы AB для любой матрицы B, на которую A можно умножить справа. Если матрица B обратима, то $A = (AB)B^{-1}$ получается из матрицы AB правым умножением на матрицу B^{-1}, и значит, число $x\in K$, делящее все $k\times k$ миноры матрицы AB, делит и все $k\times k$ миноры матрицы A. Мы заключаем, что наибольший общий делитель $k\times k$ миноров любой матрицы A не меняется при умножении матрицы A справа на обратимые матрицы. Аналогично проверяется, что наибольший общий делитель $k\times k$ миноров матрицы A не меняется при умножении матрицы A на обратимые матрицы слева. Обозначим наибольший общий делитель всех $k\times k$ миноров матрицы A через $\Delta_k(A)$.

Если кольцо K является областью главных идеалов, то по теор. 9.1 на стр. 150 для любой матрицы A найдутся такие обратимые матрицы L и R, что у матрицы $D_A = LAR$ все элементы d_{ij} с $i\neq j$ нулевые, и $d_{ii} \mid d_{jj}$ при $i<j$. Поскольку $\Delta_k(D_A) = d_{11}\ldots d_{kk}$ и $\Delta_k(A) = \Delta_k(D_A)$, мы заключаем, что $d_{ii} = \Delta_i(A)/\Delta_{i-1}(A)$, если $\Delta_{i-1}(A)\neq 0$, а если $\Delta_k(A) = 0$ при каком-то k, то $d_{jj} = 0$ при всех $j \geqslant k$. Это даёт новое доказательство независимости нормальной формы Смита[1] D_A и инвариантных множителей d_{ii} матрицы A от способа её приведения к нормальной форме Смита.

Пример 11.4 (дискриминант соизмеримой подрешётки и формула Пика)
Пусть $\mathbb{Z}$-подмодуль $U\subset\mathbb{Z}^n$ таков, что фактор $\mathbb{Z}^n/U$ конечен. Обозначим через $\boldsymbol{e}$ какой-нибудь базис в $\mathbb{Z}^n$, а через $\boldsymbol{u} = \boldsymbol{e}\,C_{\boldsymbol{eu}}$ — какой-нибудь базис в U. Абсолютная величина определителя матрицы $C_{\boldsymbol{eu}}$ называется *дискриминантом* соизмеримой[2] с $\mathbb{Z}^n$ подрешётки U и обозначается

$$D_U \stackrel{\text{def}}{=} |\det C_{\boldsymbol{eu}}|\,.$$

Упражнение 11.8. Покажите, что если матрица $C\in\mathrm{Mat}_n(K)$ обратима, то $\det C$ обратим в K.

Из упражнения вытекает, что дискриминант не зависит от выбора базисов $\boldsymbol{e}$ и $\boldsymbol{u}$, так как для любых других базисов $\boldsymbol{v} = \boldsymbol{e}\,C_{\boldsymbol{ev}}$ в $\mathbb{Z}^n$ и $\boldsymbol{w} = \boldsymbol{u}\,C_{\boldsymbol{uw}}$ в L матрицы переходов $C_{\boldsymbol{ve}} = C_{\boldsymbol{ev}}^{-1}$ и $C_{\boldsymbol{uw}}$, будучи обратимыми над $\mathbb{Z}$, имеют определители ±1, откуда

$$|\det C_{\boldsymbol{vw}}| = |\det(C_{\boldsymbol{ve}}C_{\boldsymbol{eu}}C_{\boldsymbol{uw}})| = |\det(C_{\boldsymbol{ve}})\,\det(C_{\boldsymbol{eu}})\,\det(C_{\boldsymbol{uw}})| = |\det C_{\boldsymbol{eu}}|\,.$$

[1] См. n° 9.1.1 на стр. 150.
[2] См. предл. 10.3 на стр. 183.

Беря качестве $\boldsymbol{e}$ и $\boldsymbol{u}$ взаимные базисы $v_1, \ldots, v_n$ и $\lambda_1 e_1, \ldots, \lambda_n e_n$, заключаем, что дискриминант $D_U = \lambda_1 \ldots \lambda_n$ равен числу элементов в факторе $\mathbb{Z}^n/U \simeq \mathbb{Z}/(\lambda_1) \oplus \ldots \oplus \mathbb{Z}/(\lambda_n)$.

На геометрическом языке[1] дискриминант D_U решётки $L \subset \mathbb{Z}^n \subset \mathbb{R}^n$ равен евклидову объёму[2] параллелепипеда Π, натянутого в пространстве $\mathbb{R}^n$ на какой-нибудь базис решётки U. Такой параллелепипед называется *фундаментальным параллелепипедом* решётки U. Его сдвиги на векторы решётки покрывают всё пространство $\mathbb{R}^n$, не имея при этом общих внутренних точек. Каждый элемент фактора $\mathbb{Z}^n/U$ представляется точкой, лежащей в Π. При этом каждая внутренняя точка Π не сравнима по модулю U ни с какими другими точками из Π, каждая внутренняя точка любой $(n-1)$-мерной гиперграни Π сравнима ещё ровно с одной точкой из Π, лежащей на параллельной гиперграни, каждая внутренняя точка любой $(n-2)$-мерной грани Π сравнима ровно с тремя точками из Π, лежащими на трёх параллельных $(n-2)$-мерных гранях, и т. д. Каждая вершина Π сравнима с остальными $2^n - 1$ вершинами. Мы заключаем, что объём Π, равный числу элементов в факторе $\mathbb{Z}^n/U$, может быть вычислен по *формуле Пика*:

$$\operatorname{Vol}\Pi = \sum\nolimits_{d=0}^{n} p_d / 2^{n-d},$$

где p_d при $d < n$ обозначает число точек, лежащих внутри d-мерных граней Π, а p_n — число внутренних точек самого Π.

11.3.3. Соотношения Лапласа. Для каждого набора из m возрастающих индексов

$$J = (j_1, \ldots, j_m) \subset \{1, \ldots, n\}$$

положим $\deg J \stackrel{\text{def}}{=} m$, $|J| \stackrel{\text{def}}{=} j_1 + \ldots + j_m$ и обозначим через $\bar{J} = (\bar{j}_1, \ldots, \bar{j}_{n-m}) = \{1, \ldots, n\} \smallsetminus J$ дополнительный к J набор из $n-m$ возрастающих индексов. Для произвольной квадратной матрицы $A = (a_{ij}) \in \operatorname{Mat}_n(K)$ рассмотрим в грассмановой алгебре $K\langle \xi_1, \ldots, \xi_n \rangle$ набор из n линейных форм

$$\alpha_j = \xi_1 a_{1j} + \xi_2 a_{2j} + \ldots + \xi_n a_{nj}, \quad \text{где} \quad 1 \leqslant j \leqslant r, \tag{11-13}$$

или, в матричных обозначениях, $(\alpha_1, \ldots, \alpha_n) = (\xi_1, \ldots, \xi_n)\, A$. Для двух наборов индексов I, J одинаковой длины $\deg I = \deg J = m$ произведения

$$\alpha_J = \alpha_{j_1} \wedge \ldots \wedge \alpha_{j_m} \quad \text{и} \quad \alpha_{\bar{I}} = \alpha_{\bar{i}_1} \wedge \ldots \wedge \alpha_{\bar{i}_{n-m}}$$

имеют дополнительные степени m и $n-m$. Перемножая их по формуле (11-10), получим[3]

$$\alpha_J \wedge \alpha_{\bar{I}} = \begin{cases} (-1)^{|J| + \frac{m(m+1)}{2}} \alpha_1 \wedge \ldots \wedge \alpha_n & \text{при } I = J \\ 0 & \text{при } I \neq J \end{cases} \tag{11-14}$$

Подставляя в равенство (11-14) разложения (11-13) и пользуясь формулами (11-12), в левой части равенства получим

$$\Big(\sum_M \xi_M a_{MJ}\Big) \wedge \Big(\sum_L \xi_L a_{L\bar{I}}\Big) = (-1)^{\frac{m(m+1)}{2}} \xi_1 \wedge \ldots \wedge \xi_n \sum_M (-1)^{|M|} a_{MJ} a_{\overline{MI}},$$

[1] См. лекцию http://video.bogomolov-lab.ru/gorod/ps/stud/geom_ru/2122/lec_08.pdf.

[2] См. раздел 1.2.1 на стр. 133 лекции
http://video.bogomolov-lab.ru/gorod/ps/stud/geom_ru/2122/lec_10.pdf.

[3] Знак соответствующей тасующей перестановки был вычислен в упр. 11.3 на стр. 189.

где M пробегает все индексы длины $\deg M = m$, а в правой части при $I \neq J$ по-прежнему будет 0, а при $I = J$ получится $(-1)^{\frac{m(m+1)}{2}+|J|} \det A \cdot \xi_1 \wedge \ldots \wedge \xi_n$. Мы заключаем, для любых двух наборов J, I из m столбцов произвольной квадратной матрицы $A \in \mathrm{Mat}_n(K)$ выполняются *соотношения Лапласа*

$$\sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MI}} = \begin{cases} \det A & \text{при } I = J, \\ 0 & \text{при } I \neq J, \end{cases} \tag{11-15}$$

где суммирование идёт по всем наборам M из m строк матрицы A.

При $I = J$ соотношение (11-15) даёт формулу для вычисления определителя $\det A$ через всевозможные миноры a_{MJ} порядка m, сосредоточенные в m фиксированных столбцах матрицы A с номерами J, и *дополнительные* к ним миноры $a_{\overline{JM}}$ порядка $n - m$, равные определителям матриц, получающихся из A вычёркиванием всех строк и столбцов, содержащих минор a_{MJ}:

$$\det A = \sum_M (-1)^{|M|+|J|} a_{MJ} a_{\overline{MJ}}\,. \tag{11-16}$$

Произведение $(-1)^{|M|+|J|} a_{\overline{MJ}}$ называется *алгебраическим дополнением* к минору a_{MJ}. При $I \neq J$ соотношение (11-15) с точностью до знака имеет вид

$$\sum_M (-1)^{|M|+|I|} a_{MJ} a_{\overline{MI}} = 0 \tag{11-17}$$

и называется *теоремой об умножении на чужие алгебраические дополнения*, поскольку левая часть в (11-17) отличается от (11-16) тем, что миноры a_{MJ} умножаются не на свои алгебраические дополнения, а на дополнения к сосредоточенным в другом наборе столбцов $I \neq J$ минорам a_{MI}.

Упражнение 11.9. Установите транспонированный вариант соотношений Лапласа

$$\sum_M (-1)^{|I|+|M|} a_{JM} a_{\overline{IM}} = \begin{cases} \det A & \text{при } I = J \\ 0 & \text{при } I \neq J. \end{cases} \tag{11-18}$$

Если обозначить через $\Lambda^m A^\vee$ матрицу размера $\binom{n}{m} \times \binom{n}{m}$, клетки которой, как и у матрицы $\Lambda^m A$, нумеруются m-элементными подмножествами $I, J \subset \{1, \ldots, n\}$, но в клетке (IJ) стоит *алгебраическое дополнение* к JI-минору[1] матрицы A, т. е. $(-1)^{|I|+|J|} a_{\overline{JI}}$, то все соотношения (11-15) и (11-18) можно свернуть в одно матричное равенство

$$\Lambda^m A \cdot \Lambda^m A^\vee = \Lambda^m A^\vee \cdot \Lambda^m A = \det(A) \cdot E\,, \tag{11-19}$$

где E — единичная матрицу размера $\binom{n}{d} \times \binom{n}{d}$. Матрица $\Lambda^m A^\vee$ называется *присоединённой* к матрице $\Lambda^m A$.

Пример 11.5 (соотношение Плюккера)
Рассмотрим 2×4 матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix}$$

[1] Обратите внимание, что индексы I и J преставились!

с элементами из кольца $K = \mathbb{Z}[a_{11}, \dots, a_{22}]$ многочленов от восьми переменных a_{ij} и обозначим через $A_{ij} = a_{1i}a_{2j} - a_{1j}a_{2i}$, где $1 \leqslant i < j \leqslant 4$, её 2×2 минор, образованный i-м и j-м столбцами. Раскладывая нулевой определитель

$$0 = \det \begin{pmatrix} A \\ A \end{pmatrix} = \det \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix}$$

по первым двум строкам, заключаем, что шесть миноров A_{ij} связаны *соотношением Плюккера*

$$A_{12}A_{34} - A_{13}A_{24} + A_{14}A_{23} = 0\,. \tag{11-20}$$

Упражнение 11.10. Убедитесь, для любого поля $\Bbbk$ и любых шести чисел $A_{ij} \in \Bbbk$, удовлетворяющих соотношению (11-20), существует матрица $A \in \mathrm{Mat}_{2\times 4}(\Bbbk)$ с 2×2 минорами A_{ij}.

Мы заключаем, что шесть чисел A_{ij} из поля $\Bbbk$ являются минорами 2×4 матрицы с элементами из $\Bbbk$ если и только если они удовлетворяют соотношению Плюккера (11-20).

Пример 11.6 (определитель пучка матриц)
Рассмотрим квадратные матрицы $A, B \in \mathrm{Mat}_n(K)$ и пару коммутирующих переменных x, y. Матрица $x\,A + y\,B$ имеет элементы в $K[x, y]$, и её определитель $\det(x\,A + y\,B)$ является однородным многочленом степени n от x и y. Покажем, что его коэффициент при $x^m y^{n-m}$ равен

$$\mathrm{tr}(\Lambda^m A \cdot \Lambda^m B^\vee) = \sum\nolimits_{IJ} (-1)^{|I|+|J|} a_{IJ} b_{\overline{IJ}}\,, \tag{11-21}$$

где суммирование идёт по всем m-элементным подмножествам $I, J \subset \{1, \dots, n\}$. Для этого рассмотрим наборы линейных форм $(\alpha_1, \dots, \alpha_n) = (\xi_1, \dots, \xi_n)\,A$ и $(\beta_1, \dots, \beta_n) = (\xi_1, \dots, \xi_n)\,B$ от грассмановых переменных $\xi_1, \dots, \xi_n$. Тогда

$$\det(xA + yB) \cdot \xi_1 \wedge \ldots \wedge \xi_n = (x\alpha_1 + y\beta_1) \wedge (x\alpha_2 + y\beta_2) \wedge \ \ldots \ \wedge (x\alpha_n + y\beta_n)\,.$$

Моном $x^m y^{n-m}$ возникает при выборе первого слагаемого в каких-либо m скобках, скажем, с номерами $i_1, \dots, i_m$, и второго слагаемого во всех остальных скобках. Вклад такого произведения в коэффициент при $x^m y^{n-m}$ равен

$$\begin{aligned} \mathrm{sgn}(i_1, \dots, i_m, \bar{i}_1, \dots, \bar{i}_{n-m}) \cdot \alpha_{i_1} \wedge \ldots \wedge \alpha_{i_k} \wedge \beta_{\bar{i}_1} \wedge \ldots \wedge \beta_{\bar{i}_{n-m}} = \\ = (-1)^{\frac{m(m+1)}{2}+|I|} \alpha_I \wedge \beta_{\bar{I}} = (-1)^{\frac{m(m+1)}{2}+|I|} \Big(\sum_J \xi_J a_{JI}\Big) \wedge \Big(\sum_M \xi_M b_{M\bar{I}}\Big) = \\ = (-1)^{\frac{m(m+1)}{2}+|I|} \sum_{JM} a_{JI} \cdot b_{M\bar{I}} \cdot \xi_J \wedge \xi_M = \Big(\sum_J (-1)^{|I|+|J|} a_{JI} \cdot b_{\overline{JI}}\Big) \cdot \xi_1 \wedge \ldots \wedge \xi_n. \end{aligned}$$

Коэффициент при $x^m y^{n-m}$ в $\det(x\,A + y\,B)$ равен сумме этих вкладов по всем наборам I из m возрастающих номеров, что и даёт формулу (11-21).

11.4. Присоединённая матрица. При $m = 1$ в вычислениях из n° 11.3.3 на стр. 195 наборы $I = (i), J = (j)$ содержат по одному индексу и миноры $a_{IJ} = a_{ij}$ превращаются в матричные элементы, так что $\Lambda^1 A = A$. Присоединённая матрица $\Lambda^1 A^\vee$ в этом случае обозначается просто $A^\vee = (a^\vee_{ij})$ и называется *присоединённой* к матрице A. Она имеет в клетке (i,j) определитель $(n-1)\times(n-1)$-подматрицы, получающейся из A выкидыванием креста с центром в клетке (j,i), т. е.

$$a^\vee_{ij} = (-1)^{i+j} a_{\overline{ji}}\,.$$

Соотношения Лапласа из форм. (11-19) на стр. 196 в этом случае превращаются в равенства

$$AA^\vee = A^\vee A = \det(A)\cdot E \tag{11-22}$$

в алгебре матриц $\mathrm{Mat}_n(K)$.

11.4.1. Формула для обратной матрицы. Если определитель матрицы $A \in \mathrm{Mat}_n(K)$ обратим в K, то по (11-22) матрица A тоже обратима, и $A^{-1} = A^\vee/\det A$. Наоборот, если матрица A обратима, то $1 = \det E = \det(AA^{-1}) = \det(A)\det(A^{-1})$, и $\det A$ обратим в K. Мы получаем

Предложение 11.3
Квадратная матрица $A \in \mathrm{Mat}_n(K)$ с элементами из произвольного коммутативного кольца K с единицей обратима если и только если $\det A$ обратим в K, и в этом случае $A^{-1} = A^\vee/\det A$. □

Пример 11.7
Для матриц размера 2×2 и 3×3 с определителем 1

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}^{-1} = \begin{pmatrix} (a_{22}a_{33} - a_{23}a_{32}) & -(a_{12}a_{33} - a_{13}a_{31}) & (a_{12}a_{23} - a_{13}a_{22}) \\ -(a_{21}a_{33} - a_{23}a_{31}) & (a_{11}a_{33} - a_{13}a_{31}) & -(a_{11}a_{23} - a_{13}a_{21}) \\ (a_{21}a_{32} - a_{22}a_{31}) & -(a_{11}a_{32} - a_{12}a_{32}) & (a_{11}a_{22} - a_{12}a_{21}) \end{pmatrix}.$$

В общем случае все элементы матриц в правых частях надо поделить на $\det A$.

11.4.2. Разложение определителя по строке или столбцу. Вычисляя элемент в позиции ii первого произведения в (11-22), получаем равенство

$$\det A = \sum\nolimits_{j=1}^{n} (-1)^{i+j} a_{ij} A_{ij} \tag{11-23}$$

которое называется *разложением определителя по i-той строке*. Симметричным образом, вычисление jj-того элемента второго произведения в (11-22) даёт *разложение по j-му столбцу*

$$\det A = \sum\nolimits_{i=1}^{n} (-1)^{i+j} a_{ij} A_{ij}\,. \tag{11-24}$$

Например, разложение определителя 3×3 по первому столбцу имеет вид:

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \\ = a_{11}\left(a_{22}a_{33} - a_{23}a_{32}\right) - a_{21}\left(a_{12}a_{33} - a_{13}a_{32}\right) + a_{31}\left(a_{12}a_{23} - a_{13}a_{22}\right)\,.$$

11.4.3. Правило Крамера для систем однородных линейных уравнений. Рассмотрим систему n линейных однородных уравнений на $n+1$ неизвестных

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ a_{20}x_0 + a_{21}x_1 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n0}x_1 + a_{n1}x_1 + \ldots + a_{nn}x_n = 0 \end{cases} \tag{11-25}$$

и построим по матрице $A = (a_{ij})$ её коэффициентов вектор $\alpha = (A_0, A_1, \ldots, A_n) \in K^{n+1}$, у которого i-я координата равна умноженному на $(-1)^i$ определителю квадратной $n\times n$-матрицы, получающейся из $n \times (n+1)$-матрицы A выкидыванием i-того столбца:

$$A_i = (-1)^i \det \begin{pmatrix} a_{1,0} & \ldots & a_{1,i-1} & a_{1,i+1} & \ldots & a_{1,n} \\ a_{2,0} & \ldots & a_{2,i-1} & a_{2,i+1} & \ldots & a_{2,n} \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ a_{n,0} & \ldots & a_{n,i-1} & a_{n,i+1} & \ldots & a_{n,n} \end{pmatrix} \tag{11-26}$$

Покажем, что вектор α является решением системы (11-25). Дописывая к матрице A сверху ещё один экземпляр её i-той строки, мы получим квадратную матрицу размера $(n+1)\times(n+1)$ с нулевым определителем. Раскладывая этот определитель по верхней строке, получаем равенство $a_{i0}A_0 + \ldots + a_{in}A_n = 0$, справедливое при каждом i.

Упражнение 11.11. Проверьте, что если кольцо $K = \Bbbk$ является полем, то уравнения (11-25) линейно независимы если и только если $\alpha \neq 0$, и в этом случае решения системы (11-25) образуют в $\Bbbk^{n+1}$ одномерное векторное подпространство, порождённое вектором α.

Например, в векторном пространстве $\Bbbk^3$ пересечение не совпадающих плоскостей

$$\begin{cases} a_1x + a_2y + a_3z = 0 \\ b_1x + b_2y + b_3z = 0 \end{cases}$$

является прямой с направляющим вектором $(a_2b_3 - a_3b_2,\ -a_1b_3 + a_3b_1,\ a_1b_2 - a_2b_1)$.

11.4.4. Правило Крамера для систем неоднородных уравнений. По предл. 8.3 на стр. 139 столбцы $v_1, \ldots, v_n$ квадратной матрицы $C \in \mathrm{Mat}_n(K)$ образуют базис модуля K^n если и только если матрица C обратима, что по предл. 11.3 равносильно обратимости в K её определителя $\det(v_1, \ldots, v_n) = \det C$. Если это так, то коэффициенты разложения

$$w = x_1v_1 + \ldots + x_nv_n$$

произвольного вектора $w \in K^n$ по базису $v_1, \ldots, v_n$ вычисляются по *правилу Крамера*

$$x_i = \frac{\det\left(v_1, \ldots, v_{i-1},\ w,\ v_{i+1}, \ldots, v_n\right)}{\det(v_1, \ldots, v_n)}, \tag{11-27}$$

так как

$$\begin{aligned} \det\left(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_n\right) &= \det\Big(v_1, \ldots, v_{i-1}, \sum\nolimits_\nu x_\nu v_\nu, v_{i+1}, \ldots, v_n\Big) = \\ &= \sum\nolimits_\nu x_\nu \det\left(v_1, \ldots, v_{i-1}, v_\nu, v_{i+1}, \ldots, v_n\right) = x_i \det\left(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_n\right). \end{aligned}$$

11.4.5. Тождество Гамильтона – Кэли. Для любого коммутативного кольца K с единицей кольцо квадратных матриц $\mathrm{Mat}_n(K[t])$ с элементами из кольца многочленов $K[t]$ совпадает с кольцом многочленов $\mathrm{Mat}_n(K)[t]$ от переменной t с коэффициентами в $\mathrm{Mat}_n(K)$, поскольку каждую матрицу, в клетках которой стоят многочлены от t, можно записать как многочлен от t с матричными коэффициентами и наоборот. Например,

$$\begin{pmatrix} 3t^2+2t & t^3-1 \\ 2t+3 & t^3+t-1 \end{pmatrix} = t^3\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + t^2\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} + t\begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ 3 & -1 \end{pmatrix}.$$

Определение 11.1 (характеристический многочлен)
Для матрицы $A = (a_{ij}) \in \mathrm{Mat}_n(K)$ многочлен

$$\chi_A(t) \stackrel{\text{def}}{=} \det(tE - A) = t^n - \sigma_1(A)\cdot t^{n-1} + \ \ldots\ + (-1)^{n-1}\sigma_{n-1}(A)\cdot t + (-1)^n\sigma_n(A) \in K[t]$$

называется *характеристическим многочленом* матрицы A. Коэффициент при t^{n-k} в характеристическом многочлене обозначается через $(-1)^k\sigma_k(A)$.

Упражнение 11.12. Убедитесь, что число $\sigma_k(A) \in K$ равно сумме *главных* $k \times k$ миноров[1] матрицы A. В частности, $\sigma_1(A) = \mathrm{tr}(A)$ и $\sigma_n(A) = \det A$ суть *след* и *определитель* матрицы A.

Теорема 11.1 (тождество Гамильтона – Кэли)
Рассмотрим кольцо $K = \mathbb{Z}[a_{ij}]$ многочленов с целыми коэффициентами от n^2 переменных a_{ij}, где $1 \leqslant i, j \leqslant n$. Матрица $A = (a_{ij}) \in \mathrm{Mat}_n(K)$ удовлетворяет в $\mathrm{Mat}_n(K)$ соотношению $\chi_A(A) = 0$.

Доказательство. Согласно форм. (11-22) на стр. 198, в кольце $\mathrm{Mat}_n(K[t])$ выполняется соотношение $\det(tE-A)\cdot E = (tE-A)(tE-A)^\vee$, где $(tE-A)^\vee \in \mathrm{Mat}_n(K[t])$ — матрица, присоединённая[2] к $(tE - A)$. Перепишем это равенство в виде равенства между многочленами от t с коэффициентами в кольце матриц $\mathrm{Mat}_n(K)$:

$$t^nE - \sigma_1(A)\,t^{n-1}E + \ldots + (-1)^n\sigma_n(A)\,E = (tE - A)(t^mA_m + \ldots + t\,A_1 + A_0),$$

где $A_0, A_1, \ldots, A_m \in \mathrm{Mat}_n(K)$ — некоторые матрицы. Подставляя в него $t = A$, получаем в кольце $\mathrm{Mat}_n(K)$ равенство $\chi_A(A)\cdot E = 0$, откуда $\chi_A(A) = 0$. □

Упражнение 11.13. Пусть $f(t) = \sum_{i=0}^m t^iA_i$, $g(t) = \sum_{j=0}^n t^jB_j \in \mathrm{Mat}_r(K)[t]$ и

$$h(t) = f(t)g(t) = \sum\nolimits_{k=0}^{m+n} t^kH_k \in \mathrm{Mat}_r(K)[t]\,,\ \text{где } H_k = \sum_{i+j=k} A_iB_j\,,$$

а матрица $C \in \mathrm{Mat}_r(K)$ такова, что $CA_i = A_iC$ при всех i. Убедитесь, что $f(C)g(C) = h(C)$ в $\mathrm{Mat}_r(K)$.

[1] Т. е. определителей таких $k\times k$ подматриц в A, главная диагональ которых является подмножеством главной диагонали матрицы A.

[2] См. n° 11.4 на стр. 198.

11.5. Результант. Пусть многочлены $f(x) = a_0 + a_1x + \ldots + a_nx^n$ и $g(x) = b_0 + b_1x + \ldots + b_mx^m$ имеют коэффициенты в произвольном поле $\Bbbk$ и $a_nb_m \neq 0$. Обозначим через $V_k \subset \Bbbk[x]$ векторное пространство многочленов степени строго меньше k. Наличие у f и g общего корня в каком-нибудь поле $\mathbb{F} \supset \Bbbk$ равносильно тому, что $\deg \text{нод}(f, g) \geqslant 1$, а это в свою очередь эквивалентно существованию таких не равных одновременно нулю многочленов $h_1 \in V_m$ и $h_2 \in V_n$, что $fh_1 + gh_2 = 0$.

Упражнение 11.14. Убедитесь в этом.

Мы заключаем, что многочлены f и g тогда и только тогда имеют общий корень в каком-нибудь расширении $\mathbb{F} \supset \Bbbk$, когда $\Bbbk$-линейное отображение

$$V_m \oplus V_n \to V_{m+n}, \quad (h_1, h_2) \mapsto fh_1 + gh_2, \tag{11-28}$$

имеет ненулевое ядро. Поскольку $\dim(V_m \oplus V_n) = m + n = \dim V_{m+n}$, это условие выражается равенством нулю определителя матрицы отображения (11-28) в каких-нибудь базисах. В стандартных базисах $(1,0), (x,0), \ldots, (x^{m-1},0), (0,1), (0,x), \ldots, (0,x^{n-1})$ в $V_m \oplus V_n$ и $1, x, \ldots, x^{m+n-1}$ в V_{m+n} отображение (11-28) имеет матрицу

$$\underbrace{\left.\begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{m-1} & \ddots & b_0 \\ a_n & \ddots & a_1 & b_m & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{m-1} \\ & & a_n & & & b_m \end{pmatrix}\right\}}_{m+n} \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \tag{11-29}$$
$$\underbrace{\qquad\qquad}_{m} \quad \underbrace{\qquad\qquad\qquad}_{n}$$

(в столбцах записаны коэффициентов многочленов f и g, последовательно сдвигаемые на одну клетку вниз при движении слева направо, все остальные элементы матрицы нулевые). Определитель матрицы (11-29) называется *детерминантом Сильвестра* многочленов f, g. Таким образом, многочлены $f, g \in \Bbbk[x]$ имеют общий корень в некотором расширении $\mathbb{F} \supset \Bbbk$ поля $\Bbbk$, если и только если их детерминант Сильвестра обращается в нуль.

Рассмотрим теперь кольцо $K = \mathbb{Z}[a_n, b_m, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ и многочлены

$$\begin{aligned} A(x) &= a_0 + a_1x + \ldots + a_nx^n \stackrel{\text{def}}{=} a_n \prod_{i=1}^{n} (x - \alpha_i) \\ B(x) &= b_0 + b_1x + \ldots + b_mx^m \stackrel{\text{def}}{=} b_m \prod_{j=1}^{n} (x - \beta_j), \end{aligned} \tag{11-30}$$

лежащие в кольце $K[x]$. Элемент $R_{A,B}$ кольца K, задаваемый равенствами

$$R_{A,B} \stackrel{\text{def}}{=} a_n^m b_m^n \prod_{ij} (\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} B(\alpha_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} A(\beta_j) \tag{11-31}$$

называется *результантом* многочленов (11-30). Будучи симметрическим как по переменным α_i, так и по переменным β_j, результант лежит в подкольце кольца K, состоящем из многочленов от a_n, b_m и от элементарных симметрических многочленов $e_k(\alpha_1, \ldots, \alpha_n)$ и $e_\ell(\beta_1, \ldots, \beta_m)$.

Предложение 11.4
Результант $R_{A,B}$ равен в кольце K детерминанту Сильвестра многочленов (11-30). Кроме того, существуют такие многочлены $\varphi, \psi \in K[x]$, что $A(x)\cdot\varphi(x) + B(x)\cdot\psi(x) = R_{A,B}$.

Доказательство. Обозначим матрицу (11-29) через S. По предыдущему для любых многочленов $\varphi(x) = \varphi_0 + \varphi_1 x + \ldots + \varphi_{n-1}x^{n-1}$ и $\psi(x) = \psi_0 + \psi_1 x + \ldots + \psi_{m-1}x^{m-1}$ столбец коэффициентов многочлена $A\varphi + B\psi$ является результатом умножения столбца $(\varphi_0, \ldots, \varphi_{m-1}, \psi_0, \ldots, \psi_{n-1})^t$ слева на матрицу S. Из равенства $S\cdot S^\vee = \det(S)\cdot E$ вытекает, что в первом столбце матрицы $S^\vee$ выписаны друг под другом коэффициенты таких многочленов $\varphi, \psi \in K[x]$, что

$$A(x)\cdot\varphi(x) + B(x)\cdot\psi(x) = \det S \in K\,. \tag{11-32}$$

Рассмотрим $\det S \in \mathbb{Z}[a_n, b_m, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ как многочлен от α_i с коэффициентами в кольце многочленов от всех остальных переменных. Полагая $\alpha_i = \beta_j$ и подставляя в равенство (11-32) $x = \alpha_i = \beta_j$ получаем в левой части нуль, поскольку при $\alpha_i = \beta_j$ оба многочлена $A(x)$ и $B(x)$ обращаются в нуль при $x = \alpha_i = \beta_j$. Поэтому $\det S$ делится в кольце K на все разности $a_i - \beta_j$. Так как кольцо $K = \mathbb{Z}[a_n, b_m, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ факториально, а все эти разности неприводимы и попарно не ассоциированы, $\det S$ делится на $\prod_{ij}(\alpha_i - \beta_j)$. С другой стороны, по формулам Виета $a_k = (-1)^{n-k}a_n e_{n-k}(\alpha_1, \ldots, \alpha_n)$ и $b_k = (-1)^{m-k}b_m e_{m-k}(\beta_1, \ldots, \beta_m)$, где e_i — элементарные симметрические многочлены. Поэтому первые m столбцов матрицы S делятся на a_n, а последние n — на b_m. Тем самым $\det S$ делится на $a_n^m b_m^n \prod_{ij}(\alpha_i - \beta_j) = R_{A,B}$. Поскольку лексикографически старшие члены у $\det S$ и $R_{A,B}$ оба равны $a_n^m b_m^n (\alpha_1 \ldots \alpha_n)^m$, мы заключаем, что частное от деления равно 1. □

Пример 11.8 (исключение переменных)
Над алгебраически замкнутым полем $\Bbbk$ пара чисел $(x_0, y_0) \in \Bbbk^2$ тогда и только тогда является решением системы полиномиальных уравнений $f(x,y) = g(x,y) = 0$, где $f, g \in \Bbbk[x,y]$, когда многочлены $f(x,y) = f_x(y)$ и $g(x,y) = g_x(y)$, рассматриваемые как многочлены от y с коэффициентами в кольце $\Bbbk[x]$, имеют при $x = x_0$ общий корень $y = y_0$, что равносильно обращению в нуль при $x = x_0$ результанта $R_{f_x, g_x} \in \Bbbk[x]$ этих двух многочленов от y. Таким образом каждая система из двух полиномиальных уравнений на x, y сводится к одному полиномиальному уравнению на x — обращению в нуль детерминанта Сильвестра, составленного из лежащих в $\Bbbk[x]$ коэффициентов многочленов $f_x, g_x \in \Bbbk[x][y]$. Эта процедура называется *исключением переменной* y из уравнений $f(x,y) = g(x,y) = 0$.

Задачи для самостоятельного решения к §11

Во всех задачах к этому параграфу $\Bbbk$ означает произвольное поле, а K — произвольное коммутативное кольцо с единицей.

Задача 11.1. Вычислите а) $\det\begin{pmatrix} 0 & -4 & -1 \\ -4 & 4 & 0 \\ -5 & 1 & 0 \end{pmatrix}$ б) $\det\begin{pmatrix} -1 & 3 & -4 \\ 0 & -3 & 2 \\ 0 & -4 & -1 \end{pmatrix}$ в) $\det\begin{pmatrix} 1 & 4 & -1 \\ 0 & -2 & -1 \\ 3 & -1 & -3 \end{pmatrix}$

г) $\det\begin{pmatrix}-3 & -3 & 1\\ 4 & 3 & 0\\ -1 & 1 & 1\end{pmatrix}$ д) $\det\begin{pmatrix}4 & 2 & 0 & 0\\ -1 & 2 & -4 & 0\\ 3 & 0 & 1 & 2\\ -2 & -2 & 0 & 1\end{pmatrix}$ е) $\det\begin{pmatrix}-1 & 0 & -2 & 3\\ -3 & -4 & -3 & 2\\ 0 & -4 & -2 & 1\\ 4 & 3 & 0 & 3\end{pmatrix}$ ж) $\det\begin{pmatrix}4 & 2 & -4 & 0\\ -3 & 0 & -1 & 0\\ -4 & 1 & 2 & -1\\ -3 & 2 & 2 & -1\end{pmatrix}$

Задача 11.2. Не прибегая к методу Гаусса вычислите

а) $\begin{pmatrix}1 & 1 & 1\\ 2 & 3 & 0\\ 1 & -1 & 6\end{pmatrix}^{-1}$ б) $\begin{pmatrix}1 & 3 & -2\\ 1 & 3 & -1\\ -3 & -8 & 5\end{pmatrix}^{-1}$ в) $\begin{pmatrix}1 & -3 & 3\\ 2 & -6 & 7\\ -3 & 10 & -13\end{pmatrix}^{-1}$.

Задача 11.3. При помощи правила Крамера решите системы уравнений:

а) $\begin{cases}x_1 + 2x_2 - x_3 = 8\\ 2x_1 + 5x_2 - 4x_3 = 20\\ x_1 + x_2 + 2x_3 = 3\end{cases}$ б) $\begin{cases}x_1 + 3x_2 + 3x_3 = 5\\ -3x_1 - 9x_2 - 8x_3 = -17\\ -x_1 - 2x_2 - 3x_3 = -2\end{cases}$ в) $\begin{cases}x_1 + 3x_2 + 3x_3 = 5\\ -3x_1 - 9x_2 - 8x_3 = -17\\ -x_1 - 2x_2 - 3x_3 = -2\end{cases}$

г) $\begin{cases}x_1 - 2x_2 - 5x_3 = 0\\ 2x_1 - 3x_2 - 9x_3 = 0\end{cases}$ д) $\begin{cases}x_1 - x_2 + x_3 + 2x_4 = 0\\ -2x_1 + 2x_2 - x_3 - 2x_4 = 0\\ 3x_1 - 2x_2 + 3x_3 + 8x_4 = 0\end{cases}$ е) $\begin{cases}x_1 + x_2 + 3x_3 + 3x_4 = 0\\ x_1 + 2x_2 + 5x_3 + 5x_4 = 0\\ -x_1 + 2x_2 + 4x_3 + 5x_4 = 0\end{cases}$.

Задача 11.4. Покажите, что определитель верхнетреугольной матрицы равен произведению диагональных элементов.

Задача 11.5. Вычислите $\operatorname{sgn}(n,\ (n-1),\ \dots,\ 2,\ 1)$ и $\det\begin{pmatrix}0 & & 1\\ & \iddots & \\ 1 & & 0\end{pmatrix}$.

Задача 11.6. Для произвольных квадратных матриц A и B выразите через $\det A$ и $\det B$

а) $\det\begin{pmatrix}A & *\\ 0 & B\end{pmatrix}$ б) $\det\begin{pmatrix}0 & A\\ B & *\end{pmatrix}$.

Задача 11.7. Как меняется определитель при отражении относительно побочной[1] диагонали?

Задача 11.8. Две строки матрицы 3×3-матрицы заполнены целыми числами так, что нод чисел в каждой из этих строк равен единице. Всегда ли третью строку этой матрицы можно заполнить целыми числами так, чтобы определитель матрицы оказался равным единице?

Задача 11.9. Двое по очереди заполняют целыми числами клетки матрицы 3×3. Первый выигрывает, если в результате получится вырожденная матрица. Кто победит?

Задача 11.10. Числа $1, 2, \dots, n^2$ всеми возможными способами организуются в квадратные матрицы размера $n\times n$. Найдите сумму определителей всех этих матриц.

Задача 11.11. Вычислите определитель матрицы с нулями на главной диагонали и единицами во всех остальных местах.

Задача 11.12. Покажите, что определитель тридиагональной матрицы с 1 по главной диагонали и непосредственно над ней и -1 непосредственно под ней является числом Фибоначчи[2].

Задача 11.13. Вычислите определители матриц

а) $\begin{pmatrix}x & y & z & 1\\ y & z & x & 1\\ z & x & y & 1\\ \frac{x+z}{2} & \frac{x+y}{2} & \frac{y+z}{2} & 1\end{pmatrix}$ б) $\begin{pmatrix}x & y & 0 & \cdots & 0\\ 0 & x & y & \ddots & \vdots\\ \vdots & \ddots & \ddots & \ddots & 0\\ 0 & \cdots & 0 & x & y\\ y & 0 & \cdots & 0 & x\end{pmatrix}$ в) $\begin{pmatrix}a_0 & 1 & 1 & \cdots & 1\\ 1 & a_1 & 0 & \cdots & 0\\ 1 & 0 & a_2 & \ddots & \vdots\\ \vdots & \vdots & \ddots & \ddots & 0\\ 1 & 0 & \cdots & 0 & a_n\end{pmatrix}$.

[1] Т. е. ведущей из левого нижнего угла в правый верхний.

[2] См. прим. 4.6 на стр. 67.

Задача 11.14. Для двух наборов чисел $\alpha_1, \dots, \alpha_n$, $\beta_1, \dots, \beta_n \in \mathbb{R}$ вычислите
а) $\det\left(\alpha_i\beta_j\right)$ б) $\det\bigl(\cos(\alpha_i - \beta_j)\bigr)$ в) $\det\left(\alpha_i^{j-1}\right)$ г*) $\det\left(\alpha^{j-i-1 \pmod n}\right)$.

Задача 11.15. Сколько имеется над полем из q элементов $n \times n$ матриц а) определителя 1 б) произвольно заданного определителя в) с ненулевым определителем?

Задача 11.16. Покажите, что для линейной независимости функций $f_1, \dots, f_n$ в векторном пространстве всех функций $M \to \Bbbk$ на произвольном множестве M необходимо и достаточно существования n таких точек $x_1, \dots, x_n \in M$, что $\det\left(f_i(t_j)\right) \neq 0$.

Задача 11.17 (теорема об окаймляющих минорах). Пусть матрица A содержит такую невырожденную квадратную подматрицу размера $m \times m$, что все содержащие её подматрицы размера $(m+1) \times (m+1)$ вырождены. Докажите, что $\operatorname{rk} A = m$.

Задача 11.18* (матричная теорема о деревьях). Вершины связного графа Γ без петель[1] и кратных рёбер[2] занумерованы числами от 1 до n. Матрица $A = (a_{ij})$ имеет диагональными элементами a_{ii} взятые со знаком минус количества рёбер, выходящих из i-той вершины, а остальные a_{ij} равны единице, если вершины i и j соединены ребром, и нулю — если не соединены. Убедитесь, что $\det A = 0$ и докажите, что а) все алгебраические дополнения A_{ii} к элементам главной диагонали отличны от нуля и равны между собой б) Γ дерево если и только если все $A_{ii} = 1$.

Задача 11.19. Пусть $AB = E$. Докажите соотношение $a_{IJ} = (-1)^{|I|+|J|} b_{\overline{J}\overline{I}}$ на дополнительные миноры матриц A и B.

Задача 11.20. Вычислите все частные производные $\dfrac{\partial^k \det(A)}{\partial a_{i_1 j_1} \partial a_{i_2 j_2} \dots \partial a_{i_k j_k}}$.

Задача 11.21. Покажите, что однородный грассманов многочлен ω степени 2 тогда и только тогда является произведением двух линейных, когда $\omega \wedge \omega = 0$.

Задача 11.22. Существует ли комплексная 2×4 матрица с множеством 2×2 миноров
а) $\{2, 3, 4, 5, 6, 7\}$ б) $\{3, 4, 5, 6, 7, 8\}$?
Если да — приведите пример такой матрицы, если нет — объясните, почему.

Задача 11.23. Не прибегая к методу Гаусса вычислите инвариантные множители матриц
а) $\begin{pmatrix} 15 & -6 & 3 \\ -15 & 3 & 6 \end{pmatrix}$ б) $\begin{pmatrix} 17 & -5 & -37 \\ -21 & 0 & 21 \\ 3 & 2 & 5 \end{pmatrix}$ в) $\begin{pmatrix} -3 & 24 & -27 & 9 \\ 9 & 6 & -3 & 3 \end{pmatrix}$.

Задача 11.24. нод 2×2 миноров целочисленной 3×3 матрицы равен 12. Может ли её определитель быть равен а) 24 б) 36 в) 48 г) 60? Может ли нод элементов этой матрицы быть равен д) 1 е) 2 ж) 3 з) 4? Если да — приведите пример такой матрицы, если нет — объясните, почему.

Задача 11.25. Сколько элементов в $\mathbb{Z}^4/L$, где $L \subset \mathbb{Z}^4$ порождается столбцами матрицы
а) $\begin{pmatrix} -6 & 8 & 0 & -7 \\ 0 & -6 & 0 & 1 \\ -4 & 0 & -1 & -5 \\ 1 & 6 & 3 & 6 \end{pmatrix}$ б) $\begin{pmatrix} 2 & 0 & 3 & -6 \\ 0 & 0 & 1 & 1 \\ 4 & -5 & 7 & -6 \\ 0 & -2 & 5 & 2 \end{pmatrix}$ в) $\begin{pmatrix} 0 & -6 & 5 & 0 \\ 5 & 7 & -1 & -6 \\ 0 & -2 & -2 & 4 \\ 0 & 0 & 1 & -1 \end{pmatrix}$.

Задача 11.26 (определитель Сильвестра). Пусть многочлены

$$A(x) = a_0 x^n + \dots + a_{n-1}x + a_n \quad \text{и} \quad B(x) = b_0 x^m + \dots + b_{m-1}x + b_m$$

[1] Т. е. рёбер, ведущих из вершины в неё саму.
[2] Т. е. любые две вершины графа соединяются не более, чем одним ребром.

имеют степени $m \geqslant n$. Для каждого $\nu = 0, 1, 2, \ldots$ обозначим через d_ν определитель матрицы, которая получается выкидыванием по ν строк и ν столбцов сверху, снизу, слева и справа из матрицы[1]

$$\underbrace{\left(\begin{array}{ccccccccc}
a_0 & \ldots & \ldots & a_{n-1} & a_n & & & & \\
 & a_0 & \ldots & \ldots & a_{n-1} & a_n & & & \\
 & & \ddots & & & \ddots & \ddots & & \\
 & & & a_0 & \ldots & \ldots & a_{n-1} & a_n & \\
 & & & & b_0 & \ldots & b_{m-1} & b_n & \\
 & & & \iddots & & \iddots & \iddots & & \\
 & & \iddots & & \iddots & \iddots & & & \\
 & b_0 & \ldots & b_{m-1} & b_m & & & & \\
b_0 & \ldots & b_{m-1} & b_m & & & & &
\end{array}\right)}_{m+n} \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \end{array} \tag{11-33}$$

Покажите, что индекс первого ненулевого члена последовательности $d_0, d_1, d_2, \ldots$ совпадает со степенью $\deg \text{нод}(A, B)$.

Задача 11.27. Для многочленов $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ и $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$ произведения $R(f, g) \stackrel{\text{def}}{=} a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j)$ и $D(f) \stackrel{\text{def}}{=} a_n^{2n-2} \prod_{i<j}(\alpha_i - \alpha_j)^2$ называются соответственно *результантом* этих многочленов и *дискриминантом* многочлена f. Выразите:

а) $D(f)$ через $R(f, f')$ б) $D(fg)$ через $D(f)$, $D(g)$ и $R(f, g)$.

Задача 11.28. Исключите x из систем уравнений: а) $5x^2-6xy+5y^2-16 = 2x^2-xy+y^2-x-y-4 = 0$

б) $4x^2 - 7xy + y^2 + 13x - 2y - 3 = 9x^2 - 14xy + y^2 + 28x - 4y - 5 = 0$.

Задача 11.29. Докажите, что дискриминант приведённого многочлена n-й степени с корнями $\alpha_1, \ldots, \alpha_n$ равен $\det(\alpha_j^{n-i})$.

Задача 11.30 (циркулянт). Выразите определитель матрицы, строки которой являются последовательными циклическими перестановками строки $(\alpha_0, \alpha_1, \ldots, \alpha_n) \in \mathbb{C}^{n+1}$, через значения полинома $f(x) = \alpha_0 x^n + \ldots + \alpha_{n-1}x + \alpha_n$ на корнях $\sqrt[n+1]{1} \in \mathbb{C}$.

[1] Пустые места заполнены нулями.

§12. Пространства с оператором

12.1. Классификация пространств с оператором. Пусть $\Bbbk$ — произвольное поле, V — конечномерное векторное пространство над $\Bbbk$, а $F\colon V \to V$ — линейный эндоморфизм пространства V. Мы будем называть пару (F, V) *пространством с оператором* или просто *оператором* над $\Bbbk$. Линейное отображение $C\colon U_1 \to U_2$ между пространствами с операторами (F_1, U_1) и (F_2, U_2) называется *гомоморфизмом*, если $F_2 \circ C = C \circ F_1$. В этом случае говорят, что диаграмма

$$\begin{array}{ccc} U_1 & \xrightarrow{C} & U_2 \\ {\scriptstyle F_1}\uparrow & & \uparrow{\scriptstyle F_2} \\ U_1 & \xrightarrow[C]{} & U_2 \end{array}$$

коммутативна[1]. Если гомоморфизм C биективен, операторы $F_1\colon U_1 \to U_1$ и $F_2\colon U_2 \to U_2$ называются *изоморфными* или *подобными*. Поскольку в этом случае $F_2 = CF_1C^{-1}$, то говорят, что оператор F_2 получается из F_1 *сопряжением* посредством изоморфизма C.

Подпространство $U \subset V$ называется F*-инвариантным*, если $F(U) \subset U$. В этом случае пара $(F|_U, U)$ тоже является пространством с оператором и вложение $U \hookrightarrow V$ представляет собою гомоморфизмом пространств с операторами. Оператор, не имеющий инвариантных подпространств, отличных от нуля и всего пространства, называется *неприводимым* или *простым*.

Упражнение 12.1. Покажите, что оператор умножения на класс $[t]$ в факторкольце $\mathbb{R}[t]/(t^2+1)$ неприводим.

Оператор $F\colon V \to V$ называется *разложимым*, если V раскладывается в прямую сумму двух ненулевых F-инвариантных подпространств, и *неразложимым* — в противном случае. Все простые операторы неразложимы.

Упражнение 12.2. Покажите, что оператор умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(t^n)$ при всех $n > 1$ приводим, но неразложим.

Таким образом, над любым полем $\Bbbk$ имеются неразложимые пространства с оператором любой размерности. Очевидно, что всякое пространство с оператором является прямой суммой неразложимых.

12.1.1. Пространство с оператором как $\Bbbk[t]$-модуль. Задание на пространстве V линейного оператора $F\colon V \to V$ эквивалентно заданию на V структуры модуля над кольцом многочленов $\Bbbk[t]$. В самом деле, структура $\Bbbk[t]$-модуля включает в себя операцию умножения векторов на переменную $t\colon v \mapsto tv$, которая является линейным отображением $V \to V$. Если обозначить его буквой F, то умножение векторов на произвольный многочлен $f(t) = a_0 + a_1t + \ldots + a_mt^m$ происходит по правилу $f(t)\,v = a_0v + a_1Fv + \ldots + a_mF^mv = f(F)\,v$, где

$$f(F) = a_0\mathrm{Id}_V + a_1F + \ldots + a_mF^m$$

есть результат вычисления многочлена f на элементе F в $\Bbbk$-алгебре $\mathrm{End}(V)$. Наоборот, каждый линейный оператор $F\colon V \to V$ задаёт на V структуру $\Bbbk[t]$-модуля, в котором умножение вектора $v \in V$ на многочлен $f(t) \in \Bbbk[t]$ происходит по формуле $f(t)\,v \stackrel{\text{def}}{=} f(F)\,v$. Мы будем обозначать такой $\Bbbk[t]$-модуль через V_F.

[1]Произвольная диаграмма отображений называется *коммутативной*, если композиции отображений вдоль любых двух путей с общим началом и концом одинаковы.

Гомоморфизм $C : V_F \to W_G$ между $\Bbbk[t]$-модулями, которые задаются линейными операторами $F : V \to V$ и $G : W \to W$, представляет собою $\Bbbk$-линейное отображение $C : V \to W$, перестановочное с умножением векторов на t, т. е. такое что $C \circ F = G \circ C$. Мы заключаем, что гомоморфизмы пространств с операторами — это то же самое, что $\Bbbk[t]$-линейные отображения между задаваемыми этими операторами $\Bbbk[t]$-модулями. В частности, операторы $F : V \to V$ и $G : W \to W$ изоморфны, если и только если изоморфны $\Bbbk[t]$-модули V_F и W_G.

Векторное подпространство $U \subset V$ является $\Bbbk[t]$-подмодулем в модуле V_F, если и только если оператор умножения на t переводит U в себя, т. е. тогда и только тогда, когда это подпространство F-инвариантно. Аналогично, разложимость V в прямую сумму инвариантных подпространств означает разложимость $\Bbbk[t]$-модуля V_F в прямую сумму $\Bbbk[t]$-подмодулей.

Если векторное пространство V конечномерно над $\Bbbk$, то $\Bbbk[t]$-модуль V_F конечно порождён, поскольку любой набор векторов, линейно порождающих V над $\Bbbk$, порождает и модуль V_F над $\Bbbk[t]$. В каноническом разложении конечномерного над $\Bbbk$ модуля V_F в прямую сумму свободного модуля и подмодуля кручения[1] свободное слагаемое отсутствует, так как оно бесконечномерно над $\Bbbk$. Таким образом, из теоремы об элементарных делителях[2] и теоремы об инвариантных множителях[3] мы получаем следующие два эквивалентных друг другу описания пространств с оператором над произвольным полем $\Bbbk$.

Теорема 12.1 (жорданово описание в терминах элементарных делителей)
Любой линейный оператор в конечномерном векторном пространстве над произвольным полем $\Bbbk$ подобен оператору умножения на класс $[t]$ в прямой сумме факторколец

$$\Bbbk[t]/(p_1^{m_1}(t)) \oplus \ldots \oplus \Bbbk[t]/(p_k^{m_k}(t)), \tag{12-1}$$

где все многочлены $p_\nu(t) \in \Bbbk[t]$ приведены и неприводимы, и слагаемые могут повторяться. Операторы умножения на класс $[t]$, действующие в суммах

$$\Bbbk[t]/(p_1^{m_1}(t)) \oplus \ldots \oplus \Bbbk[t]/(p_k^{m_k}(t)) \quad \text{и} \quad \Bbbk[t]/(q_i^{n_1}(t)) \oplus \ldots \oplus \Bbbk[t]/(q_\ell^{n_\ell}(t))$$

изоморфны, если и только если $k = \ell$ и прямые слагаемые можно переставить так, что $p_\nu = q_\nu$ и $m_\nu = n_\nu$ при всех ν. □

Теорема 12.2 (фробениусово описание в терминах инвариантных множителей)
Любой линейный оператор в конечномерном векторном пространстве над произвольным полем $\Bbbk$ подобен оператору умножения на класс $[t]$ в прямой сумме факторколец

$$\Bbbk[t]/(f_1) \oplus \ldots \oplus \Bbbk[t]/(f_r), \tag{12-2}$$

где $r \in \mathbb{N}$, а $f_1, \ldots, f_r \in \Bbbk[t]$ — такие приведённые многочлены, что $f_i \mid f_j$ при $i < j$. Два таких оператора на пространствах $\Bbbk[t]/(f_1) \oplus \ldots \oplus \Bbbk[t]/(f_r)$ и $\Bbbk[t]/(g_1) \oplus \ldots \oplus \Bbbk[t]/(g_s)$ подобны, если и только если $r = s$ и $f_i = g_i$ при всех i. □

[1] См. теор. 10.4 на стр. 175.
[2] См. теор. 10.3 на стр. 174.
[3] См. 10-8 на стр. 177.

12.1.2. Элементарные делители и инвариантные множители. Многочлены $f_1, \dots, f_r \in \Bbbk[t]$ из теор. 12.2 называются *инвариантными множителями* оператора $F : V \to V$, а дизъюнктное объединение[1] всех многочленов $p_\nu^{m_\nu}$ из теор. 12.1 называется *набором элементарных делителей* и обозначается через $\mathcal{El}(F)$. Инвариантные множители и элементарные делители связаны китайской теоремой об остатках: $\Bbbk[t]/(f_1) \oplus \dots \oplus \Bbbk[t]/(f_r) \simeq \bigoplus_{p^m \in \mathcal{El}(F)} \Bbbk[t]/(p^m)$ и однозначно определяют друг друга, как это объяснялось в n° 10.2 на стр. 173.

Следствие 12.1
Линейные операторы F и G подобны тогда и только тогда, когда $\mathcal{El}(F) = \mathcal{El}(G)$. □

Следствие 12.2
Линейный оператор неразложим тогда и только тогда, когда он подобен оператору умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(p^m)$, где $p \in \Bbbk[t]$ неприводим и приведён. Неразложимый оператор неприводим, если и только если $m = 1$. □

Следствие 12.3
Многочлен $f \in \Bbbk[t]$ тогда и только тогда аннулирует оператор $F : V \to V$, когда он делится на все элементарные делители оператора F. Аннулирующий оператор F приведённый многочлен наименьшей степени равен последнему инвариантному множителю f_r из разложения (12-2).□

Упражнение 12.3. Пусть пространство с оператором (F, V) разлагается в прямую сумму F-инвариантных подпространств U_i. Покажите, что $\mathcal{El}(F) = \bigsqcup_i \mathcal{El}(F|_{U_i})$.

12.1.3. Отыскание элементарных делителей. Фиксируем в пространстве V какой-либо базис $\boldsymbol{v} = (v_1, \dots, v_n)$ над полем $\Bbbk$ и обозначим через $F_{\boldsymbol{v}} \in \mathrm{Mat}_n(\Bbbk)$ матрицу оператора $F : V \to V$ в этом базисе. Напомню[2], что она однозначно определяется тем, что $F(\boldsymbol{v}) = \boldsymbol{v}\, F_{\boldsymbol{v}}$ или, подробнее,

$$(F(v_1), \dots, F(v_n)) = (v_1, \dots, v_n)\, F_{\boldsymbol{v}}\,.$$

Так как векторы v_i линейно порождают пространство V над $\Bbbk$, они тем более порождают модуль V_F над $\Bbbk[t]$, и $V_F = \Bbbk[t]^n/R_{\boldsymbol{v}}$, где подмодуль $R_{\boldsymbol{v}} = \ker \pi_{\boldsymbol{v}} \subset \Bbbk[t]^n$ является ядром эпиморфизма[3] $\pi_{\boldsymbol{v}} : \Bbbk[t]^n \to V_F$, переводящего стандартный базисный вектор $e_i \in \Bbbk[t]^n$ в вектор $v_i \in V$, и состоит из всех $\Bbbk[t]$-линейных соотношений между векторами $\boldsymbol{v}$ в V_F. Таким образом, инвариантные множители оператора F суть отличные от единицы инвариантные множители подмодуля $R_{\boldsymbol{v}} \subset \Bbbk[t]^n$.

Лемма 12.1
Если записывать элементы свободного модуля $\Bbbk[t]^n$ в виде координатных столбцов с элементами из $\Bbbk[t]$, то подмодуль соотношений $\ker \pi_{\boldsymbol{v}} \subset \Bbbk[t]^n$ линейно порождается над $\Bbbk[t]$ столбцами матрицы $tE - F_{\boldsymbol{v}}$.

Доказательство. Пусть $F_{\boldsymbol{v}} = \left(f_{ij}\right)$. Тогда j-й столбец матрицы $tE - F_{\boldsymbol{v}}$ выражается через стандартный базис $\boldsymbol{e}$ модуля $\Bbbk[t]^n$ как $te_j - \sum_{i=1}^n e_i f_{ij}$. Применяя к этому вектору гомоморфизм $\pi_{\boldsymbol{v}}$,

[1] Каждый элементарный делитель p^m входит в него ровно столько раз, сколько прямых слагаемых вида $\Bbbk[t]/(p^m)$ имеется в разложении (12-1).

[2] См. **??** на стр. **??**.

[3] См. n° 10.1 на стр. 170.

получаем $\pi_v\Big(te_j - \sum_{i=1}^n e_i f_{ij}\Big) = tv_j - \sum_{i=1}^n v_i f_{ij} = Fv_j - \sum_{i=1}^n v_i f_{ij} = 0$. Тем самым все столбцы матрицы $tE - F_v$ лежат в $\ker \pi_v$. Рассмотрим теперь произвольный вектор $h(t) \in \Bbbk[t]^n$ и запишем его в виде многочлена от t с коэффициентами в $\Bbbk^n$ (ср. с n° 11.4.5 на стр. 200):

$$h(t) = t^m h_m + t^{m-1} h_{m-1} + \ldots + t h_1 + h_0\,, \text{ где } h_i \in \Bbbk^n\,.$$

Этот многочлен можно поделить слева с остатком на многочлен $tE - F_v$ точно также, как делят «уголком» обычные полиномы с постоянными коэффициентами[1]. В результате получим равенство вида $t^m h_m + \ldots + t h_1 + h_0 = (tE - F_v)\cdot(t^{m-1} g_{m-1} + \ldots + t g_1 + g_0) + r$, где $g_i, r \in \Bbbk^n$.

Упражнение 12.4. Убедитесь в этом и проверьте, что остаток от деления $h(t)$ на $tE - A$, где $A \in \mathrm{Mat}_n(\Bbbk)$, равен $A(\ldots A(Ah_m + h_{m-1}) + \ldots + h_1) + h_0 = A^m h_m + \ldots + Ah_1 + h_0 = h(A)$.

Иными словами, вычитая из любого столбца $h(t) \in \Bbbk[t]^n$ подходящую $\Bbbk[t]$-линейную комбинацию столбцов матрицы $tE - F_v$, можно получить вектор $r \in \Bbbk^n$, т. е. $\Bbbk$-линейную комбинацию $r = \sum \lambda_i e_i$ стандартных базисных векторов $e_i \in \Bbbk[t]^n$. Так как столбцы матрицы $tE - F_v$ лежат в $\ker \pi_v$, мы заключаем, что $\pi_v(h(t)) = \pi_v(r) = \sum \lambda_i v_i$. Если $h \in \ker \pi_v$, то $\sum \lambda_i v_i = 0$, что возможно только когда все $\lambda_i = 0$, ибо векторы $v_i \in V$ линейно независимы над $\Bbbk$. Тем самым $r = 0$ для всех $h \in \ker \pi_v$, т. е. $\ker \pi_v$ содержится в $\Bbbk[t]$-линейной оболочке столбцов матрицы $tE - F_v$. □

Следствие 12.4
Множество $\mathcal{El}(F)$ является дизъюнктным объединением степеней p^m неприводимых приведённых многочленов из разложений инвариантных множителей $f_i(t)$ матрицы $tE - F_v$. Последние равны диагональным элементам $d_{ii}(t)$ нормальной формы Смита[2] матрицы $tE - F_v$ и могут быть вычислены по формулам[3] $f_i(t) = \Delta_i(tE - F_v)/\Delta_{i-1}(tE - F_v)$, где $\Delta_i(tE - F_v)$ означает нод всех $k \times k$ миноров матрицы $tE - F_v$. □

12.1.4. Характеристический многочлен. Произведение всех элементарных делителей линейного оператора $F\colon V \to V$, по сл. 12.4 равное определителю $\Delta_n = \det(tE - F_v)$, где F_v — матрица оператора F в каком-либо базисе $\boldsymbol{v}$ пространства V, называется *характеристическим многочленом* оператора F и обозначается

$$\chi_F(t) \stackrel{\text{def}}{=} \det(tE - F_v) = \prod_{p^m \in \mathcal{El}(F)} p^m\,.$$

Из предыдущего вытекает, что характеристический многочлен не зависит от выбора базиса и что подобные операторы имеют одинаковые характеристические многочлены.

Упражнение 12.5. Убедитесь прямым вычислением, что для всех $A \in \mathrm{Mat}_n(\Bbbk)$, $C \in \mathrm{GL}_n(\Bbbk)$ выполняется равенство $\det(tE - CAC^{-1}) = \det(tE - A)$.

Пример 12.1 (характеристический многочлен разложимого оператора)
Если пространство с оператором (F, V) распадается в прямую сумму пространств с операторами (G, U) и (H, W), то в базисе пространства $V = U \oplus W$, который получен объединением базиса в U и базиса в W, матрица $tE - F$ имеет блочно диагональный вид

$$tE - F = \begin{pmatrix} tE - G & 0 \\ 0 & tE - H \end{pmatrix}\,.$$

[1] См. n° 3.2 на стр. 44.
[2] См. n° 9.1.1 на стр. 150.
[3] См. прим. 11.3 на стр. 194.

Раскладывая её определитель по первым $\dim U$ столбцам[1], заключаем, что $\chi_F(t) = \chi_G(t)\,\chi_H(t)$. Это вполне согласуется с упр. 12.3 на стр. 208.

Упражнение 12.6. Убедитесь, что для любого приведённого многочлена $f \in \Bbbk[t]$ характеристический многочлен оператора умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(f)$ равен f.

12.1.5. Минимальный многочлен. Для каждого неприводимого приведённого многочлена $p \in \Bbbk[t]$ обозначим через $m_p(F)$ максимальный показатель m, с которым p^m присутствует в наборе $\mathcal{El}(F)$ элементарных делителей оператора F, а для тех неприводимых приведённых многочленов $p \in \Bbbk[x]$, степени которых не представлены в $\mathcal{El}\,F$, положим $m_p(F) = 0$. Таким образом, $m_p(F) = 0$ для всех неприводимых приведённых $p \in \Bbbk[x]$ кроме конечного числа. В этих обозначениях сл. 12.3 на стр. 208 можно переформулировать следующим образом: аннулирующий оператор F приведённый многочлен $\mu_F(t)$ наименьшей возможной степени совпадает с инвариантным множителем оператора F наибольшей степени и равен

$$\mu_F(t) = f_r = \prod_p p^{m_p(F)}, \tag{12-3}$$

где произведение берётся по всем приведённым неприводимым $p \in \Bbbk[t]$. Многочлен $\mu_F(t)$ называется *минимальным многочленом* оператора $F : V \to V$. Он порождает ядро гомоморфизма

$$\mathrm{ev}_F : \Bbbk[t] \to \mathrm{End}_{\Bbbk}(V), \quad f(t) \mapsto f(F),$$

вычисления многочленов на операторе F и делит в $\Bbbk[t]$ все аннулирующие оператор F многочлены, включая характеристический многочлен $\chi_F(t) = \det(tE - F)$. Согласно сл. 12.4 на стр. 209 инвариантный множитель наибольшей степени оператора F равен отношению $\det(tE - F)$ к нод всех миноров порядка $n-1$ матрицы $tE - F$, где $n = \dim V$. Таким образом, $\chi_F / \mu_F = \Delta_{n-1}(tE - F)$ для любого ненулевого линейного оператора F на n-мерном векторном пространстве.

Пример 12.2 (отыскание минимального многочлена)
Вычисление минимального многочлена оператора $F : V \to V$ по явной детерминантной формуле довольно трудоёмко, и на практике обычно используют следующие соображения. Для каждого вектора $v \in V$ существует такой приведённый многочлен $\mu_{v,F}(t)$ наименьшей степени, что $\mu_{v,F}(F)v = 0$. Чтобы написать его явно, надо найти наименьшее такое $k \in \mathbb{N}$, что вектор $F^k v$ линейно выражается через векторы $v, Fv, \dots, F^{k-1}v$. Если это выражение имеет вид $F^k v = \mu_1 F^{k-1}v + \dots + \mu_{k-1}Fv + \mu_k v$, то $\mu_{v,F}(t) = t^k - \mu_1 t^{k-1} - \dots - \mu_{k-1}t - \mu_k$.

Упражнение 12.7. Убедитесь, что любой аннулирующий оператор F многочлен делится на все многочлены $\mu_{v,F}$, где $v \in V$.

Мы заключаем, что минимальный многочлен μ_F оператора F равен нок многочленов $\mu_{v_i,F}$ каких-нибудь векторов $v = v_1, \dots, v_m$, линейно порождающих пространство V над $\Bbbk$.

Упражнение 12.8. Убедитесь в этом.

Вычислим, к примеру, минимальный многочлен оператора $F : \mathbb{Q}^4 \to \mathbb{Q}^4$, заданного в стандартном базисе $e_1, \dots, e_4$ матрицей

$$A = \begin{pmatrix} -2 & -3 & 3 & 3 \\ 4 & 6 & -4 & -4 \\ 1 & 2 & 0 & -1 \\ 3 & 3 & -3 & -2 \end{pmatrix}$$

[1] См. формулу (11-16) на стр. 196.

Векторы[1]

$$e_1 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad Fe_1 = \begin{pmatrix}-2\\4\\1\\3\end{pmatrix}, \quad F^2e_1 = \begin{pmatrix}4\\0\\3\\-3\end{pmatrix}$$

линейно независимы. Чтобы выяснить, выражается ли через них вектор[2]

$$F^3e_1 = \begin{pmatrix}-8\\16\\7\\9\end{pmatrix},$$

необходимо решить неоднородную систему с расширенной матрицей

$$\left(\begin{array}{ccc|c} 1 & -2 & 4 & -8 \\ 0 & 4 & 0 & 16 \\ 0 & 1 & 3 & 7 \\ 0 & 3 & -3 & 9 \end{array}\right).$$

Методом Гаусса преобразуем эту матрицу к приведённому ступенчатому виду

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

и получаем решение $(-4, 4, 1)$, т. е. $F^3e_1 = -4e_1 + 4Fe_1 + F^2e_1$. Таким образом, минимальный многочлен от оператора F, аннулирующий вектор e_1, равен $F^3 - F^2 - 4F + 4E$. Вычисляя

$$A^2 = \begin{pmatrix}4&3&-3&-3\\0&4&0&0\\3&6&-2&-3\\-3&-3&3&4\end{pmatrix} \quad \text{и} \quad A^3 = \begin{pmatrix}-8&-9&9&9\\16&24&-16&-16\\7&14&-6&-7\\9&9&-9&-8\end{pmatrix},$$

убеждаемся, что $A^3 - A^2 - 4A + 4E = 0$. Тем самым, $\mu_F = t^3 - t^2 - 4t + 4$.

Упражнение 12.9. Как действует умножение на класс $[t]$ в факторкольце $\Bbbk[t]/(t-\lambda)$ и в прямой сумме конечного множества таких факторколец?

12.1.6. Линейные операторы над алгебраически замкнутым полем. Если основное поле $\Bbbk$ алгебраически замкнуто, то неприводимые приведённые многочлены в $\Bbbk[t]$ исчерпываются линейными двучленами $(t-\lambda)$, где $\lambda \in \Bbbk$. Оператор умножения на класс $[t] = [\lambda] + [t-\lambda]$ в факторкольце $\Bbbk[t]/\big((t-\lambda)^m\big)$ является суммой скалярного оператора $\lambda\,\mathrm{Id}: [g] \mapsto \lambda[g]$, умножающего все векторы на λ, и оператора умножения на класс $[t-\lambda]$, который действует на состоящий из векторов $e_i = \big[(t-\lambda)^{m-i}\big]$, $1 \leqslant i \leqslant m$, базис пространства $\Bbbk[t]\,/\,\big((t-\lambda)^m\big)$ по правилу

$$0 \leftarrow\!\shortmid e_1 \leftarrow\!\shortmid e_2 \leftarrow\!\shortmid e_3 \leftarrow\!\shortmid \ \ldots\ \leftarrow\!\shortmid e_{m-1} \leftarrow\!\shortmid e_m\,. \tag{12-4}$$

[1] Векторы Fe_1 и F^2e_1 суть первые столбцы матриц A и A^2.

[2] Это первый столбец матрицы A^3.

Таким образом, умножение на класс $[t]$ задаётся в базисе $e_1, \dots, e_n$ матрицей

$$J_m(\lambda) \stackrel{\text{def}}{=} \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}, \tag{12-5}$$

которая называется *жордановой клеткой* размера m с *собственным числом* λ. По теор. 12.1 каждый линейный оператор F над алгебраически замкнутым полем подобен оператору умножения на класс $[t]$ в прямой сумме факторколец вида $\Bbbk[t]/\big((t-\lambda)^m\big)$, и два таких оператора подобны, если и только если прямые суммы отличаются друг от друга перестановкой слагаемых. На языке матриц сказанное означает, что любая квадратная матрица A над алгебраически замкнутым полем $\Bbbk$ сопряжена блочно диагональной матрице, по главной диагонали которой располагаются жордановы клетки (12-5), причём эта блочно диагональная матрица однозначно с точностью до перестановки клеток определяется матрицей A. Она называется *жордановой нормальной формой* матрицы A. Две матрицы сопряжены, если и только если у них одинаковые с точностью до перестановки клеток жордановы нормальные формы.

Объединение всех жордановых клеток оператора $F : V \to V$ с заданным собственным числом $\lambda \in \Bbbk$ представляет собою матрицу, описывающую действие оператора F на подмодуле $(t-\lambda)$-кручения, который обозначается $K_\lambda \stackrel{\text{def}}{=} \{v \in V \mid \exists m \in \mathbb{N} : (\lambda \operatorname{Id} - F)^m v = 0\}$ и называется *корневым подпространством* оператора F, отвечающим собственному числу λ. Как $\Bbbk[t]$-модуль он изоморфен прямой сумме $\Bbbk[t]/((t-l)^{m_1}) \oplus \dots \oplus \Bbbk[t]/((t-l)^{m_\ell})$, в которой собраны все элементарные делители оператора F вида $(t-\lambda)^m$. Упорядоченный по нестрогому убыванию $m_1 \geqslant \dots \geqslant m_\ell$ набор показателей $(m_1, \dots, m_\ell)$ называется *цикловым типом* корневого подпространства K_λ. Его удобно изображать диаграммой Юнга из строк длины $m_1, \dots, m_\ell$. Эти показатели в точности равны размерам жордановых клеток с оператора F с собственным числом λ. Наибольший из них m_1 равен кратности корня $t = \lambda$ в минимальном многочлене $\mu_F(t)$ оператора F и и обозначается m_λ. Сумма $m_1 + \dots + m_\ell$ всех показателей равна кратности того же корня $t = \lambda$ в характеристическом многочлене $\chi_F(t)$. Обратите внимание, что характеристический и минимальный многочлены имеют одинаковый набор корней. Он называется *спектром* оператора F и обозначается $\operatorname{Spec} F$, а сами корни $\lambda \in \operatorname{Spec} F$ называются *собственными числами* или *собственными значениями* оператора F.

По лем. 10.2 на стр. 176 высота $\Bbbk$-го столбца диаграммы $(m_1, \dots, m_\ell)$ равна размерности векторного пространства $\ker(F-\lambda E)^k / \ker(F-\lambda E)^{k-1}$ над полем $\Bbbk[t]/(t-\lambda) \simeq \Bbbk$, т. е. разности $\dim \ker(F-\lambda E)^k - \dim \ker(F-\lambda E)^{k-1}$. Таким образом, для отыскания жордановой нормальной формы оператора F над алгебраически замкнутым полем достаточно взять какой-нибудь аннулирующий оператор F многочлен[1] $f \in \Bbbk[t]$, разложить его на линейные множители:

$$f(t) = \prod_\lambda (t-\lambda)^{m(\lambda)}$$

и для каждого корня λ многочлена f вычислить размерности $d_k = \dim \ker(F-\lambda E)^k$ для всех таких $k \geqslant 1$, что $d_k > d_{k-1}$, где мы полагаем $d_0 = 0$. При наступлении равенства[2] $d_{k+1} = d_k$,

[1] Например, характеристический многочлен $\chi_F(t) = \det(tE - F)$.

[2] А оно заведомо наступит при некотором $k \leqslant m(\lambda)$.

вычисление прекращается. Размеры $m_1 \geqslant \ldots \geqslant m_\ell$ жордановых клеток оператора F с собственным числом λ равны длинам строк диаграммы Юнга, k-тый столбец которой имеет длину $d_k - d_{k-1}$.

Пример 12.3 (отыскание жордановой нормальной формы)
Найдём жордановы нормальные формы матриц

$$A = \begin{pmatrix} 2 & -1 & -3 & 1 \\ -9 & -1 & 8 & -1 \\ -1 & -1 & 0 & 1 \\ -1 & 2 & 2 & -2 \end{pmatrix}, \; B = \begin{pmatrix} 5 & 5 & 7 & 1 \\ 6 & 4 & 7 & 1 \\ -6 & -5 & -8 & -1 \\ 3 & 1 & 5 & 1 \end{pmatrix}, \; C = \begin{pmatrix} -2 & 3 & 5 & 1 \\ 3 & 1 & 7 & 2 \\ -6 & 3 & -1 & -1 \\ -9 & 5 & 2 & -3 \end{pmatrix}.$$

Вычисляя след, сумму главных 2×2-миноров, сумму главных 3×3-миноров и определитель каждой из матриц, находим характеристические многочлены, после чего раскладываем их на линейные множители:

$$\chi_A(t) = t^4 + t^3 - 7t^2 - 13t - 6 = (x+1)^2(x+2)(x-3),$$
$$\chi_B(t) = t^4 - 2t^3 - 3t^2 + 4t + 4 = (x+1)^2(x-2)^2,$$
$$\chi_C(t) = t^4 + 5t^3 + 6t^2 - 4t - 8 = (t-1)(t+2)^3.$$

Таким образом, матрица A имеет два одномерных корневых подпространства с собственными числами -2 и 3 и двумерное корневое подпространство с собственным числом -1, цикловой типа которого (2) или $(1,1)$. Первому случаю отвечает $\dim\ker(A+E) = 1$, или $\operatorname{rk}(A+E) = 3$, а второму — $\dim\ker(A+E) = 2$, или $\operatorname{rk}(A+E) = 2$. Так как левый верхний угловой 3×3 минор матрицы $A + E$ равен

$$\det\begin{pmatrix} 3 & -1 & -3 \\ -9 & 0 & 8 \\ -1 & -1 & 1 \end{pmatrix} = 8 - 3 - 9 = -4,$$

мы заключаем, что имеет место первое, т. е. у A одна жорданова клетка размера 2×2 с собственным числом -1, и жорданова нормальная форма матрицы A такова:

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Матрица B имеет два двумерных корневых подпространства с собственными числами $\lambda = -1, 2$. Их цикловые типы, как и выше, определяются размерностями ядер матриц

$$(B+E) = \begin{pmatrix} 6 & 5 & 7 & 1 \\ 6 & 5 & 7 & 1 \\ -6 & -5 & -7 & -1 \\ 3 & 1 & 5 & 2 \end{pmatrix} \quad \text{и} \quad (B-2E) = \begin{pmatrix} 3 & 5 & 7 & 1 \\ 6 & 2 & 7 & 1 \\ -6 & -5 & -10 & -1 \\ 3 & 1 & 5 & -1 \end{pmatrix}.$$

Поскольку первая матрица имеет ранг 2, а вторая — 3, мы заключаем, что B имеет две клетки 1×1 с собственным числом -1 и одну клетку 2×2 с собственным числом 2, т. е. жорданова

нормальная форма матрицы B такова:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Матрица C имеет одну жорданову клетку 1×1 с собственным числом 1 и трёхмерное корневое подпространство с собственным числом -2, цикловой тип которого может быть (3), или (2, 1), или (1, 1, 1). Эти случаи тоже отличаются друг от друга размерностью ядра оператора $C+2E$, которая равна для них соответственно 1, 2, или 3. Так как ранг матрицы

$$C+2E=\begin{pmatrix} 0 & 3 & 5 & 1 \\ 3 & 3 & 7 & 2 \\ -6 & 3 & 1 & -1 \\ -9 & 5 & 2 & -1 \end{pmatrix}$$

равен 3, мы заключаем, что имеет место первый случай, и жорданова нормальная форма матрицы C такова:

$$\begin{pmatrix} -2 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

12.1.7. Нормальные формы матриц над незамкнутыми полями. Так как матрица умножения на t в факторкольце $k[x]/(f)$, где $f=t^m+a_1t^{m-1}+\ldots+a_m$, имеет в базисе из классов многочленов $t^{m-1},\ldots,t,1$ вид

$$F(f)\stackrel{\text{def}}{=}\begin{pmatrix} -a_1 & 1 & & & \\ -a_2 & 0 & 1 & & \\ \vdots & \vdots & \ddots & \ddots & \\ -a_{d-1} & 0 & \ldots & 0 & 1 \\ -a_d & 0 & \ldots & 0 & 0 \end{pmatrix}, \tag{12-6}$$

из теор. 12.2 на стр. 207 вытекает, что каждая матрица над произвольным полем $\Bbbk$ подобна единственной блочно диагональной матрице, составленной из блоков $F(f_1),\ldots,F(f_r)$ вида (12-6), где $f_i\mid f_j$ при $i<j$. Такая блочно диагональная матрица называется *фробениусовой нормальной формой*. Обратите внимание, что последний многочлен f_r в нормальной форме Фробениуса равен минимальному многочлену μ_F оператора F.

Аналогом жордановой клетки (12-5) над произвольным полем $\Bbbk$ является матрица умножения на класс $[t]$ в факторкольце $\Bbbk[t]/(p^m)$, где $p=t^d+a_1t^{d-1}+\ldots+a_d\in\Bbbk[t]$ — неприводимый приведённый многочлен, записанная в базисе

$$p^{m-1}t^{d-1},\ldots,p^{m-1}t,p^{m-1},\ p^{m-2}t^{d-1},\ldots,p^{m-2}t,p^{m-2},\ \ldots,\ldots,\ldots,\ t^{d-1},\ldots,t,1\,, \tag{12-7}$$

который состоит из m последовательных фрагментов вида $p^kt^{m-1},\ldots,p^kt,p^k$ длины d, получающихся из самого правого фрагмента $t^{d-1},\ldots,t,1$ умножением на p^k, где $k=0,1,\ldots,m-1$.

Упражнение 12.10. Убедитесь, что классы многочленов (12-7) действительно образуют базис в $\Bbbk[t]/(p^m)$.

Так как умножение на t переводит класс $p^k t^\ell$ в классы многочленов

$$\begin{aligned} p^k t^{\ell+1}, &\text{ при } 0 \leqslant \ell \leqslant d-2, \\ p^{k+1} - a_1 p^k t^{d-1} + \ldots + a_d p^k, &\text{ при } \ell = d-1,\ k \leqslant m-2, \\ -a_1 p^{m-1} t^{d-1} + \ldots + a_d p^{m-1}, &\text{ при } \ell = d-1,\ k = m-1, \end{aligned}$$

эта матрица имеет вид

$$J_m(p) \stackrel{\text{def}}{=} \begin{pmatrix} -a_1 & 1 & & & & & & & & & & \\ -a_2 & 0 & 1 & & & & & & & & & \\ \vdots & 0 & \ddots & 1 & & & & & & & & \\ -a_d & \vdots & \ddots & 0 & 1 & & & & & & & \\ & 0 & \ddots & 0 & -a_1 & 1 & & & & & & \\ & & \ddots & \vdots & -a_2 & 0 & \ddots & & & & & \\ & & & 0 & \vdots & 0 & \ddots & \ddots & & & & \\ & & & & -a_d & \vdots & \ddots & \ddots & 1 & & & \\ & & & & & 0 & \ddots & \ddots & 0 & 1 & & \\ & & & & & & \ddots & \ddots & 0 & -a_1 & 1 & \\ & & & & & & & \ddots & \vdots & -a_2 & 0 & \ddots \\ & & & & & & & & 0 & \vdots & \vdots & \ddots \\ & & & & & & & & & -a_d & 0 & \ldots \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ 1 \\ 0 \end{matrix} \tag{12-8}$$

где расположенная над главной диагональ заполнена единицами, а на главной диагонали и $d-1$ диагоналях под нею стоят последовательности вида

$$-a_i, \underbrace{0, \ldots, 0}_{d-1}, -a_i, \underbrace{0, \ldots, 0}_{d-1}, \ \ldots\ , -a_i \underbrace{0, \ldots, 0}_{d-i},$$

где $i = 1, \ldots, d$, а все остальные клетки матрицы нулевые.

Упражнение 12.11. Убедитесь, что при $d = 1$ и $p = t - \lambda$ матрица (12-8) превращается в жорданову клетку (12-5).

Из теор. 12.1 на стр. 207 вытекает, что каждая матрица над произвольным полем $\Bbbk$ подобна блочно диагональной матрице, состоящей из обобщённых жордановых клеток (12-8), и две такие матрицы подобны, если и только если они получаются друг из друга перестановкой клеток.

Например, умножение на t в вещественном векторном пространстве

$$V = \mathbb{R}[t]/\left((t^2+1)^2\right) \oplus \mathbb{R}[t]/\left((t+1)^2\right) \oplus \mathbb{R}[t]/(t+1)$$

имеет над полем $\mathbb{R}$ жорданову нормальную форму из трёх клеток размеров 4, 2, 1:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

а его фробениусова нормальна форма получается из разложения $V = \mathbb{R}[t]/(f_1) \oplus \mathbb{R}[t]/(f_2)$, где $f_1 = t+1$, $f_2 = (t^2+1)^2(t+1)^2 = t^6 + 2t^5 + 3t^4 + 4t^3 + 3t^2 + 2t + 1$, и содержит две клетки:

$$\begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ -3 & 0 & 1 & 0 & 0 & 0 & 0 \\ -4 & 0 & 0 & 1 & 0 & 0 & 0 \\ -3 & 0 & 0 & 0 & 1 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \tag{12-9}$$

Умножение на t в аналогичном комплексном векторном пространстве

$$W = \mathbb{C}[t]/\big((t^2+1)^2\big) \oplus \mathbb{C}[t]/\big((t+1)^2\big) \oplus \mathbb{C}[t]/(t+1) \simeq$$
$$\simeq \mathbb{C}[t]/\big((t-i)^2\big) \oplus \mathbb{C}[t]/\big((t+i)^2\big) \oplus \mathbb{C}[t]/\big((t+1)^2\big) \oplus \mathbb{C}[t]/(t+1)$$

имеет над полем $\mathbb{C}$ жорданову нормальную форму из 4-х клеток размеров 2, 2, 2, 1:

$$\begin{pmatrix} -i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

а его фробениусова нормальная форма совпадает с (12-9).

В общем случае объединение всех жордановых клеток (12-8), отвечающих данному неприводимому приведённому многочлену $p \in \Bbbk[t]$, описывает действие оператора $F\colon V \to V$ на подмодуле $p(F)$-кручения

$$K_p \stackrel{\text{def}}{=} \{v \in V \mid \exists\, m \in \mathbb{N}\colon\ p(F)^m v = 0\} \simeq \Bbbk[t]/(p^{m_1}) \oplus \ldots \oplus \Bbbk[t]/(p^{m_\ell})$$

(в правой части собраны все элементарные делители оператора F вида p^m). Упорядоченный по нестрогому убыванию $m_1 \geqslant \ldots \geqslant m_\ell$ набор показателей $(m_1, \ldots, m_\ell)$ называется *цикловым типом* подпространства K_p. Наибольший из них m_1 равен степени, в которой p входит в разложение минимального многочлена $\mu_F(t)$ на неприводимые множители в кольце $\Bbbk[t]$ и обозначается m_p. Сумма $m_1 + \ldots + m_\ell$ всех показателей равна степени, в которой p входит в разложение характеристического многочлена $\chi_F(t)$. По лем. 10.2 на стр. 176 высота $\Bbbk$-го столбца диаграммы Юнга $(m_1, \ldots, m_\ell)$ равна размерности векторного пространства $\ker p(F)^k \,/\, \ker p(F)^{k-1}$ над полем $\Bbbk[t]/(p)$, которое в свою очередь является векторным пространством размерности $\deg p$ над полем $\Bbbk$. Поэтому высота k-того столбца диаграммы $(m_1, \ldots, m_\ell)$ равна отношению

$$(\dim_{\Bbbk} \ker p(F)^k - \dim_{\Bbbk} \ker p(F)^{k-1}) / \deg p\,.$$

Пример 12.4

Выясним, подобны ли друг другу над полем $\mathbb{F}_5$ матрицы

$$A = \begin{pmatrix} 2 & 4 & 0 & 2 \\ 4 & 1 & 4 & 3 \\ 4 & 0 & 4 & 2 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{и} \quad B = \begin{pmatrix} 4 & 2 & 4 & 2 \\ 3 & 3 & 3 & 2 \\ 2 & 3 & 3 & 0 \\ 0 & 1 & 1 & 3 \end{pmatrix}.$$

Обе матрицы имеют один и тот же характеристический многочлен

$$\det(tE - A) = \det(tE - B) = t^4 + 2t^3 + 3t^2 + 2t + 1 = (t^2 + t + 1)^2\,,$$

где $p(t) = t^2 + t + 1 \in \mathbb{F}_5[t]$ неприводим над $\mathbb{F}_5$. Поэтому всё пространство $\mathbb{F}_5^4$ является модулем p-кручения и имеет цикловой тип (2) или (1, 1). В первом случае многочлен p не аннулирует матрицу, а во втором — аннулирует. Так как

$$A^2 = \begin{pmatrix} 4 & 0 & 2 & 3 \\ 4 & 4 & 4 & 2 \\ 3 & 4 & 2 & 3 \\ 4 & 1 & 1 & 3 \end{pmatrix}, \quad \text{а} \quad B^2 = \begin{pmatrix} 0 & 3 & 1 & 3 \\ 2 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 0 & 4 & 4 & 1 \end{pmatrix},$$

и тем самым $p(A) = A^2 + A + E \neq 0$, а $p(B) = B^2 + B + E = 0$, мы заключаем, что матрицы не подобны. Отметим, что из проделанных вычислений вытекает, что жорданова и фробениусова нормальные формы матрицы A имеют соответственно вид

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} -2 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ -2 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

а жорданова нормальная форма матрицы B совпадает с фробениусовой и имеет вид

$$\begin{pmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

12.2. Специальные классы операторов. В этом разделе мы подробно остановимся на свойствах нескольких специальных классов операторов, играющих важную роль в различных задачах из разных областей математики.

12.2.1. Нильпотентные операторы. Линейный оператор $F\colon V \to V$ называется *нильпотентным*, если $F^m = 0$ для некоторого $m \in \mathbb{N}$. Так как нильпотентный оператор аннулируется многочленом t^m, все его элементарные делители являются степенями t. В частности, минимальный многочлен тоже является степенью t и, будучи делителем характеристического многочлена, имеет степень не выше $\dim V$. Поэтому в определении нильпотентного оператора можно без ограничения общности считать, что $m \leqslant \dim V$. По теор. 12.1 нильпотентный оператор изоморфен оператору умножения на класс $[t]$ в прямой сумме факторколец вида

$$\Bbbk[t]/(t^{\nu_1}) \oplus \ldots \oplus \Bbbk[t]/(t^{\nu_k})\,, \tag{12-10}$$

и два таких оператора изоморфны друг другу, если и только если выписанные в порядке нестрогого убывания наборы показателей $\nu_1 \geqslant \nu_2 \geqslant \ldots \geqslant \nu_k$ у них одинаковы. Таким образом, нильпотентные операторы над произвольным полем $\Bbbk$ взаимно однозначно соответствуют диаграммам Юнга ν. Диаграмма $\nu(F)$, характеризующая нильпотентный оператор F, называется его *цикловым типом*.

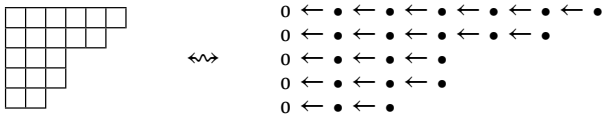
Умножение на t действует на состоящий из векторов $e_i = [t^{m-i}]$ базис в $\Bbbk[t]/(t^m)$ так[1]:

$$0 \leftarrow e_1 \leftarrow e_2 \leftarrow e_3 \leftarrow \ \dots \ \leftarrow e_{m-1} \leftarrow e_m$$

и имеет в этом базисе матрицу

$$J_m(0) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 1 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

которая называется *нильпотентной жордановой клеткой* размера m. Тем самым, для нильпотентного оператора F циклового типа $\nu(F)$ в пространстве V имеется базис, векторы которого размещаются по клеткам диаграммы $\nu(F)$ так, что F переводит каждый из них в левый соседний, а все векторы самого левого столбца — в нуль:



(12-11)

Базис такого вида называется *циклическим* или *жордановым* базисом нильпотентного оператора F, а наборы базисных векторов, стоящие по строкам диаграммы, называются *жордановыми цепочками*. Так как сумма длин первых m столбцов диаграммы $\nu(F)$ равна $\dim\ker F^m$, длина m-того столбца диаграммы $\nu(F)$ равна $\dim\ker F^m - \dim\ker F^{m-1}$.

12.2.2. Полупростые операторы. Прямая сумма простых[2] пространств с операторами называется *полупростым* или *вполне приводимым* пространством с оператором.

Предложение 12.1
Следующие свойства оператора $F : V \to V$ эквивалентны друг другу:

1) V является прямой суммой неприводимых F-инвариантных подпространств

2) V линейно порождается неприводимыми F-инвариантными подпространствами

3) для каждого ненулевого F-инвариантного подпространства $U \subsetneq V$ существует такое F-инвариантное подпространство $W \subset V$, что $V = U \oplus W$

4) оператор F подобен умножению на класс $[t]$ в прямой сумме факторколец

$$\Bbbk[t]/(p_1) \oplus \Bbbk[t]/(p_2) \oplus \dots \oplus \Bbbk[t]/(p_r),$$

где $p_i \in \Bbbk[t]$ приведены и неприводимы[3] (но не обязательно различны).

[1] См. формулу (12-4) на стр. 211.
[2] В другой терминологии — неприводимых, см. начало n° 12.1 на стр. 206.
[3] Иными словами, в прямой сумме (12-1) из теор. 12.1 все показатели степеней $m_i = 1$.

Доказательство. Импликация (1) ⇒ (2) очевидна. Импликация (2) ⇒ (3) вытекает из лем. 9.1 на стр. 131. Для лучшего понимания происходящего повторим её доказательство в нашем нынешнем контексте. Для каждого неприводимого F-инвариантного подпространства $L \subset V$ пересечение $L \cap U$, будучи F-инвариантным подпространством в L, либо нулевое, либо совпадает с L. Если все неприводимые инвариантные подпространства $L \subset V$ лежат в U, то $U = V$ в силу (2), и доказывать нечего. Если есть ненулевое неприводимое F-инвариантное подпространство $L_1 \subset V$ с $L_1 \cap U = 0$, заменим U на $U \oplus L_1$ и повторим рассуждение. Поскольку размерность подпространства U на каждом таком шагу строго увеличивается, через конечное число шагов получится равенство $U \oplus L_1 \oplus \ldots \oplus L_k = V$, и можно взять $W = L_1 \oplus \ldots \oplus L_k$.

Чтобы доказать импликацию (3) ⇒ (4), покажем сначала, что если свойство (3) выполнено для пространства V, то оно выполнено и для каждого F-инвариантного подпространства $H \subset V$. Рассмотрим любое инвариантное подпространство $U \subset H$ и отыщем в V такие инвариантные подпространства Q и R, что $V = H \oplus Q = U \oplus Q \oplus R$. Рассмотрим проекцию $\pi : V \twoheadrightarrow H$ с ядром Q и положим $W = \pi(R)$.

Упражнение 12.12. Проверьте, что $H = U \oplus W$.

Итак, если свойство (3) выполнено для прямой суммы факторколец (12-1) из теор. 12.1, то оно выполнено и для каждого слагаемого этой суммы. Однако по сл. 12.2 пространство $\Bbbk[t]/(p^m)$ при $m > 1$ приводимо, но неразложимо.

Импликация (4) ⇒ (1) также немедленно вытекает из сл. 12.2. □

Следствие 12.5 (из доказательства предл. 12.1)
Ограничение полупростого оператора на инвариантное подпространство также является полупростым оператором. □

12.2.3. Циклические векторы. Вектор $v \in V$ называется *циклическим вектором* линейного оператора $F : V \to V$, если его F-орбита v, Fv, F^2v, F^3v, , … линейно порождает пространство V над полем $\Bbbk$. Иначе можно сказать, что вектор v порождает модуль V_F над $\Bbbk[t]$.

Предложение 12.2
Следующие свойства оператора $F : V \to V$ эквивалентны друг другу:

1) F обладает циклическим вектором

2) F подобен умножению на класс $[t]$ в факторкольце $\Bbbk[t]/(f)$, где $f \in \Bbbk[t]$

3) простые основания всех элементарных делителей оператора F попарно различны

4) минимальный многочлен оператора F совпадает с характеристическим.

Доказательство. Условия (2), (3), (4) очевидно эквивалентны и означают, что оператор F подобен умножению на $[t]$ в прямой сумме факторколец $\Bbbk[t]/(p_1^{m_1}) \oplus \ldots \oplus \Bbbk[t]/(p_r^{m_r})$, где все неприводимые приведённые многочлены $p_1, \ldots, p_r$ попарно различны. Импликация (2) ⇒ (1) тоже очевидна: $\Bbbk[t]$-модуль $\Bbbk[t]/(f)$ порождается над $\Bbbk[t]$ классом $[1]$. Наоборот, если модуль V_F порождается над $\Bbbk[t]$ одним вектором v, то $V_F \simeq \Bbbk[t]/\ker\pi$, где эпиморфизм $\pi : \Bbbk[t] \twoheadrightarrow V_F$ переводит $h(t)$ в $h(F)v$. Поскольку $\Bbbk[t]$ — область главных идеалов, $\ker\pi = (f)$ для некоторого $f \in \Bbbk[t]$, откуда $V \simeq \Bbbk[t]/(f)$. □

12.2.4. Собственные подпространства и собственные числа. Максимальное по включению ненулевое подпространство в V, на котором оператор $F : V \to V$ действует как умножение на скаляр $\lambda \in \Bbbk$, называется *собственным подпространством* оператора F с *собственным числом* или *собственным значением* λ и обозначается $V_\lambda \stackrel{\text{def}}{=} \{v \in V \mid F(v) = \lambda v\} = \ker(\lambda \operatorname{Id}_V - F)$. Ненулевые векторы $v \in V_\lambda$ называются *собственными векторами* оператора F с собственным числом[1] λ.

Предложение 12.3
Любой набор собственных векторов с попарно различными собственными числами линейно независим.

Доказательство. Пусть собственные векторы $v_1, \dots, v_m$ имеют попарно разные собственные числа $\lambda_1, \dots, \lambda_m$ и линейно зависимы. Рассмотрим линейное соотношение между ними, в котором задействовано минимально возможное число векторов. Пусть это будут векторы $e_1, \dots, e_k$. Тогда $k \geqslant 2$ и $e_k = x_1 e_1 + \dots + x_{k-1} e_{k-1}$, где все $x_i \in \Bbbk$ отличны от нуля. При этом $\lambda_k e_k = F(e_k) = \sum x_i F(e_i) = \sum x_i \lambda_i e_i$. Вычитая из этого равенства предыдущее, умноженное на λ_k, получаем более короткую зависимость $x_1(\lambda_1 - \lambda_k)e_1 + \dots + x_{k-1}(\lambda_{k-1} - \lambda_k)e_{k-1} = 0$ с ненулевыми коэффициентами. □

Следствие 12.6
Сумма ненулевых собственных подпространств с попарно разными собственными числами является прямой. □

12.2.5. Спектр. Множество собственных чисел линейного оператора $F : V \to V$, т. е. всех таких $\lambda \in \Bbbk$, что $V_\lambda = \ker(\lambda \operatorname{Id}_V - F) \neq 0$, называется *спектром*[2] оператора F и обозначается

$$\operatorname{Spec} F = \{\lambda \in \Bbbk \mid \ker(\lambda \operatorname{Id}_V - F) \neq 0\} = \{\lambda \in \Bbbk \mid \det(tE - F) = 0\},$$

или $\operatorname{Spec}_\Bbbk F$, если важно явно указать основное поле. Так как $\ker(\lambda \operatorname{Id}_V - F) \neq 0$, если и только если $\det(tE - F) = 0$, спектр представляет собою множество корней характеристического многочлена $\chi_F(t) = \det(tE - F)$ в поле $\Bbbk$. Над алгебраически замкнутым полем спектр любого оператора не пуст и совпадает с множеством собственных чисел жордановых клеток оператора F, о котором шла речь в n° 12.1.6 на стр. 211 выше. Над произвольным полем количество различных собственных чисел в спектре не превосходит $\deg \chi_F = \dim V$, что согласуется со сл. 12.6, согласно которому

$$\sum_{\lambda \in \operatorname{Spec} F} \dim V_\lambda \leqslant \dim V. \tag{12-12}$$

Упражнение 12.13. Покажите, что $\operatorname{Spec} F$ содержится в множестве корней любого многочлена, аннулирующего F.

Если известен спектр F, отыскание собственных подпространств сводится к решению систем линейных однородных уравнений $(\lambda \operatorname{Id}_V - F)\, v = 0$, которые гарантированно имеют ненулевые решения при $\lambda \in \operatorname{Spec} F$.

Следствие 12.7
Над алгебраически замкнутым полем $\Bbbk$ любой оператор обладает хотя бы одним ненулевым собственным подпространством. □

[1] Или собственным значением.
[2] Ср. с n° 12.1.6 на стр. 211.

Упражнение 12.14. Покажите, что над алгебраически замкнутым полем $\Bbbk$ оператор F нильпотентен, если и только если $\operatorname{Spec} F = \{0\}$, и приведите пример оператора, для которого неравенство (12-12) строгое.

12.2.6. Диагонализуемые операторы. Оператор $F : V \to V$ называется *диагонализуемым*, если в V имеется базис, в котором F записывается диагональной матрицей. Такой базис состоит из собственных векторов оператора F, а элементы диагональной матрицы суть собственные числа F, причём каждое собственное число $\lambda \in \operatorname{Spec} F$ встречается на диагонали ровно столько раз, какова кратность корня $t = \lambda$ в характеристическом многочлене $\chi_F(t)$ и какова размерность собственного подпространства V_λ. Иначе можно сказать, что диагонализуемый оператор F подобен оператору умножения на класс $[t]$ в прямой сумме факторколец[1] $\Bbbk[t]/(t-\lambda) \simeq \Bbbk$, где λ пробегает $\operatorname{Spec} F$, и каждое такое прямое слагаемое представлено в сумме ровно $\dim V_\lambda$ раз.

Предложение 12.4
Следующие свойства линейного оператора $F : V \to V$ эквивалентны:

1) F диагонализуем

2) пространство V линейно порождается собственными векторами оператора F

3) все элементарные делители F имеют вид $(t-\lambda)$, $\lambda \in \Bbbk$

4) характеристический многочлен $\chi_F(t) = \det(tE - F)$ полностью раскладывается в $\Bbbk[t]$ на линейные множители, и кратность каждого его корня λ равна размерности собственного подпространства V_λ

5) оператор F можно аннулировать многочленом, который раскладывается в $\Bbbk[t]$ в произведение попарно различных линейных множителей.

Доказательство. Эквивалентность свойств (3) и (5) очевидна. Эквивалентность свойств (1), (2), (3) и импликация (1) $\Rightarrow$ (4) были установлены перед формулировкой предл. 12.4. Из (4) вытекает, что $\sum \dim V_\lambda = \deg \chi_F = \dim V$. Поэтому прямая по сл. 12.6 сумма всех различных собственных подпространств V_λ совпадает с V, что даёт импликацию (4) $\Rightarrow$ (1). □

Следствие 12.8
Если оператор $F : V \to V$ диагонализуем, то его ограничение на любое инвариантное подпространство тоже диагонализуемо на этом подпространстве.

Доказательство. Это вытекает из свойства (5) предл. 12.4. □

Упражнение 12.15. Убедитесь, что над алгебраически замкнутым полем диагонализуемость равносильна полупростоте.

[1] Ср. с упр. 12.9 на стр. 211.

12.2.7. Что стоит за аннулирующим многочленом? Если известно разложение на простые множители того или иного многочлена, аннулирующего линейный оператор[1] $F : V \to V$, то это, во-первых, оставляет лишь конечное число возможностей для набора элементарных делителей $\mathcal{El}(F)$ оператора F, а во-вторых, позволяет явно строить F-инвариантные подпространства в V и/или раскладывать V в прямую сумму таких подпространств в терминах действия F непосредственно на пространстве V.

Пример 12.5 (инвариантные подпространства вещественного оператора)
Покажем, что над полем вещественных чисел $\mathbb{R}$ любой конечномерный линейный оператор F обладает одномерным или двумерным инвариантным подпространством. Пусть $\chi_F = q_1 \dots q_m$, где $q_i \in \mathbb{R}[t]$ — неприводимые приведённые линейные или квадратичные многочлены, не обязательно различные. Применим нулевой оператор $0 = \chi_F(F) = q_1(F) \circ q_2(F) \circ \dots \circ q_m(F)$ к какому-нибудь ненулевому вектору $v \in V$. При некотором $i \geqslant 0$ получится такой ненулевой вектор $w = q_{i+1}(F) \circ \dots \circ q_m(F)\, v$, что $q_i(F)\, w = 0$. Если $q_i(t) = t - \lambda$ линеен, то $F(w) = \lambda w$ и вектор w порождает одномерное F-инвариантное подпространство. Если $q_i(t) = t^2 - \alpha t - \beta$ квадратичен, то $F(Fw) = \alpha F(w) + \beta w$ лежит в линейной оболочке векторов w и Fw, которая тем самым является F-инвариантным подпространством размерности не больше 2.

Пример 12.6 (инволюции)
Линейный оператор $\sigma : V \to V$ называется *инволюцией*, если он удовлетворяет соотношению $\sigma^2 = \mathrm{Id}_V$, т. е. аннулируется многочленом $t^2 - 1$. Тождественная инволюция $\sigma = \mathrm{Id}_V$ называется *тривиальной*. Так как $t^2 - 1 = (t+1)(t-1)$ является произведением различных линейных множителей, все инволюции диагонализуемы, причём спектр любой инволюции исчерпывается числами ± 1. Таким образом, любое пространство V с инволюцией $\sigma \neq \pm\mathrm{Id}_V$ распадается в прямую сумму $V = V_+ \oplus V_-$ собственных подпространств $V_+ = \ker(\sigma - \mathrm{Id}_V) = \mathrm{im}(\sigma + \mathrm{Id}_V)$ и $V_- = \ker(\sigma + \mathrm{Id}_V) = \mathrm{im}(\sigma - \mathrm{Id}_V)$ с собственными числами ± 1, и любой вектор $v \in V$ однозначно записывается как $v = v_+ + v_-$, где $v_\pm \in V_\pm$ находятся по формулам $v_+ = (v+Fv)/2$, $v_- = (v-Fv)/2$.

Теорема 12.3 (теорема о разложении)
Пусть линейный оператор $F : V \to V$ на произвольном[2] векторном пространстве V над произвольным полем $\Bbbk$ аннулируется произведением $q = q_1 \dots q_r$ попарно взаимно простых многочленов $q_i \in \Bbbk[t]$. Положим $Q_j = q/q_j$. Тогда $\ker q_j(F) = \mathrm{im}\, Q_j(F)$ при всех j, эти подпространства F-инвариантны, и V является прямой суммой тех из них, что отличны от нуля.

Доказательство. Так как $q(F) = q_i(F) \circ Q_j(F) = 0$, имеем включение $\mathrm{im}\, Q_i(F) \subset \ker q_i(F)$. Поэтому достаточно показать, что V линейно порождается образами операторов $Q_i(F)$, а сумма ядер $\ker q_i(F)$ прямая[3], т. е. $\ker q_i(F) \cap \sum_{j \neq i} \ker q_j(F) = 0$ для всех i. Первое вытекает из того, что $\dots(Q_1, \dots, Q_r) = 1$, а значит, существуют такие $h_1, \dots, h_r \in \Bbbk[t]$, что $1 = \sum Q_j(t) h_j(t)$. Подставляя в это равенство $t = F$ и применяя обе части к произвольному вектору $v \in V$, получаем разложение $v = Ev = \sum Q_j(F) h_j(F) v \in \sum \mathrm{im}\, Q_j(F)$. Второе вытекает из взаимной простоты q_i и Q_i, в силу которой существуют такие $g, h \in \Bbbk[t]$, что $1 = g(t) \cdot q_i(t) + h(t) \cdot Q_i(t)$. Подставим сюда $t = F$ и применим обе части полученного равенства $E = g(F)\, q_i(F) + h(F) \circ Q_i(F)$ к произвольному вектору $v \in \ker q_i(F) \cap \sum_{j \neq i} \ker q_j$. Так как $\ker q_j(F) \subset \ker Q_i(F)$ при всех $j \neq i$, получим $v = Ev = g(F)\, q_i(F)\, v + h(F)\, Q_i(F)\, v = 0$, что и требовалось. □

[1] Например, характеристического многочлена $\chi_F(t) = \det(tE - F)$.

[2] Возможно даже бесконечномерном.

[3] См. предл. 6.2 на стр. 106.

Пример 12.7 (проекторы)
Линейный оператор $\pi : V \to V$ называется *идемпотентом* или *проектором*, если он аннулируется многочленом $t^2 - t = t(t-1)$, т. е. удовлетворяет соотношению $\pi^2 = \pi$. По теор. 12.3 образ любого идемпотента $\pi : V \to V$ совпадает с подпространством его неподвижных векторов: $\operatorname{im}\pi = \ker(\pi - \mathrm{Id}_V) = \{v \mid \pi(v) = v\}$, и всё пространство распадается в прямую сумму $V = \ker\pi \oplus \operatorname{im}\pi$. Тем самым, оператор π проектирует V на $\operatorname{im}\pi$ вдоль $\ker\pi$. Отметим, что оператор $\mathrm{Id}_V - \pi$ тоже является идемпотентом и проектирует V на $\ker\pi$ вдоль $\operatorname{im}\pi$. Таким образом, задание прямого разложения $V = U \oplus W$ равносильно заданию пары идемпотентных эндоморфизмов $\pi_1 = \pi_1^2$ и $\pi_2 = \pi_2^2$ пространства V, связанных соотношениями $\pi_1 + \pi_2 = 1$ и $\pi_1\pi_2 = \pi_2\pi_1 = 0$.

Упражнение 12.16. Выведите из этих соотношений, что $\ker\pi_1 = \operatorname{im}\pi_2$ и $\operatorname{im}\pi_1 = \ker\pi_2$.

12.3. Функции от операторов. Всюду в этом разделе мы предполагаем, что линейный оператор $F : V \to V$ действует на конечномерном векторном пространстве V над полем $\mathbb{R}$ или $\mathbb{C}$, которое мы будем обозначать через $\mathbb{K}$, и аннулируется многочленом

$$\alpha(t) = (t-\lambda_1)^{m_1} \dots (t-\lambda_r)^{m_r}, \text{ где } \lambda_i \neq \lambda_j \text{ при } i \neq j, \tag{12-13}$$

который полностью разлагается на линейные множители в $\mathbb{K}[t]$. Последнее означает, что минимальный и характеристический многочлены оператора F тоже полностью разлагался на линейные множители в $\mathbb{K}[t]$, и в практических вычислениях в качестве $\alpha(t)$ обычно берётся характеристический многочлен $\chi_F(t)$ оператора F. Однако, чем меньше степень многочлена $\alpha(t)$, тем проще будут все предстоящие нам вычисления.

Сделанные нами предположения на оператор F равносильны тому, что $\mathcal{El}(F)$ исчерпывается степенями линейных двучленов $(t-\lambda)^m$, $\lambda \in \operatorname{Spec} F$. В этой ситуации $\mathbb{K}[t]$-модуль V_F является прямой суммой $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ *корневых подпространств*[1]

$$K_\lambda \stackrel{\text{def}}{=} \{v \in V \mid \exists\, m \in \mathbb{N} : (\lambda\,\mathrm{Id} - F)^m v = 0\} = \ker(\lambda\,\mathrm{Id} - F)^{m_\lambda}, \tag{12-14}$$

биективно соответствующих собственным числам $\lambda \in \operatorname{Spec} F$. Показатель m_λ в правой части формулы (12-14) равен кратности корня $t = \lambda$ минимального многочлена $\mu_F(t)$ оператора[2] F. Множество корней $\lambda_1, \dots, \lambda_r$ многочлена (12-13) содержит $\operatorname{Spec}(F)$ и для каждого $\lambda \in \operatorname{Spec} F$ показатель m_λ не больше кратности корня $t = \lambda$ многочлена (12-13).

Упражнение 12.17. Не прибегая к теор. 12.1 на стр. 207, выведите существование *корневого разложения* $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ из тождества Гамильтона – Кэли и теор. 12.3 на стр. 222.

12.3.1. Гомоморфизм вычисления. Алгебра $\mathcal{A}$, состоящая из функций $U \to \mathbb{K}$, заданных на каком-нибудь подмножестве $U \subset \mathbb{K}$, содержащем все корни многочлена (12-13), называется *алгебраически вычислимой* на операторе F, если $\mathbb{K}[t] \subset \mathcal{A}$ и для каждого корня λ кратности k многочлена (12-13) все функции $f \in \mathcal{A}$ определены в точке $\lambda \in \mathbb{K}$ вместе с первыми $k-1$ производными $f^{(\nu)} = \frac{d^\nu f}{dt^\nu}$ и допускают тейлоровское разложение вида

$$f(t) = f(\lambda) + \frac{f'(\lambda)}{1!}(t-\lambda) + \dots + \frac{f^{(k-1)}(\lambda)}{(k-1)!}(t-\lambda)^{k-1} + g_\lambda(t)\cdot(t-\lambda)^k, \tag{12-15}$$

[1] Т. е. подмодулей $(t-\lambda)$-кручения, см. n° 12.1.6 на стр. 211.

[2] Т. е. максимальному из показателей степеней элементарных делителей вида $(t-\lambda)^m$ оператора F.

где функция $g_\lambda(t)$ тоже лежит в алгебре $\mathcal{A}$.

Например, алгебра $\mathcal{A}$ всех функций, определённых в ε-окрестности каждого собственного числа $\lambda \in \operatorname{Spec} F$ и представимых в ней суммой абсолютно сходящегося степенного ряда от $(t-\lambda)$, алгебраически вычислима на операторе F. Подалгебра в $\mathcal{A}$, состоящая из всех аналитических функций[1] $\mathbb{K} \to \mathbb{K}$, алгебраически вычислима на всех операторах $F \in \operatorname{End}_{\mathbb{K}}(V)$, характеристические многочлены которых полностью разлагаются на линейные множители в $\mathbb{K}[t]$.

Теорема 12.4
В сделанных выше предположениях каждая алгебраически вычислимая на операторе $F: V \to V$ алгебра функций $\mathcal{A}$ допускает единственный такой гомоморфизм $\mathbb{K}$-алгебр $\operatorname{ev}_F: \mathcal{A} \to \operatorname{End} V$, что $\operatorname{ev}_F(p) = p(F)$ для всех многочленов $p \in \mathbb{K}[t] \subset \mathcal{A}$.

Доказательство теор. 12.4. Пусть оператор F аннулируется многочленом (12-13), и пусть искомый гомоморфизм $\operatorname{ev}_F: \mathcal{A} \to \mathbb{K}$ существует. Пространство V является прямой суммой F-инвариантных корневых подпространств $K_\lambda = \ker(F-\lambda\mathrm{Id})^{m_\lambda}$. Согласно формуле (12-15) оператор

$$f(F) = f(\lambda)\cdot E + f'(\lambda)\cdot(F-\lambda E) + \ldots + \frac{f^{(m_\lambda-1)}(\lambda)}{(m_\lambda-1)!}(F-\lambda E)^{m_\lambda-1} + g_\lambda(F)(F-\lambda E)^{m_\lambda} \tag{12-16}$$

действует на каждом подпространстве K_λ точно так же, как результат подстановки оператора F в многочлен $j_\lambda^{m_\lambda-1}f(t) \stackrel{\text{def}}{=} f(\lambda) + f'(\lambda)\cdot(t-\lambda) + \ldots + f^{(m_\lambda-1)}(\lambda)\cdot(t-\lambda)^{m_\lambda-1}/(m_\lambda-1)!$. Класс этого многочлена в факторкольце $\mathbb{K}[t]/\big((t-\lambda)^{m_\lambda}\big)$ называется $(m_\lambda-1)$-*струёй* функции $f \in \mathcal{A}$ в точке $\lambda \in \mathbb{K}$. По китайской теореме об остатках существует единственный такой многочлен $p_{f(F)}(t) \in \mathbb{K}[t]$ степени, строго меньшей $\deg\alpha(t)$, что $p_{f(F)}(t) \equiv j_\lambda^{m_\lambda-1}f(t) \,(\mathrm{mod}\,\alpha(t))$ сразу для всех корней λ многочлена α. Поскольку операторы $p_{f(F)}(F)$ и $f(F)$ одинаково действуют на каждом подпространстве K_λ, имеется равенство $f(F) = p_{f(F)}(F)$. Таким образом, гомоморфизм вычисления единствен. Остаётся убедиться, что отображение $f \mapsto p_{f(F)}(F)$ действительно является гомоморфизмом $\mathbb{K}$-алгебр. Проверим сначала, что отображение

$$\begin{gathered} J: \mathcal{A} \to \frac{\mathbb{K}[t]}{\big((t-\lambda_1)^{m_1}\big)} \times \ldots \times \frac{\mathbb{K}[t]}{\big((t-\lambda_r)^{m_r}\big)} \simeq \frac{\mathbb{K}[t]}{(\alpha)}, \\ f \mapsto \left(j_{\lambda_1}^{m_1-1}f, \ldots, j_{\lambda_s}^{m_r-1}f\right), \end{gathered} \tag{12-17}$$

сопоставляющее функции $f \in \mathcal{A}$ набор её струй[2] во всех корнях многочлена α, является гомоморфизмом $\mathbb{K}$-алгебр, т. е. $\mathbb{K}$-линейно и удовлетворяет равенству $J(fg) = J(f)J(g)$. Первое очевидно, второе достаточно установить для каждой струи j_λ^{m-1} отдельно. Используя правило Лейбница: $(fg)^{(k)} = \sum_{\nu=0}^{k}\binom{k}{\nu}f^{(\nu)}g^{(k-\nu)}$, получаем следующие равенства по модулю $(t-\lambda)^m$:

$$\begin{aligned} j_\lambda^{m-1}(fg) &= \sum_{k=0}^{m-1}\frac{(t-\lambda)^k}{k!}\sum_{\nu+\mu=k}\frac{k!}{\nu!\mu!}f^{(\nu)}(\lambda)g^{(\mu)}(\lambda) = \\ &= \sum_{k=0}^{m-1}\sum_{\nu+\mu=k}\frac{f^{(\nu)}(\lambda)}{\nu!}(t-\lambda)^\nu\cdot\frac{g^{(\mu)}(\lambda)}{\mu!}(t-\lambda)^\mu \equiv j_\lambda^{m-1}(f)j_\lambda^{m-1}(g). \end{aligned}$$

[1] Т. е. функций, задаваемых сходящимися всюду в $\mathbb{K}$ степенными рядами.

[2] Мы рассматриваем этот набор как элемент прямого произведения соответствующих колец вычетов, которое по китайской теореме об остатках изоморфно факторкольцу $\mathbb{K}[t]/(\alpha)$.

Отображение $f \mapsto p_{f(F)}(F)$ является композицией гомоморфизма (12-17) с гомоморфизмом вычисления многочленов $\mathrm{ev}_F : \mathbb{K}[t] \to \operatorname{End} V, p \mapsto p(F)$, который корректно пропускается через фактор $\mathbb{K}[t]/(\alpha)$, так как $\alpha(F) = 0$. □

Определение 12.1 (гомоморфизм вычисления)
Гомоморфизм $\mathrm{ev}_F : \mathcal{A} \to \operatorname{End} V$ из теор. 12.4 называется *вычислением* функций $f \in \mathcal{A}$ на операторе F. Линейный оператор $\mathrm{ev}_F(f) : V \to V$, в который переходит функция $f \in \mathcal{A}$ при гомоморфизме вычисления, обозначается $f(F)$ и называется *функцией f от оператора F*.

Замечание 12.1. (как относиться к функциям от операторов) Из теор. 12.4 вытекает, что если характеристический многочлен линейного оператора $F : V \to V$ полностью разлагается на линейные множители в $\mathbb{K}[t]$, то на пространстве V определены такие линейные операторы, как e^F или $\sin F$, а если $F \in \mathrm{GL}(V)$, то и такие задаваемые аналитическими вне нуля функциями операторы, как $\ln F$ или $\sqrt{F}$, причём алгебраические свойства всех этих операторов точно такие же, как у числовых функций e^t, $\sin t$, $\ln t$ и $\sqrt{t}$. В частности, все эти функции от оператора F коммутируют друг с другом и с F, а также удовлетворяют соотношениям вроде $\ln F^2 = 2 \ln F$ и $\sqrt{F}\sqrt{F} = F$. Таким образом, функции от операторов можно использовать для отыскания операторов с предписанными свойствами, например, удовлетворяющих заданному алгебраическому или дифференциальному уравнению, в частности, для извлечения корней из невырожденных операторов.

Предложение 12.5
В условиях теор. 12.4 на стр. 224 для любой функции f из алгебраически вычислимой на операторе F алгебры функций $\mathcal{A}$ спектр оператора $f(F)$ состоит из чисел $f(\lambda)$, где $\lambda \in \operatorname{Spec} F$. Если $f'(\lambda) \neq 0$, то элементарные делители $(t-\lambda)^m \in \mathcal{E}\ell(F)$ биективно соответствуют элементарным делителям $\big(t-f(\lambda)\big)^m \in \mathcal{E}\ell\big(f(F)\big)$. Если $f'(\lambda) = 0$, то каждому элементарному делителю $(t-\lambda)^m$ с $m > 1$ из $\mathcal{E}\ell(F)$ в множестве $\mathcal{E}\ell\big(f(F)\big)$ соответствует объединение нескольких элементарных делителей вида $\big(t-f(\lambda)\big)^{\ell_i}$ с $\ell_i \in \mathbb{N}$ и $\sum_i \ell_i = m$.

Доказательство. Реализуем F как оператор умножения на класс $[t]$ в прямой сумме факторколец $V = \mathbb{K}[t]/\big((t-\lambda_1)^{s_1}\big) \oplus \ldots \oplus \mathbb{K}[t]/\big((t-\lambda_r)^{s_r}\big)$. Как мы видели в доказательстве теор. 12.4 ограничение оператора $f(F)$ на корневое подпространство K_λ раскладывается в сумму скалярного оператора $f(\lambda)\,E$ и нильпотентного оператора $N = f'(\lambda)\cdot\eta + \frac{1}{2} f''(\lambda)\cdot\eta^2 + \ldots$, где $\eta : K_\lambda \to K_\lambda$ обозначает оператор умножения на класс $[t-\lambda]$. На каждом слагаемом $\mathbb{K}[t]/\big((t-\lambda)^m\big)$ оператор η имеет ровно одну жорданову цепочку максимальной длины m. Если $f'(\lambda) \neq 0$, то

$$N^{m-1} = f'(\lambda)^{m-1} \cdot \eta^{m-1} \neq 0\,.$$

Поэтому N тоже имеет ровно одну жорданову цепочку длины m. При $f'(\lambda) = 0$ и $m > 1$ равенство $N^k = 0$ наступит при $k < m$. Поэтому цикловой тип ограничения оператора N на каждое слагаемое вида $\mathbb{K}[t]/\big((t-\lambda)^m\big)$ состоит из нескольких цепочек суммарной длины m. □

Упражнение 12.18. Покажите, что матрица $J_n^{-1}(\lambda)$, обратная к жордановой клетке размера $n \times n$ с собственным числом λ, подобна матрице $J_n(\lambda^{-1})$.

12.3.2. Интерполяционный многочлен. Многочлен $p_{f(F)}(t) \in \mathbb{K}[t]$, принимающий на операторе F то же самое значение, что и функция $f \in \mathcal{A}$, называется *интерполяционным многочленом* для вычисления $f(F)$. Он однозначно определяется тем, что его степень строго меньше степени аннулирующего оператор f многочлена α и в каждом корне кратности m многочлена α сам многочлен $p_{f(F)}$ и первые его $m-1$ производные принимают те же значения, что функция f и её первые $m-1$ производные. Таким образом, при $\deg \alpha = d$ отыскание коэффициентов интерполяционного многочлена $p_{f(F)}$ сводится к решению системы из d линейных уравнений на d неизвестных.

Лемма 12.2 (об интерполяции с кратными узлами[1])
Для любых различных чисел $a_1, \ldots, a_n$ из любого поля $\Bbbk$ и произвольно заданного для каждого a_i набора из m_i значений $b_{i,0}, b_{i,1}, \ldots, b_{i,m_i-1} \in \Bbbk$ существует единственный такой многочлен $g \in \Bbbk[x]$ степени строго меньше $m = m_1 + \ldots + m_n$, что при каждом $i = 1, \ldots, n$ сам этот многочлен и первые его $m_i - 1$ производные принимают в точке a_i заданные значения

$$g(a_i) = b_{i,0},\ g'(a_i) = b_{i,1},\ \ldots\ ,\ g^{(m_i-1)}(a_i) = b_{i,m_i-1}\,,$$

где $g^{(k)}(x) = d^k g(x)/dx^k$ означает k-тую производную многочлена g.

Доказательство. Введём на m парах чисел (i,j), где $1 \leqslant i \leqslant n$, $0 \leqslant j < m_j$, какой-нибудь линейный порядок и рассмотрим отображение $F : \Bbbk[x]_{<m} \to \Bbbk^m$, переводящее каждый многочлен g степени меньше m в набор значений[2] $g^{(j)}(a_i)$, записанных в одну строку в выбранном на парах (i,j) порядке.

Упражнение 12.19. Убедитесь, что отображение F линейно.

Если $g \in \ker F$, то по предл. 3.6 на стр. 50 каждое число $a_i \in \Bbbk$ является как минимум m_i-кратным корнем многочлена g, т. е. g делится на $\prod_i (x-a_i)_i^m$, откуда $g = 0$, ибо степень произведения равна $m > \deg g$. Мы заключаем, что $\ker F = 0$. Поскольку $\dim \Bbbk[x]_{<m} = \dim \Bbbk^m$, отображение F биективно. □

Пример 12.8 (степенная функция и рекуррентные уравнения, ср. с прим. 4.6 на стр. 67)
Задача отыскания n-того члена a_n числовой последовательности $z : \mathbb{Z} \to \mathbb{K}$, $n \mapsto z_n$, решающей рекуррентное уравнение $z_n = \alpha_1 z_{n-1} + \alpha_2 z_{n-2} + \ldots + \alpha_m z_{n-m}$ с начальным условием $(z_0, \ldots, z_{n-1}) = (a_0, \ldots, a_{n-1}) \in \mathbb{K}^n$, сводится вычислению n-той степени *матрицы сдвига*

$$S = \begin{pmatrix} 0 & 0 & \ldots & 0 & \alpha_m \\ 1 & 0 & \ddots & \vdots & \alpha_{m-1} \\ 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & \alpha_2 \\ 0 & \ldots & 0 & 1 & \alpha_1 \end{pmatrix}$$

смещающей каждый фрагмент из m последовательных элементов на один шаг вправо:

$$(z_{k+1},\ z_{k+2},\ \ldots\ ,\ z_{k+m}) \cdot S = (z_{k+2},\ z_{k+3},\ \ldots\ ,\ z_{k+m+1})\,.$$

[1] Это утверждение обобщает **??** на стр. **??**.

[2] Где для единообразия обозначений мы полагаем $g^{(0)} \stackrel{\text{def}}{=} g$.

Искомый элемент a_n при этом равен первой координате вектора

$$(a_n,\, a_{n+1},\, \dots\, ,\, a_{n+m-1}) = (a_0, a_1, \dots, a_{m-1}) \cdot S^n\,.$$

Матрица $S^n = p_{S^n}(S)$ является результатом подстановки матрицы S в интерполяционный многочлен $p_{S^n}(t) \in \mathbb{K}[t]$ для вычисления на матрице S *степенной функции* $f(t) = t^n$. Обратите внимание, что $\deg p_{S^n} < m$, и коэффициенты многочлена p_{S^n} находятся решением системы из m линейных уравнений на m неизвестных.

Например, для *уравнения Фибоначчи* $a_n = a_{n-1} + a_{n-2}$ матрица сдвига имеет вид

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Интерполяционный многочлен для вычисления степенной функции t^n на этой матрице линеен. Записывая его в виде $p_{S^n}(t) = at + b$ с неопределёнными коэффициентами a и b, получаем

$$S^n = a\,S + b\,E = \begin{pmatrix} b & a \\ a & a+b \end{pmatrix}.$$

Таким образом, n-тое *число Фибоначчи*, решающее уравнение Фибоначчи с начальным условием $(a_0, a_1) = (0, 1)$, равно первой координате вектора $\left(a_n, a_{n+1}\right) = (0,1) \cdot S^n = (a, a+b)$. Матрица S аннулируется своим характеристическим многочленом

$$\chi_S(t) = t^2 - t\ \operatorname{tr} S + \det S = t^2 - t - 1 = (t - \lambda_+)(t - \lambda_-)$$

с однократными корнями $\lambda_\pm = (1 \pm \sqrt{5})/2$. Функция t^n принимает на них значения $\lambda_\pm^n$. Коэффициенты a и b находятся из системы

$$\begin{cases} a\,\lambda_+ + b = \lambda_+^n \\ a\,\lambda_- + b = \lambda_-^n\,, \end{cases}$$

и по правилу Крамера $a = \left(\lambda_+^n - \lambda_-^n\right) / \left(\lambda_+ - \lambda_-\right)$. Тем самым,

$$a_n = a = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n \cdot \sqrt{5}}\,,$$

что согласуется с прим. 4.6 на стр. 67.

Пример 12.9 (квадратный корень из оператора)
Покажем, что если поле $\Bbbk$ алгебраически замкнуто и $\operatorname{char}\Bbbk \neq 2$, то из любого биективного линейного оператора F на конечномерном векторном пространстве V над полем $\Bbbk$ можно извлечь квадратный корень, являющийся многочленом от оператора F. В прим. 4.8 на стр. 71 мы видели, что при всех целых $k \geqslant 0$ биномиальный коэффициент $\binom{2k}{k}$ нацело делится на $(k+1)$, и если $\operatorname{char}\Bbbk \neq 2$, то корректно определён биномиальный степенной ряд[1]

$$\sqrt{1+x} = \sum_{k\geqslant 0} \binom{1/2}{k} x^k = 1 + \frac{1}{2} \sum_{k\geqslant 1} \frac{(-1)^{k-1}}{4^{k-1}} \binom{2k-2}{k-1} \frac{x^k}{k}\,. \tag{12-18}$$

[1] См. формулу (4-19) на стр. 71.

Упражнение 12.20. Убедитесь в том, что квадрат многочлена, равного сумме первых $n+1$ членов этого ряда, равен $1+x$ в $\Bbbk[x]/(x^{n+1})$.

Если поле $\Bbbk$ алгебраически замкнуто, характеристический многочлен $\chi_F(t)$ оператора F разлагается на взаимно простые множители $(t-\lambda)^{m_\lambda}$, где $\lambda \in \operatorname{Spec}(F)$, и пространство V является прямой суммой F-инвариантных корневых подпространств $K_\lambda = \ker(F-\lambda\mathrm{Id})^{m_\lambda}$. Так как F биективен, все числа λ в этом разложении отличны от нуля. Для каждого $\lambda \in \operatorname{Spec}(F)$ обозначим через $p_\lambda(t) \in \Bbbk[t]$ сумму первых m_λ членов формального разложения Тэйлора функции $\sqrt{t}$ в точке λ, которое получается из (12-18) заменой переменных:

$$\sqrt{t} = \sqrt{\lambda+(t-\lambda)} = \sqrt{\lambda}\cdot\big(1+(t-\lambda)/\lambda\big)^{1/2} = \lambda^{1/2} + \frac{t-\lambda}{2\lambda^{1/2}} - \frac{(t-\lambda)^2}{8\lambda^{3/2}} + \frac{(t-\lambda)^3}{16\lambda^{5/2}} - \dots .$$

Тогда $p_\lambda^2(t) \equiv t \bmod (t-\lambda)^{m_\lambda}$ в силу упр. 12.20. По китайской теореме об остатках существует многочлен $p(t)$, сравнимый с $p_\lambda(t)$ по модулю $(t-\lambda)^{m_\lambda}$ сразу для всех $\lambda \in \operatorname{Spec}(F)$. Он имеет $p^2(t) \equiv t \bmod (t-\lambda)^{m_\lambda}$ для всех $\lambda \in \operatorname{Spec}(F)$. Поскольку квадрат оператора $p(F)$ действует на каждом корневом подпространстве K_λ точно также, как F, мы заключаем, что $p^2(F) = F$.

Замечание 12.2. (аналитически определённые функции от оператора) Гомоморфизм вычисления значений многочленов на матрице $F \in \mathrm{Mat}_n(\mathbb{C})$ можно продолжать на бóльшие алгебры функций $\mathcal{C} \supset \mathbb{C}[z]$ средствами анализа: наделим пространства $\mathcal{C}$ и $\mathrm{Mat}_n(\mathbb{C})$ той или иной топологией, представим функцию $f \in \mathcal{C}$ в виде предела $f = \lim_{k\to\infty} f_k$ какой-нибудь последовательности многочленов f_k и положим матрицу $f(F)$ равной пределу последовательности матриц $f_k(F) \in \mathrm{Mat}_n(\mathbb{C})$. Разумеется, при этом необходимо проверять, что предел $\lim_{k\to\infty} f_k(F)$ существует и зависит только от функции f, а не от выбора сходящейся к f последовательности многочленов, и отдельно следует убедиться в том, что полученное таким образом отображение $\mathrm{ev}_F : \mathcal{C} \to \mathrm{Mat}_n(\mathbb{C})$, $f \mapsto f(F)$, является гомоморфизмом алгебр[1]. Но если это так, и если переход к пределу в пространстве матриц перестановочен со сложением и умножением на константы[2], то как бы ни определялась сходимость в пространстве функций и какой бы ни была сходящаяся к функции f последовательность многочленов f_k, последовательность матриц $f_k(F)$ будет лежать в конечномерном векторном пространстве, порождённом над $\mathbb{C}$ степенями F^m с $0 \leqslant m < n$, т. е. её предел *a priori* будет многочленом от F степени, строго меньшей n, а значит, может быть вычислен при помощи подходящего интерполяционного многочлена. Если матрицы F и G подобны, т. е. $G = CFC^{-1}$ для некоторой матрицы $C \in \mathrm{GL}_k(\mathbb{C})$, то аналитически определённые функции от этих матриц тоже будут подобны: так как равенство $f_k(G) = Cf_k(F)C^{-1}$ справедливо для всех многочленов, приближающих функцию f, оно выполняется и для предельной функции в силу непрерывности линейного отображения $\mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C})$, $X \mapsto CXC^{-1}$.

12.4. Перестановочные операторы и разложение Жордана. Если линейные операторы F и G на векторном пространстве V над произвольным полем $\Bbbk$ коммутируют друг с другом, то ядро

[1] Иначе не вполне понятно, зачем оно нужно. В качестве упражнения по анализу читателю настоятельно рекомендуется попробовать самостоятельно реализовать намеченную программу, используя на пространстве функций топологию, в которой сходимость последовательности функций означает равномерную сходимость в каждом круге в $\mathbb{C}$, а на пространстве $\mathrm{Mat}_n(\mathbb{C})$ — стандартную топологию пространства $\mathbb{C}^{n^2}$, где сходимость определяется покоординатно.

[2] Т. е. $\lim\limits_{k\to\infty}(\lambda F_k + \mu G_k) = \lambda \lim\limits_{k\to\infty} F_k + \mu \lim\limits_{k\to\infty} G_k$. Это означает, в частности, что все $\mathbb{C}$-линейные отображения $\mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C})$ непрерывны.

и образ любого многочлена от оператора F переводятся оператором G в себя:

$$f(F)\,v = 0 \quad \Rightarrow \quad f(F)\,Gv = Gf(F)\,v = 0$$
$$v = f(F)\,w \quad \Rightarrow \quad Gv = Gf(F)\,w = f(F)\,Gw\,.$$

В частности, все собственные подпространства $V_\lambda = \ker(F - \lambda E)$ инвариантны относительно любого перестановочного с F оператора G.

Предложение 12.6
В конечномерном векторном пространстве V над алгебраически замкнутым полем $\Bbbk$ любое множество коммутирующих друг с другом операторов обладает общим для всех операторов собственным вектором. Над произвольным полем $\Bbbk$ любое множество коммутирующих друг с другом диагонализуемых операторов на V можно одновременно диагонализовать в некотором общем для всех операторов базисе.

Доказательство. Индукция по $\dim V$. Если все операторы скалярны (что так при $\dim V = 1$), то доказывать нечего — подойдут, соответственно, любой ненулевой вектор и любой базис. Если среди операторов есть хоть один нескалярный оператор F, то над замкнутым полем у него есть собственное подпространство строго меньшей размерности, чем V, а в диагонализуемом случае V является прямой суммой таких собственных подпространств. Каждое собственное подпространство оператора F инвариантно для всех операторов, причём если операторы диагонализуемы на всём пространстве, то их ограничения на собственные подпространства оператора F тоже диагонализуемы по сл. 12.8. Применяя к собственному подпространству (соответственно ко всем собственным подпространствам) оператора F предположение индукции, получаем требуемое. □

Пример 12.10 (конечные группы операторов)
Если m линейных операторов на конечномерном пространстве V над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \nmid m$ образуют группу G, то каждый из этих операторов аннулируется многочленом $t^m - 1$, который раскладывается в произведение m попарно различных линейных множителей[1]. Поэтому каждый оператор в группе G диагонализуем. Все операторы из группы G одновременно диагонализуются в одном общем базисе, если и только если группа G абелева.

Теорема 12.5 (разложение Жордана)
Для каждого оператора F на конечномерном векторном пространстве V над алгебраически замкнутым полем $\Bbbk$ существует единственная пара таких операторов F_d и F_n, что F_n нильпотентен, F_d диагонализуем, $F_dF_n = F_nF_d$ и $F = F_d + F_n$. Эти единственные операторы F_d и F_n являются многочленами без свободных членов от оператора F.

Доказательство. Пусть $\operatorname{Spec} F = \{\lambda_1, \dots, \lambda_r\}$. В силу алгебраической замкнутости поля $\Bbbk$, характеристический многочлен $\chi_F(t) = \prod_{\lambda\in\operatorname{Spec} F}(t-\lambda)^{m_\lambda}$ полностью разлагается на линейные множители, и пространство $V = \bigoplus_{\lambda\in\operatorname{Spec} F} K_\lambda$ является прямой суммой корневых подпространств $K_\lambda = \ker(F - \lambda\operatorname{Id})^{m_\lambda}$. В качестве диагонализуемого оператора F_d можно взять оператор, действующий на каждом корневом подпространстве K_λ умножением на λ, а в качестве нильпотентного

[1] Поскольку производная mt^{m-1} многочлена $t^m - 1$ отлична от нуля и взаимно проста с ним.

оператора F_n — разность $F_n = F - F_d$, которая действует на каждом корневом подпространстве K_λ нильпотентным оператором $F - \lambda\,\mathrm{Id}$.

Покажем, что оба эти оператора являются многочленами без свободного члена от F. Для этого достаточно представить в таком виде оператор F_d. Для каждого ненулевого $\lambda \in \operatorname{Spec} F$ обозначим через $g_\lambda \in \Bbbk[x]$ многочлен, представляющий класс λ/t в $\Bbbk[x]/\big((t-\lambda)^{m_\lambda}\big)$, а для $\lambda = 0$ положим $g_\lambda(t) = 0$. По китайской теореме об остатках существует многочлен $g \in \Bbbk[x]$, сравнимый с g_λ по модулю $(t-\lambda)^{m_\lambda}$ сразу для всех $\lambda \in \operatorname{Spec} F$. Многочлен tg_λ не имеет свободного члена, и его класс в $\Bbbk[x]/\big((t-\lambda)^{m_\lambda}\big)$ равен классу λ для всех $\lambda \in \operatorname{Spec} F$. Поэтому оператор $g(F)$ действует на каждом корневом подпространстве K_λ как умножение на λ, т. е. совпадает с F_d.

Будучи многочленами от F, операторы F_d и $F_n = F - F_d$ перестановочны между собою и с F. Это доказывает существование операторов F_d и F_n с требуемыми свойствами, включающими в себя и последнее утверждение предложения. Докажем их единственность.

Пусть есть ещё одно разложение $F = F'_d + F'_n$, в котором F'_d диагонализуем, F'_n нильпотентен и $F'_d F'_n = F'_n F'_d$. Из последнего равенства вытекает, что F'_d и F'_n перестановочны с любым многочленом от $F = F'_d + F'_n$, в частности, с построенными выше F_d и F_n. Поэтому каждое собственное подпространство V_λ оператора F_d переводится оператором F'_d в себя[1], причём F'_d диагонализуем[2] на каждом V_λ. Если бы оператор F'_d имел на V_λ собственный вектор с собственным значением $\mu \neq \lambda$, то этот вектор был бы собственным для оператора $F_n - F'_n = F_d - F'_d$ с собственным значением $\lambda - \mu \neq 0$, что невозможно, так как оператор $F_n - F'_n$ нильпотентен.

Упражнение 12.21. Докажите, что разность двух перестановочных нильпотентных операторов нильпотентна.

Следовательно, оператор F'_d действует на каждом собственном подпространстве V_λ оператора F_d как умножение на λ, откуда $F'_d = F_d$. Тогда и $F'_n = F - F'_d = F - F_d = F_n$. □

Определение 12.2
Операторы F_d и F_n из теор. 12.5 называются, соответственно, *диагонализуемой* и *нильпотентной* составляющими оператора F.

Замечание 12.3. Поскольку операторы F_d и F_n являются многочленами от F, каждое F-инвариантное подпространство $U \subset V$ является инвариантным для F_d и F_n.

Задачи для самостоятельного решения к §12

Задача 12.1. Найдите степень минимального многочлена квадратной матрицы ранга 1.

Задача 12.2. Существует ли (1) над полем $\mathbb{Q}$ (2) над каким-нибудь полем оператор с характеристическим и минимальным многочленами
а) $\chi(t) = (t^6+1)$, $\mu(t) = (t^2+1)$ б) $\chi(t) = (t-1)^2(t-2)^3$, $\mu(t) = (t-1)(t-2)$
в) $\chi(t) = (t-1)^5(t-2)^5$, $\mu(t) = (t-1)^2(t-2)^3$? Если да, то приведите пример.

[1] См. n° 12.4 на стр. 228.
[2] См. сл. 12.8 на стр. 221.

Задача 12.3. Перечислите, с точностью до подобия, все рациональные матрицы с характеристическим многочленом а) $(x-2)^3$ б) $(x-3)^4$ в) x^4-1 г) $(x^4-1)^2$. Какие из них диагонализуемы? Какие полупросты? У каких есть циклический вектор?

Задача 12.4. Найдите минимальные многочлены и элементарные делители следующих матриц над полем $\mathbb{F}_5$: а) $\begin{pmatrix}1&1\\2&2\end{pmatrix}$ б) $\begin{pmatrix}1&1&0\\2&2&-2\\-2&-2&1\end{pmatrix}$ в) $\begin{pmatrix}1&1&0&-1\\2&2&-2&2\\-2&-2&1&-2\\1&-2&1&-2\end{pmatrix}$. Какие из них диагонализуемы? Какие полупросты? У каких есть циклический вектор?

Задача 12.5. Над полями $\mathbb{F}_p$ с $p = 2, 3, 5$ перечислите с точностью до подобия все а) 2×2 матрицы б) невырожденные 2×2 матрицы в) 2×2 матрицы определителя 1.

Задача 12.6. Перечислите, с точностью до подобия, все такие матрицы $A \in \mathrm{Mat}_3(\mathbb{F}_3)$, что $A^4 = A$.

Задача 12.7. Пусть минимальный многочлен оператора $F\colon V \to V$ является произведением попарно взаимно простых многочленов g_i. Покажите, что $V = \bigoplus U_i$, где $F(U_i) \subset U_i$ и минимальный многочлен ограничения $F|_{U_i}$ равен g_i при всех i.

Задача 12.8. Найдите все инвариантные подпространства оператора с диагональной матрицей.

Задача 12.9. Найдите собственные числа, собственные подпространства и минимальный многочлен оператора $\sum x_i \frac{\partial}{\partial x_i}$ на пространстве $\mathbb{Q}[x_1, \dots, x_n]_{\leqslant n}$ многочленов степени не выше n.

Задача 12.10. Линейный оператор $\mathbb{R}^n \to \mathbb{R}^n$ имеет матрицу с числами $\lambda_1, \dots, \lambda_n$ на побочной диагонали и нулями в остальных местах. Когда он диагонализуем?

Задача 12.11. Существуют ли $(n+1)$-мерные векторные подпространства в $\mathrm{End}(\Bbbk^n)$, состоящие из попарно перестановочных диагонализуемых операторов $\Bbbk^n \to \Bbbk^n$?

Задача 12.12. Диагонализуем ли над $\mathbb{Q}$ оператор F, удовлетворяющий уравнению

$$F^3 = 6F^2 - 11F + 6E?$$

Задача 12.13. Установите биекцию между разложениями $V = U_1 \oplus \dots \oplus U_s$ и такими разложениями $\mathrm{Id}_V = \pi_1 + \dots \pi_s$ в $\mathrm{End}\, V$, что $\pi_i^2 = \pi_i$ при всех i и $\pi_i\pi_j = \pi_j\pi_i = 0$ при всех $i \neq j$.

Задача 12.14. Докажите следующие свойства проекторов[1] $\pi_U, \pi_W\colon V \to V$ с образами $U, W \subset V$: а) $\pi_U + \pi_W$ является проектором если и только если $\pi_U\pi_W = 0$, и в этом случае $\pi_U + \pi_W = \pi_{U+W}$ б) $\pi_U\pi_W$ является проектором если и только если $\pi_U\pi_W = \pi_W\pi_U$, и в этом случае $\pi_U\pi_W = \pi_{U\cap W}$ в) $U \subset W$ если и только если $\pi_W\pi_U = \pi_U$.

Задача 12.15. Покажите, что любые два коммутирующих линейных оператора $F, G\colon \mathbb{C}^n \to \mathbb{C}^n$ в некотором базисе можно одновременно записать верхнетреугольными матрицами.

Задача 12.16. Вычислите $\mathrm{Hom}_{\Bbbk[x]}\big(\Bbbk[x]/(f), \Bbbk[x]/(g)\big)$ и его размерность.

Задача 12.17 (циклические векторы). Вектор $v \in V$ называется *циклическим* для линейного оператора $F\colon V \to V$, если векторы вида $F^k v$, где $k \geqslant 0$, линейно порождают V. Верно ли, что каждый ненулевой вектор $v \in V$ является циклическим для F, если а) характеристический многочлен оператора F неприводим б) степень минимального многочлена оператора F равна $\dim V$?

[1] См. прим. 12.7 на стр. 223.

Задача 12.18. Есть ли циклический вектор у оператора $\mathbb{Q}^4 \to \mathbb{Q}^4$ с матрицей $\begin{pmatrix} * & * & * & * \\ 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \end{pmatrix}$?

Задача 12.19. Положим $Z_F \stackrel{\text{def}}{=} \{G \in \operatorname{End}(V) \mid FG = GF\}$, $\Bbbk[F] \stackrel{\text{def}}{=} \{h(F) \mid h \in \Bbbk[t]\}$. Верно ли, что а) равенство $Z_F = \Bbbk[F]$ равносильно наличию циклического вектора б) если поле алгебраически замкнуто и оператор G перестановочен со всеми операторами из Z_F, то $G \in \Bbbk[F]$?

Задача 12.20. Всюду плотны ли матрицы с циклическим вектором а) в $\operatorname{Mat}_n(\mathbb{C})$ б) в $\operatorname{Mat}_n(\mathbb{R})$?

Задача 12.21 (принцип расщепления). Покажите, что: а) диагонализуемые операторы всюду плотны в $\operatorname{End}(\mathbb{C}^n)$ б) если утверждение про матрицу A записывается системой полиномиальных соотношений с целыми коэффициентами на матричные элементы a_{ij}, то из его справедливости для какого-нибудь всюду плотного множества матриц A в $\operatorname{Mat}_n(\mathbb{C})$ или в $\operatorname{Mat}_n(\mathbb{R})$ вытекает, что оно верно для всех матриц над любым коммутативным кольцом в) если система полиномиальных соотношений на a_{ij} из предыдущего пункта не меняется при заменах $A \mapsto CAC^{-1}$ с произвольными обратимыми комплексными матрицами[1] C, то её достаточно проверить для диагональных комплексных матриц г) чтобы доказать тождество Гамильтона – Кэли $\chi_A(A) = 0$ для всех матриц A над любым коммутативным кольцом, его достаточно проверить для диагональных комплексных матриц (и сделайте эту проверку).

Задача 12.22. Свяжем с матрицей $A \in \operatorname{Mat}_n(K)$, где K — любое коммутативное кольцо, линейные отображения $L_A, R_A, \operatorname{ad}_A, \operatorname{Ad}_A : \operatorname{Mat}_n(K) \to \operatorname{Mat}_n(K)$, заданные правилами а) $L_A(X) = AX$ б) $R_A(X) = XA$ в) $\operatorname{ad}_A(X) = AX - XA$ г) $\operatorname{Ad}_A(X) = AXA^{-1}$ (тут предполагается, что A обратима). С помощью принципа расщепления найдите их следы и определители.

Задача 12.23. Те же вопросы про линейные эндоморфизмы, которые матрица A задаёт на пространстве а) грассмановых б) обычных однородных многочленов степени 2 от строки переменных $\xi = (\xi_1, \dots, \xi_n)$ по правилу $f(\xi) \mapsto f(\xi A)$.

Задача 12.24. Над произвольным коммутативным кольцом K с единицей докажите для любых матриц $A \in \operatorname{Mat}_{m\times n}(K)$ и $B \in \operatorname{Mat}_{n\times m}(K)$ равенство $\chi_{AB}(t)/\chi_{BA}(t) = t^{m-n}$.

Задача 12.25. Матрица $A = \begin{pmatrix} -7 & -9 \\ -8 & -2 \end{pmatrix}$ задаёт на пространстве всех матриц размера 2×2 линейный оператор $X \mapsto AXA^{-1}$. Найдите минимальный многочлен этого оператора.

Задача 12.26. Матрица $A = \begin{pmatrix} -1 & -1 \\ -2 & -8 \end{pmatrix}$ задаёт на пространстве всех матриц размера 2×2 линейный оператор $X \mapsto AX + XA$. Найдите минимальный многочлен этого оператора.

Задача 12.27. Найдите собственные числа, собственные и корневые подпространства[2] и выясните, диагонализуем ли линейный оператор $F : \mathbb{Q}^3 \to \mathbb{Q}^3$ с матрицей

а) $\begin{pmatrix} -5 & -3 & 0 \\ 6 & 4 & 0 \\ -18 & -9 & 1 \end{pmatrix}$ б) $\begin{pmatrix} -2 & 16 & 5 \\ -1 & 3 & 1 \\ 3 & 0 & 0 \end{pmatrix}$ в) $\begin{pmatrix} -2 & -2 & 1 \\ 1 & 8 & -5 \\ 2 & 20 & -12 \end{pmatrix}$ г) $\begin{pmatrix} -8 & -2 & -5 \\ -14 & -5 & -10 \\ 14 & 8 & 13 \end{pmatrix}$

Задача 12.28. Найдите минимальные многочлены и ЖНФ следующих матриц над полем $\mathbb{C}$:

[1] Т. е. является утверждением не про матрицу A, но про линейный оператор $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ с матрицей A в некотором базисе.

[2] Т. е. явно укажите в них какие-нибудь базисы.

а) $\begin{pmatrix}-1 & 0 & 0\\ -2 & -4 & 3\\ -2 & -3 & 2\end{pmatrix}$ б) $\begin{pmatrix}-1 & -3 & -1\\ -1 & 1 & 1\\ -1 & 3 & -1\end{pmatrix}$ в) $\begin{pmatrix}-2 & -2 & 2 & 0\\ 1 & 0 & -4 & -3\\ 1 & 2 & -6 & -3\\ -1 & -2 & 5 & 2\end{pmatrix}$ г) $\begin{pmatrix}3 & -3 & -1 & -1\\ 2 & -2 & -2 & -1\\ 0 & 0 & 1 & 0\\ -2 & 3 & 4 & 2\end{pmatrix}$.

Задача 12.29. Найдите размерности корневых подпространств и минимальный многочлен линейного оператора $F\colon \mathbb{Q}^4 \to \mathbb{Q}^4$ с матрицей

а) $\begin{pmatrix}-9 & -5 & -11 & 6\\ 27 & 14 & 27 & -14\\ -25 & -12 & -22 & 11\\ -37 & -18 & -35 & 18\end{pmatrix}$ б) $\begin{pmatrix}-11 & -5 & 0 & -2\\ 40 & 17 & 2 & 4\\ -24 & -8 & -5 & 4\\ -28 & -10 & -5 & 3\end{pmatrix}$ в) $\begin{pmatrix}9 & 4 & 4 & 1\\ -21 & -10 & -12 & -3\\ -17 & -5 & 3 & 1\\ -29 & -11 & -8 & -3\end{pmatrix}$

Задача 12.30. Найдите ЖНФ а) операторов $\partial/\partial x$ и $x\,\partial/\partial x$ на пространстве $\mathbb{C}[x]_{\leqslant n}$ многочленов степени $\leqslant n$ б) оператора $\partial/\partial x$ на пространстве $e^{cx}\mathbb{C}[x]_{\leqslant n}$ функций вида $e^{cx}f(x)$, где $c \in \mathbb{C}$ фиксировано, а $f \in \mathbb{C}[x]_{\leqslant n}$.

Задача 12.31. Линейный оператор $\mathbb{Q}^3 \mapsto \mathbb{Q}^3$ имеет в стандартном базисе матрицу

$$\begin{pmatrix}-5 & -6 & 6\\ 15 & 16 & -15\\ 12 & 12 & -11\end{pmatrix}.$$

Существует ли в $\mathbb{Q}^3$ такой базис, в котором этот оператор записывается матрицей

а) $\begin{pmatrix}12 & -6 & 1\\ 28 & -14 & 2\\ 11 & -6 & 2\end{pmatrix}$ б) $\begin{pmatrix}-8 & 9 & -9\\ 6 & -5 & 6\\ 12 & -12 & 13\end{pmatrix}$?

Задача 12.32. Существует ли такая вещественная 3×3-матрица A, что

$$A^4 = \begin{pmatrix}3 & -3 & 1\\ 1 & -1 & 1\\ -4 & 3 & -2\end{pmatrix}?$$

Если да, приведите пример такой матрицы, если нет, объясните, почему.

Задача 12.33. Существует ли такая комплексная матрица A, что

а) $e^A = \begin{pmatrix}-2 & 2 & 1\\ 2 & -3 & -2\\ -5 & 6 & 4\end{pmatrix}$ б) $e^A = \begin{pmatrix}3 & 1 & -2\\ 8 & 5 & -9\\ 1 & -2 & 3\end{pmatrix}$

в) $A^6 = \begin{pmatrix}6 & 10 & 1\\ -3 & -7 & -1\\ 13 & 22 & 2\end{pmatrix}$ г) $A^5 = \begin{pmatrix}6 & 10 & 1\\ -3 & -7 & -1\\ 13 & 22 & 2\end{pmatrix}$ д) $A^6 = \begin{pmatrix}0 & -1 & 1\\ 7 & 6 & -5\\ 2 & 1 & 1\end{pmatrix}$?

Если да, предъявите такую матрицу явно. Если нет, объясните почему.

Задача 12.34. Найдите ЖНФ квадрата $J_m^2(\lambda)$ жордановой клетки размера $m\times m$ с собственным числом а) $\lambda \neq 0$ б) $\lambda = 0$.

Задача 12.35. Для сходящегося в окрестности точки $\lambda \in \mathbb{C}$ ряда $f \in \mathbb{C}[\![z]\!]$ выразите элементы матрицы $f(J_m(\lambda))$ через значения f и его производных в точке λ.

Задача 12.36. Равносильна ли нильпотентность линейного оператора F над алгебраически замкнутым полем $\Bbbk$ тому, что $\operatorname{tr} F^k = 0$ при всех $1 \leqslant k \leqslant n$, если а*) $\operatorname{char}\Bbbk = 0$ б) $\operatorname{char}\Bbbk \neq 0$?

Задача 12.37. Пусть операторы F и G таковы, что $FG - GF = G$. Покажите, что G нильпотентен.

Задача 12.38 (лемма Барта). Докажите, что над алгебраически замкнутым полем любые два линейных оператора F, G с $\operatorname{rk}(FG - GF) = 1$ имеют общий собственный вектор.

Задача 12.39. Докажите для коммутирующих операторов F и G равенства[1] $(F+G)_s = F_s + G_s$ и $(F+G)_n = F_n + G_n$.

[1] F_s и F_n означают полупростое и нильпотентное слагаемые разложения Жордана оператора F из теор. 12.5 на стр. 229

§13. Аффинные и проективные пространства

13.1. Аффинные пространства. Множество A называется *аффинным пространством* над векторным пространством V, если каждой упорядоченной паре точек $a, b \in A$ сопоставлен вектор $\overrightarrow{ab} \in V$ так, что для любой точки $p \in A$ отображение *векторизации с центром в* p

$$v_p : A \to V\,, \quad q \mapsto \overrightarrow{pq}\,,$$

взаимно однозначно, и для любых трёх (не обязательно различных) точек $a, b, c \in A$ выполняется *правило треугольника* $\overrightarrow{ab} + \overrightarrow{bc} = \overrightarrow{ac}$.

Упражнение 13.1. Выведите из этих свойств, что: а) $\overrightarrow{aa} = 0$ для всех точек $a \in A$ б) $\overrightarrow{pq} = -\overrightarrow{qp}$ для всех точек $p, q \in A$ в) $\overrightarrow{ab} = \overrightarrow{dc} \Leftrightarrow \overrightarrow{bc} = \overrightarrow{ad}$ для любой четвёрки точек $a, b, b, d \in A$.

Иначе можно сказать, что каждому вектору $v \in V$ сопоставлено биективное *преобразование сдвига*[1] *на вектор* v

$$\tau_v : A \to A\,, \quad p \mapsto p + v\,,$$

со следующими двумя свойствами: для каждой пары точек $p, q \in A$ имеется единственный такой вектор $v \in V$, что $p + v = q$, и для любых векторов $u, w \in V$ выполняется равенство

$$\tau_u \circ \tau_v = \tau_{u+w}\,.$$

Это определение эквивалентно предыдущему: вектор $v \in V$ со свойством $p + v = q$, о котором идёт речь во втором определении, это вектор $\overrightarrow{pq}$ из первого определения, а правило треугольника из первого определения означает равенство $\tau_u \circ \tau_v = \tau_{u+w}$ во втором.

Упражнение 13.2. Убедитесь в этом и покажите, что во втором определении требование биективности всех преобразований $\tau_v : A \to A$ можно заменить требованием, чтобы сдвиг на нулевой вектор действовал тождественно: $\tau_0 = \mathrm{Id}_A$.

Пример 13.1 (аффинное координатное пространство $\mathbb{A}^n(\Bbbk)$)
Множество $\mathbb{A}^n(\Bbbk)$, точками которого являются упорядоченные наборы чисел $p = (p_1, \ldots, p_n)$ из поля $\Bbbk$, и каждой паре точек p, q сопоставляется вектор $\overrightarrow{pq} = q - p = (q_1 - p_1, \ldots, q_n - p_n) \in \Bbbk^n$, очевидно удовлетворяет предыдущим определениям. Оно называется *аффинным координатным пространством* над полем $\Bbbk$ и как множество совпадает с векторным пространством $\Bbbk^n$, однако структура аффинного пространства и структура векторного пространства — это две *разные* дополнительные структуры, заданные на одном и том же множестве.

Пример 13.2 (приведённые многочлены)
Пространство $\mathcal{P}_n$, точками которого являются приведённые[2] многочлены степени n с коэффициентами в поле $\Bbbk$ не является векторным пространством, поскольку сумма двух приведённых многочленов $p = x^n + p_1 x^{n-1} + \ldots + p_n$ и $q = x^n + q_1 x^{n-1} + \ldots + q_n$, как и произведение приведённого многочлена на отличное от 1 число, не являются приведёнными многочленами. Однако разности $q - p = (q_1 - p_1)x^{n-1} + \ldots + (q_n - p_n)$ при фиксированном p находятся в биекции с векторами из векторного пространства $\Bbbk[x]_{\leqslant(n-1)}$ всех многочленов степени не выше $n-1$, и эта биекция очевидно удовлетворят предыдущим определениям. Поэтому пространство $\mathcal{P}_n$ является аффинным пространством над векторным пространством $\Bbbk[x]_{\leqslant(n-1)}$.

[1] Или *откладывание вектора* v от точек $p \in A$.

[2] Т. е. со старшим коэффициентом 1.

Пример 13.3 (дополнительные подпространства)
Рассмотрим векторное пространство V и его собственное ненулевое подпространство $W \subsetneq V$. Покажем, что множество всех таких подпространств $U \subset V$, что $V = U \oplus W$, является аффинным пространством над векторным пространством $\mathrm{Hom}(V/W, W)$. Любые два дополнительные к W подпространства U_1, U_2 изоморфно отображаются на V/W при факторизации $\pi_W : V \twoheadrightarrow V/W$. Поэтому у каждого класса $[v] = [v_1] = [v_2] \in V/W$ имеются единственные представители $v_1 \in U_1$ и $v_2 \in U_2$, а их разность $v_2 - v_1 \in W$. Сопоставим каждой упорядоченной паре дополнительных к W подпространств U_1, U_2 линейное отображение $\overrightarrow{U_1U_2} \in \mathrm{Hom}(V/W, W)$, переводящее класс $[v] \in V/W$ в разность $v_2 - v_1$.

Упражнение 13.3. Убедитесь, что $\overrightarrow{U_1U_2} + \overrightarrow{U_2U_3} = \overrightarrow{U_1U_3}$.

Если зафиксировать подпространство U_1 и отождествить его с V/W при помощи отображения π_W, биекция между $\mathrm{Hom}(U_1, W)$ и дополнительными к W подпространствами $U_2 \subset U_1 \oplus W$ сопоставляет линейному отображению $\varphi : U_1 \to W$ его график

$$U_2 = \Gamma_\varphi \stackrel{\text{def}}{=} \{(u_1, \varphi(u_1)) \in U_1 \oplus W \mid u_1 \in U_1\}$$

Упражнение 13.4. Убедитесь, что отображение векторных пространств $\varphi : U \to W$ линейно если и только если его график $\Gamma_\varphi = \{(u, \varphi(u)) \in U \oplus W \mid u \in U\}$ является векторным подпространством в $U \oplus W$, что задаёт биекцию между $\mathrm{Hom}(U, W)$ и множеством векторных подпространств $L \subset U \oplus W$, изоморфно проектирующихся на U вдоль W.

Пример 13.4 (аффинизация векторного пространства)
Из каждого векторного пространства V можно изготовить аффинное пространство $\mathbb{A}(V)$, которое называется *аффинизацией* векторного пространства V. Точками пространства $\mathbb{A}(V)$ по определению являются векторы из V. В пространстве $\mathbb{A}(V)$ имеется выделенная точка 0, отвечающая нулевому вектору, а все остальные точки продуктивно воспринимать как «концы» всевозможных «радиус-векторов» $v \in V$, отложенных от нулевой точки. Сдвиг $\tau_v : \mathbb{A}(V) \to \mathbb{A}(V)$ переводит точку a, отвечающую радиус-вектору $a \in V$, в точку $a + v$, отвечающую радиус-вектору $a + v$.

13.1.1. Аффинные подпространства. Для любой точки p аффинного пространства A над векторным пространством V и любого векторного подпространства $U \subset V$ множество точек

$$\Pi(p, U) = p + U = \{\tau_u(p) \mid u \in U\}$$

называется проходящим через точку p *аффинным подпространством* в A с *направляющим векторным пространством* U. Размерность аффинного пространства $\Pi(p, U)$ по определению полагается равной размерности $\dim U$ его направляющего векторного подпространства.

Пример 13.5 (прямые и плоскости)
Одномерные и двумерные аффинные подпространства называются *прямыми* и *плоскостями* соответственно. Аффинная прямая представляет собою ГМТ вида $p + vt$, где p — некоторая точка, v — ненулевой вектор, а t пробегает $\Bbbk$. Аффинная плоскость — ГМТ вида $p + \lambda u + \mu w$, где p — некоторая точка, u, w — пара непропорциональных векторов, а $(\lambda, \mu) \in \Bbbk^2$.

Упражнение 13.5 (параллелограммы). Скажем, что четыре различные точки a, b, c, d образуют *параллелограмм* $abcd$, если они лежат в одной плоскости и прямая (ab) не пересекается с прямой (cd), а прямая (ad) не пересекается с прямой (bc). Убедитесь, что $abcd$ параллелограмм если и только если выполняются следующие эквивалентные друг другу условия: (1) $\overrightarrow{ab} = \overrightarrow{dc}$ (2) $\overrightarrow{ad} = \overrightarrow{bc}$ (3) $\overrightarrow{ac} = \overrightarrow{ab} + \overrightarrow{ad}$.

Пример 13.6 (системы линейных уравнений)
Множество решений совместной системы линейных уравнений[1] $Ax = b$ на вектор $x \in \Bbbk^n$, где $A \in \mathrm{Mat}_{m\times n}(\Bbbk)$ и $b \in \Bbbk^m$ заданы, представляет собой аффинное подпространство в $\mathbb{A}^n(\Bbbk)$. Его направляющее векторное пространство $U = \{x \in \Bbbk^n \mid Ax = 0\}$ имеет размерность[2] $n - \operatorname{rk} A$. Любое аффинное подпространство $p + U \subset \mathbb{A}(V)$ является множеством решений системы из $\dim V - \dim U$ линейных уравнений $\xi(x) = \xi(p)$, где $x \in V$ — неизвестный переменный вектор, а ковекторы ξ пробегают какой-нибудь базис в $\mathrm{Ann}(U) \subset V^*$.

Предложение 13.1
Аффинные подпространства $p + U$ и $q + W$ пересекаются если и только если $\overrightarrow{pq} \in U + W$, и в этом случае их пересечение является аффинным пространством с направляющим векторным пространством $U \cap W$.

Доказательство. Равенство $\overrightarrow{pq} = u + w$ равносильно равенству $p + u = q - w$, означающему, что точка $r = p + u = q - w \in (p + U) \cap (q + W)$. Если такая точка r существует, то для любой лежащей в пересечении $(p + U) \cap (q + W)$ точки $r' = p + u' = q + w'$ вектор $\overrightarrow{rr'} = u' - u = w' + w \in U \cap W$. Наоборот, для любого вектора $v \in U \cap W$ точка $r + v$ лежит в $(p + U) \cap (q + W)$. □

Пример 13.7 (аффинные подпространства заданного направления)
Если аффинное пространство $A = \mathbb{A}(V)$ является аффинизацией векторного пространства V, то аффинные подпространства $\Pi(p, U) = p + U = [p]_U$ с заданным направляющим пространством $U \subset V$ суть не что иное, как классы векторов $p \in V$ по модулю подпространства U. Таким образом, аффинные подпространства с заданным направляющим пространством U находятся в естественной биекции с векторами факторпространства V/U.

Следствие 13.1
Следующие условия на аффинные подпространства $p + U$ и $q + U$ с одним и тем же направляющим подпространством $U \subset V$ эквивалентны: (1) $\overrightarrow{pq} \in U$ (2) $p \in q + U$ (3) $q \in p + U$ (4) $p + U = q + U$ (5) $(p + U) \cap (q + W) \neq \varnothing$. □

Предложение 13.2
Точки $p_0, p_1, \ldots, p_k$ аффинного пространства $\mathbb{A}$ тогда и только тогда, когда не содержатся ни в каком $(k-1)$-мерном аффинном подпространстве, когда векторы $\overrightarrow{p_0p_1}, \ldots, \overrightarrow{p_0p_k}$ линейно независимы, и в этом случае через точки $p_0, p_1, \ldots, p_k$ проходит единственное k-мерное аффинное подпространство.

Доказательство. Линейная зависимость k векторов $\overrightarrow{p_0p_i}$ равносильна тому, что их линейная оболочка имеет размерность не больше $k - 1$. Это в свою очередь означает, что в V найдётся $(k-1)$-мерное векторное подпространство U, содержащее все векторы $\overrightarrow{p_0p_i}$. Последнее равносильно тому, что $(k-1)$-мерное аффинное подпространство $p_0 + U$ содержит все точки p_i. Если векторы $\overrightarrow{p_0p_i}$ линейно независимы, то они составляют базис в любом содержащем их k-мерном векторном подпространстве $U \subset V$, и значит, любое такое подпространство совпадает с их линейной оболочкой. Поскольку прохождение аффинного пространства $p_0 + U$ через все точки p_i равносильно тому, что все векторы $\overrightarrow{p_0p_i}$ лежат в U, мы заключаем, что такое пространство $p_0 + U$ ровно одно и его направляющее векторное пространство U представляет собою линейную оболочку векторов $\overrightarrow{p_0p_i}$. □

[1] См. n° 8.5 на стр. 144.
[2] См. n° 8.5.1 на стр. 144.

13.1.2. Аффинные координаты. Набор $(p; e_1, \dots, e_n)$, состоящий из точки p аффинного пространства A над векторным пространством V и базиса $e_1, \dots, e_n$ в V, называется *аффинным репером с началом* в p. С каждым аффинным репером связана *аффинная система координат*, сопоставляющая точке $q \in A$ набор коэффициентов $x = (x_1, \dots, x_n)$ разложения

$$\overrightarrow{pq} = x_1 e_1 + \dots + x_n e_n\,.$$

Он называется *аффинными координатами* точки q в репере $(p; e_1, \dots, e_n)$. Так как точки $q \in A$ находятся в биекции с векторами $\overrightarrow{pq} \in V$, а эти векторы — с наборами координат $x \in \Bbbk^n$, аффинная координатная система задаёт биекцию между точками пространства A и координатными наборами $x \in \Bbbk^n$. В n-мерном аффинном пространстве любой набор из $n+1$ не лежащих в одной гиперплоскости точек $p_0, p_1, \dots, p_n$ в задаёт координатный репер с началом в точке p_0 и базисными векторами $e_i = \overrightarrow{p_0 p_i} \in V$.

13.2. Аффинные отображения. Отображение $\varphi\colon A \to B$ между аффинными пространствами A и B, ассоциированными с векторными пространствами U и W, называется *аффинным*, если хотя бы для одной точки $a \in A$ отображение векторных пространств

$$D_\varphi\colon U \to W\,, \quad \overrightarrow{ax} \mapsto \overrightarrow{\varphi(a)\varphi(x)} \tag{13-1}$$

линейно. В этом случае для любой пары точек $p, q \in A$

$$D_\varphi(\overrightarrow{pq}) = D_\varphi(\overrightarrow{aq}) - D_\varphi(\overrightarrow{ap}) = \overrightarrow{\varphi(a)\varphi(q)} - \overrightarrow{\varphi(a)\varphi(p)} = \overrightarrow{\varphi(p)\varphi(q)}\,.$$

Поэтому, заменяя в определении отображения (13-1) точку a на точку p, мы получим то же самое отображение $D_\varphi\colon U \to W$. В частности, оно тоже будет линейным. Не зависящее от выбора точки $a \in A$ линейное отображение (13-1) называется *дифференциалом* аффинного отображения φ.

Упражнение 13.6. Убедитесь, что композиция аффинных отображений аффинна с дифференциалом $D_{\varphi\psi} = D_\varphi D_\psi$.

Если аффинные отображения φ, ψ имеют равные дифференциалы, то для всех $p, q \in A$

$$\overrightarrow{\varphi(p)\varphi(q)} = D_\varphi(\overrightarrow{pq}) = D_\psi(\overrightarrow{pq}) = \overrightarrow{\psi(p)\psi(q)}\,,$$

что по упр. 13.1 на стр. 235 равносильно равенству $\overrightarrow{\varphi(p)\psi(p)} = \overrightarrow{\varphi(q)\psi(q)}$ и означает, что вектор $w = \overrightarrow{\varphi(p)\psi(p)}$ не зависит от выбора точки $p \in A$, т. е. $\psi = \tau_w \circ \varphi$ является композицией отображения φ и сдвига $\tau_w\colon B \to B$, $p \mapsto p + w$, на вектор w.

Предложение 13.3
Для любого набора из $n+1$ не лежащих в одной гиперплоскости точек $p_0, p_1, \dots, p_n$ в n-мерном аффинном пространстве A и произвольного набора из $n+1$ точек $q_0, q_1, \dots, q_n$ любого аффинного пространства B существует единственное такое аффинное отображение $\varphi\colon A \to B$, что $\varphi(p_i) = q_i$ при всех i.

Доказательство. Обозначим через U, W векторные пространства, подлежащие аффинным пространствам A, B. Если отображение φ существует, то его дифференциал $D_\varphi\colon U \to W$ переводит n векторов $\overrightarrow{p_0 p_i}$, составляющих базис в U, в заданные n векторов $\overrightarrow{q_0 q_i} \in W$. По предл. 6.4 такое линейное отображение D_φ существует, единственно и переводит вектор $u = \sum x_i \cdot \overrightarrow{p_0 p_i}$ в вектор $D_\varphi(u) = \sum x_i \cdot \overrightarrow{q_0 q_i}$. Поэтому аффинное отображение φ тоже существует, единственно и переводит точку $a = p_0 + \sum x_i \cdot \overrightarrow{p_0 p_i}$ в точку $\varphi(a) = q_0 + \sum x_i \cdot \overrightarrow{q_0 q_i}$. □

Следствие 13.2
Аффинное отображение из n-мерного аффинного пространства в себя биективно если и только если оно переводит какие-нибудь $n+1$ не лежащих в одной гиперплоскости точек в точки, также не лежащие в одной гиперплоскости. Для любых двух упорядоченных наборов из $n+1$ точек, в каждом из которых точки не лежат в одной гиперплоскости, существует единственное биективное аффинное отображение, переводящее первый набор во второй.

Доказательство. Аффинное отображение биективно если и только если биективен его дифференциал. Дифференциал биективен если и только если он переводит базис в базис. Векторы, соединяющие одну из $n+1$ точек со всеми остальными, образуют базис если и только если эти $n+1$ точек не лежат в одной гиперплоскости. □

13.3. Полуаффинные преобразования. Всюду в этом разделе мы по умолчанию считаем, что $\dim V \geqslant 2$. Биективное отображение $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ называется *полуаффинным преобразованием*, если оно переводит прямые в прямые. Такие отображения составляют группу преобразований аффинного пространства $\mathbb{A}(V)$ в смысле n° 1.6 на стр. 16.

Упражнение 13.7. Убедитесь, что полуаффинное преобразование φ переводит параллелограммы[1] в параллелограммы.

Из этого упражнения и упр. 13.5 на стр. 236 вытекает, что равенство $\overrightarrow{pq} = \overrightarrow{rs}$ влечёт за собою равенство $\overrightarrow{\varphi(p)\varphi(q)} = \overrightarrow{\varphi(r)\varphi(s)}$, причём даже тогда, когда точки p, q, r, s коллинеарны (см. рис. 13⋄1): выберем вектор $\overrightarrow{xy} = \overrightarrow{pq} = \overrightarrow{rs}$ на параллельной (pq) прямой $(xy) \neq (pq)$ и воспользуемся параллелограммами $pxyq$ и $rxys$. Таким образом, каждое полуаффинное отображение $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ корректно задаёт отображение векторов

$$D_\varphi : V \to V\,, \quad \overrightarrow{pq} \mapsto \overrightarrow{\varphi(p)\varphi(q)}\,, \tag{13-2}$$

которое называется *дифференциалом* отображения φ. Отображение φ однозначно восстанавливается, если известны его дифференциал и образ $\varphi(p)$ какой-нибудь точки p: произвольная точка q тогда переходит в $\varphi(q) = \varphi(p) + \overrightarrow{\varphi(p)\varphi(q)} = \varphi(p) + D_\varphi(\overrightarrow{pq})$.

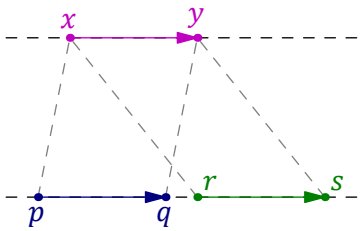


Рис. 13⋄1. Корректность определения D_φ.

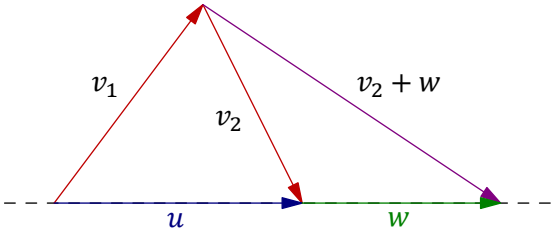


Рис. 13⋄2. Аддитивность D_φ.

Так как φ переводит параллелограмм со сторонами u, w в параллелограмм со сторонами $D_\varphi(u)$ и $D_\varphi(w)$, дифференциал аддитивен:

$$D_\varphi(u+w) = D_\varphi(u) + D_\varphi(w)\,, \tag{13-3}$$

[1] См. упр. 13.5 на стр. 236.

причём это равенство справедливо даже когда векторы u и w пропорциональны, поскольку вектор u всегда можно представить в виде суммы векторов v_1 и v_2, каждый из которых не пропорционален u, как на рис. 13⋄2, и тогда

$$D_\varphi(u+w) = D_\varphi(v_1+v_2+w) = D_\varphi(v_1) + D_\varphi(v_2+w) = \\ = D_\varphi(v_1) + D_\varphi(v_2) + D_\varphi(w) = D_\varphi(v_1+v_2) + D_\varphi(w) = D_\varphi(u) + D_\varphi(w)\,.$$

Так как φ переводит прямые в прямые, D_φ переводит векторы, пропорциональные данному ненулевому вектору v, в векторы, пропорциональные $D_\varphi(v)$. Поэтому каждый ненулевой вектор $v \in V$ задаёт отображение $\psi_v\colon \Bbbk \to \Bbbk$, значение которого на числе $\lambda \in \Bbbk$ определяется равенством

$$D_\varphi(\lambda v) = \psi_v(\lambda)\cdot D_\varphi(v)\,. \tag{13-4}$$

Лемма 13.1
Отображение $\psi = \psi_v\colon \Bbbk \to \Bbbk$ не зависит от v и является автоморфизмом поля $\Bbbk$.

Доказательство. Поскольку отображение ψ_v является ограничением биективного и переводящего прямые в прямые отображения φ на прямую, оно тоже биективно для каждого v. Покажем, что $\psi_u = \psi_w$ для любых двух непропорциональных векторов u, w. Так как пересекающиеся в одной точке прямые переходят в прямые, которые тоже пересекаются в одной точке, векторы $D_\varphi(u)$ и $D_\varphi(w)$ не пропорциональны и образуют базис своей линейной оболочки. Из аддитивности D_φ вытекает, что

$$\begin{array}{c} D_\varphi(\lambda(u+w)) = \psi_{u+w}(\lambda)\cdot D_\varphi(u+w) = \psi_{u+w}(\lambda)\cdot D_\varphi(u) + \psi_{u+w}(\lambda)\cdot D_\varphi(w) \\ \| \\ D_\varphi(\lambda u+\lambda w) = D_\varphi(\lambda u) + D_\varphi(\lambda w) = \psi_u(\lambda)\cdot D_\varphi(u) + \psi_w(\lambda)\cdot D_\varphi(w)\,. \end{array}$$

Из единственности разложения вектора по базису мы заключаем, что для всех $\lambda \in \Bbbk$ выполняются равенства $\psi_u(\lambda) = \psi_{u+w}(\lambda) = \psi_w(\lambda)$, что и требовалось.

Если векторы u и w пропорциональны, то для любого непропорционального им вектора v будут выполняться равенства $\psi_u = \psi_v = \psi_w$. Таким образом, отображение ψ_v одно и то же для всех v и может быть обозначено просто ψ. Далее, из аддитивности D_φ вытекают равенства

$$\psi(\lambda+\mu)\cdot D_\varphi(v) = D_\varphi\left((\lambda+\mu)v\right) = D_\varphi(\lambda v+\mu v) = D_\varphi(\lambda v) + \varphi(\mu v) = \\ = \psi(\lambda)\cdot D_\varphi(v) + \psi(\mu)\cdot D_\varphi(v) = (\psi(\lambda)+\psi(\mu))\cdot D_\varphi(v)\,,$$

откуда $\psi(\lambda+\mu) = \psi(\lambda)+\psi(\mu)$. Равенства

$$\psi(\lambda\mu)\cdot D_\varphi(v) = D_\varphi\left((\lambda\mu)v\right) = D_\varphi\left(\lambda(\mu v)\right) = \psi(\lambda)\cdot D_\varphi(\mu v) = \psi(\lambda)\psi(\mu)\cdot D_\varphi(v)$$

показывают, что $\psi(\lambda\mu) = \psi(\lambda)\cdot\psi(\mu)$. □

Определение 13.1
Отображение $F\colon U \to W$ векторных пространств над полем $\Bbbk$ называется *полулинейным*, если существует такой автоморфизм $\psi\colon \Bbbk \xrightarrow{\sim} \Bbbk$, что $F(\lambda u+\mu w) = \psi(\lambda)F(u)+\psi(\mu)F(w)$ для всех векторов $u, w \in U$ и всех чисел $\lambda, \mu \in \Bbbk$. Автоморфизм ψ называется *скручивающим автоморфизмом* полулинейного отображения F.

Замечание 13.1. Если скручивающий автоморфизм тождествен, то полулинейное отображение линейно. Так как простые поля $\mathbb{F}_p$ и $\mathbb{Q}$, а также поле $\mathbb{R}$ не имеют автоморфизмов, отличных от тождественного[1], все полулинейные над этими полями отображения автоматически линейны.

Пример 13.8
Рассмотрим комплексное координатное пространство $\mathbb{C}^n$. Отображение

$$\sigma : \mathbb{C}^n \to \mathbb{C}^n, \quad (z_1, \dots, z_n) \mapsto (\overline{z}_1, \dots, \overline{z}_n),$$

не является $\mathbb{C}$-линейным, поскольку $\sigma(zv) = \overline{z}\sigma(v)$ для всех $z \in \mathbb{C}$ и $v \in \mathbb{C}^n$. Оно полулинейно со скручивающим автоморфизмом $\psi : z \mapsto \overline{z}$. При этом σ задаёт полуаффинное преобразование $\mathbb{A}(\mathbb{C}^n) \to \mathbb{A}(\mathbb{C}^n)$: прямая $p + \mathbb{C}\, v$ переходит в прямую $\sigma(p) + \mathbb{C}\, \sigma(v)$.

Теорема 13.1
Пусть $\dim V \geqslant 2$. Если отображение $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ биективно и переводит прямые в прямые, то существует такое полулинейное биективное отображение $D_\varphi : V \to V$, что

$$\varphi(q) = \varphi(p) + D_\varphi(\overrightarrow{pq})$$

для всех $p, q \in \mathbb{A}(V)$. Наоборот, если отображение $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ таково, что для некоторой точки $a \in \mathbb{A}(V)$, некоторого полулинейного биективного отображения $D_\varphi : V \to V$ и всех $x \in\in \mathbb{A}(V)$ выполняется равенство $\varphi(x) = \varphi(a) + D_\varphi(\overrightarrow{ax})$, то φ полуаффинно.

Доказательство. Первая импликация вытекает из формул (13-3), (13-4) и лем. 13.1. Докажем вторую. Если $\varphi(x) = \varphi(a) + D_\varphi(\overrightarrow{px})$ для некоторого a и всех x, то[2]

$$D_\varphi(\overrightarrow{pq}) = D_\varphi(\overrightarrow{aq}) - D_\varphi(\overrightarrow{ap}) = \overrightarrow{\varphi(a)\varphi(q)} - \overrightarrow{\varphi(a)\varphi(p)} = \overrightarrow{\varphi(p)\varphi(q)}$$

для всех p, q. Поэтому для всех $p \in \mathbb{A}(V)$, $u \in V$ и $t \in \Bbbk$

$$\varphi(p + tu) = \varphi(p) + D_\varphi(tu) = \varphi(p) + \psi(t)\, D_\varphi(u),$$

где $\psi : \Bbbk \xrightarrow{\sim} \Bbbk$ — скручивающий автоморфизм полулинейного отображения D_φ. Так как он биективен, прямая $p + \Bbbk\, u$ переходит в прямую $\varphi(p) + \Bbbk\, D_\varphi(u)$. □

Следствие 13.3
Над полями $\mathbb{F}_p$, $\mathbb{Q}$ и $\mathbb{R}$ все переводящие прямые в прямые биективные преобразования аффинных пространств размерности $\geqslant 2$ аффинны. □

13.4. Проективные пространства. С каждым $(n+1)$-мерным векторным пространством V над произвольным полем $\Bbbk$ помимо $(n+1)$-мерного аффинного пространства $\mathbb{A}^{n+1} = \mathbb{A}(V)$ связано n-мерное *проективное пространство* $\mathbb{P}_n = \mathbb{P}(V)$, точками которого по определению являются одномерные векторные подпространства в V или, что то же самое, проходящие через нуль аффинные прямые в $\mathbb{A}(V)$. Чтобы наблюдать их как «обычные точки», внутрь $\mathbb{A}(V)$ следует поместить экран — не содержащую нуля аффинную гиперплоскость, как на рис. 13⋄3. Каждая такая гиперплоскость однозначно задаётся неоднородным линейным уравнением $\xi(x) = 1$, где $\xi \in V^*$ — ненулевая линейная форма на V, и называется *аффинной картой* U_ξ на $\mathbb{P}(V)$.

[1] См. упр. 2.16 на стр. 35 и прим. 2.9 на стр. 35.
[2] Ср. с аналогичным рассуждением после форм. (13-1) на стр. 238.

Упражнение 13.8. Убедитесь, что сопоставление $\xi \mapsto U_\xi$ задаёт биекцию между ненулевыми ковекторами $\xi \in V^*$ и не проходящими через начало координат аффинными гиперплоскостями в $\mathbb{A}(V)$.

В карте U_ξ видны все одномерные подпространства, порождённые векторами $v \in V$, на которых $\xi(v) \neq 0$. Дополнение $\mathbb{P}_n \smallsetminus U_\xi$ состоит из одномерных подпространств, лежащих в параллельном экрану U_ξ векторном подпространстве $\operatorname{Ann}\xi \subset V$ размерности n. Таким образом, невидимые в карте U_ξ точки n-мерного проективного проективного пространства $\mathbb{P}_n = \mathbb{P}(V)$ образуют $(n-1)$-мерное проективное пространство $\mathbb{P}_{n-1} = \mathbb{P}(\operatorname{Ann}\xi)$. Оно называется *бесконечно удалённой гиперплоскостью* карты U_ξ. Точки этой гиперплоскости можно воспринимать как *направления* в аффинной карте U_ξ. Итерируя это рассуждение, заключаем, что n-мерное проективное пространство $\mathbb{P}_n$ разбивается в дизъюнктное объединение аффинных пространств: $\mathbb{P}_n = U_\xi \sqcup \mathbb{P}(\operatorname{Ann}\xi) = \mathbb{A}^n \sqcup \mathbb{P}_{n-1} = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \mathbb{P}_{n-2} = \ldots = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \ldots \sqcup \mathbb{A}^0$ всех промежуточных размерностей от 0 до n, где $\mathbb{A}^0 = \mathbb{P}_0$ — это одна точка.

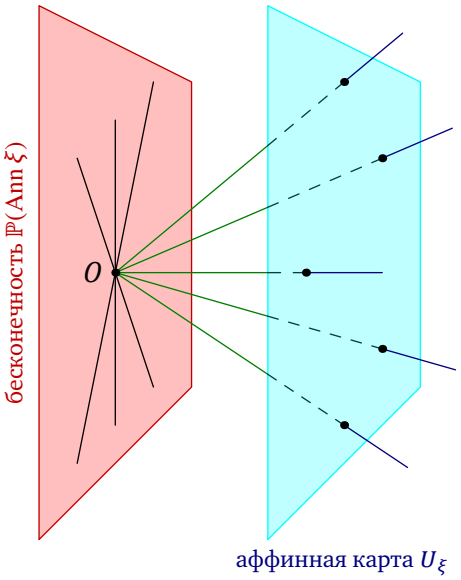


Рис. 13◇3. Проективный мир.

Упражнение 13.9. Какое соотношение на q получится, если независимо подсчитать количества точек в левой и правой части этого равенства над конечным полем из q элементов?

13.4.1. Глобальные однородные координаты. Зафиксируем в V координаты $x_0, x_1, \ldots, x_n$ относительно какого-нибудь базиса $e_0, e_1, \ldots, e_n$. Два ненулевых вектора

$$v = (x_0, x_1, \ldots, x_n) \quad \text{и} \quad w = (y_0, y_1, \ldots, y_n)$$

задают одну и ту же точку $p \in \mathbb{P}_n$ если и только если их координаты пропорциональны. Последнее равносильно равенству отношений[1] $x_\mu : x_\nu = y_\mu : y_\nu$ для всех $0 \leqslant \mu \neq \nu \leqslant n$. Иначе говоря, с точкой $p \in \mathbb{P}_n$ взаимно однозначно связаны не координаты ненулевого вектора, задающего эту точку, а только отношения $(x_0 : x_1 : \ldots : x_n)$ между ними. Эти отношения называется *однородными координатами* точки p в базисе $e_0, e_1, \ldots, e_n$.

13.4.2. Локальные аффинные координаты. Любой набор ковекторов $\xi_1, \ldots, \xi_n \in V^*$, дополняющий ковектор ξ до базиса в V^*, задаёт в аффинной карте U_ξ аффинную систему координат с началом в точке e_0 и базисными векторами $e_1, \ldots, e_n$, где $e_0, e_1, \ldots, e_n$ это двойственный к $\xi, \xi_1, \ldots, \xi_n$ базис пространства V.

Упражнение 13.10. Убедитесь, что $e_0 \in U_\xi$, а $e_1, \ldots, e_n$ составляют базис в $\operatorname{Ann}\xi$.

Каждое наблюдаемое в карте U_ξ одномерное подпространство, порождённое ненулевым вектором $v \in V$, изображается в нём точкой $v/\xi(v) \in U_\xi$ с аффинными координатами

$$t_i = \xi_i\big(v/\xi(v)\big) = \xi_i(v)/\xi(v), \quad \text{где} \quad 1 \leqslant i \leqslant n.$$

[1] При этом равенства вида $0 : x = 0 : y$ и $x : 0 = y : 0$, в которых x и y либо одновременно отличны от нуля, либо одновременно нулевые, тоже допускаются и считаются истинными.

Обратите внимание, что локальные аффинные координаты точки $v \in \mathbb{P}(V)$ являются не линейными, а дробно линейными функциями от глобальных однородных координат этой точки.

Пример 13.9 (проективная прямая)
Проективная прямая $\mathbb{P}_1 = \mathbb{P}_1(\Bbbk) = \mathbb{P}(\Bbbk^2)$ целиком покрывается двумя аффинными картами $U_0 = U_{x_0}$ и $U_1 = U_{x_1}$, которые представляют собою прямые $x_0 = 1$ и $x_1 = 1$ в аффинном пространстве $\Bbbk^2$, см. рис. 13⋄4.

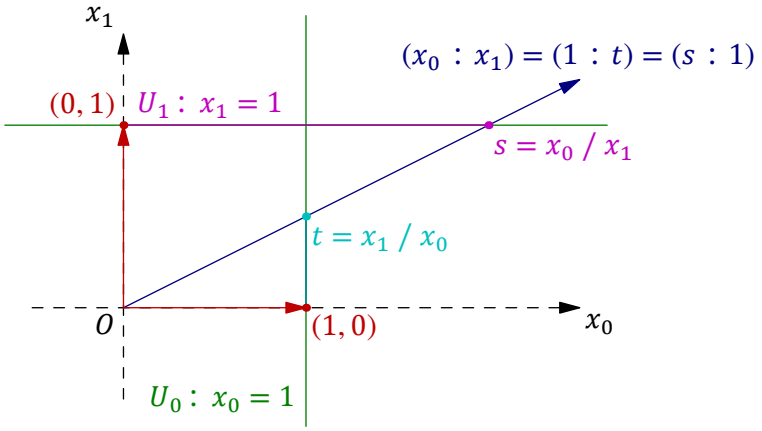


Рис. 13⋄4. Стандартные карты на $\mathbb{P}_1$.

В карте U_0 видны все одномерные подпространства в $\Bbbk^2$ кроме вертикальной координатной оси $(0 : 1)$, которая является единственной бесконечно удалённой точкой этой карты. В качестве локальной аффинной координаты на U_0 годится функция $t = x_1/x_0$. В карте U_1 видны все точки $(x_0 : x_1) = \left(\frac{x_0}{x_1} : 1\right)$, у которых $x_1 \neq 0$, и в качестве локальной аффинной координаты в этой карте можно взять функцию $t = x_0/x_1$. Единственной бесконечно удалённой точкой для карты U_1 является горизонтальная координатная ось $(1 : 0)$. Координаты s и t одной и той же точки $(x_0 : x_1) \in \mathbb{P}_1$, видимой сразу в обеих картах, связаны соотношением $t = 1/s$.

Упражнение 13.11. Убедитесь в этом.

Таким образом, проективная прямая $\mathbb{P}_1(\Bbbk)$ является результатом склейки двух аффинных прямых $\mathbb{A}^1 = \Bbbk$ с координатами s и t вдоль дополнения до начал координат по правилу: точка с координатой s на первой прямой отождествляется с точкой с координатой $t = 1/s$ на второй.

13.4.3. Касательное пространство в точке. Пусть точка $p \in \mathbb{P}(V)$ задаётся одномерным векторным подпространством $L \subset V$. Каждая содержащая p аффинная карта $U_\xi \subset \mathbb{P}(V)$ является аффинным пространством над векторным пространством $T_p = \operatorname{Hom}(L, V/L)$, которое называется *касательным* векторным пространством к $\mathbb{P}(V)$ в точке p. В самом деле, $V = L \oplus \operatorname{Ann}(\xi)$ и каждый класс в V/L однозначно записывается как $[w]$ с $w \in \operatorname{Ann}(\xi)$, что канонически отождествляет V/L с $\operatorname{Ann}(\xi)$. Каждое не лежащее в $\operatorname{Ann}(\xi)$ одномерное подпространство биективно проектируется на L вдоль $\operatorname{Ann}(\xi)$ и стало быть является графиком $\Gamma_\tau = \{(v, \tau(v)) \in L \oplus \operatorname{Ann}(\xi) \mid v \in L\}$ однозначно определённого отображения $\tau : L \to \operatorname{Ann}(\xi)$. Согласно упр. 13.4 на стр. 236, сопоставление линейному отображению $L \to \operatorname{Ann}(\xi)$ его графика задаёт биекцию между $\operatorname{Hom}(L, \operatorname{Ann}(\xi))$ и не лежащими в $\operatorname{Ann}(\xi)$ одномерными подпространствами $N \subset V$. Будем называть радиус вектором $\overrightarrow{LN}$ такого подпространства N отображение $\tau_N \in \operatorname{Hom}(L, \operatorname{Ann}(\xi)) \simeq \operatorname{Hom}(L, V/L) = T_p$, графиком которого является N.

Упражнение 13.12. Сопоставим одномерным подпространствам $M, N \not\subset \operatorname{Ann}(\xi)$ вектор $\overrightarrow{MN} = \tau_M - \tau_N \in T_p$. Убедитесь, что это сопоставление удовлетворяет условиям из n° 13.1 на стр. 235 и задаёт на множестве не лежащих в $\operatorname{Ann}(\xi)$ одномерных подпространств в V структуру аффинного пространства над T_p.

Точка $p \in \mathbb{P}(V)$ видна в карте $U_\xi \subset \mathbb{A}(V)$ как вектор $v = U_\xi \cap L$ с $\xi(v) = 1$. Точка $q = p + \tau$, получающаяся из неё откладыванием радиус вектора $\tau \in T_p$, видна в карте U_ξ как $U_\xi \cap \Gamma_\tau = v + \tau(v)$, где через $\tau(w) \in \operatorname{Ann}(\xi)$ обозначен единственный лежащий в $\operatorname{Ann}(\xi)$ представитель класса $\tau(v) \in V/L$.

13.4.4. Проективные подпространства. Проективизация $\mathbb{P}(U) \subset \mathbb{P}(V)$ векторного подпространства $U \subset V$ называются *проективным подпространством* в $\mathbb{P}(V)$. Например, через любые две различные точки a, b в $\mathbb{P}(V)$ проходит единственная проективная прямая (ab). Она является проективизацией линейной оболочки непропорциональных векторов a, b и состоит из всевозможных ненулевых линейных комбинаций $\lambda a + \mu b$, рассматриваемых с точностью до пропорциональности. Отношение $(\lambda : \mu)$ коэффициентов в разложения вектора $v = \lambda a + \mu b \in (ab)$ можно использовать в качестве внутренней однородной координаты точки v на проективной прямой (ab).

Упражнение 13.13. Убедитесь, что k-мерное проективное подпространство наблюдается в любой задевающей его аффинной карте как k-мерное аффинное подпространство.

Предложение 13.4
Для любых двух проективных подпространств $K, L \subset \mathbb{P}_n$ выполняется неравенство

$$\dim(K \cap L) \geqslant \dim K + \dim L - n\,.$$

Доказательство. Пусть $\mathbb{P}_n = \mathbb{P}(V)$, $L = \mathbb{P}(U)$, $\mathbb{P}(W)$, где $U, W \subset V$ — векторные подпространства. Тогда $K \cap L = \mathbb{P}(U \cap W)$ имеет размерность $\dim K \cap L = \dim(U \cap W) - 1 \geqslant \dim U + \dim W - \dim V - 1 = \dim K + 1 + \dim L + 1 - (n+1) - 1 = \dim K + \dim L - n$. □

Упражнение 13.14. Убедитесь, что любые две прямые на $\mathbb{P}_2$ пересекаются.

13.4.5. Дополнительные подпространства и проекции. Проективные подпространства

$$K = \mathbb{P}(U) \quad \text{и} \quad L = \mathbb{P}(W)$$

в $\mathbb{P}_n = \mathbb{P}(V)$ называются *дополнительными*, если $K \cap L = \varnothing$ и $\dim K + \dim L = n - 1$. Например, любые две непересекающиеся прямые в $\mathbb{P}_3$ дополнительны. На языке линейной алгебры дополнительность проективных подпространств означает, что подлежащие им векторные подпространства $U, W \subset V$ имеют $U \cap V = 0$ и $\dim U + \dim W = \dim K + 1 + \dim L + 1 = n + 1 = \dim V$, откуда $V = U \oplus W$. В этом случае любой вектор $v \in V$ имеет единственное разложение $v = u + w$ с $u \in U$ и $w \in W$. Если вектор v не лежит ни в U, ни в W, обе компоненты этого разложения отличны от нуля. Это означает, что для любой точки $p \notin K \sqcup L$ существует единственная проходящая через p прямая ℓ, пересекающая как K, так и L.

Упражнение 13.15. Убедитесь в этом.

Всякая пара дополнительных подпространств $K, L \subset \mathbb{P}_n$ задаёт *проекцию из K на L*

$$\pi_L^K : (\mathbb{P}_n \smallsetminus K) \to L\,, \tag{13-5}$$

которая тождественно действует на L и переводит каждую точку $p \in \mathbb{P}_n \smallsetminus (K \sqcup L)$ в точку пересечения подпространства L с той единственной прямой, которая проходит через точку p и пересекает оба подпространства K и L. На языке линейной алгебры, проекция переводит каждый вектор $v = u + w$ с ненулевой компонентой $w \in W$ в эту компоненту. В однородных координатах $(x_0 : x_1 : \ldots : x_n)$, согласованных с разложением $V = U \oplus W$ так, что начальный кусок $(x_0 : x_1 : \ldots : x_m)$ является координатами в K, а остаток $(x_{m+1} : x_{m+2} : \ldots : x_n)$ — координатами в L, проекция π_L^K просто удаляет первые $m+1$ координат x_ν с $0 \leqslant \nu \leqslant m$.

13.4.6. Проективная двойственность. Проективизации $\mathbb{P}_n = \mathbb{P}(V)$ и $\mathbb{P}_n^\times \stackrel{\text{def}}{=} \mathbb{P}(V^*)$ двойственных друг другу векторных пространств V и V^* называются *двойственными* проективными пространствами. Геометрически, каждое из них есть пространство гиперплоскостей в другом: соотношение $\varphi(v) = 0$ на вектор $v \in V$ ковектор $\varphi \in V^*$ линейно как по v, так и по φ, и задаёт при фиксированном $\varphi \in \mathbb{P}_n^\times$ гиперплоскость в $\mathbb{P}_n$, а при фиксированном $v \in \mathbb{P}_n$ — гиперплоскость в $\mathbb{P}_n^\times$, состоящую из всех гиперплоскостей в $\mathbb{P}_n$, проходящих через точку $v \in \mathbb{P}_n$. Так как две линейные формы задают одну и ту же гиперплоскость в векторном пространстве если и только если они пропорциональны, гиперплоскости в проективном пространстве биективно соответствуют точкам двойственного проективного пространства.

Напомню[1], что между векторными подпространствами дополнительных размерностей в V и V^* имеется каноническая биекция $U \leftrightarrows \operatorname{Ann}(U)$, которая оборачивает включения и переводит суммы в пересечения, а пересечения — в суммы. На языке проективной геометрии это означает, что множество гиперплоскостей, содержащих заданное m-мерное проективное подпространство $K = \mathbb{P}(U) \subset \mathbb{P}_n$, представляет собою проективное подпространство $K^\times \stackrel{\text{def}}{=} \mathbb{P}(\operatorname{Ann} U) \subset \mathbb{P}_n^\times$ размерности $n - m - 1$, и при каждом $m = 0, 1, \ldots, (n-1)$ соответствие $K \leftrightarrows K^\times$ между m-мерными проективными подпространствами в $\mathbb{P}_n$ и $(n{-}m{-}1)$-мерными проективными подпространствами в $\mathbb{P}_n^\times$ взаимно однозначно и оборачивает включения. Это соответствие называется *проективной двойственностью*. Оно позволяет переговаривать геометрические утверждения в эквивалентные двойственные геометрические утверждения, подчас довольно сильно отличающиеся от исходных.

Например, условие коллинеарности трёх точек двойственно условию наличия у трёх гиперплоскостей общего подпространства коразмерности 2.

Поскольку биекция $U \leftrightarrows \operatorname{Ann}(U)$ переводит пересечения векторных пространств в суммы и наоборот, соответствие $K \leftrightarrows K^\times$ переводит пересечение $K \cap L$ проективных подпространств в *линейное соединение*[2] $J(K^\times, L^\times)$ — объединение всех проективных прямых[3] $(\varphi\psi)$ с $\varphi \in K^\times$, $\psi \in L^\times$. Наоборот, линейное соединение $J(K, L)$ двойственно пересечению $K^\times \cap L^\times$.

Упражнение 13.16. Убедитесь, что $\mathbb{P}(U + W) = J\big(\mathbb{P}(U), \mathbb{P}(W)\big)$ в $\mathbb{P}(V)$ для любых ненулевых векторных подпространств $U, W \subset V$.

13.5. Проективные преобразования. Всякий линейный изоморфизм векторных пространств $F : U \xrightarrow{\sim} W$ задаёт биекцию $\overline{F} : \mathbb{P}(U) \xrightarrow{\sim} \mathbb{P}(W)$ между одномерными подпространствами в U и W, которая называется *линейным проективным преобразованием* или *проективным изоморфизмом*.

[1] См. теор. 7.5 на стр. 126.

[2] Обозначение J является сокращением от английского *join*.

[3] Здесь и далее удобно считать, что «прямая» (aa) это одна точка a.

Пример 13.10 (перспектива между гиперплоскостями)
Покажем, что для любой пары проективных гиперплоскостей L_1, $L_2 \subset \mathbb{P}_n = \mathbb{P}(V)$ и произвольной точки $p \notin L_1 \cup L_2$ центральная проекция гиперплоскости L_1 из точки p на гиперплоскость L_2 задаёт проективный изоморфизм между L_1 и L_2, который мы будем обозначать $p : L_1 \xrightarrow{\sim} L_2$ и называть *перспективой* с центром в p. Пусть $L_1 = \mathbb{P}(U)$, $L_2 = \mathbb{P}(W)$ и $p = \mathbb{P}(\Bbbk \cdot e)$. Тогда $V = W \oplus \Bbbk \cdot e$, ибо $p \notin L_2$, и центральная проекция из p задаётся ограничением линейной проекции $V \twoheadrightarrow W$ вдоль одномерного подпространства $\Bbbk \cdot e$ на подпространство $U \subset V$. Так как $p \notin L_1$, подпространство U имеет нулевое пересечение с ядром проекции и, стало быть, проектируется на W изоморфно.

Теорема 13.2
Для любых двух векторных пространств U, W одинаковой размерности $\dim U = \dim W = n+1$ и упорядоченных наборов из $n+2$ точек $p_0, p_1, \ldots, p_{n+1} \in \mathbb{P}(U)$, $q_0, q_1, \ldots, q_{n+1} \in \mathbb{P}(W)$, в каждом из которых никакие $n+1$ точек не лежат в одной гиперплоскости, существует единственный с точностью до пропорциональности линейный изоморфизм $F : U \xrightarrow{\sim} W$, такой что $\overline{F}(p_i) = q_i$ при всех i.

Доказательство. Зафиксируем какие-нибудь ненулевые векторы u_i и w_i, представляющие точки p_i и q_i, и возьмём наборы векторов $\boldsymbol{u} = (u_0, u_1, \ldots, u_n)$ и $\boldsymbol{w} = (w_0, w_1, \ldots, w_n)$ в качестве базисов векторных пространств U и W. В силу наложенных на точки условий все коэффициенты в разложениях $u_{n+1} = \alpha_0 u_0 + \alpha_1 u_1 + \ldots + \alpha_n u_n$ и $w_{n+1} = \beta_0 w_0 + \beta_1 w_1 + \ldots + \beta_n w_n$ векторов u_{n+1} и w_{n+1} по этим базисам отличны от нуля, так как, к примеру, при $\alpha_i = 0$ точка p_{n+1} оказывается в одной гиперплоскости $x_i = 0$ с n базисными точками p_ν, где $\nu \neq i$. Отображение $\overline{F} : \mathbb{P}(U) \to \mathbb{P}(W)$ переводит p_i в q_i если и только если $F(u_i) = \lambda_i w_i$ для некоторых ненулевых $\lambda_i \in \Bbbk$. Поэтому матрица $F_{\boldsymbol{wu}}$ оператора F в базисах $\boldsymbol{u}$ и $\boldsymbol{w}$ диагональна с ненулевыми элементами $\lambda_0, \lambda_1, \ldots, \lambda_n$ на диагонали, причём каждый диагональный элемент удовлетворяет равенству $\lambda_i \alpha_i = \lambda_{n+1} \beta_i$, выражающему равенство i-х координат векторов $F(u_{n+1}) = \lambda_{n+1} w_{n+1}$. Таким образом, набор диагональных элементов $\lambda_i = \lambda_{n+1} \alpha_i / \beta_i$ матрицы оператора F определяется однозначно с точностью до умножения на произвольную ненулевую константу λ_{n+1}. □

Следствие 13.4
Два линейных изоморфизма тогда и только тогда задают равные проективные изоморфизмы, когда они пропорциональны. □

13.5.1. Проективные автоморфизмы прямой. Проективные преобразования прямой называются *гомографиями* и образуют группу[1], которая обозначается $\mathrm{PGL}_2(\Bbbk)$. Элементы этой группы биективно соответствуют классам пропорциональности обратимых 2×2 матриц

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Класс такой матрицы действует на $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ по правилу

$$(x_0 : x_1) \mapsto \big((ax_0 + bx_1) : (cx_0 + dx_1)\big).$$

В стандартной аффинной карте $U_1 \simeq \mathbb{A}^1$ с аффинной координатой $t = x_0/x_1$, это действие имеет вид дробно линейного преобразования $t \mapsto (at + b)/(ct + d)$. Единственное дробно линейное

[1] В смысле n° 1.6 на стр. 16.

преобразование, переводящее три различные точки a, b, c в точки ∞, 0, 1 имеет вид

$$t \mapsto \frac{t-b}{t-a} \cdot \frac{c-a}{c-b}\,. \tag{13-6}$$

Образ точки $d \in \mathbb{P}_1$ при таком преобразовании называется *двойным отношением*[1] упорядоченной четвёрки точек a, b, c, d и обозначается

$$[a,\ b,\ c,\ d] \stackrel{\text{def}}{=} \frac{(a-c)(b-d)}{(a-d)(b-c)}\,.$$

По построению, двойное отношение четырёх различных точек может принимать любые значения кроме ∞, 0 и 1, и при фиксированных a, b, c отображение

$$\mathbb{P}_1 \smallsetminus \{a,b,c\} \xrightarrow{\sim} \mathbb{P}_1 \smallsetminus \{\infty, 0, 1\}\,, \quad t \mapsto [a,\ b,\ c,\ t]$$

биективно. Поскольку разность аффинных координат $x = x_0/x_1$ и $y = y_0/y_1$ любых двух точек из карты U_1 с точностью до ненулевого множителя совпадает с определителем матрицы однородных координат этих точек:

$$x - y = \frac{x_0}{x_1} - \frac{y_0}{y_1} = \frac{x_0y_1 - x_1y_0}{x_1y_1} = \frac{1}{x_1y_1} \det \begin{pmatrix} x_0 & y_0 \\ x_1 & y_1 \end{pmatrix}, \tag{13-7}$$

двойное отношение точек $p_1, p_2, p_3, p_4 \in \mathbb{P}_1$ можно записать как

$$\begin{gathered} [p_1,\ p_2,\ p_3,\ p_4] = \frac{(p_1 - p_3)\,(p_2 - p_4)}{(p_1 - p_4)\,(p_2 - p_3)} = \frac{\det(p_1, p_3) \cdot \det(p_2, p_4)}{\det(p_1, p_4) \cdot \det(p_2, p_3)}\,, \\ \text{где } \det(p,q) = \det \begin{pmatrix} p_0 & q_0 \\ p_1 & q_1 \end{pmatrix} \text{ для точек } p = (p_0 : p_1),\ q = (q_0, q_1) \in \mathbb{P}(\Bbbk^2). \end{gathered} \tag{13-8}$$

Предложение 13.5
Две упорядоченные четвёрки точек тогда и только тогда переводятся одна в другую гомографией, когда их двойные отношения одинаковы.

Доказательство. Пусть гомографии φ_p и φ_q переводят упорядоченные тройки точек $p_1,\ p_2,\ p_3$ и $q_1,\ q_2,\ q_3$ в тройку $\infty,\ 0,\ 1$. Если $[p_1,\ p_2,\ p_3,\ p_4] = [q_1,\ q_2,\ q_3,\ q_4]$, то $\varphi_p(p_4) = \varphi_q(q_4)$ и гомография $\varphi_q^{-1} \circ \varphi_p$ переводит $p_1,\ p_2,\ p_3,\ p_4$ в $q_1,\ q_2,\ q_3,\ q_4$. Наоборот, если существует гомография ψ, переводящая $p_1,\ p_2,\ p_3,\ p_4$ в $q_1,\ q_2,\ q_3,\ q_4$, то гомография $\varphi_p \circ \psi^{-1}$ переводит четвёрку $q_1,\ q_2,\ q_3,\ q_4$ в четвёрку $\infty,\ 0,\ 1,\ [p_1,\ p_2,\ p_3,\ p_4]$, откуда $[p_1,\ p_2,\ p_3,\ p_4] = [q_1,\ q_2,\ q_3,\ q_4]$. □

Следствие 13.5
Правая часть равенства (13-8) не зависит от выбора однородных координат, а средняя часть, содержащая разности аффинных координат точек, не зависит ни от выбора аффинной карты, ни от выбора локальной аффинной координаты в ней, при условии, что эта карта содержит все четыре точки, т. е. значения p_1, p_2, p_3, p_4 конечны.

[1] По-английски *cross-ratio*.

Доказательство. Поскольку замена однородных координат является проективным преобразованием, первое утверждение следует из предл. 13.5. Второе утверждение является следствием первого. □

Упражнение 13.17. Докажите сл. 13.5 прямым вычислением и убедитесь, что в аффинной карте с нулём в b и бесконечностью в a для точек $c = b + \gamma a$ и $d = b + \delta a$ с аффинными координатами $\gamma, \delta \in \Bbbk$ двойное отношение $[a, b, c, d] = \delta/\gamma$.

Предложение 13.6
Биекция $\varphi : \mathbb{P}_1 \xrightarrow{\sim} \mathbb{P}_1$ является проективным преобразованием если и только если она сохраняет двойные отношения.

Доказательство. Пусть φ переводит точки a, b и c в ∞, 0 и 1. Если φ сохраняет двойные отношения, то каждая точка $t \in \mathbb{P}_1 \smallsetminus \{a, b, c\}$ переходит в точку

$$\varphi(t) = [a, b, c, t] = \frac{(t-b)(c-a)}{(t-a)(c-b)}\,.$$

Таким образом, преобразование φ дробно линейно. □

13.6. Алгебраические многообразия. Рассмотрим $(n+1)$-мерное векторное пространство U с базисом $x_0, x_1, \ldots, x_n$ над полем $\Bbbk$. Алгебра многочленов $\Bbbk[x_0, x_1, \ldots, x_n]$ от коммутирующих переменных $x_0, x_1, \ldots, x_n$ с коэффициентами из $\Bbbk$ называется *симметрической алгеброй* векторного пространства U и обозначается SU. Как векторное пространство над $\Bbbk$ она является прямой суммой $SU = \bigoplus_{k \geqslant 0} S^k U$ счётного множества конечномерных векторных подпространств $S^k U$, состоящих из однородных многочленов степени k от $x_0, x_1, \ldots, x_n$. Пространство $S^k U$ называется *k-й симметрической степенью* векторного пространства U. Не привязанные к базису обозначения и названия уместны, поскольку ни одно из пространств $S^k U$ не зависит от выбора базиса: при $k = 0$ пространство $S^0 U = \Bbbk$ одномерно и состоит из констант, при $k = 1$ пространство $S^1 U = U$ состоит из всевозможных линейных комбинаций базисных векторов x_i и канонически отождествляется с U, а при $k > 1$ пространство $S^k U$ представляет собою линейную оболочку всевозможных произведений $u_1 \ldots u_k$, составленных из k векторов $u_i \in U$, т. е. тоже не зависит от выбора базиса $x_0, x_1, \ldots, x_n$ в U.

В ситуации, когда пространство $U = V^*$ двойственно векторному пространству V, а базис $x_0, x_1, \ldots, x_n$ двойствен базису $e_0, e_1, \ldots, e_n$ в V, каждый многочлен $f(x_0, x_1, \ldots, x_n) \in SV^*$ задаёт *полиномиальную функцию*

$$f : V \to \Bbbk, \quad \lambda_0 v_0 + \lambda_1 v_1 + \ldots + \lambda_k v_k \mapsto f(\lambda_0, \lambda_1, \ldots, \lambda_n)\,,$$

сопоставляющую вектору v результат вычисления многочлена f на координатах вектора v. Возникающий таким образом гомоморфизм алгебры многочленов в алгебру функций из V в $\Bbbk$:

$$SV^* \to \Bbbk^V \tag{13-9}$$

тоже не зависит от выбора двойственных базисов в V и V^*, так как переводит каждый ковектор $\varphi \in V^*$ в ту самую линейную функцию $\varphi : V \to \Bbbk$, которой является этот ковектор, а каждое произведение $\varphi_1 \ldots \varphi_k$ — в функцию $v \mapsto \varphi_1(v) \ldots \varphi_k(v)$.

Упражнение 13.18. Убедитесь в этом!

Поскольку такие произведения линейно порождают SV^*, линейное отображение (13-9) однозначно определяется их образами, а они от выбора базиса не зависят.

Упражнение 13.19. Убедитесь, что для конечномерного векторного пространства V над полем $\Bbbk$ гомоморфизм (13-9) инъективен если и только если поле $\Bbbk$ бесконечно, и сюръективен если и только если поле $\Bbbk$ конечно.

13.6.1. Аффинные алгебраические многообразия. Множество нулей многочлена $f \in SV^*$, рассматриваемого как функция $f : V \to \Bbbk$, называется *аффинной алгебраической гиперповерхностью* степени $d = \deg f$ в аффинном пространстве $\mathbb{A}(V)$ и обозначается через[1]

$$V(f) \stackrel{\text{def}}{=} \{p \in \mathbb{A}(V) \mid f(p) = 0\}\,.$$

Пересечения аффинных алгебраических гиперповерхностей, т. е. фигуры, задаваемые в аффинном пространстве системами полиномиальных уравнений на координаты точек, называются *аффинными алгебраическими многообразиями*. Простейшими примерами таковых являются аффинные подпространства — они задаются системами линейных уравнений.

13.6.2. Проективные гиперповерхности. Важное отличие проективной геометрии от аффинной заключается в том, что непостоянный многочлен $f \in SV^* \smallsetminus S^0V^*$ не задаёт никакой функции на проективном пространстве $\mathbb{P}(V)$, так как значения $f(v)$ и $f(\lambda v)$ на пропорциональных векторах обычно различны. Тем не менее, множество векторов $v \in V$ на которых обращается в нуль *однородный* многочлен $f \in S^kV$ является корректно определённой геометрической фигурой в $\mathbb{P}(V)$, так как равенства $f(v) = 0$ и $f(\lambda v) = \lambda^k f(v) = 0$ эквиваленты друг другу для любых ненулевых $v \in V$ и $\lambda \in \Bbbk$. Иными словами, аффинное многообразие $V(f) \subset \mathbb{A}(V)$ вместе с каждым ненулевым вектором содержит порождённое им одномерное подпространство. Множество этих одномерных подпространств называется *проективной алгебраической гиперповерхностью степени* k, задаваемой однородным многочленом $f \in S^kV$, и тоже обозначается $V(f) \subset \mathbb{P}(V)$. Пересечения гиперповерхностей, задаваемые в проективном пространстве системами однородных полиномиальных уравнений, называются *проективными алгебраическими многообразиями*. Простейшими примерами являются проективные подпространства — они задаются системами однородных линейных уравнений.

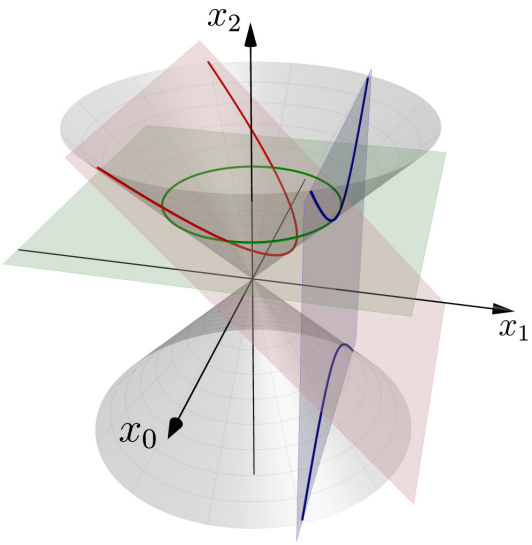


Рис. 13⋄5. Аффинные изображения проективной коники.

Пример 13.11 (аффинные коники)
Однородное уравнение второй степени

$$x_0^2 + x_1^2 = x_2^2 \tag{13-10}$$

[1] Буква «V» в этом традиционном обозначении является аббревиатурой слова *variety* и не имеет отношения к букве V, обозначающей векторное пространство.

задаёт в аффинном пространстве $\mathbb{A}^3 = \mathbb{A}(\mathbb{R}^3)$ конус, изображённый на рис. 13⋄5. Прямолинейные образующие этого конуса являются точками проективной плоскости $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$ и составляют в ней фигуру, которая называется *гладкой коникой*. В аффинной карте U_{x_1}, где $x_1 = 1$, в локальных аффинных координатах $t_0 = x_0/x_1$ и $t_2 = x_2/x_1$ уравнение (13-10) превращается в уравнение $t_2^2 - t_0^2 = 1$, задающее гиперболу. В аффинной карте U_2, где $x_2 = 1$, в локальных координатах $t_0 = x_0/x_2$, $t_1 = x_1/x_2$ уравнение (13-10) становится уравнением окружности $t_0^2 + t_1^2 = 1$. В карте $U_{x_1+x_2}$, где $x_1 + x_2 = 1$, в локальных координатах

$$t = x_0/(x_1 + x_2) \quad \text{и} \quad s = (x_2 - x_1)/(x_2 + x_1)$$

после переноса x_1^2 из левой части (13-10) направо и деления обеих частей на $x_2 + x_1$ уравнение (13-10) преобразуется в уравнение параболы $t^2 = s$. Таким образом, аффинные окружность, гипербола и парабола являются изображения одной и той же проективной кривой (13-10) в различных аффинных картах. Вид кривой (13-10) в карте $U_\xi \subset \mathbb{P}_2$ определяется тем, как расположена по отношению к кривой бесконечно удалённая прямая $\xi(x) = 0$ этой карты: когда эта прямая не пересекается с кривой, касается её или пересекает её в двух разных точках, кривая (13-10) выглядит на дополнительной к этой прямой аффинной карте, соответственно, как эллипс, парабола или гипербола, см. рис. 13⋄5.

13.6.3. Проективное замыкание аффинной гиперповерхности. Каждая аффинная алгебраическая гиперповерхность $V(f) \subset \mathbb{A}^n = \mathbb{A}(\Bbbk^n)$ степени d может быть расширена до проективной гиперповерхности $V(\overline{f}) \subset \mathbb{P}_n = \mathbb{P}(\Bbbk^{n+1})$, которая называется *проективным замыканием* аффинной гиперповерхности $V(f)$ и строится следующим образом. Обозначим координаты в исходное аффинном пространстве через $(x_1, \dots, x_n)$ и вложим его в проективное пространство с однородными координатами $(x_0 : x_1 : \dots : x_n)$ в качестве аффинной карты U_0, на которой $x_0 = 1$. Запишем (неоднородный) многочлен f в виде

$$f(x_1, \dots, x_n) = f_0 + f_1(x_1, \dots, x_n) + f_2(x_1, \dots, x_n) + \dots + f_d(x_1, \dots, x_n),$$

где каждый многочлен f_k однороден степени k. Образуем из f однородный многочлен

$$\overline{f}(x_0, x_1, \dots, x_n) \stackrel{\text{def}}{=} f_0\, x_0^d + f_1(x_1, \dots, x_n)\, x_0^{d-1} + \dots + f_d(x_1, \dots, x_n),$$

умножив в f каждый моном на такую степень переменной x_0, чтобы степени всех мономов стали равны d. Многочлен $\overline{f}$ превращается обратно в f, если положить в нём $x_0 = 1$. Поэтому аффинная гиперповерхность $V(f) = V(\overline{f}) \cap U_0$ является изображением своего проективного замыкания $V(\overline{f}) \subset \mathbb{P}_n$ в аффинной карте U_{x_0}. Точки проективного замыкания, лежащие в бесконечно удалённой по отношению карте U_0 проективной гиперплоскости $x_0 = 0$, образуют в ней проективную гиперповерхность, которая в однородных координатах $(x_1 : \dots : x_n)$ описывается однородным уравнением $f_d(x_1, \dots, x_n) = 0$ и называется поверхностью *асимптотических направлений* аффинной гиперповерхности $V(f)$. Подчеркнём, что аффинная прямая, проведённая в асимптотическом направлении, может не быть асимптотой аффинной гиперповерхности в том смысле, который принят в математическом анализе.

Пример 13.12 (каспидальная кубика)
Проективным замыканием аффинной кубической кривой $x_2 = x_1^3$ является проективная кубическая кривая $x_0^2 x_2 = x_1^3$, имеющая ровно одну бесконечно удалённую точку $p = (0 : 0 : 1)$, которой в исходной аффинной карте U_{x_0} отвечает направление второй координатной оси x_2.

Обратите внимание, что никакая параллельная этой оси прямая $x_1 = \text{const}$ не является асимптотой функции $x_2 = x_1^3$ в смысле математического анализа. Точка p видна в аффинной карте U_{x_2}, на которой $x_2 = 1$. В этой карте кривая задаётся уравнением $x_0^2 = x_1^3$ и представляет собой полукубическую параболу с остриём[1] в точке p.

Задачи для самостоятельного решения к §13

Задача 13.1. Сколько k-мерных аффинных подпространств имеется в n-мерном аффинном пространстве над конечным полем из q элементов?

Задача 13.2. Может ли аффинное пространство над бесконечным полем оказаться объединением конечного числа подпространств меньшей размерности?

Задача 13.3. В аффинном пространстве $\mathbb{A}^4$ заданы не пересекающиеся двумерная плоскость Π с направляющим векторным пространством U и прямая ℓ с вектором скорости $v \notin U$. Опишите объединение всех прямых (ab) с $a \in \ell$ и $b \in \Pi$.

Задача 13.4 (линейные комбинации точек). Пусть в аффинном пространстве A над векторным пространством V над полем $\Bbbk$ заданы точки $p_1, \dots, p_m$, а в поле $\Bbbk$ — числа $x_1, \dots, x_m$. Зафиксируем точку $a \in A$. Докажите, что

а) вектор $\overrightarrow{x_1p_1 + \dots + x_mp_m} \stackrel{\text{def}}{=} x_1\overrightarrow{ap}_1 + \dots + x_m\overrightarrow{ap}_m \in V$ не зависит от выбора точки a если и только если $\sum x_i = 0$ (в этом случае такой вектор называется *векторной комбинацией* или *вектором* точек p_i с весами x_i)

б) любая линейная комбинация векторных комбинаций любых наборов точек является векторной комбинацией точек из объединения этих наборов

в) точка $x_1p_1 + \dots + x_mp_m \stackrel{\text{def}}{=} a + x_1\overrightarrow{ap}_1 + \dots + x_m\overrightarrow{ap}_m \in A$ не зависит от выбора точки a если и только если $\sum x_i = 1$ (в этом случае точка $x_1p_1 + \dots + x_mp_m$ называется *барицентрической комбинацией* или *барицентром* точек p_i с весами x_i)

г) любая барицентрическая комбинация барицентрических комбинаций любых наборов точек является барицентрической комбинацией точек из объединения этих наборов.

Задача 13.5. Отрезок, соединяющий одну из точек $p_1, \dots, p_k$ с равновесным барицентром остальных, называется *медианой* набора точек p_i. Покажите, что все медианы пересекаются в одной точке и выясните, в каком отношении[2] она делит каждую из медиан.

Задача 13.6 (барицентрические координаты). Пусть точки $p_0, p_1, \dots, p_n$ аффинного пространства A размерности n не лежат в одной гиперплоскости. Покажите, что сопоставление

$$(x_0, x_1, \dots, x_n) \mapsto x_0p_0 + x_1p_1 + \dots + x_np_n$$

устанавливает биекцию между наборами весов $(x_0, x_1, \dots, x_n) \in \Bbbk^{n+1}$ с единичной суммой и точками[3] пространства A.

Задача 13.7. Нарисуйте в $\mathbb{R}^2$ все точки, барицентрические координаты (α, β, γ) которых относительно данных трёх неколлинеарных точек a, b, c удовлетворяют условиям: а) $\alpha, \beta, \gamma > 0$ б) $\alpha, \beta > 0$, $\gamma < 0$ в) $\alpha = \beta$ г) $\alpha, \beta > 1/3$, $\gamma > 0$ д) $\alpha \geqslant \beta$ е) $\alpha \geqslant \beta \geqslant \gamma$.

[1] По-английски *cusp*. Кальку *каспе* частенько используют и в русском.

[2] Говорят, что точка c делит отрезок $[a, b]$ в отношении $\alpha : \beta$, если $\beta \cdot \vec{ca} + \alpha \cdot \vec{cb} = 0$.

[3] Набор весов, отвечающий заданной точке $a \in A$, называется *барицентрическими координатами* точки a относительно точек $p_0, p_1, \dots, p_n$.

Задача 13.8. В условиях предыдущей задачи напишите соотношения на (α, β, γ), задающие:
а) шесть треугольников, на которые $\triangle abc$ разрезается медианами
б) треугольники гомотетичные[1] $\triangle abc$ с коэффициентами 3 и $1/3$ относительно точки пересечения медиан.

Задача 13.9 (четырёхмерный куб). Фигура $I^4 \stackrel{\text{def}}{=} \{x \in \mathbb{R}^4 \mid \forall\, i\ |x_i| \leqslant 1\}$ называется *стандартным четырёхмерным кубом*. Нарисуйте какую-нибудь двумерную параллельную проекцию четырёхмерного куба, у которой все вершины различны. Сколько у четырёхмерного куба вершин, рёбер, двумерных и трёхмерных граней? Нарисуйте развёртку трёхмерной поверхности[2] четырёхмерного куба и напишите инструкцию по склейке[3] из неё четырёхмерного куба. В скольких кубиках побываешь, когда гуляешь по трёхмерной поверхности четырёхмерного куба так, что выходишь из каждого кубика сквозь двумерную грань а) противоположную б) соседнюю слева к той, сквозь которую вошёл?

Задача 13.10. При каких $c \in \mathbb{R}$ четырёхмерный куб пересекается с трёхмерной гиперплоскостью

$$x_1 + \ldots + x_4 = c?$$

Нарисуйте все трёхмерные многогранники, которые высекаются из куба такими гиперплоскостями. Если задача вызывает затруднения, потренируйтесь сначала на аналогичных сечениях трёхмерного куба[4] в $\mathbb{R}^3$.

Задача 13.11. Обозначим через a, b, c, d, e концы стандартных базисных векторов в $\mathbb{R}^5$, а через x — середину отрезка, соединяющего центры треугольников $\triangle abc$ и $\triangle cde$. Проходящая через x прямая yz имеет точку y на прямой ae, а точку z — в плоскости bcd. найдите $\overrightarrow{xy} : \overrightarrow{yz}$.

Задача 13.12. Пусть точка p лежит строго внутри[5] невырожденного симплекса[6] $abcde \subset \mathbb{R}^4$. Можно ли провести через P
а) двумерную плоскость, не пересекающую ни одной прямой, проходящей через какие-нибудь две вершины симплекса $abcde$
б) двумерную плоскость, не пересекающую ни одной двумерной плоскости, проходящей через какие-нибудь три вершины симплекса $abcde$
в) прямую, не пересекающую ни одной двумерной плоскости, проходящей через какие-нибудь три вершины симплекса $abcde$?

Задача 13.13. В четырёхмерном аффинном пространстве над бесконечным полем задано конечное множество двумерных аффинных плоскостей. Всегда ли найдётся двумерная плоскость

---

[1] *Гомотетия* с центром $c \in A$ и коэффициентом $\lambda \in \Bbbk$ — это отображение $\gamma_{c,\lambda} : A \to A, x \mapsto c + \lambda \vec{cx}$

[2] Она представляет собою трёхмерный многогранник, собранный из обычных трёхмерных кубиков.

[3] Укажите, какие пары двумерных граней трёхмерных кубов надлежит склеить друг с другом и как именно.

[4] Алгебраически и те и другие сечения можно описывать в барицентрических координатах относительно треугольника (соотв. тетраэдра) с вершинами в точках пересечения плоскости с тремя (соотв. четырьмя) рёбрами куба, выходящими из вершины $(-1,-1,-1)$ (соотв. $(-1,-1,-1,-1)$) или же относительно центрально симметричного ему треугольника (соотв. тетраэдра), высекаемого рёбрами, входящими в противоположную вершину.

[5] Т. е. является барицентрической комбинацией точек a, b, c, d, e со строго положительными весами.

[6] Невырожденным *симплексом* размерности k в $\mathbb{R}^n$ называется множество всех неотрицательных барицентрических комбинаций заданных $k+1$ не лежащих в одном $(k-1)$-мерном аффинном подпространстве точек, которые называются *вершинами* симплекса. Симплексы размерностей 1, 2, 3 обычно называют *отрезком*, *треугольником* и *тетраэдром*.

а) не пересекающая ни одну из них
б) пересекающая каждую из них ровно в одной точке?

Задача 13.14. Нетождественное биективное аффинное отображение $\mathbb{A}^n \to \mathbb{A}^n$ коммутирует со всеми сдвигами. Верно ли, что оно само сдвиг?

Задача 13.15. Докажите, что биективное аффинное преобразование φ, дифференциал которого не имеет ненулевых неподвижных векторов[1], обязательно имеет неподвижную точку.

Задача 13.16. Пусть биективное аффинное преобразование $\varphi\colon \mathbb{R}^n \to \mathbb{R}^n$ таково, что $\varphi^m = \mathrm{Id}$ для некоторого $m \in \mathbb{N}$. Докажите, что φ имеет неподвижную точку.

Задача 13.17. Обозначим через U и W наименьшие по включению аффинные подпространства в $\mathbb{A}^4(\mathbb{Q})$, проходящие, соответственно, через
а) точки $(-4,-4,6,1)$, $(-4,-5,9,0)$, $(-8,-1,21,-4)$, $(-10,-1,33,-8)$ и точки $(4,-15,-14,-3)$, $(-13,25,-23,21)$, $(-11,17,-13,13)$, $(-9,9,-3,5)$.
б) точки $(-4,-5,3,-3)$, $(0,7,-5,-4)$, $(-7,-14,9,0)$, $(-10,-23,15,0)$ и точки $(-7,-14,11,6)$, $(-14,-35,28,20)$, $(-9,-20,17,14)$, $(-1,4,-5,-11)$
в) точки $(7,-7,-5,10)$, $(0,2,3,-9)$, $(17,-19,-19,38)$, $(-2,5,4,-14)$ и точки $(1,3,-3,-5)$, $(-4,14,-8,-16)$, $(16,-30,12,28)$, $(-3,13,-11,-13)$.
Найдите $\dim U$, $\dim W$ и $\dim U \cap W$ или докажите, что $U \cap W = \varnothing$.

Задача 13.18. Рассмотрим в $\mathbb{R}^3$ точки $a = (1,-2,3)$, $b = (-3,1,-2)$, $c = (2,-3,1)$, $d = (7,-5,1)$. Сколько прямых проходит через начало координат и пересекает обе прямые (ab) и (cd)? В каком отношении делит начало координат отрезок с концами в точках пересечения?

Задача 13.19. Сколько k-мерных проективных подпространств в $\mathbb{P}_n(\mathbb{F}_q)$?

Задача 13.20. Рассмотрим в $\mathbb{P}_n = \mathbb{P}(V)$ аффинную карту $U_\xi = \{v \in V \mid \xi(v) = 1\}$, отвечающую ненулевому ковектору $\xi \in V^*$, и k-мерное проективное подпространство $K = \mathbb{P}(W) \subset \mathbb{P}_n$ — проективизацию $(k+1)$-мерного векторного подпространства $W \subset V$. Убедитесь, что либо $K \cap U_\xi = \varnothing$, либо $K \cap U_\xi$ наблюдается в аффинном пространстве U_ξ как k-мерное аффинное подпространство.

Задача 13.21. Подмножество $\Phi \subset \mathbb{P}_n(\Bbbk)$ таково, что в каждой аффинной карте, с которой оно пересекается, его видно как k-мерное аффинное подпространство. Верно ли, что $\Phi = \mathbb{P}(W)$ для некоторого $(k+1)$-мерного векторного подпространства $W \subset \Bbbk^{n+1}$ а) если поле $\Bbbk \neq \mathbb{F}_2$ б*) если $\Bbbk = \mathbb{F}_2$? Всегда ли есть аффинная карта, где Φ вообще не видно?

Задача 13.22. Гомография $\sigma\colon \mathbb{P}_1 \xrightarrow{\sim} \mathbb{P}_1$ называется *инволюцией*, если $\sigma^2 = \mathrm{Id}$. Покажите, что над алгебраически замкнутым полем каждая нетождественная инволюция на $\mathbb{P}_1$
а) имеет ровно две различные неподвижные точки
б) в подходящей аффинной карте выглядит как центральная симметрия
в) если $\sigma(p) = p$ и $\sigma(q) = q$, то $\sigma(x) = y \iff [x,y,p,q] = -1$
г) если $\sigma(\alpha) = \beta \neq \alpha$ и $\sigma(\gamma) = \delta \neq \gamma$, то $\sigma(x) = x \iff [\alpha,\beta,\gamma,x]^2 = [\alpha,\beta,\gamma,\delta]$.

Задача 13.23. Постройте инволюцию без неподвижных точек на $\mathbb{P}_1(\mathbb{R})$. Может ли инволюция вещественной проективной прямой иметь ровно одну неподвижную точку?

Задача 13.24. Найдите образы точек ∞, 0, 1, -1, 3 комплексной проективной прямой при инволюции с неподвижными точками а) $2, 1/2$ б) $-3, 2$.

Задача 13.25. Найдите неподвижные точки инволюции комплексной проективной прямой, при которой а) $1 \leftrightarrow 0, 2 \leftrightarrow \infty$ б) $1 \leftrightarrow \infty, 3 \leftrightarrow 0$.

[1] Т. е. таких $v \neq 0$, что $D_\varphi(v) = v$.

Задача 13.26. Опишите все такие преобразования из PGL_2, что а) $\infty \mapsto \infty$ б) $(\infty, 0) \mapsto (\infty, 0)$ в) $(\infty, 0, 1) \mapsto (0, \infty, 1)$ г) $(\infty, 0, 1) \mapsto (1, 0, \infty)$ д) $(\infty, 0, 1) \mapsto (\infty, 1, 0)$ и без вычислений получите из этого описания формулы

$$[p_2, p_1, p_3, p_4] = [p_1, p_2, p_3, p_4]^{-1}, \quad [p_1, p_3, p_2, p_4] = 1 - [p_1, p_2, p_3, p_4],$$
$$[p_3, p_2, p_1, p_4] = \frac{[p_1, p_2, p_3, p_4]}{[p_1, p_2, p_3, p_4] - 1}.$$

Задача 13.27. Пусть $[p_1, p_2, p_3, p_4] = \vartheta$. Найдите $[p_{g(1)}, p_{g(2)}, p_{g(3)}, p_{g(4)}]$ для всех перестановок $g \in S_4$ и выясните, сколько различных значений при этом получится в зависимости от $\vartheta \in \Bbbk \smallsetminus \{0, 1\}$.

Задача 13.28. Покажите, что через любые 5 различных точек на $\mathbb{P}_2$ проходит кривая второй степени.

Задача 13.29 (нормальные рациональные кривые). Пусть $\operatorname{char} \Bbbk = 0$. Зафиксируем линейно независимые однородные многочлены n-й степени $f_0, f_1, \ldots, f_n \in \Bbbk[x_0, x_1]$ и попарно различные точки $p_0, p_1, \ldots, p_n \in \mathbb{P}_1$. Рассмотрим три отображения $\mathbb{P}_1 \to \mathbb{P}_n$, посылающие точку $a = (\alpha_0 : \alpha_1) \in \mathbb{P}_1$ в точки с однородными координатами
а) $(\alpha_0^n : \alpha_0^{n-1}\alpha_1 : \ldots : \alpha_0\alpha_1^{n-1} : \alpha_1^n)$ б) $\big(f_0(a) : \ldots : f_n(a)\big)$
в) $\big(\det^{-1}(p_0, a) : \ldots : \det^{-1}(p_n, a)\big)$, где $\det(b, a) \stackrel{\text{def}}{=} \beta_0\alpha_1 - \beta_1\alpha_0$ для $b = (\beta_0 : \beta_1)$.
Докажите, что все три отображения инъективны, а их образы являются алгебраическими многообразиями и переводятся друг в друга подходящими проективными преобразованиями $\mathbb{P}_n \xrightarrow{\sim} \mathbb{P}_n$. Кривые, которые получаются из них всевозможными проективными преобразованиями называются *нормальными рациональными*.

Задача 13.30. Покажите, что никакие $n + 1$ точек нормальной рациональной кривой в $\mathbb{P}_n$ не лежат в одной гиперплоскости.

Задача 13.31. Фиксируем $n + 3$ точки $p_1, \ldots, p_n$, a, b, $c \in \mathbb{P}_n$ так, чтобы никакие $n + 1$ из них не лежали в одной гиперплоскости.
а) Убедитесь, что гиперплоскости, проходящие через все точки p_ν с $\nu \neq i$, образуют в двойственном проективном пространстве $\mathbb{P}_n^\times$ прямую. Обозначим её через $\ell_i \subset \mathbb{P}_n^\times$.
б) Обозначим через $\psi_{ij} : \ell_j \xrightarrow{\sim} \ell_i$ гомографию, переводящую три проходящие через точки a, b, c гиперплоскости прямой ℓ_j соответственно в три проходящие через точки a, b, c гиперплоскости прямой ℓ_i. Покажите что $\bigcup_{H \in \ell_1} H \cap \psi_{21}(H) \cap \ldots \cap \psi_{n1}(H)$ это нормальная рациональная кривая.

Задача 13.32. Покажите, что через каждые $n+3$ точки в $\mathbb{P}_n$, никакие $n+1$ из которых не лежат в одной гиперплоскости, можно провести единственную нормальную рациональную кривую.

§14. Евклидовы пространства

14.1. Скалярное произведение. Векторное пространство V над полем вещественных чисел $\mathbb{R}$ называется *евклидовым*, если задана билинейная[1] функция $V \times V \to \mathbb{R}$, которая называется *скалярным произведением* или *евклидовой структурой* и сопоставляет паре векторов $u, w \in V$ число $(u, w) \in \mathbb{R}$ так, что $(u, w) = (w, u)$ для всех $u, w \in V$ и $(v, v) > 0$ для всех ненулевых $v \in V$. Первое свойство называется *симметричностью*, второе — *положительностью* или *положительной определённостью*.

Пример 14.1 (координатное евклидово пространство)
На пространстве $\mathbb{R}^n$ есть *стандартное* евклидово скалярное произведение, сопоставляющее векторам $u = (x_1, \dots, x_n)$ и $w = (y_1, \dots, y_n)$ число

$$(u, w) \stackrel{\text{def}}{=} x_1 y_1 + \dots + x_n y_n. \tag{14-1}$$

Упражнение 14.1. Убедитесь, что оно билинейно, симметрично и положительно.

Пример 14.2 (пространство непрерывных функций)
Зададим на пространстве вещественных непрерывных функций на отрезке $[a, b]$ скалярное произведение формулой

$$(f, g) \stackrel{\text{def}}{=} \int_a^b f(x) g(x)\, dx\,. \tag{14-2}$$

Упражнение 14.2. Убедитесь, что оно билинейно, симметрично и положительно.

Если понимать функции $[a, b] \to \mathbb{R}$ как элементы прямого произведения[2] $\mathbb{R}^{[a,b]}$ континуального семейства одномерных пространств $\mathbb{R}$, занумерованных точками отрезка, то на формулу (14-2) можно смотреть как на прямое обобщение формулы (14-1), и это обобщение можно варьировать: рассматривать вместо непрерывных другие классы функций со свойством

$$f \not\equiv 0 \;\Rightarrow\; \int_a^b f^2(x)\, dx > 0$$

(например, многочлены степени не выше n), заменить отрезок $[a, b]$ какой-нибудь другой фигурой, по которой можно интегрировать, и т. п.

14.1.1. Ортонормальные базисы. Если $(u, w) = 0$, векторы u и w называются *перпендикулярными*. Набор векторов $v_1, \dots, v_k$ называется *ортогональным*, если $(v_i, v_j) = 0$ для всех $i \neq j$. Ортогональный набор ненулевых векторов автоматически линейно независим, так как скалярно умножая равенство $\lambda_1 v_1 + \dots + \lambda_k v_k = 0$ на вектор v_i, получаем $\lambda_i (v_i, v_i) = 0$, откуда $\lambda_i = 0$.

Ортогональный набор векторов $e_1, \dots, e_k$ называется *ортонормальным*, если $(e_i, e_i) = 1$ для всех i. Такой набор автоматически является базисом своей линейной оболочки, и разложение $v = \sum x_i e_i$ произвольного вектора $v \in \operatorname{span}(e_1, \dots, e_k)$ по этому базису имеет коэффициенты $x_i = (e_i, v)$, а скалярное произведение векторов $u = \sum x_i e_i$ и $w = \sum y_i e_i$ вычисляется по формуле (14-1).

Упражнение 14.3. Проверьте оба эти факта.

[1] Т. е. линейная по каждому из двух аргументов, см. n° 8.1 на стр. 131.
[2] См. прим. 6.8 на стр. 104.

Предложение 14.1 (ортогонализация Грама – Шмидта)
Пусть не все векторы $u_1, \ldots, u_m$ нулевые. Тогда в их линейной оболочке существует такой ортонормальный базис $e_1, \ldots, e_n$, что при каждом k линейная оболочка векторов $u_1, \ldots, u_k$ лежит в линейной оболочке векторов $e_1, \ldots, e_k$.

Доказательство. Выбрасывая из набора нулевые векторы, будем считать, что все $u_i \neq 0$. В качестве первого вектора искомого базиса возьмём $e_1 = u_1 / \sqrt{(u_1, u_1)}$. Тогда

$$(e_1, e_1) = 1 \quad \text{и} \quad \operatorname{span}(e_1) = \operatorname{span}(u_1)\,.$$

Допустим по индукции, что для векторов $u_1, \ldots, u_k$ уже построены такие ортонормальные векторы $e_1, \ldots, e_i$, что $i \leqslant k$ и

$$\operatorname{span}(e_1, \ldots, e_i) = \operatorname{span}(u_1, \ldots, u_k)\,. \tag{14-3}$$

Положим $w_{i+1} = u_{k+1} - \sum_{v=1}^{i} (u_{k+1}, e_v) \cdot e_v$. Так как для каждого уже построенного вектора e_j выполняется равенство $(w_{i+1}, e_j) = (u_{k+1}, e_j) - (u_{k+1}, e_j)(e_j, e_j) = 0$ вектор w_{i+1} ортогонален подпространству (14-3). Если $w_{i+1} = 0$, то вектор u_{k+1} лежит в подпространстве (14-3) и индуктивное предположение выполнятся для наборов $u_1, \ldots, u_{k+1}$ и $e_1, \ldots, e_i$. Если $w_{i+1} \neq 0$, полагаем $e_{i+1} = w_{i+1} / \sqrt{(w_{i+1}, w_{i+1})}$ и заключаем, что индуктивное предположение выполнятся для наборов $u_1, \ldots, u_{k+1}$ и $e_1, \ldots, e_{i+1}$. □

Следствие 14.1
В каждом конечномерном евклидовом пространстве имеется ортонормальный базис. □

14.1.2. Матрицы Грама. С каждыми двумя наборами векторов

$$\boldsymbol{u} = (u_1, \ldots, u_n) \quad \text{и} \quad \boldsymbol{w} = (w_1, \ldots, w_m) \tag{14-4}$$

евклидова пространства V связана таблица их попарных скалярных произведений — матрица

$$G_{\boldsymbol{uw}} \stackrel{\text{def}}{=} \big((u_i, w_j)\big) \in \operatorname{Mat}_{n\times m}(\mathbb{R})\,, \tag{14-5}$$

в i-й строке и j-м столбце которой находится скалярное произведение (u_i, w_j). Она называется *матрицей Грама* наборов (14-4). Согласно n° 8.2 на стр. 137, скалярное произведение $V \times V \to \mathbb{R}$ задаёт умножение матриц $\operatorname{Mat}_{n\times s}(V) \times \operatorname{Mat}_{s\times m}(V) \to \operatorname{Mat}_{n\times m}(\mathbb{R})$, и матрица Грама

$$G_{\boldsymbol{uw}} = \boldsymbol{u}^t \boldsymbol{w}$$

является произведением транспонированного к строке $\boldsymbol{u} = (u_1, \ldots, u_n)$ столбца $\boldsymbol{u}^t$ и строки $\boldsymbol{w}$. Если наборы векторов $\boldsymbol{u}$ и $\boldsymbol{w}$ линейно выражаются через наборы $\boldsymbol{e} = (e_1, \ldots, e_r)$ и $\boldsymbol{f} = (f_1, \ldots, f_s)$ по формулам $\boldsymbol{u} = \boldsymbol{e}\, C_{\boldsymbol{eu}}$ и $\boldsymbol{w} = \boldsymbol{f}\, C_{\boldsymbol{fw}}$, где $C_{\boldsymbol{eu}} \in \operatorname{Mat}_{r\times m}(\mathbb{R})$ и $C_{\boldsymbol{fw}} \in \operatorname{Mat}_{s\times k}(\mathbb{R})$, то матрица Грама $G_{\boldsymbol{uw}}$ пересчитывается через матрицу Грама $G_{\boldsymbol{ef}}$ по формуле

$$G_{\boldsymbol{uw}} = \boldsymbol{u}^t \boldsymbol{w} = \big(\boldsymbol{e} C_{\boldsymbol{eu}}\big)^t \boldsymbol{f}\, C_{\boldsymbol{fw}} = C_{\boldsymbol{eu}}^t \boldsymbol{e}^t \boldsymbol{f}\, C_{\boldsymbol{fw}} = C_{\boldsymbol{eu}}^t G_{\boldsymbol{ef}} C_{\boldsymbol{fw}}\,. \tag{14-6}$$

В частности, скалярное произведение произвольных векторов

$$u = \boldsymbol{u}\boldsymbol{x} \in \operatorname{span}(u_1, \ldots, u_n) \text{ и } w = \boldsymbol{w}\boldsymbol{y} \in \operatorname{span}(w_1, \ldots, w_m)\,, \quad \text{где} \quad \boldsymbol{x} \in \mathbb{R}^n\,,\ \boldsymbol{y} \in \mathbb{R}^m\,,$$

равно $(u, w) = \boldsymbol{x}^t G_{\boldsymbol{uw}} \boldsymbol{y}$.

При $\boldsymbol{w} = \boldsymbol{u}$ таблица умножения векторов из набора $\boldsymbol{u} = (u_1, \ldots, u_n)$ обозначается

$$G_{\boldsymbol{u}} \stackrel{\text{def}}{=} G_{\boldsymbol{u},\boldsymbol{u}} = \boldsymbol{u}^t\boldsymbol{u} = \big((u_i, u_j)\big) \in \mathrm{Mat}_{n\times n}(\mathbb{R})$$

и называется матрицей Грама набора $\boldsymbol{u}$. Правило преобразования (14-6) приобретает для таких матриц вид

$$G_{\boldsymbol{u}} = C_{\boldsymbol{eu}}^t G_{\boldsymbol{e}} C_{\boldsymbol{eu}}\,. \tag{14-7}$$

Определитель $\Gamma_{\boldsymbol{u}} \stackrel{\text{def}}{=} \det G_{\boldsymbol{u}}$ называется *определителем Грама* набора векторов $\boldsymbol{u}$. Ортонормальность набора векторов $\boldsymbol{e} = (e_1, \ldots, e_n)$ означает, что $G_{\boldsymbol{e}} = E$, и в этом случае $\Gamma_{\boldsymbol{e}} = \det E = 1$.

Предложение 14.2
Для любого набора векторов $\boldsymbol{w} = (w_1, \ldots, w_m)$ выполняется неравенство $\Gamma_{\boldsymbol{w}} \geqslant 0$, которое обращается в равенство если и только если этот набор линейно зависим. Если набор $\boldsymbol{w}$ линейно независим, а набор векторов $\boldsymbol{e} = (e_1, \ldots, e_m)$ составляет ортонормальный базис в линейной оболочке $\mathrm{span}(w_1, \ldots, w_m)$, то $\Gamma_{\boldsymbol{w}} = \det^2 C_{\boldsymbol{ew}}$, где матрица $C_{\boldsymbol{ew}}$ составлена из столбцов координат векторов w_j в ортонормальном базисе $\boldsymbol{e}$.

Доказательство. Пусть существует такой ненулевой столбец $\boldsymbol{x} = (x_1, \ldots, x_m)^t \in \mathbb{R}^m$, что

$$\boldsymbol{w}\boldsymbol{x} = x_1 w_1 + \ldots + x_m w_m = 0\,.$$

Умножая это равенство справа на столбец $\boldsymbol{w}^t$, получаем $G_{\boldsymbol{w}}\boldsymbol{x} = 0$. Это означает, что столбцы матрицы $G_{\boldsymbol{w}}$ линейно зависимы. Поэтому $\Gamma_{\boldsymbol{w}} = \det G_{\boldsymbol{w}} = 0$. Если векторы $w_1, \ldots, w_m$ линейно независимы, их линейная оболочка m-мерна, и по предл. 14.1 на стр. 256 в ней имеется ортонормальный базис $\boldsymbol{e} = (e_1, \ldots, e_m)$. Тогда $G_{\boldsymbol{w}} = C_{\boldsymbol{ew}}^t G_{\boldsymbol{e}} C_{\boldsymbol{ew}} = C_{\boldsymbol{ew}}^t C_{\boldsymbol{ew}}$, и $\det G_{\boldsymbol{w}} = \det^2 C_{\boldsymbol{ew}} > 0$, так как матрица перехода $C_{\boldsymbol{ew}}$ обратима[1] и её определитель ненулевой[2]. □

Пример 14.3 (неравенство Коши – Буняковского – Шварца)
Для пары векторов $u, w \in V$ неотрицательность их определителя Грама

$$\det \begin{pmatrix} (u,u) & (u,w) \\ (w,u) & (w,w) \end{pmatrix} \geqslant 0$$

выражается неравенством

$$(u,u)\cdot(w,w) \geqslant (u,w)^2\,, \tag{14-8}$$

которое называется *неравенством Коши – Буняковского – Шварца* и превращается в равенство если и только если векторы u и w пропорциональны.

Пример 14.4 (продолжение прим. 14.1 на стр. 255)
В пространстве $\mathbb{R}^n$ со стандартной евклидовой структурой из прим. 14.1 неравенство (14-8) утверждает, что для любых наборов вещественных чисел $x_1, \ldots, x_n$ и $y_1, \ldots, y_n$

$$(x_1^2 + \ldots + x_n^2)(y_1^2 + \ldots + y_n^2) \geqslant (x_1 y_1 + \ldots + x_n y_n)^2\,,$$

и равенство равносильно пропорциональности наборов.

[1] См. предл. 8.3 на стр. 139.
[2] См. предл. 11.3 на стр. 198.

Пример 14.5 (продолжение прим. 14.2 на стр. 255)
Для интегралов из прим. 14.2 неравенство (14-8) принимает вид

$$\left(\int_a^b f^2(x)\,dx\right)\cdot\left(\int_a^b g^2(x)\,dx\right)\geqslant\left(\int_a^b f(x)g(x)\,dx\right)^2,$$

где равенство равносильно тому, что одна из функций f, g получается из другой умножением на константу.

14.2. Объём. Функция n аргументов $\omega: V\times\dots\times V\to\Bbbk$ на n-мерном векторном пространстве V над произвольным полем $\Bbbk$ называется *объёмом ориентированного n-мерного параллелепипеда* или *формой n-мерного объёма*, если её значение не меняется при добавлении к любому из аргументов произвольной кратности любого другого аргумента:

$$\omega(\dots,u+\lambda w,\dots,w,\dots)=\omega(\dots,u,\dots,w,\dots),$$

а при умножении любого из аргументов на число её значение умножается на это число:

$$\omega(\dots,\lambda v,\dots)=\lambda\,\omega(\dots,v,\dots).$$

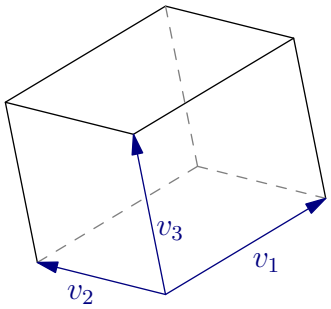


Рис. 14⋄1. Параллелепипед.

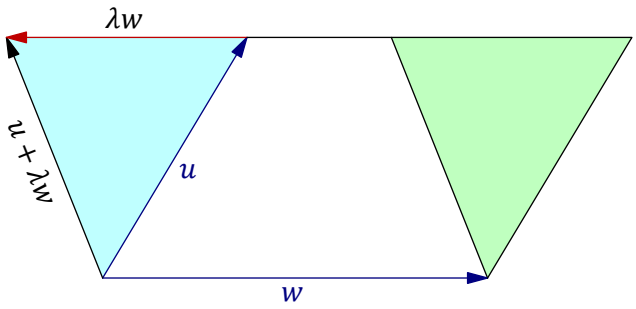


Рис. 14⋄2. Параллельный перекос.

Над полем вещественных чисел $\Bbbk=\mathbb{R}$ первое свойство означает, что объём параллелепипеда, натянутого на векторы $v_1,\dots,v_n$, не меняется при сдвиге двух противоположных $(n-1)$-мерных граней друг относительно друга в направлении любого параллельного этим граням ребра[1] и умножается на λ при умножении любого ребра на λ. При $\lambda=-1$ последнее условие означает, что объём меняет знак при смене ориентации[2] параллелепипеда, что и объясняет эпитет «ориентированный» в его названии.

Лемма 14.1
Каждая форма n-мерного объёма ω линейна по каждому аргументу, знакопеременна[3], и обращается в нуль, когда аргументы линейно зависимы (в частности, кососимметрична[4]).

[1] Параллельная проекция происходящего на двумерную плоскость, порождённую ребром, вдоль которого делается сдвиг, и ребром, соединяющим сдвигаемые грани, изображена на рис. 14⋄2. Отрезанная справа и приклеенная слева призмы получаются друг из друга параллельным переносом.

[2] См. **??** на стр. **??**.

[3] Функция нескольких аргументов называется *знакопеременной*, если при перестановке любых двух аргументов она меняет знак.

[4] Напомню, что функция нескольких аргументов называется *кососимметричной*, если она обращается в нуль, когда какие-нибудь два аргумента совпадают. Так как содержащий два одинаковых вектора набор векторов линейно зависим, кососимметричность является частью третьего свойства

Доказательство. Сначала установим последнее свойство. Пусть один из векторов линейно выражается через остальные, к примеру, $v_1 = \lambda_2 v_2 + \cdots + \lambda_n v_n$. Тогда

$$\omega(v_1, \dots, v_n) = \omega(\lambda_2 v_2 + \dots + \lambda_n v_n, v_2, \dots, v_n) = \omega(0, v_2, \dots, v_n) = \\ = \omega(0 \cdot 0, v_2, \dots, v_n) = 0 \cdot \omega(0, v_2, \dots, v_n) = 0\,.$$

Теперь докажем линейность по каждому аргументу, т. е. равенство

$$\omega(\dots, \lambda u + \mu w, \dots) = \lambda\,\omega(\dots, u, \dots) + \mu\,\omega(\dots, w, \dots)\,. \tag{14-9}$$

Когда оба набора аргументов в правой части линейно зависимы, набор аргументов в левой части тоже линейно зависим, и обе части (14-9) нулевые по уже доказанному. Поэтому без ограничения общности можно считать, что аргументы первого слагаемого в правой части (14-9) образуют базис пространства V. Тогда $w = \varrho u + v$, где v является линейной комбинацией остальных $n-1$ аргументов, и левая часть (14-9) равна

$$\omega(\dots, \lambda u + \mu\varrho u + \mu v, \dots) = \omega(\dots, (\lambda + \mu\varrho)u, \dots) = (\lambda + \mu\varrho)\omega(\dots, u, \dots)\,,$$

а второе слагаемое правой части переписывается как $\mu\omega(\dots, \varrho u + v, \dots) = \mu\varrho \cdot \omega(\dots, u, \dots)$, что и доказывает равенство (14-9). Знакопеременность следует из линейности и кососимметричности[1]: $0 = \omega(\dots, (u+w), \dots, (u+w), \dots) = \omega(\dots, u, \dots, w, \dots) + \det(\dots, w, \dots, u, \dots)$. □

Теорема 14.1
Для любого базиса $\boldsymbol{e} = (e_1, \dots, e_n)$, любого набора векторов $\boldsymbol{v} = (v_1, \dots, v_n)$ и любой формы объёма ω справедливо равенство $\omega(v_1, \dots, v_n) = \omega(e_1, \dots, e_n)\,\det C_{\boldsymbol{ev}}$, где $C_{\boldsymbol{ev}}$ — матрица координат векторов $\boldsymbol{v}$ в базисе[2] $\boldsymbol{e}$. В частности, все формы объёма пропорциональны друг другу и образуют одномерное векторное пространство.

Доказательство. Так как форма ω линейна по каждому аргументу и кососимметрична, вычисление, аналогичное проделанному в форм. (11-12) на стр. 193

$$\omega(v_1, \dots, v_n) = \omega\Big(\sum_{i_1} e_{i_1} c_{i_1 1}, \dots, \sum_{i_n} e_{i_n} c_{i_n n}\Big) = \sum_{i_1, \dots, i_n} c_{i_1 1} \cdots c_{i_n n}\,\omega(e_{i_1}, \dots, e_{i_n}) = \\ = \omega(e_1, \dots, e_n) \sum_{g \in S_n} \operatorname{sgn}(g) c_{g(1)1} c_{g(2)2} \cdots c_{g(n)n} = \omega(e_1, \dots, e_n)\,\det C_{\boldsymbol{ev}}$$

доказывает первое утверждение. Поскольку определитель, как функция от столбцов матрицы, обладает всеми свойствами формы объёма, эта формула при любом значении константы

$$\omega(e_1, \dots, e_n) \in \mathbb{k}$$

задаёт форму объёма. Это доказывает второе утверждение. □

[1] Ср. с сл. 11.4 на стр. 190.
[2] Т. е. $\boldsymbol{v} = \boldsymbol{e}\,C_{\boldsymbol{ev}}$.

14.2.1. Евклидов объём. Из теор. 14.1 вытекает, что форма объёма однозначно задаётся своим значением на каком-нибудь базисе. Форма объёма называется *евклидовой*, если она принимает значение 1 на каком-нибудь ортонормальном базисе. Так как определитель матрицы перехода между ортонормальными базисами равен ± 1, имеется ровно две такие формы, отличающиеся друг от друга знаком. Каждая из них принимает одинаковые значения на одинаково ориентированных[1] базисах и противоположные по знаку значения на противоположно ориентированных базисах. Таким образом, выбор одной из этих форм в качестве формы объёма на V эквивалентен *выбору ориентации* на V. Абсолютная величина формы евклидова объёма

$$\mathrm{Vol}(v_1, \dots, v_n) \stackrel{\text{def}}{=} |\omega(v_1, \dots, v_n)|$$

не зависит от выбора ориентации и называется *евклидовым объёмом* параллелепипеда, натянутого на векторы $(v_1, \dots, v_n)$.

Предложение 14.3
Квадрат евклидова объёма равен определителю Грама: $\mathrm{Vol}^2(v_1, \dots, v_n) = \det\left(v_i, v_j\right)$.

Доказательство. Пусть векторы $\boldsymbol{e} = (e_1, \dots, e_n)$ образуют ортонормальный базис пространства V. Тогда матрица Грама векторов $\boldsymbol{v} = (v_1, \dots, v_n) = \boldsymbol{e}\, C_{\boldsymbol{ev}}$ равна $G_{\boldsymbol{v}} = C_{\boldsymbol{ev}}^t C_{\boldsymbol{ev}}$ и $\det G_{\boldsymbol{v}} = \det^2 C_{\boldsymbol{ev}} = \mathrm{Vol}^2(v_1, \dots, v_n)$, так как $\omega(v_1, \dots, v_n) = \omega(e_1, \dots, e_n) \cdot \det C_{\boldsymbol{ev}}$. □

Пример 14.6 (дискриминант соизмеримой подрешётки и формула Пика)
Пусть $\mathbb{Z}$-подмодуль $U \subset \mathbb{Z}^n$ таков, что фактор $\mathbb{Z}^n / U$ конечен. Обозначим через $\boldsymbol{e}$ какой-нибудь базис в $\mathbb{Z}^n$, а через $\boldsymbol{u} = \boldsymbol{e}\, C_{\boldsymbol{eu}}$ — какой-нибудь базис в U. Абсолютная величина определителя матрицы $C_{\boldsymbol{eu}}$ называется *дискриминантом* соизмеримой[2] с $\mathbb{Z}^n$ подрешётки U и обозначается

$$D_U \stackrel{\text{def}}{=} |\det C_{\boldsymbol{eu}}|\,.$$

Дискриминант не зависит от выбора базисов $\boldsymbol{e}$ и $\boldsymbol{u}$, так как для любых других базисов $\boldsymbol{v} = \boldsymbol{e}\, C_{\boldsymbol{ev}}$ в $\mathbb{Z}^n$ и $\boldsymbol{w} = \boldsymbol{u}\, C_{\boldsymbol{uw}}$ в L матрицы переходов $C_{\boldsymbol{ve}} = C_{\boldsymbol{ev}}^{-1}$ и $C_{\boldsymbol{uw}}$, будучи обратимыми над $\mathbb{Z}$, имеют определители ± 1, откуда $|\det C_{\boldsymbol{vw}}| = |\det(C_{\boldsymbol{ve}} C_{\boldsymbol{eu}} C_{\boldsymbol{uw}})| = |\det(C_{\boldsymbol{ve}}) \det(C_{\boldsymbol{eu}}) \det(C_{\boldsymbol{uw}})| = |\det C_{\boldsymbol{eu}}|$. Беря качестве $\boldsymbol{e}$ и $\boldsymbol{u}$ взаимные базисы[3] $v_1, \dots, v_n$ и $\lambda_1 e_1, \dots, \lambda_n e_n$, заключаем, что дискриминант $D_U = \lambda_1 \dots \lambda_n$ равен числу элементов в факторе

$$\mathbb{Z}^n / U \simeq \mathbb{Z}/(\lambda_1) \oplus \dots \oplus \mathbb{Z}/(\lambda_n)\,.$$

На геометрическом языке, дискриминант D_U решётки $L \subset \mathbb{Z}^n \subset \mathbb{R}^n$ равен евклидову объёму параллелепипеда Π, натянутого в пространстве $\mathbb{R}^n$ на какой-нибудь базис решётки U. Такой параллелепипед называется *фундаментальным параллелепипедом* решётки U. Его сдвиги на векторы решётки покрывают всё пространство $\mathbb{R}^n$, не имея при этом общих внутренних точек. Каждый элемент фактора $\mathbb{Z}^n / U$ представляется точкой, лежащей в Π. При этом каждая внутренняя точка Π не сравнима по модулю U ни с какими другими точками из Π, каждая внутренняя точка любой $(n-1)$-мерной гиперграни Π сравнима ещё ровно с одной точкой из Π, лежащей на параллельной гиперграни, каждая внутренняя точка любой $(n-2)$-мерной грани Π сравнима ровно с тремя точками из Π, лежащими на трёх параллельных $(n-2)$-мерных

[1] См. **??** на стр. **??**.
[2] См. предл. 10.3 на стр. 183.
[3] См. теор. 10.2 на стр. 171.

гранях, и т. д. Каждая вершина Π сравнима с остальными $2^n - 1$ вершинами. Мы заключаем, что объём Π, равный числу элементов в факторе $\mathbb{Z}^n/U$, может быть вычислен по *формуле Пика*:

$$\operatorname{Vol}\Pi = \sum\nolimits_{d=0}^{n} p_d / 2^{n-d},$$

где p_d при $d < n$ обозначает число точек, лежащих внутри d-мерных граней Π, а p_n — число внутренних точек самого Π.

14.3. Евклидова двойственность. Каждым вектор v евклидова пространства V задаёт линейный функционал скалярного умножения на этот вектор:

$$g_v : V \to \mathbb{R}, \quad u \mapsto (u, v).$$

Так как этот функционал линейно зависит от v, возникает линейное отображение

$$G_V : V \to V^*, \quad v \mapsto g_v, \tag{14-10}$$

которое называется *евклидовой корреляцией*. Так как $g_V(v) = (v, v) \neq 0$ для всех $v \neq 0$, ковектор $g_v \neq 0$ при $v \neq 0$. Поэтому отображение (14-10) инъективно, а значит, является изоморфизмом векторных пространств, если пространство V конечномерно. Таким образом, каждый линейный функционал на конечномерном евклидовом векторном пространстве однозначно представляется в виде скалярного произведения с некоторым вектором.

Упражнение 14.4. Убедитесь, что матрица отображения G_V в любом базисе $\boldsymbol{v}$ пространства V и двойственном ему базисе $\boldsymbol{v}^*$ пространства V^* совпадает с матрицей Грама G_v базиса v.

14.3.1. Двойственные базисы. Для любого базиса $\boldsymbol{u} = (u_1, \dots, u_n)$ в V, прообразы

$$u_1^\times, \dots, u_n^\times \in V$$

координатных функционалов $u_1^*, \dots, u_n^* \in V^*$ при изоморфизме (14-10) образуют в V базис, который называется *евклидово двойственным* к $\boldsymbol{u}$ и обозначается $\boldsymbol{u}^\times = (u_1^\times, \dots, u_n^\times)$. Векторы этого базиса однозначно определяются из соотношений

$$(u_i, u_j^\times) = \begin{cases} 0 & \text{при } i \neq j \\ 1 & \text{при } i = j. \end{cases} \tag{14-11}$$

В терминах матриц Грама[1] эти соотношения означают, что $G_{\boldsymbol{u}\boldsymbol{u}^\times} = \boldsymbol{u}^t\boldsymbol{u}^\times = E$. Согласно форм. (14-7) на стр. 257 матрица $C_{\boldsymbol{u}\boldsymbol{u}^\times}$, линейно выражающая базис $\boldsymbol{u}^\times$ через базис $\boldsymbol{u}$ по формуле $\boldsymbol{u}^\times = \boldsymbol{u}C_{\boldsymbol{u}\boldsymbol{u}^\times}$, удовлетворяет равенству $E = G_{\boldsymbol{u}\boldsymbol{u}^\times} = G_{\boldsymbol{u}}C_{\boldsymbol{u}\boldsymbol{u}^\times}$, т. е. обратна к матрице Грама базиса $\boldsymbol{u}$. Тем самым,

$$(u_1^\times, \dots, u_n^\times) = (u_1, \dots, u_n) \cdot G_{\boldsymbol{u}}^{-1}. \tag{14-12}$$

Ортонормальность базиса равносильна тому, что он совпадает со своим евклидово двойственным.

Упражнение 14.5. Убедитесь, что $u_i^{\times\times} = u_i$.

[1] См. формулу (14-5) на стр. 256.

По определению двойственного базиса[1], каждый вектор $v \in V$ раскладывается по произвольному базису $u_1, \dots, u_n$ с коэффициентами, равными скалярным произведениям этого вектора с соответствующими векторами двойственного базиса:

$$v = \sum_i e_i \cdot (v, e_i^\times), \tag{14-13}$$

в чём легко удостовериться и непосредственно, скалярно умножив обе части этого равенства на $u_i^\times$ для каждого i.

14.3.2. Ортогоналы. При помощи изоморфизма корреляции (14-10) обсуждавшаяся в n° 7.4 на стр. 121 двойственность $U \leftrightarrow \operatorname{Ann} U$ между подпространствами дополнительных размерностей в V и в V^* преобразуется в двойственность между подпространствами дополнительных размерностей в самом V. А именно, обозначим через

$$U^\perp = \{w \in V \mid \forall\, u \in U\ (u, w) = 0\} = G_V^{-1} \operatorname{Ann} U$$

прообраз аннулятора $\operatorname{Ann}(U) \subset V^*$ подпространства $U \subset V$ при изоморфизме $G_V : V \xrightarrow{\sim} V^*$ из форм. (14-10) на стр. 261. Подпространство $U^\perp$ называется *ортогоналом* или *ортогональным дополнением* к U. По сл. 7.9 на стр. 125

$$\dim U^\perp = \dim \operatorname{Ann} U = \dim V - \dim U\,, \tag{14-14}$$

а из сл. 7.10 на стр. 125 и теор. 7.5 на стр. 126 вытекает, что соответствие $U \leftrightarrow U^\perp$ задаёт оборачивающую включения инволютивную биекцию между подпространствами дополнительных размерностей в V, и эта биекция переводит суммы подпространств в пересечения, а пересечения — в суммы, т. е. для любых $U, W \subset V$ выполняются равенства

$$U^{\perp\perp} = U\,, \quad (U + W)^\perp = U^\perp \cap W^\perp\,, \quad (U \cap W)^\perp = U^\perp + W^\perp\,. \tag{14-15}$$

14.4. Расстояния и углы. Вещественное число $|v| \stackrel{\text{def}}{=} \sqrt{(v, v)}$ называется *длиной* вектора v. Скалярное произведение $V \times V \to \mathbb{R}$ восстанавливается из функции длины $V \to \mathbb{R}$, $v \mapsto |v|$, по формуле

$$(u, w) = \frac{1}{2}\left(|u + w|^2 - |u|^2 - |w|^2\right)\,. \tag{14-16}$$

Число $|p - q|$ называется *евклидовым расстоянием* между точками p, q аффинного пространства $\mathbb{A}(V)$. Функция $\varrho : \mathbb{A}(V) \times \mathbb{A}(V) \to \mathbb{R}_{\geqslant 0}$, $\varrho(p, q) = |p - q|$, симметрична, зануляется только при $p = q$, и для любых $a, b, c \in \mathbb{A}(V)$ удовлетворяет *неравенству треугольника*

$$\varrho(a, b) + \varrho(b, c) \geqslant \varrho(a, c)\,,$$

которое вытекает из предл. 14.4 ниже. В анализе такие функции ϱ называются *метриками*.

Предложение 14.4 (неравенство треугольника)
В евклидовом пространстве для любых векторов u, w выполняется неравенство

$$|u + w| \leqslant |u| + |w|\,, \tag{14-17}$$

которое обращается в равенство если и только если векторы u и w *сонаправлены*, т. е. один получается из другого умножением на *неотрицательное* число.

[1] См. n° 7.4.1 на стр. 122.

Доказательство. Возводя обе части (14-17) в квадрат, получаем эквивалентное неравенство

$$(u+w,u+w) \leqslant (u,u) + 2\,|u|\cdot|w| + (w,w)\,.$$

После раскрытия скобок в левой части и очевидных сокращений получаем неравенство

$$(u,w) \leqslant |u|\cdot|w|\,.$$

Оно заведомо выполняется в строгой форме при $(u,w) < 0$, а при $(u,w) \geqslant 0$ превращается в неравенство Коши – Буняковского – Шварца (14-8), которое становится равенством если и только если $w = \lambda u$, где $\lambda \geqslant 0$, так как $\lambda(u,u) = (u,w) \geqslant 0$. □

14.4.1. Евклидов угол. В каждом одномерном подпространстве L евклидова пространства имеются ровно два вектора длины 1, отличающиеся друг от друга знаком: если $L = \mathbb{R}\,v$ порождается вектором v, то это векторы $\pm v/|v|$. Если заданы два одномерных подпространства $L_1 = \mathbb{R}\,v_1$ и $L_2 = \mathbb{R}\,v_2$, то знаки всегда можно выбрать так, чтобы скалярное произведение направляющих векторов единичной длины стало положительным и тем самым оказалось равно

$$|(v_1,v_2)|/(|v_1|\cdot|v_2|)\,.$$

В силу неравенства Коши – Буняковского – Шварца (14-8) это число лежит на отрезке $[0,\,1]$. Поэтому существует единственное такое число $\measuredangle(L_1,L_2) \in [0,\pi/2]$, что

$$\cos\measuredangle(L_1,L_2) = \frac{|(v_1,v_2)|}{|v_1|\cdot|v_2|}\,.$$

Оно называется *евклидовым углом* между одномерными подпространствами L_1, L_2. С точки зрения школьной геометрии пара пересекающихся прямых на плоскости задаёт две пары вертикальных углов, минимальный из которых равен $\measuredangle(L_1,L_2)$, а смежный с ним равен $\pi - \measuredangle(L_1,L_2)$.

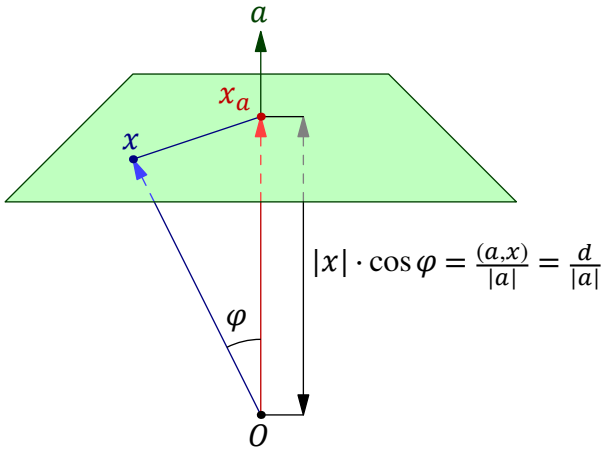


Рис. 14⋄3. ГМТ $x:\ (a,x) = d$.

Евклидовым углом между векторами u, w евклидова пространства называется единственное такое число $\measuredangle(u,w) \in [0,\pi]$, что

$$\cos\measuredangle(u,w) = \frac{(v_1,v_2)}{|v_1|\cdot|v_2|}\,. \tag{14-18}$$

Пример 14.7 (уравнение гиперплоскости)
Линейное неоднородное уравнение $a_1x_1+\ldots+a_nx_n = d$ на координаты $x_1,\ldots,x_n$ относительно ортонормального базиса n-мерного евклидова пространства V можно переписать как

$$(a,x) = d\,, \tag{14-19}$$

где $a \in V$ и $d \in \mathbb{R}$ заданы, а $x \in V$ — переменный вектор. Соотношение (14-19) означает, что $|x|\cdot\cos\measuredangle(a,x) = d/|a|$, т. е. перпендикуляры, опущенные из точек x на выпущенную из нуля в направлении вектора a прямую попадают в одну и ту же точку x_a этой прямой, имеющую координату $d/|a|$ относительно базисного вектора $a/|a|$ единичной длины, см. рис. 14⋄3. Это

согласуется с тем, что направляющим векторным пространством гиперплоскости[1] (14-19) является *ортогонал* $a^\perp = \{x \in V \mid (a,x) = 0\}$ к вектору a. Мы заключаем, что уравнение (14-19) задаёт в аффинном пространстве $\mathbb{A}(V)$ гиперплоскость, перпендикулярную вектору a и удалённую от нуля на расстояние $|d|/|a|$ вдоль вектора a, если $d > 0$, и в противоположную сторону, если $d < 0$.

Пример 14.8 (срединный перпендикуляр)
Покажем, что в евклидовом аффинном пространстве $\mathbb{A}^n$ ГМТ x, равноудалённых от двух заданных точек $p_0 \neq p_1$, представляет собою гиперплоскость, перпендикулярную вектору $\overrightarrow{p_0p_1}$ и проходящую через середину $(p_0+p_1)/2$ отрезка $[p_0,p_1]$. Эта гиперплоскость называется *срединным перпендикуляром* к отрезку $[p_0,p_1]$. Равенство длин $|x,p_0| = |x,p_1|$ равносильно равенству скалярных произведений $(\overrightarrow{xp}_0, \overrightarrow{xp}_0) = (\overrightarrow{xp}_1, \overrightarrow{xp}_1)$, т. е. равенству

$$(p_0 - x, p_0 - x) = (p_1 - x, p_1 - x)\,,$$

где буквы p_0, p_1, x обозначают радиус-векторы соответствующих точек, выпущенные из произвольно выбранной начальной точки $O \in \mathbb{A}^n$. После раскрытия скобок и сокращений, получаем $(p_0,p_0) - 2\,(p_0,x) = (p_1,p_1) - 2\,(p_1,x)$ или, что то же самое,

$$2\,(p_1 - p_0, x) = (p_1,p_1) - (p_0,p_0)\,. \tag{14-20}$$

Это уравнение задаёт гиперплоскость, перпендикулярную вектору $\overrightarrow{p_0p_1} = p_1 - p_0$ и проходящую через точку $(p_0+p_1)/2$, ибо последняя, очевидно, равноудалена от p_0 и p_1.

14.5. Ортогональные проекции. Так как $\dim U + \dim U^\perp = \dim V$ и $U \cap U^\perp = 0$, ибо $(u,u) = 0$ только для $u = 0$, подпространства U и $U^\perp$ дополнительны друг другу, т. е. $V = U \oplus U^\perp$ и каждый вектор $v \in V$ допускает единственное разложение

$$v = v_U + v_{U^\perp}\,, \quad \text{где} \quad v_U \in U\,,\ v_{U^\perp} \in U^\perp\,. \tag{14-21}$$

Компоненты $v_U \in U$ и $v_{U^\perp} \in U^\perp$ этого разложения называются, соответственно *ортогональной проекцией* вектора v на U и его *нормальной составляющей* относительно U. Сопоставление каждому вектору $v \in V$ ого ортогональной проекции на U задаёт линейное отображение

$$\pi_U : V = U \oplus U^\perp \twoheadrightarrow U\,, \quad v = v_U + v_{U^\perp} \mapsto v_U\,,$$

которое называется *ортогональным проектированием* V на U.

Предложение 14.5
Ортогональная проекция $v_U \in U$ произвольного вектора $v \in V$ на подпространство $U \subset V$ однозначно характеризуется любым из следующих эквивалентных друг другу свойств:

1) $v - v_U \in U^\perp$ 2) $\forall\, u \in U \quad (u,v) = (u,v_U)$ 3) $\forall\, u \in U \quad u \neq v_U \ \Rightarrow\ |v-u| > |v-v_U|$

и может найдена по формуле

$$v_U = \sum_i (v, u_i^\times)\, u_i\,, \tag{14-22}$$

где $u_1, \ldots, u_m$ и $u_1^\times, \ldots, u_m^\times$ — произвольные евклидово двойственные базисы в U.

[1] Т. е. множеством решений соответствующего однородного уравнения $(a,x) = 0$, см. n° 8.5 на стр. 144 и прим. 13.6 на стр. 237.

Доказательство. Равносильность свойств (1) и (2) очевидна: оба утверждают, что векторы v_U и $v - v_U$ являются компонентами вектора v в прямом разложении $V = U \oplus U^\perp$. Если $u = v_U + w$, где $w \in U$ отличен от нуля, то

$$(v-u, v-u) = (v_{U^\perp} - w, v_{U^\perp} - w) = (v_{U^\perp}, v_{U^\perp}) + (w, w) > (v_{U^\perp}, v_{U^\perp}).$$

Поэтому ортогональная проекция v_U вектора v на подпространство U обладает свойством (3). А так как вектор, обладающий свойством (3), очевидным образом единствен, свойство (3) равносильно свойствам (1) и (2). Для завершения доказательства достаточно проверить, что определённый по формуле (14-22) вектор v_U обладает свойством (2). Так как свойство (2) линейно по $u \in U$, достаточно убедиться, что оно выполняется для базисных векторов $u = u_1^\times, \dots, u_m^\times$, что имеет место: $(v_U, u_v^\times) = \sum_i (u_i, u_v^\times) \cdot (v, u_i^\times) = (v, u_v^\times)$ для каждого v. □

Следствие 14.2
В евклидовом аффинном пространстве $\mathbb{A}(V)$ для любого непустого аффинного подпространства $\Pi \subsetneq \mathbb{A}(V)$ и любой точки $a \notin \Pi$ существует единственная точка $a_\Pi \in \Pi$, удовлетворяющая двум эквивалентным друг другу условиям:

1) вектор $\overrightarrow{aa_\Pi}$ перпендикулярен любому вектору $\overrightarrow{pq}$ с $p, q \in \Pi$

2) $|aq| > |aa_\Pi|$ для любой отличной от a_Π точки $q \in \Pi$.

Доказательство. Выберем какую-нибудь точку $p \in \Pi$ в качестве начальной отождествим точки $a \in \mathbb{A}(V)$ с их радиус-векторами $\overrightarrow{oa} \in V$. Аффинное подпространство Π станет векторным подпространством $U \subset V$, а точке $a \in A$ сопоставится её радиус вектор $v = \overrightarrow{pa} \in V$. Остаётся применить к ним предл. 14.5. □

14.5.1. Расстояние до подпространства. Точка $a_\Pi \in \Pi$ из сл. 14.2 называется *ортогональной проекцией* точки a на аффинное подпространство $\Pi \subset \mathbb{A}(V)$. Длина $|a - a_\Pi|$ называется *расстоянием* от точки a до подпространства Π. По свойству (1) из предл. 14.5 это расстояние равно длине $\left|\overrightarrow{qp}_{U^\perp}\right|$ ортогональной проекции вектора $\overrightarrow{qp}$, где $q \in \Pi$ — любая точка, на ортогональное дополнение $U^\perp$ к направляющему векторному пространству $U \subset V$ аффинного подпространства Π.

Пример 14.9 (расстояние от точки до гиперплоскости)
Направляющим векторным пространством гиперплоскости $\Pi \subset \mathbb{A}(V)$ с аффинным уравнением $(a, x) = d$, где $a \in V$ — заданный вектор, является ортогонал $a^\perp \subset V$ к вектору a. Расстояние от произвольной точки $p \in \mathbb{A}(V)$ до гиперплоскости Π равно расстоянию между их ортогональными проекциями на одномерное подпространство, порождённое вектором a. Евклидово двойственным к a базисным вектором этого подпространства является $a/(a, a)$. Поэтому точка p проектируется в вектор $a \cdot (a, p)/(a, a)$, а все точки $x \in \Pi$ — в вектор $a \cdot (x, p)/(a, a) = a \cdot d/(a, a)$. Разность между ими имеет длину $|(a, p) - d| \cdot |a|/(a, a) = |(a, p) - d|/|a|$.

Пример 14.10 (евклидов объём через площадь основания и высоту)
Рассмотрим в евклидовом пространстве линейно независимый набор $\boldsymbol{w} = (v, u_1, \dots, u_n)$ из $n+1$ векторов и обозначим через U линейную оболочку его поднабора $\boldsymbol{u} = (u_1, \dots, u_n)$, состоящего из последних n векторов. Вектор v единственным образом представляется в виде суммы $v = v_U + v_{U^\perp}$, где $v_U \in U$, а вектор $v_{U^\perp}$ лежит в одномерном ортогональном дополнении $U^\perp$

к подпространству U в линейной оболочке W набора векторов $\boldsymbol{w}$. Вектор $v_{U^\perp}$ называется *высотой* параллелепипеда $(v, u_1, \dots, u_n)$, опущенной из вершины v на основание $\boldsymbol{u}$. Длина этой высоты равна расстоянию от вершины v до подпространства U или, что то же самое, длине ортогональной проекции $v_{U^\perp}$ вектора v на $U^\perp$. Так как вектор v_U является линейной комбинацией векторов u_i, в координатах относительно любого ортонормального базиса в W квадрат ориентированного объёма натянутого на векторы $\boldsymbol{w}$ параллелепипеда равен

$$\det^2(v, u_1, \dots, u_n) = \det^2(v - v_U, u_1, \dots, u_n) = \det^2(v_{U^\perp}, u_1, \dots, u_n) = \Gamma_{(v_{U^\perp}, u_1, \dots, u_n)}.$$

Единственным ненулевым элементом первой строки и первого столбца определителя Грама векторов $v_{U^\perp}, u_1, \dots, u_n$ является стоящий в левом верхнем углу квадрат $|v_{U^\perp}|^2$. Поэтому

$$\operatorname{Vol}^2(v, u_1, \dots, u_n) = \Gamma_{(v_{U^\perp}, u_1, \dots, u_n)} = |v_{U^\perp}|^2 \cdot \Gamma_{(u_1, \dots, u_n)} = |v_{U^\perp}|^2 \cdot \operatorname{Vol}^2(u_1, \dots, u_n).$$

Иначе говоря, $(n+1)$-мерный евклидов объём параллелепипеда $\boldsymbol{w}$ равен произведению n-мерного евклидова объёма основания $\boldsymbol{u}$ на длину опущенной на него высоты:

$$\operatorname{Vol}_{n+1}(v, u_1, \dots, u_n) = |v_{U^\perp}| \cdot \operatorname{Vol}_n(u_1, \dots, u_n). \tag{14-23}$$

Пример 14.11 (расстояние между аффинными подпространствами)
Рассмотрим в аффинном пространстве $\mathbb{A}(V)$, ассоциированном с евклидовым векторным пространством V, аффинные подпространства $K = p + U$ и $L = q + W$ с направляющими векторными пространствами $U, W \subset V$. Пусть эти пространства не пересекаются[1], т. е. $\overrightarrow{pq} \notin U + W$. Для любых двух векторов $x = p + u \in K$ и $y = q + w \in L$ расстояние $|y - x| = |\overrightarrow{pq} - (w - u)|$ достигает своего минимума по $u \in U$, $w \in W$ тогда и только тогда, когда вектор $w - u = \overrightarrow{pq}_{U+W}$ является ортогональной проекцией вектора $\overrightarrow{pq}$ на подпространство $U + W$ и этот минимум равен расстоянию между вектором $\overrightarrow{pq}$ и подпространством $U + W$, т. е. длине ортогональной проекции $\overrightarrow{pq}_{(U+W)^\perp}$ вектора $\overrightarrow{pq}$ на подпространство $(U + W)^\perp$. Это число называется *расстоянием* между аффинными подпространствами K, L и обозначается

$$|K, L| = \left|\overrightarrow{pq}_{(U+W)^\perp}\right| = \min_{x \in K,\, y \in L} |y - x| \tag{14-24}$$

Если $K \cap L \neq \varnothing$, т. е. $\overrightarrow{pq} \in U + W$, мы полагаем $|K, L| = 0$, что согласуется с равенством (14-24), так как в этом случае $\overrightarrow{pq}_{(U+W)^\perp} = 0$. Если векторы $v_1, \dots, v_k$ составляют базис подпространства $U + W$, то вектор $\overrightarrow{pq}_{(U+W)^\perp}$ является опущенной из вершины q высотой параллелепипеда, натянутого на векторы $\overrightarrow{pq}, v_1, \dots, v_k$, и длину этой высоты можно вычислять при помощи формулы (14-23):

$$|K, L| = \frac{\operatorname{Vol}_{k+1}(\overrightarrow{pq}, v_1, \dots, v_k)}{\operatorname{Vol}_k(v_1, \dots, v_k)} = \sqrt{\frac{\Gamma_{(\overrightarrow{pq}, v_1, \dots, v_k)}}{\Gamma_{(v_1, \dots, v_k)}}}, \tag{14-25}$$

где Vol_m означает m-мерный евклидов объём.

14.5.2. Угол между вектором и подпространством. Рассмотрим в евклидовом векторном пространстве V векторное подпространство $U \subset V$ и вектор $v \in V$, не лежащий ни в U, ни в $U^\perp$. Тогда абсолютная величина угла[2] между этим вектором и ненулевыми векторами $u \in U$ заключена в пределах $0 < |\measuredangle(v, u)| < \pi/2$ и достигает своего минимума на единственном с

[1] См. предл. 13.1 на стр. 237.
[2] См. формулу (14-18) на стр. 263.

точностью до умножения на положительную константу векторе u, равном ортогональной проекции v_U вектора v на подпространство U. В самом деле, наименьшему значению угла отвечает наибольшее значение его косинуса

$$\cos(\measuredangle(v,u)) = \frac{(v,u)}{|v|\cdot|u|} = \frac{(v_U,u)}{|v|\cdot|u|} = (v_U/|v_U|, u/|u|)\cdot\frac{|v_U|}{|v|}$$

(второе равенство выполняется в силу свойства (2) из предл. 14.5 на стр. 264). Последний сомножитель в правой части не зависит от u, а первый — в силу неравенства Коши – Буняковского – Шварца[1] — не превосходит произведения длин $\left|v_U/|v_U|\right|\cdot\left|u/|u|\right| = 1$ и в точности равен этому произведению если и только если векторы v_U и u сонаправлены. Угол $\varphi\in[0,\pi/2]$, однозначно определяемый из равенства $\cos\varphi = |v_U|/|v|$, называется *евклидовым углом* между ненулевым вектором v и подпространством U. При $v\in U$ и $v\in U^\perp$ эта формула даёт $\varphi = 0$ и $\varphi = \pi/2$, так как в этих случаях $v_U = v$ и $v_U = 0$ соответственно. Обратите внимание, что каждый из возникающих в этих двух крайних случаях углов по-прежнему является минимальным среди углов между вектором v и ненулевыми векторами $u\in U$.

Так как $|v_{U^\perp}| = |v|\cdot\sin\varphi$, евклидов угол φ между вектором v и подпространством U также можно вычислять при помощи форм. (14-23) на стр. 266:

$$\sin\varphi = \frac{|v_{U^\perp}|}{|v|} = \frac{\sqrt{\Gamma_{(v,u_1,\dots,u_k)}}}{|v|\sqrt{\Gamma_{(u_1,\dots,u_k)}}}, \tag{14-26}$$

где $u_1,\dots,u_k$ — произвольный базис подпространства U.

14.6. Векторные произведения. Зафиксируем в n-мерном евклидовом векторном пространстве V *ориентацию*[2], т. е. одну из двух евклидовых форм объёма $\omega: V\times\ldots\times V\to\mathbb{R}$. Каждый упорядоченный набор из $n-1$ векторов $v_1,\dots,v_{n-1}\in V$ задаёт линейный функционал

$$V\to\mathbb{R},\ u\mapsto\omega(u,v_1,\dots,v_{n-1}).$$

Вектор, который является прообразом этого функционала относительно евклидовой корреляции[3] $G_V: V\xrightarrow{\sim} V^*$ обозначается $[v_1,\dots,v_{n-1}]$ и называется *векторным произведением* векторов $v_1,\dots,v_{n-1}$. Он однозначно определяется тем, что для всех $u\in V$

$$\omega_e(u,v_1,\dots,v_{n-1}) = (u,[v_1,\dots,v_{n-1}]), \tag{14-27}$$

Предложение 14.6
Фиксируем любой положительно ориентированный ортонормальный базис в V, запишем координаты векторов $v_1,\dots,v_{n-1}$ в этом базисе по столбцам $n\times(n-1)$ матрицы A и обозначим через A_i умноженный на $(-1)^{i-1}$ определитель её $(n-1)\times(n-1)$-подматрицы, дополнительной к i-й строке[4]. Тогда вектор $[v_1,\dots,v_{n-1}]$ имеет в этом базисе координаты $(A_1,\dots,A_n)$.

Доказательство. Припишем слева к матрице A столбец координат $(x_1,\dots,x_n)$ переменного вектора $u\in V$. Определитель полученной матрицы $\det(u,v_1,\dots,v_{n-1}) = \omega(u,v_1,\dots,v_{n-1})$. Раскладывая его по первому столбцу, заключаем, что он равен скалярному произведению векторов с координатами $(x_1,\dots,x_n)$ и $(A_1,\dots,A_n)$. □

[1] См. формулу (14-8) на стр. 257.
[2] См. **??** на стр. **??** и n° 14.2.1 на стр. 260.
[3] См. формулу (14-10) на стр. 261.
[4] Подобно тому, как это делалось во втором правиле Крамера из n° 11.4.3 на стр. 199.

Предложение 14.7
Вектор $[v_1, \dots, v_{n-1}]$ перпендикулярен векторам $v_1, \dots, v_{n-1}$, а его длина равна евклидову объёму $(n-1)$-мерного параллелепипеда, натянутого на векторы $v_1, \dots, v_{n-1}$. Если она ненулевая, направление вектора $[v_1, \dots, v_{n-1}]$ таково, что базис $[v_1, \dots, v_{n-1}], v_1, \dots, v_{n-1}$ положительно ориентирован.

Доказательство. Подставляя в формулу (14-27) вектор $u = v_i$, получаем

$$(v_i, [v_1, \dots, v_{n-1}]) = \omega_e(v_i, v_1, \dots, v_{n-1}) = 0\,,$$

что доказывает первое утверждение. Подставляя $u = [v_1, \dots, v_{n-1}]$, получаем

$$\omega([v_1, \dots, v_{n-1}], v_1, \dots, v_{n-1}) = \big|[v_1, \dots, v_{n-1}]\big|^2 \geqslant 0\,.$$

В силу первого утверждения вектор $[v_1, \dots, v_{n-1}]$ является высотой параллелепипеда, объём которого стоит в левой части последней формулы. Согласно прим. 14.10 этот объём равен произведению длины $\big|[v_1, \dots, v_{n-1}]\big|$ на евклидов объём $(n-1)$-мерного параллелепипеда, натянутого на векторы $v_1, \dots, v_{n-1}$. Отсюда вытекают второе и третье утверждения. □

Следствие 14.3
Векторы $v_1, \dots, v_{n-1} \in \mathbb{R}^n$ линейно зависимы если и только если $[v_1, \dots, v_{n-1}] = 0$. □

Пример 14.12 (векторное произведение в $\mathbb{R}^3$)
Векторное произведение в трёхмерном координатном пространстве $\mathbb{R}^3$ со стандартной ориентацией представляет собою бинарную операцию $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, $(u, w) \mapsto [u, w]$, и часто обозначается[1] $u \times w$. Формула (14-27) в этом случае утверждает, что ориентированный объём параллелепипеда, натянутого на векторы

$$(a, b, c) = (e_1, e_2, e_3) \cdot \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix},$$

равен скалярному произведению вектора $a = (a_1, a_2, a_3)$ с вектором

$$\begin{aligned} [b, c] \stackrel{\text{def}}{=} (b_2c_3 - b_3c_2,\ -b_1c_3 + b_3c_1,\ b_1c_2 - b_2c_1) = \\ = \left(\det\begin{pmatrix} b_2 & c_2 \\ b_3 & c_3 \end{pmatrix},\ -\det\begin{pmatrix} b_1 & c_1 \\ b_3 & c_3 \end{pmatrix},\ \det\begin{pmatrix} b_1 & c_1 \\ b_2 & c_2 \end{pmatrix}\right), \end{aligned} \tag{14-28}$$

в чём несложно убедиться, раскладывая по первому столбцу определитель

$$\det\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = a_1 \cdot \big(b_2c_3 - b_3c_2\big) + a_2 \cdot \big(-b_1c_3 + b_3c_1\big) + a_3 \cdot \big(b_1c_2 - b_2c_1\big) = (a, [b, c])\,.$$

Так как $(b, [b, c]) = \det(b, b, c) = 0$ и $(c, [b, c]) = \det(c, b, c) = 0$, вектор $[b, c]$ перпендикулярен векторам b и c, а квадрат его длины $\big([b, c], [b, c]\big) = \mathrm{Vol}_3\big([b, c], b, c\big) = \big|[b, c]\big| \cdot \mathrm{Vol}_2(b, c)$, откуда $\big|[b, c]\big| = \mathrm{Vol}_2(b, c)$.

[1] В английской литературе векторное произведение даже и называется *cross-product*.

Задачи для самостоятельного решения к §14

Задача 14.1. Три вектора в евклидовом пространстве $\mathbb{R}^3$ таковы, что все скалярные произведения между ними неотрицательны. Всегда ли найдётся такой ортонормальный базис в $\mathbb{R}^3$, что все три эти вектора окажутся в одном координатном октанте?

Задача 14.2. Точки $p_0, p_1, \dots, p_k \in \mathbb{R}^n$ не содержатся в одной $(k-1)$-мерной плоскости. Опишите ГМТ, равноудалённых от всех этих точек.

Задача 14.3. Два вектора в евклидовом пространстве лежат по одну сторону от данной гиперплоскости[1]. Угол между векторами тупой. Верно ли, что угол между их ортогональными проекциями на эту гиперплоскость тоже тупой?

Задача 14.4. Какое максимальное число векторов можно выпустить из начала координат n-мерного евклидова пространства так, чтобы все попарные углы между ними были тупыми?

Задача 14.5. В координатах относительно стандартного ортонормального базиса в $\mathbb{R}^4$ найдите ортогональную проекцию

а) вектора $(-4, -1, -3, 4)$ на линейную оболочку векторов

$$(1, -2, -3, 3)\,, \quad (-2, 4, 7, -8)\,, \quad (2, -4, -3, 0)$$

и на ортогональное дополнение к ней.

б) вектора $(-1, 3, -4, 0)$ на подпространство, заданное уравнениями

$$\begin{cases} x_1 - 2x_2 - 2x_3 - 3x_4 = 0 \\ -3x_1 + 6x_2 + 7x_3 + 10x_4 = 0 \\ 2x_1 - 4x_2 - 6x_3 - 8x_4 = 0\,. \end{cases}$$

и на ортогональное дополнение к нему.

Задача 14.6. Прямая ℓ в евклидовом пространстве $\mathbb{R}^4$ проходит через точки

$$(-68/7, 8/7, 29/7, -15/7) \quad \text{и} \quad (-48/7, 18/7, 4/7, -25/7)\,,$$

а плоскость Π задаётся уравнениями

$$\begin{cases} x_1 + 2x_2 + x_3 - 2x_4 = -5 \\ -5x_1 - 6x_2 + x_3 + 6x_4 = 33 \end{cases}$$

Найдите $\min |b - a|$ по всем $a \in \ell$, $b \in \Pi$ и те a, b, на которых он достигается.

Задача 14.7. Найдите все углы между диагоналями[2] четырёхмерного куба.

Задача 14.8 (стандартный куб). В стандартном n-мерном кубе

$$I_n\{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \forall\, i\ |x_i| \leqslant 1\}$$

[1] Речь идёт про *векторную* гиперплоскость, т. е. про векторное подпространство коразмерности 1. Говорят, что $u, w \in V$ лежат по одну сторону от такой гиперплоскости $U \subset V$, если $(a, u) \cdot (a, w) > 0$, где $a \in U^\perp$ — любой ненулевой вектор.

[2] Т. е. отрезками, соединяющими противоположные (центрально симметричные относительно центра куба) вершины.

найдите:
а) количество граней каждой из возможных размерностей
б) число диагоналей, ортогональных заданной внутренней диагонали
в) длину внутренней диагонали (диаметр описанного шара) и её предел при $n \to \infty$
г) угол между внутренней диагональю и ребром и его предел при $n \to \infty$
д) отношения, в которых внутренняя диагональ делится ортогональными проекциями на неё всех вершин куба.

Задача 14.9 (симплекс). В стандартном n-мерном симплексе

$$\Delta_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1} \mid \sum x_i = 1 \text{ и все } x_i \geqslant 0\}$$

найдите
а) радиусы вписанного и описанного шаров и их пределы при $n \to \infty$
б) угол между ребром и не содержащей его $(n-1)$-мерной гранью
в) угол между ребром и противолежащей ему $(n-2)$-мерной гранью[1]
г) расстояние между не пересекающимися гранями размерностей k и m.

Задача 14.10 (кокуб). Выпуклая оболочка[2] центров граней стандартного n-мерного куба[3] называется стандартным n-мерным *кокубом*. Задайте стандартный n-мерный кокуб системой линейных неоднородных неравенств и найдите количество его граней в каждой размерности, а также радиус вписанного в него шара и его предел при $n \to \infty$.

Задача 14.11* (октаплекс). Нарисуем в $\mathbb{R}^4$ стандартный куб I^4 и гомотетичный стандартному кокуб, все вершины которого лежат на описанной вокруг I^4 сфере. Выпуклая оболочка вершин куба и кокуба называется *октаплексом*. Подсчитайте у него
а) количество граней в каждой из размерностей
б) длины рёбер и радиус вписанного шара
и выясните,
в) как выглядят трёхмерные гиперграни и каковы их объёмы
г) как выглядят двумерные грани и каковы их площади.

Задача 14.12. Найдите радиус шара, описанного в евклидовом пространстве $\mathbb{R}^5$ вокруг пирамиды с вершиной в точке $(1, 0, 0, 0, 0)$, основанием которой является лежащий в гиперплоскости $x_1 = 0$ правильный четырёхмерный симплекс, описанный около единичного шара с центром в нуле.

Задача 14.13. Четырёхмерный шар лежит в углу четырёхмерного куба со стороной 1 возле вершины a, касаясь всех сходящихся в a трёхмерных граней куба, а также трёхмерной гиперплоскости, проходящей через все вершины куба, соединённые с a ребром. Ещё один такой же шар с аналогичными свойствами лежит в противоположном к a углу куба. Найдите расстояние между центрами шаров.

Задача 14.14. В каждую вершину n-мерного куба со стороной 2 помещён n-мерный шар радиуса 1 с центром в вершине куба. Шар B с центром в центре куба касается внутри куба всех шаров с центрами в вершинах. При каких n шар B целиком содержится в кубе?

[1] Т. е. аффинной оболочкой $n-1$ вершин, не являющихся концами этого ребра.

[2] *Выпуклой оболочкой* набора точек в аффинном пространстве называется множество всех конечных барицентрических комбинаций этих точек с неотрицательными весами, см. зад. 13.4 (в) на стр. 251.

[3] Т. е. концов стандартных базисных векторов и векторов, противоположных к ним.

Задача 14.15. Убедитесь, что векторное произведение $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ кососимметрично[1] и не ассоциативно, но удовлетворяет *правилу Лейбница*[2] $u \times (v \times w) = (u \times v) \times w + v \times (u \times w)$.

Задача 14.16. Докажите для векторных произведений в $\mathbb{R}^3$ равенства

а) $\big[a, [b, c]\big] = b \cdot (a, c) - c \cdot (a, b)$

б) $\big[[a, b], [a, c]\big] = a \cdot \omega(a, b, c)$, где ω — форма евклидова объёма, принимающая значение 1 на положительно ориентированных базисах.

в) $\big([a, b], [c, d]\big) = \det \begin{pmatrix} (a, c) & (a, d) \\ (b, c) & (b, d) \end{pmatrix}$.

Задача 14.17. Найдите угол и расстояние между прямыми, заданными в стандартном ортонормальном базисе евклидова пространства $\mathbb{R}^3$ уравнениями

$$\begin{cases} x - 2y - 2z = 5 \\ 3x - 5y - 4z = 13 \end{cases} \quad \text{и} \quad \begin{cases} x + y + z = 0 \\ 3x + 4y + 5z = -3\,. \end{cases}$$

Задача 14.18. Отображение евклидова аффинного пространства в себя называется *движением*, если оно сохраняет расстояния между точками. Докажите, что каждое движение

а) переводит прямые в прямые

б) является аффинным преобразованием, дифференциал которого сохраняет скалярное произведение векторов.

Задача 14.19. Существует ли движение евклидова аффинного пространства $\mathbb{R}^3$, переводящее прямые

$$\begin{cases} -2x_1 - 5x_2 + 5x_3 = 19 \\ 4x_1 + 4x_2 - 7x_3 = -29 \end{cases} \quad \text{и} \quad \begin{cases} -x_1 + 11x_2 - 2x_3 = -10 \\ -7x_1 - 7x_2 + 10x_3 = 26 \end{cases}$$

соответственно в прямые

а) $\begin{cases} 10x_1 - 5x_2 - x_3 = -22 \\ -22x_1 + 14x_2 + 7x_3 = 37 \end{cases}$ и $\begin{cases} -35x_1 + 19x_2 + 14x_3 = -7 \\ 3x_1 - 2x_2 - 2x_3 = 2 \end{cases}$

б) $\begin{cases} x_1 + 2x_2 + 3x_3 = 10 \\ -8x_1 + 4x_2 + x_3 = 5 \end{cases}$ и $\begin{cases} -7x_1 - 7x_2 - 10x_3 = -29 \\ 8x_1 + 5x_2 + 8x_3 = 25\,, \end{cases}$

Если нет, объясните, почему. Если да, явно напишите, как это движение действует на стандартный координатный репер.

[1] Т. е. $v \times v = 0$ для всех v.

[2] Которое часто записывают в виде $[u, [v, w]] + [v, [w, u]] + [w, [u, v]] = 0$ и называют *тождеством Якоби*.

§15. Пространства с билинейной формой

Всюду в этом параграфе через V обозначается конечномерное векторное пространство над произвольным полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$.

15.1. Билинейные формы. Отображение $\beta : V \times V \to \Bbbk$ называется *билинейной формой* на векторном пространстве V, если оно линейно по каждому из двух аргументов[1]. Билинейные формы можно воспринимать как обобщённые скалярные произведения — не симметричные и определённые над произвольным полем (в частности, не положительные).

Упражнение 15.1. Убедитесь, что билинейные формы образуют векторное подпространство в пространстве всех функций $V \times V \to \Bbbk$.

Согласно n° 8.2 на стр. 137, каждая билинейная форма $\beta : V \times V \to \Bbbk$ задаёт умножение матриц $\operatorname{Mat}_{n\times s}(V) \times \operatorname{Mat}_{s\times m}(V) \to \operatorname{Mat}_{n\times m}(\Bbbk)$, при котором произведением векторов $u, w \in \Bbbk$ является число $uw = \beta(u,w) \in \Bbbk$. Обратите внимание, что это произведение, вообще говоря, не коммутативно. Если заданы два набора векторов $\boldsymbol{u} = (u_1, \dots, u_n)$, $\boldsymbol{w} = (w_1, \dots w_m)$, то в результате умножения столбца $\boldsymbol{u}^t$ на строку $\boldsymbol{w}$ получится матрица попарных скалярных произведений[2]

$$B_{\boldsymbol{uw}} \stackrel{\text{def}}{=} \boldsymbol{u}^t\boldsymbol{w} = \big(\beta(u_i, w_j)\big) \in \operatorname{Mat}_{n\times m}(\Bbbk)\,.$$

Она называется *матрицей Грама* наборов $\boldsymbol{u}, \boldsymbol{w}$ и формы β. При $\boldsymbol{u} = \boldsymbol{w}$ мы пишем $B_{\boldsymbol{u}}$ вместо $B_{\boldsymbol{uu}}$, и в этом случае определитель $\det B_{\boldsymbol{u}} \in \Bbbk$ называется *определителем Грама* формы β и векторов $\boldsymbol{u}$. Зависимость матрицы Грама от $\boldsymbol{u}$, $\boldsymbol{v}$ точно такая же, как в евклидовом пространстве[3].

Упражнение 15.2. Убедитесь, что при $\boldsymbol{u} = \boldsymbol{e}\,C_{\boldsymbol{eu}}$ и $\boldsymbol{w} = \boldsymbol{f}\,C_{\boldsymbol{fw}}$

$$B_{\boldsymbol{uw}} = C_{\boldsymbol{eu}}^t B_{\boldsymbol{ef}} C_{\boldsymbol{fw}} \quad \text{и} \quad B_{\boldsymbol{u}} = C_{\boldsymbol{eu}}^t B_{\boldsymbol{e}} C_{\boldsymbol{eu}}\,. \tag{15-1}$$

В частности, если векторы $\boldsymbol{e} = (e_1, \dots e_n)$ образуют базис в V, а векторы $u = \boldsymbol{e}\,x$ и $w = \boldsymbol{e}\,y$ заданы столбцами $x, y \in \Bbbk^n$ своих координат в этом базисе, то

$$\beta(u,w) = x^t B_{\boldsymbol{e}} y\,. \tag{15-2}$$

Так как любая квадратная матрица $B_{\boldsymbol{e}} \in \operatorname{Mat}_n(\Bbbk)$ задаёт по этой формуле билинейную форму на пространстве V, сопоставление билинейной форме её матрицы Грама в каком-либо фиксированном базисе пространства V устанавливает биекцию между пространством билинейных форм на n-мерном векторном пространстве V и пространством матриц размера $n \times n$.

Упражнение 15.3. Убедитесь, что эта биекция линейна.

15.1.1. Корреляции. Задать билинейную форму $\beta : V \times V \to \Bbbk$ — то же самое, что сопоставить каждому вектору $v \in V$ линейно зависящий от v функционал правого скалярного умножения на v:

$$\beta^\wedge(v) : V \to \Bbbk\,, \quad u \mapsto \beta(u,v)\,. \tag{15-3}$$

[1] Т. е., $\beta(x_1u_1 + x_2u_2, y_1w_1 + y_2w_2) = \sum_{i,j=1}^2 x_iy_j\beta(u_i,w_j)$ при всех $u_1, u_2, w_1, w_2 \in V$ и $x_1, x_2, y_1, y_2 \in \Bbbk$, ср. с n° 8.1 на стр. 131.

[2] Буква «B» в обозначении матрицы является заглавной версией строчной буквы «β», обозначающей форму.

[3] См. n° 14.1.2 на стр. 256.

Возникающее таким образом линейное отображение

$$\beta^\wedge : V \to V^*, \quad v \mapsto \beta^\wedge(v) \tag{15-4}$$

называется *правой корреляцией* билинейной формы β. Билинейное отображение $\beta : V \times V \to \Bbbk$ восстанавливается из линейного отображения $\beta^\wedge : V \to V^*$ по формуле $\beta(u, w) = \beta^\wedge w(u)$.

Если фиксировать в V и V^* двойственные базисы $\boldsymbol{e} = (e_1, \dots e_n)$ и $\boldsymbol{e}^* = (e_1^*, \dots e_n^*)$, то матрица $B_{\boldsymbol{e}^*\boldsymbol{e}}^\wedge$ линейного отображения (15-4) в этих базисах имеет в клетке (i, j) значение i-той координаты функционала $\beta^\wedge e_j : u \mapsto \beta(u, e_j)$ в базисе $\boldsymbol{e}^*$, равное[1] значению этого функционала на базисном векторе e_i, т. е. скалярному произведению $\beta(e_i, e_j)$. Таким образом, матрица правой корреляции (15-4) совпадёт с матрицей Грама формы β. Мы заключаем, что сопоставление билинейной форме β её правой корреляции $\beta^\wedge$ устанавливает линейный изоморфизм пространства билинейных форм на V с пространством линейных отображений $V \to V^*$.

Симметричным образом, каждый вектор $v \in V$ задаёт линейный функционал

$$^\wedge\beta(v) : V \to \Bbbk, \quad u \mapsto \beta(v, u) \tag{15-5}$$

левого скалярного умножения на v, и таким образом возникает *левая корреляция*

$$^\wedge\beta : V \to V^*, \quad v \mapsto {}^\wedge\beta(v), \tag{15-6}$$

которая служит правой корреляцией для *транспонированной* формы

$$\beta^t(u, w) \stackrel{\text{def}}{=} \beta(w, u),$$

матрица Грама которой транспонирована к матрице Грама формы β. Поэтому матрица левой корреляции (15-6) в двойственных базисах $\boldsymbol{e}$ и $\boldsymbol{e}^*$ пространств V и V^* равна транспонированной матрице Грама $B_{\boldsymbol{e}}^t$ формы β в базисе $\boldsymbol{e}$.

Упражнение 15.4. Убедитесь, что левая и правая корреляции являются двойственными друг другу линейными операторами[2] $V \to V^*$.

15.1.2. Ядра, ранг и коранг. Векторные пространства

$$\begin{aligned} V^\perp &= \ker \beta^\wedge = \{u \in V \mid \forall\, v \in V\ \beta(v, u) = 0\} \\ {}^\perp V &= \ker {}^\wedge\beta = \{u \in V \mid \forall\, v \in V\ \beta(u, v) = 0\} \end{aligned} \tag{15-7}$$

называются соответственно *правым* и *левым* ядром билинейной формы β. Вообще говоря, это различные подпространства в V: в координатах относительно любого базиса $\boldsymbol{e}$ пространства V правое ядро состоит из таких *столбцов* x, что $B_{\boldsymbol{e}} x = 0$, а левое — из таких *строк* x, что $x B_{\boldsymbol{e}} = 0$, где $B_{\boldsymbol{e}}$ — матрица Грама формы β в базисе $\boldsymbol{e}$. Тем не менее, у этих пространств равные размерности

$$\dim V^\perp = \dim {}^\perp V = \dim V - \operatorname{rk} B_{\boldsymbol{e}},$$

в силу того, что $\dim\ker\beta^\wedge = \dim V - \dim\operatorname{im}\beta^\wedge$, $\dim\ker{}^\wedge\beta = \dim V - \dim\operatorname{im}{}^\wedge\beta$, а образы операторов $x \mapsto B_{\boldsymbol{e}} x$ и $x \mapsto x B_{\boldsymbol{e}}$ суть линейные оболочки столбцов и строк матрицы $B_{\boldsymbol{e}}$, размерности

[1] См. n° 7.4.1 на стр. 122.

[2] Отображение φ^*, двойственное в смысле n° 7.4.4 на стр. 127 к отображению $\varphi : V \to V^*$, действует из пространства $V^{**} \simeq V$ в пространство V^*, т. е. как и φ является отображением $V \to V^*$.

которых равны $\operatorname{rk} B_{\boldsymbol{e}}$ по теореме о ранге матрицы[1]. Это рассуждение заодно доказывает, что ранг матрицы Грама не зависит от выбора базиса, ибо размерности ядра и образа линейного отображения (15-4) от базиса не зависят. Ранг матрицы Грама называется *рангом* билинейной формы β и обозначается $\operatorname{rk}\beta$. Разность $\dim V - \operatorname{rk}\beta = \dim V^{\perp} = \dim {}^{\perp}V$ называется *корангом* формы β и обозначается $\operatorname{cork}\beta$.

15.1.3. Изометрии. Линейное отображение $f : U \to W$ между векторными пространствами U и W, на которых заданы билинейные формы β и γ, называется *изометрическим* или *гомоморфизмом пространств с билинейными формами*, если для любых векторов $u_1, u_2 \in U$ выполняется равенство $\beta(u_1, u_2) = \gamma\bigl(f(u_1), f(u_2)\bigr)$. Билинейные формы β и γ называются *изоморфными*, если между пространствами U и W имеется изометрический линейный изоморфизм.

Если произвольно зафиксировать в U и W базисы $\boldsymbol{u} = (u_1, \dots, u_n)$ и $\boldsymbol{w} = (w_1, \dots, w_m)$, то отображение $f : U \to W$ с матрицей $F_{\boldsymbol{wu}}$ в этих базисах является изометрическим если и только если матрица Грама набора векторов $f(\boldsymbol{u}) = (f(u_1), \dots, f(u_n)) = \boldsymbol{w}\, F_{\boldsymbol{wu}}$ равна матрице Грама базиса $\boldsymbol{u}$. Согласно упр. 15.2 на стр. 272 это равносильно матричному равенству

$$F_{\boldsymbol{wu}}^{t} B_{\boldsymbol{w}} F_{\boldsymbol{wu}} = B_{\boldsymbol{u}}\,. \tag{15-8}$$

15.2. Невырожденность. Билинейная форма β называется *невырожденной*[2], если она удовлетворяет условиям следующего ниже предл. 15.1. Формы, не удовлетворяющие этим условиям, называются *вырожденными* или *особыми*.

Предложение 15.1 (критерии невырожденности)
Следующие свойства билинейной формы β на конечномерном векторном пространстве V равносильны друг другу:

1) в V существует базис с ненулевым определителем Грама
2) любой базис в V имеет ненулевой определитель Грама
3) левая корреляция ${}^{\wedge}\beta : V \xrightarrow{\sim} V^*$ является изоморфизмом
4) правая корреляция $\beta^{\wedge} : V \xrightarrow{\sim} V^*$ является изоморфизмом
5) для любого ненулевого вектора $v \in V$ существует такой вектор $u \in V$, что $\beta(v, u) \neq 0$
6) для любого ненулевого вектора $v \in V$ существует такой вектор $u \in V$, что $\beta(u, v) \neq 0$
7) для любой линейной функции $\varphi : V \to \Bbbk$ существует такой вектор $v \in V$, что
$$\varphi(u) = \beta(v, u) \quad \text{для всех } u \in V$$
8) для любой линейной функции $\varphi : V \to \Bbbk$ существует такой вектор $v \in V$, что
$$\varphi(u) = \beta(u, v) \quad \text{для всех } u \in V\,,$$

причём при выполнении этих условий вектор v в последних двух пунктах определяется формой φ однозначно.

[1] См. прим. 7.11 на стр. 126.
[2] А также *неособой* или *регулярной*.

Доказательство. Поскольку $\dim V = \dim V^*$, биективность, инъективность и сюръективность линейного отображения $V \to V^*$ равносильны друг другу и тому, что это отображение задаётся невырожденной матрицей в каких-нибудь базисах. Поэтому условия (3), (5), (7) и условия (4), (6), (8), утверждающие, соответственно, биективность, обращение в нуль ядра и сюръективность операторов $\hat{}\beta$ и $\beta\hat{}$, равносильны между собой и условию (1), означающему, что транспонированные друг другу матрицы этих операторов обратимы. Условие (1) равносильно условию (2) в силу форм. (15-1) на стр. 272, из которой вытекает, что определители Грама двух базисов $\boldsymbol{e}$ и $\boldsymbol{f}$ связаны друг с другом по формуле $\det B_{\boldsymbol{e}} = \det B_{\boldsymbol{f}} \cdot \det^2 C_{\boldsymbol{fe}}$, где $C_{\boldsymbol{fe}}$ — матрица перехода[1] от базиса $\boldsymbol{e}$ к базису $\boldsymbol{f}$. □

Пример 15.1 (евклидова форма)
Симметричная билинейная форма на координатном пространстсве $\Bbbk^n$ с единичной матрицей Грама E в стандартном базисе называется *евклидовой*. Эта форма невырождена и над полем $\Bbbk = \mathbb{R}$ задаёт евклидову структуру[2] на пространстве $\mathbb{R}^n$. Над отличными от $\mathbb{R}$ полями свойства этой формы могут существенно отличаться от свойств евклидовой структуры. Например, над полем $\mathbb{C}$ ненулевой вектор $e_1 - ie_2 \in \mathbb{C}^2$ имеет нулевой скалярный квадрат.

Упражнение 15.5. Приведите пример n-мерного подпространства в $\mathbb{C}^{2n}$, на которое евклидова форма ограничивается в тождественно нулевую форму.

Базисы, в которых матрица Грама евклидовой формы равна E называются *ортонормальными*. Из теор. 15.1 на стр. 280, которую мы докажем ниже, вытекает, что над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ любая невырожденная симметричная билинейная форма изометрически изоморфна евклидовой.

Пример 15.2 (гиперболическая форма)
Симметричная билинейная форма h на чётномерном координатном пространстве $\Bbbk^{2n}$, матрица Грама которой в стандартном базисе равна

$$H = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}, \tag{15-9}$$

где 0 и E — нулевая и единичная матрицы размера $n \times n$, называется *гиперболической*. Она невырождена и над алгебраически замкнутым полем изометрически изоморфна евклидовой форме: ортонормальный базис гиперболической формы состоит из векторов

$$\varepsilon_{2\nu-1} = \bigl(e_\nu - e_{n+\nu}\bigr)/\sqrt{-2} \quad \text{и} \quad \varepsilon_{2\nu} = \bigl(e_\nu + e_{n+\nu}\bigr)/\sqrt{2}\,, \quad 1 \leqslant \nu \leqslant n\,.$$

Над полями $\mathbb{R}$ и $\mathbb{Q}$ гиперболическая форма не изоморфна евклидовой, поскольку евклидовы скалярные квадраты всех ненулевых векторов положительны, тогда как ограничение гиперболической формы на линейную оболочку первых n базисных векторов тождественно нулевое. Базис, в котором матрица Грама гиперболической формы имеет вид (15-9), называется *гиперболическим базисом*.

[1] См. n° 8.3 на стр. 139.
[2] См. n° 14.1 на стр. 255.

Пример 15.3 (симплектическая форма)
Кососимметричная форма на чётномерном координатном пространстве $\Bbbk^{2n}$, матрица Грама которой в стандартном базисе равна

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}, \tag{15-10}$$

где E — единичная матрица размера $n\times n$, называется *симплектической*. Матрица J вида (15-10) называется *симплектической единицей*. Она имеет $J^2 = -E$ и $\det J = 1$. Таким образом, симплектическая форма невырождена. Базис, в котором матрица Грама кососимметричной формы равна J, называется *симплектическим базисом*. В теор. 16.2 на стр. 293 ниже мы покажем, что всякая невырожденная кососимметричная билинейная форма над любым полем изометрически изоморфна симплектической. Это означает, в частности, что размерность пространства с невырожденной кососимметричной формой обязательно чётна.

Упражнение 15.6. Убедитесь в том, что все кососимметричные квадратные матрицы нечётного размера над полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ вырождены.

15.2.1. Левый и правый двойственный базис. Если билинейная форма β на пространстве V невырождена, то у любого базиса $\boldsymbol{e} = (e_1, \dots e_n)$ в V есть *правый* и *левый* двойственные относительно формы β базисы $\boldsymbol{e}^\vee = (e_1^\vee, \dots, e_n^\vee)$ и ${}^\vee\boldsymbol{e} = ({}^\vee e_1, \dots, {}^\vee e_n)$ — прообразы двойственного к $\boldsymbol{e}$ базиса $\boldsymbol{e}^* = (e_1^*, \dots, e_n^*)$ в V^* относительно правой и левой корреляции соответственно. Они однозначно характеризуются соотношениями ортогональности

$$\beta\left(e_i, e_j^\vee\right) = \beta\left({}^\vee e_i, e_j\right) = \delta_{ij}, \tag{15-11}$$

которые на матричном языке означают, что взаимные матрицы Грама двойственных относительно формы β базисов единичные: $B_{\boldsymbol{e}\boldsymbol{e}^\vee} = B_{{}^\vee\boldsymbol{e}\boldsymbol{e}} = E$. Согласно форм. (15-1) на стр. 272 матрицы переходов $C_{\boldsymbol{e},\boldsymbol{e}^\vee}$ и $C_{\boldsymbol{e},{}^\vee\boldsymbol{e}}$, в j-тых столбцах которых стоят координаты векторов $e_j^\vee$ и ${}^\vee e_j$ в базисе $\boldsymbol{e}$, удовлетворяют соотношениям $B_{\boldsymbol{e}}C_{\boldsymbol{e},\boldsymbol{e}^\vee} = B_{\boldsymbol{e}\boldsymbol{e}^\vee} = E$ и $C^t_{\boldsymbol{e},{}^\vee\boldsymbol{e}}B_{\boldsymbol{e}} = B_{{}^\vee\boldsymbol{e},\boldsymbol{e}} = E$, откуда

$$C_{\boldsymbol{e},\boldsymbol{e}^\vee} = B_{\boldsymbol{e}}^{-1} \quad \text{и} \quad C_{\boldsymbol{e},{}^\vee\boldsymbol{e}} = \left(B_{\boldsymbol{e}}^t\right)^{-1}.$$

Знание двойственного к базису $\boldsymbol{e}$ относительно билинейной формы β базиса позволяет находить коэффициенты разложения любого вектора $v \in V$ по каждому из двойственных базисов как взятые с надлежащей стороны скалярные произведения вектора v с соответствующими элементами двойственного базиса:

$$v = \sum_i \beta({}^\vee e_i, v)\, e_i = \sum_i \beta(v, e_i^\vee)\, e_i = \sum_i \beta(v, e_i)\, {}^\vee e_i = \sum_i \beta(e_i, v)\, e_i^\vee. \tag{15-12}$$

Упражнение 15.7. Убедитесь в этом.

15.2.2. Изотропные подпространства. Подпространство $U \subset V$ называется *изотропным* для билинейной формы β, если эта форма ограничивается на него в тождественно нулевую форму, т. е. когда $\beta(u, w) = 0$ для всех $u, w \in U$. Например, каждое одномерное подпространство является изотропным для любой кососимметричной формы, а линейные оболочки первых n и последних n базисных векторов пространства $\Bbbk^{2n}$ изотропны для гиперболической формы из прим. 15.2 и симплектической формы из прим. 15.3.

Предложение 15.2
Размерность изотропного подпространства невырожденной билинейной формы на пространстве V не превосходит $\dim V/2$.

Доказательство. Подпространство $U \subset V$ изотропно если и только если его образ при корреляции $\beta^\wedge : V \xrightarrow{\sim} V^*$ лежит в подпространстве $\operatorname{Ann} U \subset V^*$. Так как корреляция невырожденной формы инъективна, $\dim U \leqslant \dim \operatorname{Ann} U = \dim V - \dim U$, откуда $2\dim U \leqslant \dim V$. □

Замечание 15.1. Примеры гиперболической и симплектической форм показывают, что оценка из предл. 15.2 в общем случае неулучшаема.

15.2.3. Группа изометрий. Как мы видели в n° 15.1.3 на стр. 274, линейный эндоморфизм $f : V \to V$ является изометрическим для билинейной формы β на пространстве V если и только если его матрица $F_{\boldsymbol{e}}$ в произвольном базисе $\boldsymbol{e}$ пространства V связана с матрицей Грама $B_{\boldsymbol{e}}$ этого базиса соотношением[1] $F_{\boldsymbol{e}}^t B_{\boldsymbol{e}} F_{\boldsymbol{e}} = B_{\boldsymbol{e}}$. Если форма β невырождена, то беря определители обеих частей, заключаем, что $\det^2 F_{\boldsymbol{e}} = 1$, откуда $\det F_{\boldsymbol{e}} = \pm 1$. Поэтому любая изометрия конечномерного пространства с невырожденной билинейной формой обратима. Так как композиция изометрий и обратное к изометрии отображение тоже являются изометриями, изометрические автоморфизмы пространства V образуют группу преобразований[2]. Она обозначается $\mathrm{O}_\beta(V)$ и называется *группой изометрий* или *ортогональной группой* невырожденной билинейной формы β. Изометрии определителя 1 называются *специальными* или *собственными* и образуют в группе всех изометрий подгруппу, которая обозначается $\mathrm{SO}_\beta(V)$.

Из форм. (15-8) на стр. 274 вытекает, что обратная к изометрии f изометрия имеет матрицу

$$F_{\boldsymbol{e}}^{-1} = B_{\boldsymbol{e}}^{-1} F_{\boldsymbol{e}}^t B_{\boldsymbol{e}}\,. \tag{15-13}$$

Пример 15.4 (изометрии вещественной гиперболической плоскости)
Оператор $f : H_2 \to H_2$, имеющий в стандартном гиперболическом базисе $e_1, e_2 \in H_2$ матрицу

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

является изометрическим тогда и только тогда, когда

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

что равносильно уравнениям $ac = bd = 0$ и $ad + bc = 1$, имеющим два семейства решений:

$$F_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{и} \quad \tilde{F}_\lambda = \begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}, \quad \text{где } \lambda \in \Bbbk^* = \Bbbk \smallsetminus \{0\}. \tag{15-14}$$

Над полем $\mathbb{R}$ оператор F_λ является собственным, и при $\lambda > 0$ называется *гиперболическим поворотом*, т. к. каждый вектор $v = (x, y)$, обе координаты которого ненулевые, движется при действии на него операторов F_λ с $\lambda \in (0, \infty)$ по гиперболе $xy = \text{const}$. Если положить $\lambda = e^t$ и

[1] См. формулу (15-8) на стр. 274.
[2] См. n° 1.6 на стр. 16.

перейти к ортогональному базису из векторов $p = (e_1+e_2)/\sqrt{2}$, $q = (e_1-e_2)/\sqrt{2}$, то оператор F_λ запишется в нём матрицей, похожей на матрицу евклидова поворота

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \operatorname{ch} t & \operatorname{sh} t \\ \operatorname{sh} t & \operatorname{ch} t \end{pmatrix},$$

где $\operatorname{ch} t \stackrel{\text{def}}{=} (e^t+e^{-t})/2$ и $\operatorname{sh} t \stackrel{\text{def}}{=} (e^t-e^{-t})/2$ называются *гиперболическими косинусом* и *синусом* вещественного числа t. Оператор F_λ с $\lambda < 0$ является композицией гиперболического поворота и центральной симметрии. Несобственный оператор $\widetilde{F}_\lambda$ является композицией гиперболического поворота с отражением относительно той оси гиперболы, которая пересекается с её ветвями.

15.3. Ортогональные разложения. С каждым подпространством U векторного пространства V с билинейной формой $\beta : V \times V \to \Bbbk$ связаны *левый* и *правый ортогоналы*

$$\begin{aligned} {}^{\perp}U &= \{v \in V \mid \forall\, u \in U\ \beta(v,u) = 0\}, \\ U^{\perp} &= \{v \in V \mid \forall\, u \in U\ \beta(u,v) = 0\}. \end{aligned} \tag{15-15}$$

Вообще говоря, это два разных подпространства в V.

Предложение 15.3
Если билинейная форма β на конечномерном пространстве V невырождена, то для всех подпространств $U \subset V$ выполняются равенства

$$\dim {}^{\perp}U = \dim V - \dim U = \dim U^{\perp} \quad \text{и} \quad ({}^{\perp}U)^{\perp} = U = {}^{\perp}(U^{\perp}).$$

Доказательство. Ортогоналы (15-15) являются прообразами подпространства $\operatorname{Ann} U \subset V^*$ относительно левой и правой корреляций[1] ${}^{\wedge}\beta, \beta^{\wedge} : V \xrightarrow{\sim} V^*$, которые являются изоморфизмами, если форма невырождена. Левые два равенства следуют из соотношения[2] $\dim \operatorname{Ann} U = \dim V - \dim U$. Правые два равенства вытекают из левых, поскольку оба подпространства $({}^{\perp}U)^{\perp}$ и ${}^{\perp}(U^{\perp})$ содержат U и имеют размерность $\dim U$. □

Предложение 15.4
Пусть билинейная форма β на произвольном[3] векторном пространстве V ограничивается на конечномерное подпространство $U \subset V$ в невырожденную на этом подпространстве билинейную форму $\beta|_U : U \times U \to \Bbbk$. Тогда $V = U \oplus U^{\perp}$, и проекция $v_U \in U$ каждого вектора $v \in V$ на подпространство U вдоль $U^{\perp}$ однозначно определяется тем, что $\beta(u,v) = \beta(u,v_U)$ для всех $u \in U$. Вектор v_U выражается через произвольный базис $u_1, \dots, u_n$ пространства U по формуле

$$v_U = \sum_{i=1}^{n} \beta\left({}^{\vee}u_i, v\right) u_i = \sum_{i=1}^{n} \beta\left(u_i, v\right) u_i^{\vee}, \tag{15-16}$$

где ${}^{\vee}u_1, \dots, {}^{\vee}u_n$ и $u_1^{\vee}, \dots, u_n^{\vee}$ — левый и правый двойственные[4] к $u_1, \dots, u_n$ относительно формы β базисы в U.

[1] См. n° 15.1.1 на стр. 272.
[2] См. сл. 7.9 на стр. 125.
[3] В том числе бесконечномерном.
[4] См. n° 15.2.1 на стр. 276.

Доказательство. Так как ограничение формы β на U невырождено, для любого вектора $v \in V$ существует единственный такой вектор $v_U \in U$, что линейная функция $u \mapsto \beta(u,v)$ на пространстве U задаётся правым скалярным умножением векторов из U на этот вектор v_U, т. е. для всех $u \in U$ выполняется равенство $\beta(u,v) = \beta(u,v_U)$. Поэтому разность $v - v_U \in U^\perp$. Таким образом, каждый вектор $v \in V$ представляется в виде суммы $v = v_U + (v - v_U)$ с $v \in U$ и $v - v_U \in U^\perp$. Поскольку в любом разложения $v = v'_U + w$ с $v'_U \in U$ и $w \in U^\perp$ для всех $u \in U$ выполняется равенство $\beta(u,v) = \beta(u,v'_U)$, имеем равенство $v'_U = v_U$, а значит и равенство $w = v - v'_U = v - v_U$, что доказывает первые два утверждения предложения. Последнее утверждение вытекает из форм. (15-12) на стр. 276: $v_U = \sum_i \beta({}^\vee u_i, v_U)\, u_i = \sum_i \beta({}^\vee u_i, v)\, u_i$. □

Упражнение 15.8. Докажите симметричное утверждение: $V = {}^\perp U \oplus U$ если и только если билинейная форма β ограничивается на конечномерное подпространство $U \subset V$ в невырожденную на этом подпространстве билинейную форму $\beta|_U : U \times U \to \Bbbk$; при этом проекция ${}_U v$ каждого вектора $v \in V$ на U вдоль ${}^\perp U$ однозначно определяется тем, что $\beta(v,u) = \beta({}_U v, u)$ для всех $u \in U$ и находится по формуле ${}_U v = \sum \beta\left(v, u_i^\vee\right)\, u_i = \sum \beta\left(v, u_i\right)\, {}^\vee u_i$.

15.4. Соответствия между формами и операторами. На пространстве V с билинейной формой $\beta : V \times V \to \Bbbk$ каждому линейному оператору $f : V \to V$ можно сопоставить билинейную форму $\beta_f(u,w) \stackrel{\text{def}}{=} \beta(u, fw)$ с матрицей Грама $\boldsymbol{e}^t \cdot f(\boldsymbol{e}) = \boldsymbol{e}^t \cdot \boldsymbol{e}\, F_{\boldsymbol{e}} = B_{\boldsymbol{e}} F_{\boldsymbol{e}}$ в произвольно выбранном базисе $\boldsymbol{e}$ пространства V. Поскольку на языке матриц отображение $f \mapsto \beta_f$ заключается в левом умножении матрицы оператора на матрицу Грама: $F_{\boldsymbol{e}} \mapsto B_{\boldsymbol{e}} F_{\boldsymbol{e}}$, оно линейно и обратимо, если форма β невырождена. Обратное отображение задаётся умножением матрицы оператора слева на обратную к матрице Грама матрицу. Поэтому каждая билинейная форма

$$\alpha : V \times V \to \Bbbk$$

на конечномерном векторном пространстве V с фиксированной невырожденной билинейной формой β имеет вид $\alpha(u,w) = \beta(u, f_\alpha w)$ для некоторого линейного оператора $f_\alpha : V \to V$, однозначно определяемого формой α. Матрица $F_{\boldsymbol{e}}$ оператора f_α выражается через матрицы Грама $B_{\boldsymbol{e}}$ и $A_{\boldsymbol{e}}$ форм β и α по формуле $F_{\boldsymbol{e}} = B_{\boldsymbol{e}}^{-1} A_{\boldsymbol{e}}$.

15.4.1. Канонический оператор. Задаваемая невырожденной билинейной формой β биекция между формами и операторами сопоставляет транспонированной к β форме

$$\beta^t(u,w) \stackrel{\text{def}}{=} \beta(w,u)$$

оператор $\varkappa : V \to V$, который называется *каноническим оператором* невырожденной билинейной формы β и однозначно характеризуется тем, что для всех $u, w \in V$

$$\beta(w,u) = \beta(u, \varkappa w)\,. \tag{15-17}$$

Так как $\beta(u,w) = \beta(w, \varkappa u) = \beta(\varkappa u, \varkappa w)$ для всех $u, w \in V$, канонический оператор является изометрическим. Матрица $K_{\boldsymbol{e}}$ канонического оператора в произвольном базисе $\boldsymbol{e}$ пространства V выражается через матрицу Грама $B_{\boldsymbol{e}}$ формы β по формуле $K_{\boldsymbol{e}} = B_{\boldsymbol{e}}^{-1} B_{\boldsymbol{e}}^t$.

Упражнение 15.9. Убедитесь, что при замене матрицы Грама по правилу $B \mapsto C^t B C$, где C обратима, матрица $K = B^{-1} B^t$ меняется по правилу $K \mapsto C^{-1} K C$, т. е. канонические операторы изоморфных билинейных форм подобны.

Теорема 15.1
Над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ две невырожденные билинейные формы изометрически изоморфны если и только если их канонические операторы подобны.

Доказательство. Импликация «только если» вытекает из упр. 15.9 и имеет место над любым полем. Докажем обратную импликацию. Пусть невырожденные билинейные формы α и β имеют подобные канонические операторы $\varkappa_\alpha$ и $\varkappa_\beta = g^{-1}\varkappa_\alpha g$. Тогда форма $\alpha'(u,w) = \alpha(gu, gw)$ изометрически изоморфна форме α и имеет канонический оператор $g^{-1}\varkappa_\alpha g = \varkappa_\beta$, поскольку $\alpha'(u,w) = \alpha(gu,gw) = \alpha(gw, \varkappa_\alpha gu) = \alpha'(w, g^{-1}\varkappa_\alpha gu)$ для всех u, w. Таким образом, заменяя форму α на форму α', мы без ограничения общности можем считать, что формы α и β имеют один и тот же канонический оператор $\varkappa$. Линейный оператор f, однозначно определяемый равенством $\beta(u,w) = \alpha(u, fw)$ для всех u, w, обратим в силу невырожденности форм α, β и *самосопряжён* относительно α в том смысле[1], что для всех u, w выполняется равенство

$$\alpha(fu, w) = \alpha(\varkappa^{-1}w, fu) = \beta(\varkappa^{-1}w, u) = \beta(u,w) = \alpha(u, fw)\,.$$

В прим. 12.9 на стр. 227 мы видели, что существует такой многочлен $P(t) \in \Bbbk[t]$, что оператор $h = P(f)$ удовлетворяет равенству $h^2 = f$, из которого вытекает, что h биективен. Будучи многочленом от f, оператор h тоже удовлетворяет равенству $\alpha(hu, w) = \alpha(u, hw)$ для всех u, w. Поэтому форма $\beta(u,w) = \alpha(u, fw) = \alpha(u, h^2w) = \alpha(hu, hw)$ изометрически изоморфна форме α. □

Замечание 15.2. Над алгебраически незамкнутыми полями теор. 15.1 неверна. Например, над полем $\mathbb{Q}$ имеется необозримое множество изометрически неизоморфных невырожденных симметричных[2] форм, осмысленное описание которого представляется неподъёмной задачей.

Замечание 15.3. Из теор. 15.1 вытекает, что над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ две билинейных формы изометрически изоморфны если и только если жордановы нормальные формы их канонических операторов одинаковы. В сл. 15.3 на стр. 287 ниже мы перечислим все жордановы нормальные формы, встречающиеся у канонических операторов невырожденных билинейных форм над такими полями.

Пример 15.5 (невырожденная билинейная форма типа $W_n(\lambda)$)
Обозначим через $W_n(\lambda)$ координатное векторное пространство $\Bbbk^{2n} = \Bbbk^n \oplus \Bbbk^n$ с билинейной формой β, матрица Грама которой в стандартном базисе имеет вид

$$B = \begin{pmatrix} 0 & E_n \\ J_n(\lambda) & 0 \end{pmatrix}, \tag{15-18}$$

где E_n и $J_n(\lambda)$ суть единичная матрица и жорданова клетка с собственным числом $\lambda \neq 0$ размеров $n \times n$. Эта форма несимметрична и невырождена, а её канонический оператор имеет матрицу

$$K = B^{-1}B^t = \begin{pmatrix} 0 & J_n^{-1}(\lambda) \\ E_n & 0 \end{pmatrix}\begin{pmatrix} 0 & J_n^t(\lambda) \\ E_n & 0 \end{pmatrix} = \begin{pmatrix} J_n^{-1}(\lambda) & 0 \\ 0 & J_n^t(\lambda) \end{pmatrix}.$$

[1] Мы подробнее поговорим об этом свойстве в n° 15.4.2 – n° 15.4.3 ниже.

[2] Т. е. удовлетворяющих при любых u, w равенству $\beta(u,w) = \beta(w,u)$ и тем самым имеющих тождественный канонический оператор.

Поскольку матрица $J_n^{-1}(\lambda)$ подобна матрице[1] $J_n(\lambda^{-1})$, а матрица $J_n^t(\lambda)$ — матрице[2] $J_n(\lambda)$, множество $\mathcal{E}\ell(\varkappa) = \{(t-\lambda)^m, (t-\lambda^{-1})^m\}$, т. е. ЖНФ оператора $\varkappa$ состоит из двух клеток размера $n \times n$ с собственными числами λ и λ^{-1}.

Пример 15.6 (невырожденная билинейная форма типа U_n)
Обозначим через U_n координатное векторное пространство $\Bbbk^n$ с билинейной формой β, матрица Грама которой в стандартном базисе имеет вид

$$B = \begin{pmatrix} & & & & 1 \\ & & & -1 & 1 \\ & & \iddots & -1 & \\ & (-1)^{n-2} & \iddots & & \\ (-1)^{n-1} & (-1)^{n-2} & & & \end{pmatrix} \tag{15-19}$$

(на побочной диагонали и под нею стоят чередующиеся ± 1, а в остальных местах — нули). Канонический оператор этой формы имеет матрицу

$$K = B^{-1}B^t = (-1)^{n-1}\begin{pmatrix} 1 & 2 & 1 & & \\ & 1 & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & 1 & 2 \\ & & & & 1 \end{pmatrix}$$

вида $E + 2N + N^2$, где N — нильпотентный оператор с $N^n = 0$ и $N^{n-1} \neq 0$. Поэтому жорданова нормальная форма оператора $\varkappa$ состоит из одной клетки $J_n((-1)^{n-1})$ с собственным числом 1 при нечётном n и -1 при чётном.

15.4.2. Сопряжение операторов. На пространстве V с невырожденной билинейной формой β каждому линейному оператору $f : V \to V$ можно сопоставить *правый* и *левый сопряжённые операторы*

$$f^\vee \stackrel{\text{def}}{=} \beta^{\wedge -1} \circ f^* \circ \beta^\wedge \quad \text{и} \quad {}^\vee f \stackrel{\text{def}}{=} {}^\wedge\beta^{-1} \circ f^* \circ {}^\wedge\beta\,, \tag{15-20}$$

где $f^* : V^* \to V^*$ — оператор, двойственный[3] к f, а $\beta^\wedge, {}^\wedge\beta : V \xrightarrow{\sim} V^*$ — правая и левая корреляции[4] формы β. Иначе говоря, эти операторы задаются коммутативными диаграммами

$$\begin{array}{ccc} V^* & \xrightarrow{f^*} & V^* \\ {\scriptstyle\beta^\wedge}\uparrow\wr & & \wr\uparrow{\scriptstyle\beta^\wedge} \\ V & \xrightarrow{f^\vee} & V\,, \end{array} \qquad \begin{array}{ccc} V^* & \xrightarrow{f^*} & V^* \\ {\scriptstyle{}^\wedge\beta}\uparrow\wr & & \wr\uparrow{\scriptstyle{}^\wedge\beta} \\ V & \xrightarrow{{}^\vee f} & V\,. \end{array} \tag{15-21}$$

Равенства (15-20) означают для всех $w \in V$ равенства линейных функционалов

$$f^*(\beta^\wedge(w)) = \beta^\wedge(f^\vee(w)) \quad \text{и} \quad f^*({}^\wedge\beta(w)) = {}^\wedge\beta({}^\vee f(w))$$

[1] См. упр. 12.18 на стр. 225.
[2] См. ?? на стр. ??.
[3] См. n° 7.4.4 на стр. 127.
[4] См. n° 15.1.1 на стр. 272.

на пространстве V. Применяя обе части этих равенств к произвольному вектору $u \in V$, заключаем, что левый и правый сопряжённые операторы однозначно определяются тем, что

$$\beta(fu, w) = \beta(u, f^\vee w) \quad \text{и} \quad \beta(w, fu) = \beta({}^\vee f w, u) \tag{15-22}$$

для всех $u, w \in V$. Матрицы ${}^\vee F$ и $F^\vee$ операторов $f^\vee$ и ${}^\vee f$ в любом базисе пространства V выражаются через матрицу F оператора f и матрицу Грама B формы β по формулам

$$F^\vee = B^{-1} F^t B \quad \text{и} \quad {}^\vee F = \left(B^t\right)^{-1} F^t B^t . \tag{15-23}$$

Так как транспонированные матрицы подобны[1], все четыре оператора f, f^*, $f^\vee$, ${}^\vee f$ подобны и имеют одинаковые элементарные делители.

Упражнение 15.10. Покажите, что а) ${}^\vee\left(f^\vee\right) = f = \left({}^\vee f\right)^\vee$ б) $\ker f^\vee = (\operatorname{im} f)^\perp$ в) $\operatorname{im} f^\vee = (\ker f)^\perp$ г) $\ker {}^\vee f = {}^\perp(\operatorname{im} f)$ д) $\operatorname{im} {}^\vee f = {}^\perp(\ker f)$.

Оба сопряжения являются *антиавтоморфизмами* автоморфизмами алгебры $\operatorname{End} V$ в том смысле, что они линейны, биективны, но меняют порядок сомножителей в произведениях:

$$(fg)^\vee = g^\vee f^\vee \quad \text{и} \quad {}^\vee(fg) = {}^\vee g {}^\vee f .$$

Это вытекает из равенств

$$\beta(fgu, w) = \beta(gu, f^\vee w) = \beta(u, g^\vee f^\vee w) \quad \text{и} \quad \beta(u, fgw) = \beta({}^\vee f u, gw) = \beta({}^\vee g {}^\vee f u, w) .$$

Упражнение 15.11. Покажите, что обратимый оператор $g : V \to V$ является изометрией невырожденной билинейной формы β если и только если ${}^\vee g = g^\vee = g^{-1}$.

Предложение 15.5 (рефлексивность)
Следующие условия на линейный оператор $f : V \to V$ на векторном пространстве V с невырожденной билинейной формой β эквивалентны друг другу:

$$1)\ f^{\vee\vee} = f \qquad 2)\ {}^{\vee\vee} f = f \qquad 3)\ {}^\vee f = f^\vee \qquad 4)\ \varkappa_\beta f = f \varkappa_\beta ,$$

где $\varkappa_\beta = (\beta^\wedge)^{-1} {}^\wedge \beta : V \to V$ — канонический оператор формы β.

Доказательство. Условия (1) – (3) получаются друг из друга левым и правым сопряжением обеих частей согласно упр. 15.10 (а) и очевидно эквивалентны. Условие (3) равносильно равенству $\beta^\wedge \left({}^\wedge \beta\right)^{-1} f^* = f^* \beta^\vee \left({}^\wedge \beta\right)^{-1}$ операторов на пространстве V^*. Двойственное[2] ему равенство $f(\beta^\wedge)^{-1} {}^\wedge \beta = (\beta^\wedge)^{-1} {}^\wedge \beta f$ операторов на V и есть (4). □

15.4.3. Рефлексивные операторы. Операторы $f : V \to V$, удовлетворяющие предл. 15.5, называются *рефлексивными* относительно формы β. Совпадающие левый и правый сопряжённые к рефлексивному оператору f обозначаются $f^\times \stackrel{\text{def}}{=} f^\vee = {}^\vee f$. Рефлексивные операторы образуют в $\operatorname{End}(V)$ подалгебру — централизатор канонического оператора $\varkappa_\beta$ формы $\beta(V)$:

$$Z_{\varkappa_\beta} \stackrel{\text{def}}{=} \{ f \in \operatorname{End}(V) \mid f \varkappa_\beta = \varkappa_\beta f \} .$$

[1] См. **??** на стр. **??**.
[2] См. упр. 15.4 на стр. 273.

Если β симметрична или кососимметрична, то $\varkappa_\beta = \pm\mathrm{Id}$, и все эндоморфизмы пространства V рефлексивны. Из упр. 15.11 вытекает, что все изометрии любой невырожденной формы рефлексивны.

Упражнение 15.12. Докажите, что для рефлексивного оператора f

$$(\operatorname{im} f)^\perp = \ker f^\times = {}^\perp(\operatorname{im} f) \quad \text{и} \quad (\ker f)^\perp = \operatorname{im} f^\times = {}^\perp(\ker f)\,.$$

Сопряжение $f \mapsto f^\times$ является линейной инволюцией[1] пространства $Z_{\varkappa_\beta}$ рефлексивных операторов, и если $\operatorname{char}\Bbbk \neq 2$, то последнее раскладывается в прямую сумму

$$Z_{\varkappa_\beta} = \mathrm{End}_+(V) \oplus \mathrm{End}_-(V)$$

её собственных подпространств с собственными числами ± 1: пространства *самосопряжённых* операторов

$$\mathrm{End}_+(V) \stackrel{\text{def}}{=} \{f : V \to V \mid \forall\, u, w \in V\ \beta(fu, w) = \beta(u, fw)\}$$

и пространства *антисамосопряжённых* операторов

$$\mathrm{End}_-(V) \stackrel{\text{def}}{=} \{f : V \to V \mid \forall\, u, w \in V\ \beta(fu, w) = -\beta(u, fw)\}\,.$$

Упражнение 15.13. Убедитесь, что $\mathrm{End}_\pm(V) \subset Z_{\varkappa_\beta}$ и каждый рефлексивный оператор f раскладывается как $f = f_+ + f_-$, где $f_\pm = (f \pm f^\times)/2 \in \mathrm{End}_\pm(V)$.

15.5. Неразложимые невырожденные формы. Из двух пространств V_1, V_2 с билинейными формами β_1, β_2 можно изготовить пространство $V_1 \oplus V_2$ с билинейной формой $\beta_1 \dot{+} \beta_2$, относительно которой слагаемые биортогональны друг другу и которая ограничивается на V_1 и V_2 в β_1 и β_2. Она задаётся формулой

$$\big[\beta_1 \dot{+} \beta_2\big]\big((u_1, u_2), (w_1, w_2)\big) \stackrel{\text{def}}{=} \beta_1(u_1, u_2) + \beta_2(w_1, w_2)\,,$$

и её матрица Грама в любом базисе, первые $\dim V_1$ векторов которого образуют базис в V_1 с матрицей Грама B_1, а последние $\dim V_2$ векторов — базис в V_2 с матрицей Грама B_2, имеет блочный вид

$$\begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}.$$

Пространство $V_1 \oplus V_2$ с формой $\beta_1 \dot{+} \beta_2$ обозначается $V_1 \dot{+} V_2$ и называется *биортогональной прямой суммой* форм β_1 и β_2. Форма $\beta_1 \dot{+} \beta_2$ невырождена если и только если невырождены обе формы β_1, β_2, и в этом случае её канонический оператор раскладывается в прямую сумму канонических операторов форм β_1, β_2.

Упражнение 15.14. Для гиперболических[2] и симплектических[3] пространств H_{2n} и W_{2n} постройте изометрические[4] изоморфизмы $H_{2m} \dot{+} H_{2k} \xrightarrow{\sim} H_{2(m+k)}$ и $W_{2m} \dot{+} W_{2k} \xrightarrow{\sim} W_{2(m+k)}$.

Билинейная форма β на пространстве V называется *разложимой*, если

$$V = U \oplus W \quad \text{и} \quad \beta(u, w) = \beta(w, u) = 0 \text{ для всех } u \in U, w \in W\,,$$

[1] См. прим. 12.6 на стр. 222.
[2] См. прим. 15.2 на стр. 275.
[3] См. прим. 15.3 на стр. 275.
[4] См. n° 15.1.3 на стр. 274.

где $U, W \subsetneq V$ — ненулевые собственные подпространства. В этом случае

$$V = U \dotplus W \quad \text{и} \quad \beta = \beta|_U \dotplus \beta|_W .$$

Очевидно, что каждое пространство с невырожденной билинейной формой является биортогональной прямой суммой неразложимых подпространств с невырожденными формами. Примерами неразложимых пространств являются одномерные (с любой ненулевой формой), двумерное симплектическое пространство из прим. 15.3 на стр. 275 и пространства U_n из прим. 15.6 на стр. 281.

Упражнение 15.15. Убедитесь в этом и покажите, что при $\lambda = (-1)^{n-1}$ пространство $W_n(\lambda)$ из прим. 15.5 на стр. 280 является биортогональной прямой суммой двух подпространств U_n из прим. 15.6.

В этом разделе мы перечислим все невырожденные неразложимые билинейные формы над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$. Для этого достаточно построить полный список канонических операторов таких форм с точностью до подобия, т. е. предъявить жордановы нормальные формы всех таких операторов. Напомню[1], что каждое пространство с оператором тоже является прямой суммой неразложимых, а каждый неразложимый оператор над алгебраически замкнутым полем подобен оператору умножения на t в факторкольце

$$J_\lambda^m = \Bbbk[t]/((t-\lambda)^m)$$

и действует на векторы $e_i = [(t-\lambda)^{n-i}]$, где $0 \leqslant i \leqslant n$ и $e_0 = 0$, по правилу

$$e_\nu \mapsto \lambda e_i + e_{i-1}\,, \text{ где } i = 1, \dots, n\,,$$

а вектор $e_0 = 0$ переводит в себя. Мы будем называть каждое изоморфное J_λ^m неразложимое пространство с оператором *жордановым блоком*, а образы векторов e_i в этом пространстве — *жордановой цепочкой* размера m с собственным числом λ.

Лемма 15.1 (соотношения ортогональности)
Если линейный оператор $f : V \to V$ является изометрией невырожденной билинейной формы $\beta : V \times V \to \Bbbk$, то любые две его жордановы цепочки $u_0, u_1, \dots, u_\ell$ и $w_0, w_1, \dots, w_m$ с собственными числами λ и μ биортогональны друг другу при $\lambda\mu \neq 1$, а при $\lambda\mu = 1$ и $\ell \leqslant m$ соотношения $\beta(u_i, w_j) = \beta(w_j, u_i) = 0$ выполняются для всех $i + j \leqslant m$, тогда как при $i + j = m + 1$ имеют место равенства $\beta(u_i, w_j) = (-\mu/\lambda)^{i-1}\beta(u_1, w_m)$ и $\beta(w_j, u_i) = (-\mu/\lambda)^{i-1}\beta(w_m, u_1)$.

Доказательство. Так как $\beta(u_i, w_j) = \beta(fu_i, fw_j) = \beta(\lambda u_i + u_{i-1}, \mu w_j + w_{j-1})$, при всех $1 \leqslant i \leqslant \ell$ и $1 \leqslant j \leqslant m$ справедливо соотношение

$$(1 - \lambda\mu)\beta\left(u_i, w_j\right) = \lambda\beta\left(u_i, w_{j-1}\right) + \mu\beta\left(u_{i-1}, w_j\right) + \beta\left(u_{i-1}, w_{j-1}\right). \tag{15-24}$$

Если $\lambda\mu \neq 1$, возрастающая индукция по $i + j$, начинающаяся с $i + j = 0$ и $u_0 = w_0 = 0$, показывает, что $\beta(u_i, w_j) = 0$ для всех i, j. При $\lambda\mu = 1$ соотношение (15-24) приобретает вид

$$\lambda\beta(u_i, w_{j-1}) + \mu\beta(u_{i-1}, w_j) + \beta(u_{i-1}, w_{j-1}) = 0\,.$$

Пусть по индукции $\beta(u_i, w_j) = 0$ для всех $i + j < k \leqslant m$. Тогда $\lambda\beta(u_i, w_{j-1}) = -\mu\beta(u_{i-1}, w_j)$ для всех $i + j = k$, откуда $\beta(u_i, w_{k-i}) = (-\mu/\lambda)^{i-1}\beta(u_1, w_{k-1})$ для всех $1 \leqslant i \leqslant \ell$. Если $k \leqslant m$, то $\beta(u_1, w_{k-1}) = (-\mu/\lambda)\beta(u_0, w_k) = 0$. Соотношения на $\beta(w_j, u_i)$ получаются аналогично. □

[1] См. n° 12.1.6 на стр. 211.

Следствие 15.1
Для любой изометрии f неразложимого векторного пространства с невырожденной билинейной формой β имеется следующая альтернатива:

- либо $V = K_{\pm 1}$ является корневым пространством оператора f с собственным числом $+1$ или -1
- либо $V = K_\lambda \oplus K_{\lambda^{-1}}$ является суммой двух корневых пространств с обратными друг другу собственными числами, отличными от ± 1

причём в последнем случае каждое из подпространств $K_{\lambda^{\pm 1}}$ изотропно, а нильпотентные операторы $(f-\lambda\mathrm{Id})|_{K_\lambda}$ и $(f-\lambda^{-1}\mathrm{Id})|_{K_{\lambda^{-1}}}$ имеют одинаковый цикловой тип.

Доказательство. Все утверждения кроме самого последнего вытекают из того, что по лем. 15.1 каждое корневое подпространство K_λ биортогонально всем корневым подпространствам K_μ с $\mu \neq \lambda^{-1}$. Докажем последнее утверждение. Так как оператор f изометрический, он обратим, рефлексивен и сопряжён своему обратному[1]. Поэтому $(f-\lambda\mathrm{Id})^\times = f^{-1}-\lambda\mathrm{Id} = -\lambda f^{-1}(f-\lambda^{-1}\mathrm{Id})$ и $\ker(f-\lambda\mathrm{Id})^{\times k} = \ker\bigl(-\lambda^k f^{-k}(f-\lambda^{-1}\mathrm{Id})^k\bigr) = \ker(f-\lambda^{-1}\mathrm{Id})^k$ при всех k. Это означает[2], что набор жордановых блоков с собственным числом λ у оператора $f^\times$ точно такой же, как набор жордановых блоков с собственным числом λ^{-1} у оператора f, а так как f и $f^\times$ подобны, набор жордановых блоков с собственным числом λ у них одинаков. □

Лемма 15.2
Если подпространство U переводится в себя каноническим оператором $\varkappa$ невырожденной билинейной формы, то ${}^\perp U = U^\perp$ и это подпространство тоже $\varkappa$-инвариантно.

Доказательство. Так как оператор $\varkappa$ изометрический, он биективен и рефлексивен, причём $\varkappa^\times = \varkappa^{-1}$. Если $\beta(w,u) = 0$ для всех $u \in U$, то $\beta(u,w) = \beta(w,\varkappa u) = 0$ для всех $u \in U$ так как $\varkappa(U) = U$. Наоборот, если $\beta(u,w) = 0$ для всех $u \in U$, то $\beta(w,u) = \beta(\varkappa^{-1}u, w) = 0$ для всех $u \in U$ так как $\varkappa^{-1}(U) = U$. Поэтому ${}^\perp U = U^\perp$. Наконец, если $\beta(u,w) = 0$ для всех $u \in U$, то $w \in {}^\perp U$ по уже доказанному, откуда $\beta(u,\varkappa w) = \beta(w,u) = 0$. Поэтому $\varkappa(U^\perp) = U^\perp$. □

Теорема 15.2
Жорданова нормальная форма канонического оператора $\varkappa$ невырожденной неразложимой билинейной формы β на d-мерном векторном пространстве V над алгебраически замкнутым полем $\Bbbk$ характеристики $\mathrm{char}\,\Bbbk \neq 2$ либо состоит из одного жорданова блока размера d с собственным числом $(-1)^{d-1}$ либо (что возможно только при чётном $d = 2h$) из двух жордановых блоков размера $h = d/2$ с взаимно обратными собственными числами $\lambda, \lambda^{-1} \neq (-1)^{h-1}$.

Доказательство. По сл. 15.1 пространство V либо корневое для $\varkappa$ с собственным числом $+1$ или -1, либо сумма $K_\lambda \oplus K_{\lambda^{-1}}$ двух корневых подпространств одинакового циклового типа с обратными друг другу собственными числами, отличными от ± 1.

Сначала рассмотрим второй случай. Положим $U = K_\lambda$, $W = K_{\lambda^{-1}}$ и обозначим через

$$\eta_U = (\varkappa - \lambda\mathrm{Id})|_U\,, \quad \eta_W = (\varkappa - \lambda^{-1}\mathrm{Id})|_W$$

[1] См. упр. 15.11 на стр. 282.
[2] См. ?? на стр. ??.

нильпотентные составляющие оператора $\varkappa$ на этих подпространствах, а через

$$\eta_U^\times = (\varkappa - \lambda\mathrm{Id})^\times|_W = (\varkappa^{-1} - \lambda\mathrm{Id})|_W = -\lambda\varkappa^{-1}\eta_W = \\ = -\lambda(\lambda^{-1}\mathrm{Id} + \eta_W)^{-1}\eta_W = -(\mathrm{Id} + \lambda\eta_W)^{-1}\eta_W = -\eta_W + \lambda\eta_W^2 - \lambda^2\eta_W^3 + \dots \quad (15\text{-}25)$$

ограничение на W сопряжённого к η_U оператора. Так как оба пространства U, W изотропны, а форма β невырождена, задаваемое ею спаривание[1] $\beta : U \times W \to \Bbbk$ невырождено, и

$$\beta(\eta_U u, w) = \beta(u, \eta_U^\times w)$$

для всех $u \in U, w \in W$. Пусть $\eta_U^n, \eta_W^n = 0$, но $\eta_U^{(n-1)}, \eta_W^{(n-1)} \neq 0$. Тогда $\eta_U^{\times(n-1)} = (-1)^{(n-1)}\eta_W^{(n-1)}$ в силу (15-25), и форма β корректно задаёт невырожденное спаривание

$$\overline{\beta} : \frac{U}{\ker \eta_U^{(n-1)}} \times \frac{W}{\ker \eta_W^{(n-1)}} \to \Bbbk, \quad \overline{\beta}([u],[w]) = \beta(\eta_U^{(n-1)}u, w).$$

Упражнение 15.16. Убедитесь в этом.

В частности, существуют такие $u \in U$ и $w \in W$, что $\beta(\eta_U^{(n-1)}u, w) = 1$. Рассмотрим цепочки

$$0 \leftarrow \eta_U^{n-1}u \leftarrow \dots \leftarrow \eta_U u \leftarrow u \quad \text{и} \quad 0 \leftarrow \eta_W^{(n-1)}w \leftarrow \dots \leftarrow \eta_W w \leftarrow w. \quad (15\text{-}26)$$

Так как $\operatorname{im}\eta_W^{(n-1)} \subset \ker\eta_W$ состоит из собственных для $\varkappa$ векторов с собственным числом λ^{-1},

$$\beta(\eta_W^{(n-1)}w, u) = \beta(u, \varkappa\eta_W^{(n-1)}wu) = \lambda^{-1}\beta(u, \eta_W^{(n-1)}w) = \\ = (-\lambda)^{(n-1)}\beta(u, \eta_U^{\times(n-1)}w) = (-\lambda)^{(n-1)}\beta(\eta_U^{(n-1)}u, w) = (-\lambda)^{(n-1)},$$

и по лем. 15.1 на стр. 284 матрица Грама набора векторов (15-26) состоит из двух нижнеправотреугольных блоков с ненулевыми элементами на побочной диагонали:

$$\left(\begin{array}{ccc|ccc} & & & 0 & & * \\ & 0 & & & \iddots & \vdots \\ & & & * & \cdots & * \\ \hline 0 & & * & & & \\ & \iddots & \vdots & & 0 & \\ * & \cdots & * & & & \end{array}\right)$$

Мы заключаем, что ограничение формы β на линейную оболочку L двух жордановых цепочек (15-26) невырождено. Поэтому $V = L \oplus L^\perp$, и по лем. 15.2 эта сумма биортогональна. Так как V неразложимо, $V = L$, что и утверждалось.

Теперь рассмотрим случай, когда V является корневым пространством оператора $\varkappa$ с собственным числом $\varepsilon = \pm 1$. Как и выше, положим $\eta = \varkappa - \varepsilon\mathrm{Id}$ и обозначим через

$$\eta^\times = -\varepsilon\varkappa^{-1}\eta = -\eta + \varepsilon\eta^2 - \varepsilon\eta^3 + \dots$$

сопряжённый оператор. Пусть $\eta^{n-1} \neq 0$, а $\eta^n = 0$. Тогда $\eta^{\times n-1} = (-1)^{n-1}\eta^{n-1}$, а подпространство $\ker\eta^{n-1}$ является одновременно левым и правым ортогоналом к подпространству

[1] См. лем. 7.2 на стр. 123.

$\operatorname{im}\eta^{\times^{n-1}} = \operatorname{im}\eta^{n-1}$. Поэтому правило $\overline{\beta}([u],[w]) \stackrel{\text{def}}{=} \beta(u,\eta^{n-1}w)$ корректно задаёт невырожденную билинейную форму на факторпространстве $V/\ker\eta^{n-1}$. Поскольку $\operatorname{im}\eta^{n-1} \subset \ker\eta$ состоит из собственных векторов оператора $\varkappa$ с собственным числом ε,

$$\overline{\beta}([u],[w]) = \beta(u,\eta^{n-1}w) = \beta(\eta^{\times^{n-1}}u,w) = (-1)^{n-1}\beta(\eta^{n-1}u,w) = \\ = (-1)^{n-1}\beta(w,\varkappa\eta^{n-1}u) = (-1)^{n-1}\varepsilon\beta(w,\eta^{n-1}u) = (-1)^{n-1}\varepsilon\overline{\beta}([w],[u])\,.$$

Мы заключаем, что форма $\overline{\beta}$ симметрична при $\varepsilon = (-1)^{n-1}$ и кососимметрична при $\varepsilon = (-1)^n$. По теор. 15.1 на стр. 280 в первом случае она изометрически изоморфна евклидовой форме из прим. 15.1 на стр. 275, во втором — симплектической форме из прим. 15.3 на стр. 275.

В первом случае существует такой вектор $u \in V$, что $\beta(\eta^{n-1}u,u) = 1$, и по лем. 15.1 на стр. 284 матрица Грама векторов жордановой цепочки

$$0 \overset{\eta}{\leftarrow} \eta^{n-1}u \overset{\eta}{\leftarrow} \ldots \overset{\eta}{\leftarrow} \eta u \overset{\eta}{\leftarrow} u$$

нижнеправотреугольная с ненулевыми элементами на побочной диагонали

$$\begin{pmatrix} 0 & & * \\ & \iddots & \vdots \\ * & \cdots & * \end{pmatrix}.$$

Поэтому ограничение формы β на линейную оболочку U этой жордановой цепочки невырождено, и $V = U \oplus U^{\perp}$, где $U^{\perp} = {}^{\perp}U$ по лем. 15.2. Так как V неразложимо, $V = U$ является одним жордановым блоком размера n с собственным числом $(-1)^{n-1}$.

Во втором случае существуют такие векторы $u, w \in V$, что $\beta(\eta^{n-1}u,w) = -\beta(\eta^{n-1}w,u) = 1$, а $\beta(\eta^{n-1}u,u) = \beta(\eta^{n-1}w,w) = 0$ в точности также, как в разобранном выше случае двух различных обратных другу собственных чисел. Мы заключаем, что V линейно порождается двумя жордановыми цепочками (15-26) с одинаковым собственным числом $(-1)^{(n-1)}$. □

Следствие 15.2
Невырожденные неразложимые билинейные формы на конечномерных векторных пространствах над алгебраически замкнутым полем $\Bbbk$ характеристики отличной от двух с точностью до изометрического изоморфизма исчерпываются n-мерными формами U_n из прим. 15.6 на стр. 281 и $2n$-мерными формами $W_n(\lambda)$ с $\lambda \neq (-1)^{n-1}$ из прим. 15.5 на стр. 280. Все эти формы попарно не изометричны друг другу. □

Следствие 15.3
Обратимый линейный оператор над алгебраически замкнутым полем $\Bbbk$ характеристики отличной от двух является каноническим оператором невырожденной билинейной формы если и только если все его элементарные делители $(t-\lambda)^m$ с $\lambda \neq \pm 1$ разбиваются на непересекающиеся пары вида $(t-\lambda)^m$, $(t-\lambda^{-1})^m$ и при каждом $k \in \mathbb{N}$ количества элементарных делителей $(t-1)^{2k}$ и $(t+1)^{2k-1}$ оба чётны. □

Задачи для самостоятельного решения к §15

Задача 15.1. Приведите пример билинейной формы β с $\ker {}^\wedge\beta \neq \ker \beta^\wedge$.

Задача 15.2. Приведите пример пространства с невырожденной билинейной формой и такого подпространства U в нём, что ограничение формы на U невырождено и ${}^\perp U \neq U^\perp$.

Задача 15.3. Приведите пример билинейной формы $\beta : V \times V \to \Bbbk$ и такого подпространства $U \subset V$, что $V = U \oplus \ker \beta^\wedge$, но ограничение формы β на U вырождено.

Задача 15.4. Пусть для любых двух векторов $u, w \in V$ равенства $\beta(u, w) = 0$ и $\beta(w, u) = 0$ равносильны друг другу. Покажите, что форма β симметрична или кососимметрична.

Задача 15.5. Покажите, что у всех невырожденных неразложимых билинейных форм симметричная часть $\beta_+ = (\beta + \beta^t)/2$ или кососимметричная часть $\beta_- = (\beta - \beta^t)/2$ тоже невырождена. Верно ли это для произвольной невырожденной формы?

Задача 15.6. Покажите, что ранг любой кососимметричной формы чётен.

Задача 15.7. Пусть билинейная форма на пространстве V ограничивается в невырожденную форму на конечномерном подпространстве $U \subset V$. Постройте изометрический изоморфизм между ${}^\perp U$ и $U^\perp$.

Задача 15.8 (характеристический многочлен). Пусть билинейная форма β на n-мерном пространстве имеет в некотором базисе матрицу Грама B. Многочлен

$$\chi_\beta(t_0, t_1) \stackrel{\text{def}}{=} \det\left(t_1 B - t_0 B^t\right) \in \Bbbk[t_0, t_1]$$

называется *характеристическим многочленом* формы β. Форма β называется *регулярной*, если он ненулевой, и в этом случае точки $\lambda \in \mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$, на которых он зануляется, называются *характеристическими числами*[1] формы β. Покажите, что

а) $\chi_\beta(t_1, t_0) = (-1)^n \chi_\beta(t_0, t_1)$

б) с точностью до умножения на ненулевую константу χ_β не зависит от выбора базиса

в) форма регулярна если и только если $\ker {}^\wedge\beta \cap \ker \beta^\wedge = 0$

г) изометрически изоморфные регулярные формы имеют одинаковые собственные числа

д) отличные от 0 и 1 собственные числа регулярной формы разбиваются на пары λ, λ^{-1} одинаковой кратности.

е) Как связаны собственные числа невырожденной формы и её канонического оператора?

Задача 15.9 ((анти)самомопряжённые операторы). Докажите, что

а) если подпространство U переводится в себя (анти)самосопряжённым оператором, то и оба его ортогонала $U^\perp$, ${}^\perp U$ тоже переходят в себя

б) корневые подпространства[2] K_λ и K_μ самосопряжённого (соотв. антисамосопряжённого) оператора биортогональны друг другу при $\lambda \neq \mu$ (соотв. при $\lambda \neq -\mu$)

в) невырожденный оператор f самосопряжён если и только если отвечающая ему билинейная форма $\beta_f(u, w) = \beta(u, fw)$ имеет такой же канонический оператор, как и форма β.

Задача 15.10 (преобразования Кэли). Покажите, что на пространстве с невырожденной билинейной формой имеются (нелинейные) биекции между множеством антисамосопряжённых

[1] Обратите внимание, что они принимают значения в $\Bbbk \sqcup \infty$.

[2] См. n° 12.3 на стр. 223.

операторов $f : V \to V$, спектр[1] которых не содержит -1, и множеством изометрических операторов g, спектр которых не содержит а) -1 б) $+1$, где первая биекция действует по правилу $f \mapsto (\mathrm{Id} - f)(\mathrm{Id} + f)^{-1}$, а обратная к ней — по правилу $g \mapsto (\mathrm{Id} - g)(\mathrm{Id} + g)^{-1}$, а вторая биекция действует по правилу $f \mapsto -(\mathrm{Id} - f)(\mathrm{Id} + f)^{-1}$, а обратная — по правилу $g \mapsto (\mathrm{Id} + g)(\mathrm{Id} - g)^{-1}$.

Задача 15.11. Покажите, что изометрический оператор на пространстве с невырожденной билинейной формой подобен своему обратному.

Задача 15.12. Уточните сл. 15.1 на стр. 285: докажите, что в условиях леммы при $\lambda \neq \pm 1$ оба корневых подпространства K_λ, $K_{\lambda^{-1}}$ являются жордановыми блоками[2] одинакового размера.

Задача 15.13. Билинейная форма $\mathbb{C}^3 \times \mathbb{C}^3 \to \mathbb{C}$ имеет в стандартном базисе матрицу Грама

$$\begin{pmatrix} 10 & 1 & 20 \\ 5 & 3 & 1 \\ 6 & -8 & 43 \end{pmatrix}.$$

Существует ли в $\mathbb{C}^3$ такой базис, где эта форма имеет матрицу Грама

а) $\begin{pmatrix} 7 & -11 & 20 \\ -13 & 21 & -35 \\ 14 & -21 & 44 \end{pmatrix}$ б) $\begin{pmatrix} 6 & -5 & 7 \\ -3 & 3 & -4 \\ 5 & -5 & 7 \end{pmatrix}$?

Задача 15.14 (форма Эйлера). Обозначим через $D = \frac{d}{dt} : \mathbb{Q}[t] \to \mathbb{Q}[t]$ оператор дифференцирования. Рассмотрим факторалгебру $V = \mathbb{Q}[D]/(D^{n+1})$ и отождествим двойственное к ней пространство V^* с пространством $\mathbb{Q}[t]_{\leqslant n}$ многочленов степени не выше n при помощи невырожденного спаривания из прим. 7.10 на стр. 124: свёртка $\langle f(t), \varphi(D) \rangle$ равна значению многочлена[3] $\varphi(D)f$ в нуле. Положим[4] $\gamma_n(t) = \binom{t+n}{n} = (t+1)\dots(t+n)/n! \in V^*$ и зададим на V билинейную *форму Эйлера*

$$h(\varphi, \psi) \stackrel{\text{def}}{=} \langle \gamma_n(t), \varphi(D)\psi(-D) \rangle. \tag{15-27}$$

Напишите матрицу Грама формы Эйлера базисе из операторов сдвига[5] $1, T, \dots, T^n$, где

$$T = e^D : f(t) \mapsto f(t+1),$$

убедитесь, что она невырождена, и покажите, что

а) канонический оператор формы Эйлера $\varkappa_h = T^{-(n+1)} : f(t) \mapsto f(t-n-1)$

б) форма Эйлера изометрически изоморфна над $\mathbb{C}$ форме U_{n+1} из прим. 15.6 на стр. 281.

Задача 15.15 (полуортонормальные базисы). Набор векторов $\boldsymbol{e} = (e_1, \dots, e_k)$ в пространстве с билинейной формой называется *исключительным* или *полуортонормальным*, если его матрица Грама верхняя унитреугольная, т. е. $\beta(e_i, e_i) = 1$ при всех i и $\beta(e_i, e_j) = 0$ при $i > j$. Операции L_i и R_i заменяют пару соседних векторов e_i, e_{i+1} такого набора парами $(L_{e_{i-1}} e_i, e_{i-1})$ и $(e_i, R_{e_i} e_{i-1})$, в которых

$$L_{e_{i-1}} e_i = e_i - \beta(e_{i-1}, e_i) \cdot e_{i-1} \quad \text{и} \quad R_{e_i} e_{i-1} = e_{i-1} - \beta(e_{i-1}, e_i) \cdot e_i,$$

[1] См. ?? на стр. ??.

[2] Т. е. в каждом имеется ровно одна жорданова цепочка.

[3] Т. е. результата применения дифференциального оператора $\varphi(D)$ к многочлену f, см. форм. (4-21) на стр. 71.

[4] Ср. с зад. 6.8 на стр. 112.

[5] См. прим. 4.9 на стр. 72.

а все прочие векторы оставляют без изменений. Покажите, что:

а) наборы $L_i(\boldsymbol{e})$ и $R_i(\boldsymbol{e})$ исключительны

б) $L_iR_i = R_iL_i = \mathrm{Id}$, $L_iL_j = L_jL_i$ при $|i-j| \geqslant 2$ и $L_iL_{i+1}L_i = L_{i+1}L_iL_{i+1}$

в*) Есть гипотеза, что все исключительные базисы формы Эйлера на $\mathbb{Z}$-модуле $\mathbb{Z}[\nabla]/(\nabla^{n+1})$ из зад. 7.25 на стр. 130 получаются друг из друга при помощи целочисленных изометрических автоморфизмов, операций L_i, R_i и замен базисных векторов на противоположные. В настоящее время эта гипотеза доказана только для $n \leqslant 3$.

Задача 15.16 (уравнение Маркова). Пусть несимметричная $\mathbb{Z}$-билинейная форма $\beta : \mathbb{Z}^3 \times \mathbb{Z}^3 \to \mathbb{Z}$ имеет в стандартном базисе единичный определитель Грама, а её $\mathbb{C}$-билинейное продолжение до формы $\beta_{\mathbb{C}} : \mathbb{C}^3 \times \mathbb{C}^3 \to \mathbb{C}$ на координатном пространстве $\mathbb{C}^3 \supset \mathbb{Z}^3$ неразложимо. Покажите, что

а) форма $\beta_{\mathbb{C}}$ изометрически изоморфна над $\mathbb{C}$ форме U_3 из прим. 15.6 на стр. 281

б) определитель Грама формы β равен 1 в любом базисе модуля $\mathbb{Z}^3$

в) если матрица Грама формы β в некотором базисе модуля $\mathbb{Z}^3$ имеет вид

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix},$$

то $x = 3a$, $y = 3b$ и $z = 3c$, где $a, b, c \in \mathbb{Z}$ удовлетворяют *уравнению Маркова*[1]

$$a^2 + b^2 + c^2 = 3abc \tag{15-28}$$

г) все натуральные решения (a, b, c) уравнения (15-28) получаются из решения $(1, 1, 1)$ преобразованиями, заменяющими одно из чисел a, b, c на другой корень уравнения (15-28), рассматриваемого как квадратное уравнение на соответствующую букву: из каждого решения (a, b, c) получаются ещё три решения $(3bc - a, b, c)$, $(a, 3ac - b, c)$, $(a, b, 3ab - c)$

д) любой исключительный базис модуля $\mathbb{Z}^3$ при помощи преобразований из зад. 15.15 и смены направлений базисных векторов на противоположные преобразуется в исключительный базис с матрицей Грама

$$\begin{pmatrix} 1 & 3 & 6 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix},$$

совпадающий с матрицей Грама формы Эйлера[2] на $\mathbb{Z}[\nabla]/(\nabla^3)$ из зад. 15.14 на стр. 289 в базисе из операторов сдвига $1, T, T^2$.

е*) Знаменитая *гипотеза Маркова* утверждает, что для натуральных решений

$$a_1 \geqslant b_1 \geqslant c_1 \quad \text{и} \quad a_2 \geqslant b_2 \geqslant c_2$$

уравнения (15-28) равенство $a_1 = a_2$ влечёт за собою равенства $b_1 = b_2$ и $c_1 = c_2$, т. е. что тройка натуральных решений уравнения Маркова однозначно определяется своим максимальным элементом. Вопрос открыт более 130 лет.

---

[1] Подсказка: вычислите след канонического оператора и воспользуйтесь тем, что над $\mathbb{C}$ форма изометрически изоморфна U_3.

[2] Что доказывает гипотезу из зад. 15.15 для $n = 2$, а также показывает, что форма Эйлера — единственная с точностью до изометрии неразложимая над $\mathbb{C}$ билинейная форма на $\mathbb{Z}^3$ с единичным определителем Грама, которая обладает исключительным базисом над $\mathbb{Z}$.

§16. Симметричные и кососимметричные формы

16.1. Симметричность и кососимметричность. Билинейная форма $\beta : V \times V \to \Bbbk$ называется *симметричной*, если $\beta(u, w) = \beta(w, u)$ для всех $u, w \in V$. Это равносильно равенству $\beta^\wedge = {}^\wedge\beta$ её правой и левой корреляций[1] и тому, что канонический оператор[2] $\varkappa_\beta = \mathrm{Id}_V$ тождественный.

Билинейная форма $\omega : V \times V \to \Bbbk$ называется *кососимметричной*, если $\omega(v, v) = 0$ для всех $v \in V$. Полагая $v = u + w$, заключаем, что

$$0 = \omega(u + w, u + w) = \omega(u, w) + \omega(w, u)\,,$$

откуда $\omega(u, w) = -\omega(w, u)$ для всех $u, w \in V$. Это свойство называется *знакопеременностью* и равносильно равенствам ${}^\wedge\omega = -\omega^\wedge$ и $\varkappa_\omega = -\mathrm{Id}_V$. Если $\mathrm{char}\,\Bbbk \neq 2$, то знакопеременность эквивалентна кососимметричности. Над полем характеристики 2 знакопеременность не отличается от симметричности и является строго более слабым требованием, чем кососимметричность.

Упражнение 16.1. Приведите пример знакопеременной не кососимметричной формы.

На языке матриц симметричность формы β означает, что её матрица Грама B в каком-нибудь (а значит, и в любом) базисе удовлетворяет равенству $B^t = B$, знакопеременность означает равенство $B^t = -B$, а кососимметричность дополнительно[3] означает, что все элементы на главной диагонали матрицы B нулевые. Матрицы с перечисленными свойствами называются, соответственно, *симметричными*, *знакопеременными* и *кососимметричными*.

Упражнение 16.2. Найдите размерности пространств симметричных и кососимметричных билинейных форм на n-мерном векторном пространстве.

16.1.1. Ядро. Левое и правое ядро (косо)симметричной формы β совпадают друг с другом, и подпространство $\ker\beta \stackrel{\text{def}}{=} {}^\perp V = V^\perp = \{u \in V \mid \forall\, v \in V\ \beta(v, u) = \pm\beta(u, v) = 0\}$ называется просто *ядром* формы β.

Предложение 16.1
Ограничение (косо)симметричной формы β на любое дополнительное к ядру подпространство $U \subset V$ невырождено.

Доказательство. Пусть подпространство $U \subset V$ таково, что $V = \ker\beta \oplus U$, а вектор $w \in U$ удовлетворяет для всех $u \in U$ соотношению $\beta(u, w) = 0$. Записывая произвольный вектор $v \in V$ в виде $v = e + u$ с $e \in \ker\beta$, $u \in U$, получаем $\beta(v, w) = \beta(e, w) + \beta(u, w) = 0$, откуда $w \in U \cap \ker\beta = 0$. □

Предложение 16.2
Любая (косо) симметричная билинейная форма β на пространстве V корректно определяет на факторпространстве $V/\ker\beta$ невырожденную билинейную форму $\overline{\beta}$ по формуле

$$\overline{\beta}([u], [w]) \stackrel{\text{def}}{=} \beta(u, w)\,. \tag{16-1}$$

[1] См. n° 15.1.1 на стр. 272.
[2] См. n° 15.4.1 на стр. 279.
[3] Это требование действительно дополнительное только когда $\mathrm{char}\,\Bbbk = 2$.

Доказательство. Если $[u]=[u']$, а $[w]=[w']$, то векторы $u-u'$ и $w-w'$ лежат в $\ker\beta$ и имеют нулевые левые и правые скалярные произведения с любым вектором. Поэтому

$$\overline{\beta}([u'],[w'])=\beta(u',w')=\beta\big(u+(u'-u),w+(w'-w)\big)=\beta(u,w)=\overline{\beta}([u],[w])\,,$$

что доказывает корректность формулы (16-1). Пусть класс $[u]\in V/\ker\beta$ имеет нулевое скалярное произведение $\overline{\beta}([u],[w])=0$ со всеми классами $[w]\in V/\ker\beta$. По определению формы $\overline{\beta}$ это означает, что $\beta(u,w)=0$ для всех $w\in U$, откуда $u\in\ker\beta$ и $[u]=0$. □

Предостережение 16.1. Для не(косо)симметричной формы левое и правое ядра $\ker({}^\vee\beta)$ и $\ker(\beta^\vee)$ могут быть различны, и в этом случае аналогичные предл. 16.1 и предл. 16.2 утверждения про правое или левое ядро, вообще говоря, неверны[1], а рассуждение, использованное в доказательстве предл. 16.1, устанавливает импликацию $V=U\oplus V^\perp\ \Rightarrow\ {}^\perp U\subset{}^\perp V$.

16.1.2. Ортогоналы и проекции. Если форма $\beta: V\times V\to\Bbbk$ (косо)симметрична, то левый и правый ортогоналы[2] к любому подпространства $U\subset V$ совпадают друг с другом и обозначаются

$$U^\perp=\{w\in V\mid\forall\,u\in U\ \beta(w,u)=\pm\beta(u,w)=0\}\,.$$

Если ограничение формы β на подпространство $U\subset V$ невырождено, то $V=U\oplus U^\perp$ по предл. 15.4 на стр. 278, и подпространство $U^\perp$ называется в этом случае *ортогональным дополнением* к подпространству U. Проекция $v_U\in U$ вектора $v\in V$ на U вдоль $U^\perp$ называется *ортогональной проекцией* на U. Она однозначно характеризуется тем, что $\beta(u,v)=\beta(u,\pi_U v)$ для всех $u\in U$ и вычисляется по форм. (15-16) на стр. 278:

$$v_U=\sum_{i=1}^n\beta(v,u_i^\vee)\,u_i=\sum_{i=1}^n\beta\left(u_i,v\right)\,u_i^\vee\,,\tag{16-2}$$

где $u_1,\dots,u_n$ — любой базис в U, а $u_1^\vee,\dots,u_n^\vee$ — (правый) двойственный[3] к нему относительно формы β базис.

Если форма β невырождена на всём пространстве V, то по предл. 15.3 на стр. 278

$$\dim U^\perp=\dim V-\dim U\quad\text{и}\quad U^{\perp\perp}=U$$

для всех подпространств $U\subset V$. Такая форма ограничивается в невырожденную форму на подпространстве $U\subset V$ если и только если она невырождено ограничивается на $U^\perp$.

Теорема 16.1 (теорема Лагранжа)
Каждое конечномерное векторное пространство с симметричной билинейной формой β над произвольным полем $\Bbbk$ с $\operatorname{char}\Bbbk\neq 2$ обладает базисом с диагональной матрицей Грама.

[1] См. зад. 15.3 на стр. 288.
[2] См. n° 15.3 на стр. 278.
[3] Если форма симметрична, то правый и левый двойственные базисы (см. n° 15.2.1 на стр. 276) совпадают друг с другом, и порядок сомножителей в скалярных произведениях в формуле (16-2) не важен. Если форма кососимметрична, левый и правый двойственные базисы получаются друг из друга умножением на -1 и порядок сомножителей существен.

Доказательство. Если $\dim V = 1$ или форма β нулевая, то матрица Грама любого базиса диагональна. Если форма β ненулевая, то найдётся вектор $e \in V$ с $\beta(e,e) \neq 0$, ибо иначе

$$\beta(u,w) = \big(\beta(u+w,u+w) - \beta(u-w,u-w)\big)/4 = 0$$

для всех $u, w \in V$. Зафиксируем e в качестве первого вектора искомого базиса. Поскольку ограничение формы β на одномерное подпространство $U = \Bbbk \cdot e$ невырождено, $V = U \oplus U^\perp$. По индукции, в $U^\perp$ есть базис с диагональной матрицей Грама. Дописывая его к e, получаем требуемый базис в V. □

Следствие 16.1
Над алгебраически замкнутым полем $\Bbbk$ характеристики $\mathrm{char}(\Bbbk) \neq 2$ две симметричные билинейные формы изометрически изоморфны если и только если их матрицы Грама имеют одинаковый ранг.

Доказательство. Над алгебраически замкнутым полем ненулевые диагональные элементы матрицы Грама можно сделать единичными, заменив базисные векторы e_i на $e_i/\sqrt{\beta(e_i,e_i)}$. □

Теорема 16.2 (теорема Дарбу)
Над произвольным полем $\Bbbk$ любой характеристики всякое конечномерное векторное пространство V с невырожденной кососимметричной формой ω изометрически изоморфно симплектическому пространству из прим. 15.3 на стр. 275. В частности, $\dim V$ чётна.

Доказательство. Построим в V базис, матрица Грама которого состоит из расположенных на главной диагонали 2×2-блоков вида

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{16-3}$$

В качестве первого базисного вектора возьмём произвольный ненулевой вектор $e_1 \in V$. Так как форма ω невырождена, найдётся такой вектор $w \in V$, что $\omega(e_1,w) = a \neq 0$. Положим $e_2 = w/a$. Поскольку $\omega(e_1,e_1) = 0$, векторы e_1 и e_2 не пропорциональны и порождают двумерное подпространство $U \subset V$. Матрица Грама ограничения формы ω на это подпространство в базисе e_1, e_2 имеет вид (16-3). Так как ограничение формы ω на U невырождено, $V = U \oplus U^\perp$ и ограничение формы ω на $U^\perp$ тоже невырождено. Индукция по $\dim V$ позволяет считать, что в подпространстве $U^\perp$ требуемый базис уже имеется. Добавляя к нему e_1, e_2, получаем искомый базис e_1, e_2, … , e_{2k-1}, e_{2k} в $V = U \oplus U^\perp$. Симплектический базис формы ω получается из построенного перестановкой векторов: сначала надо написать подряд все векторы с нечётными номерами, а потом — с чётными. □

16.2. Сопряжение операторов. Всюду в этом разделе мы предполагаем, что билинейная форма $\beta : V \times V \to \Bbbk$ невырождена и (косо)симметрична. Каждый линейный оператор $f : V \to V$ на пространстве с такой формой обладает двусторонне сопряжённым[1] оператором $f^\times : V \to V$, который однозначно задаётся тем, что для всех $u, w \in V$

$$\beta(fu,w) = \beta(u,f^\times w) \quad \text{и} \quad \beta(f^\times u,w) = \beta(u,fw) \tag{16-4}$$

[1] См. n° 15.4.2 на стр. 281.

(в силу (косо)симметричности формы выполнение одного из этих равенств для всех $u, w \in V$ влечёт выполнение другого). Сопряжение $f \leftrightarrow f^\times$ является линейным инволютивным[1] антиавтоморфизмом[2] алгебры $\operatorname{End} V$, которая таким образом раскладывается (как векторное пространство) в прямую сумму

$$\operatorname{End}(V) = \operatorname{End}_+(V) \oplus \operatorname{End}_-(V)$$

пространства *самосопряжённых* операторов

$$\operatorname{End}_+(V) \stackrel{\text{def}}{=} \{\varphi \in \operatorname{End}(V) \mid \forall\, u, w \in V\ \beta(fu, w) = \beta(u, fw)\}$$

и пространства *антисамосопряжённых* операторов

$$\operatorname{End}_-(V) \stackrel{\text{def}}{=} \{\varphi \in \operatorname{End}(V) \mid\ \forall\, u, w \in V\ \beta(fu, w) = -\beta(u, fw)\}\,,$$

которые являются собственными подпространствами инволюции $f \leftrightarrow f^\times$ с собственными числами $+1$ и -1. На языке матриц соотношение (16-4) переписывается в виде[3] $F^t B = BF^\times$, где $F^\times$ и F — матрицы операторов $f^\times$ и f в одном и том же (произвольном) базисе, а B — матрица Грама скалярного произведения в этом базисе. Самосопряжённость и антисамосопряжённость оператора f означают, соответственно, что матрицы F и B связаны соотношением

$$F^t B = BF \quad \text{и} \quad F^t B = -BF\,. \tag{16-5}$$

Если форма β симметрична, то сопоставление оператору $f : V \to V$ билинейной формы[4]

$$\beta_f : V \times V \to \Bbbk\,, \quad \beta_f(u, w) = \beta(u, fw)$$

задаёт изоморфизм пространства $\operatorname{End}_+(V)$ с пространством симметричных билинейных форм, а пространства $\operatorname{End}_-(V)$ — с пространством кососимметричными форм[5], так как для $f \in \operatorname{End}_\pm(V)$

$$\beta_f(u, w) = \beta(u, fw) = \pm\beta(fu, w) = \pm\beta(w, fu) = \pm\beta_f(w, u).$$

Если форма β кососимметрична, картина зеркальная — $\operatorname{End}_+(V)$ отождествляется с кососимметричными билинейными формами, а $\operatorname{End}_-(V)$ — с симметричными:

$$\beta_f(u, w) = \beta(u, fw) = \pm\beta(fu, w) = \mp\beta(w, fu) = \mp\beta_f(w, u)\,,$$

где верхние знаки отвечают самосопряжённым операторам, а нижние — антисамосопряжённым.

Лемма 16.1
Если (анти)самосопряжённый оператор $f : V \to V$ переводит подпространство $U \subset V$ в себя, то и его ортогонал $U^\perp$ тоже переходит в себя.

Доказательство. Пусть $w \in U^\perp$, т. е. $\beta(u, w) = 0$ для всех $u \in U$. Тогда $\beta(u, fw) = \pm\beta(fu, w) = 0$ для всех $u \in U$, ибо $fu \in U$. Тем самым, $fw \in U^\perp$. □

[1] Т. е. $f^{\times\times} = f$, см. упр. 15.10 на стр. 282.
[2] Т. е. $(fg)^\times = g^\times f^\times$, см. n° 15.4.2 на стр. 281.
[3] См. формулу (15-23) на стр. 282.
[4] См. n° 15.4 на стр. 279.
[5] Если $\operatorname{char} \Bbbk \neq 2$.

Лемма 16.2
Корневые подпространства K_λ и K_μ самосопряжённого (соотв. антисамосопряжённого) оператора ортогональны друг другу при $\lambda \neq \mu$ (соотв. при $\lambda \neq -\mu$).

Доказательство. Пусть $f\colon V \to V$ (анти)самосопряжён относительно симметричной формы β. Достаточно убедиться, что при $\lambda \neq \mu$ (соотв. при $\lambda \neq -\mu$) равенства

$$(f - \lambda\mathrm{Id})^\ell u = 0 \quad \text{и} \quad (f - \mu\mathrm{Id})^m w = 0$$

влекут равенство $\beta(u, w) = 0$. Воспользуемся индукцией по $\ell + m$. Если $\ell = 0$, то $u = 0$, а если $m = 0$, то $w = 0$. При $\ell, m \geqslant 1$ можно по индукции считать, что векторы $u' = (f - \lambda\mathrm{Id})\,u$ и $w' = (f - \mu\mathrm{Id})\,w$, для которых $(f - \lambda\mathrm{Id})^{\ell-1}u' = 0$ и $(f - \mu\mathrm{Id})^{m-1}w' = 0$, удовлетворяют равенствам $\beta(u', w) = 0 = \beta(u, w')$, откуда $\beta(fu, w) = \lambda\,\beta(u, w)$ и $\beta(u, fw) = \mu\,\beta(u, w)$. Так как $\beta(fu, w) = \pm\beta(u, fw)$, мы заключаем, что $(\lambda \mp \mu)\,\beta(u, w) = 0$, где верхние знаки отвечают самосопряжённому оператору, а нижние — антисамосопряжённому. □

Замечание 16.1. Обе предыдущие леммы и их доказательства остаются в силе и для несимметричных невырожденных билинейных форм, см. зад. 15.9 на стр. 288.

Пример 16.1 (самосопряжённые операторы на евклидовом пространстве)
Покажем, что каждый самосопряжённый оператор f на конечномерном вещественном евклидовом пространстве V диагонализуем в подходящем ортонормальном базисе пространства V. Это тривиально, когда $\dim V = 1$. Если $\dim V = 2$, матрица F оператора f в произвольно выбранном ортонормальном базисе симметрична в силу (16-5). Пусть

$$F = \begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

При $b = 0$ она уже диагональна. При $b \neq 0$ характеристический многочлен оператора f

$$\det(tE - F) = t^2 - (a + c) \cdot t + (ac - b^2)$$

имеет положительный дискриминант $(a + c)^2 - 4(ac - b^2) = (a - c)^2 + 4b^2$ и, тем самым, два разных вещественных корня λ, μ. Отвечающие им ненулевые собственные векторы u и w перпендикулярны по лем. 16.2. Деля каждый из векторов на его длину, получаем искомый ортонормальный базис. Пусть $\dim V \geqslant 3$. Согласно прим. 12.5 на стр. 222 у оператора f есть одномерное или двумерное инвариантное подпространство $U \subset V$. Его ортогональное дополнение $U^\perp$ тоже f-инвариантно по лем. 16.1. Применяя индукцию по $\dim V$, можно считать, что в U и $U^\perp$ есть ортонормальные базисы из собственных векторов оператора F. Объединение этих базисов даёт искомый базис в V.

На геометрическом языке установленный нами факт означает, что каждый самосопряжённый оператор f растягивает евклидово пространство в перпендикулярных друг другу направлениях. Эти направления называются *нормальными* или *главными* осями оператора f.

16.3. (Анти)самосопряжённые операторы над замкнутым полем. Всюду в этом разделе мы предполагаем, что основное поле $\Bbbk$ алгебраически замкнуто и $\operatorname{char}\Bbbk \neq 2$. Через $\beta\colon V \times V \to \Bbbk$ по-прежнему обозначается невырожденная (косо)симметричная билинейная форма.

Предложение 16.3
Пусть операторы $f, g : V \to V$ оба самосопряжены, или оба антисамосопряжены, или оба являются изометриями формы β. Если f и g подобны, то они изометрически подобны, т. е. существует такая изометрия $\psi \in \mathrm{O}_\beta(V)$, что $g = \psi f \psi^{-1}$.

Доказательство. Пусть $g = \varphi f \varphi^{-1}$ для некоторого $\varphi \in \mathrm{GL}(V)$. Тогда $g^\times = {\varphi^{-1}}^\times f^\times \varphi^\times$.

Упражнение 16.3. Убедитесь, что во всех трёх перечисленных в условии случаях последнее равенство переписывается в виде $g = {\varphi^{-1}}^\times f \varphi^\times$.

Поэтому $f = \varphi^\times g \varphi^{\times -1} = (\varphi^\times \varphi)\, f\, (\varphi^\times \varphi)^{-1}$, т. е. самосопряжённый оператор $\varphi^\times \varphi$ коммутирует с f. Любой многочлен от $\varphi^\times \varphi$ тоже самосопряжён и коммутирует с f. В прим. 12.9 на стр. 227 мы видели, что существует такой многочлен $p(t) \in \Bbbk[t]$, что оператор $\tau = p(\varphi^\times \varphi)$ имеет $\tau^2 = \varphi^\times \varphi$. Положим $\psi = \varphi \tau^{-1} = \varphi^{\times -1} \tau$. Так как τ самосопряжён, $\psi^\times = \psi^{-1}$, т. е. ψ — изометрия, а поскольку τ и f коммутируют, $\psi f \psi^{-1} = \varphi \tau f \tau^{-1} \varphi^{-1} = \varphi f \varphi^{-1} = g$. □

Упражнение 16.4. Обозначим через

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & 0 & \ddots & 1 \\ & & & \lambda \end{pmatrix} \quad \text{и} \quad Z_n \stackrel{\text{def}}{=} \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix} \tag{16-6}$$

жорданову клетку и матрицу с единицами на побочной диагонали и нулями в остальных местах. Убедитесь, что оператор с матрицей $J_n(\lambda)$ в базисе с матрицей Грама Z_n самосопряжён.

Следствие 16.2
Если невырожденная билинейная форма $\beta : V \to V$ симметрична, а оператор $f : V \to V$ самосопряжён, то V является прямой ортогональной суммой подпространств, на каждом из которых в подходящем базисе матрица оператора и матрица Грама формы суть матрицы $J_n(\lambda)$ и Z_n из формулы (16-6), и $J_n(\lambda)$ пробегает все жордановы клетки оператора f.

Доказательство. Так как все невырожденные симметричные формы изометрически изоморфны[1], в пространстве V есть базис $\boldsymbol{e}$ с блочно диагональной матрицей Грама, состоящей из блоков Z_n, размеры которых биективно соответствуют размерам жордановых клеток $J_n(\lambda)$ оператора f. Рассмотрим оператор $g : V \to V$, матрица которого в базисе $\boldsymbol{e}$ состоит их жордановых блоков $J_n(\lambda)$. По упр. 16.4 оператор g самосопряжён. По построению он подобен f. По предл. 16.3 существует такая изометрия $\psi : V \to V$, что $f = \psi g \psi^{-1}$. В базисе $\psi(\boldsymbol{e})$ оператор f имеет ту же матрицу, что g имеет в базисе $\boldsymbol{e}$. □

Упражнение 16.5. Пусть матрица F линейного оператора f в некотором базисе и матрица Грама B этого базиса имеют размер $2n \times 2n$ и вид

$$F = \begin{pmatrix} J_n(\lambda) & 0 \\ 0 & -J_n(\lambda) \end{pmatrix}, \quad B = Z_{2n} \tag{16-7}$$

[1] См. теор. 15.1 на стр. 280.

или размер $n \times n$, где n нечётно, и вид

$$F = \begin{pmatrix} 0 & 1 & & & & \\ & 0 & -1 & & 0 & \\ & & 0 & 1 & & \\ & & & \ddots & \ddots & \\ & 0 & & & 0 & -1 \\ & & & & & 0 \end{pmatrix}, \quad B = Z_n\,. \tag{16-8}$$

Убедитесь, что в обоих случаях оператор f антисамосопряжён, и при $\lambda = 0$ и нечётном n оператор (16-7) изометрически изоморфен ортогональной сумме двух операторов (16-8).

Следствие 16.3
Если невырожденная билинейная форма $\beta : V \to V$ симметрична, а оператор $f : V \to V$ антисамосопряжён, то V является прямой ортогональной суммой чётномерных подпространств, в подходящем базисе каждого из которых матрица оператора и матрица Грама формы имеют вид (16-7), где при $\lambda = 0$ размер блоков n обязательно чётен, а также нечётномерных подпространств, в подходящем базисе каждого из которых матрица оператора и матрица Грама формы имеют вид (16-8). В частности все жордановы клетки оператора f с ненулевыми собственными числами, а также нильпотентные клетки чётного размера разбиваются на непересекающиеся пары вида $J_m(\lambda), J_m(-\lambda)$.

Доказательство. Достаточно доказать только последнее утверждение, накладывающее ограничение на жорданову нормальную форму оператора f, — всё остальное выводится из него при помощи упр. 16.5 и предл. 16.3 дословно также, как в сл. 16.2. Поскольку корневые подпространства K_λ и K_μ оператора f ортогональны[1] при $\mu \neq -\lambda$, можно считать, что объемлющее пространство либо имеет вид $V = K_\lambda \oplus K_{-\lambda}$, либо $V = K_0$.

Сначала рассмотрим первый случай[2]. Положим $U = K_\lambda$, $W = K_{-\lambda}$ и обозначим через

$$\eta_U = (f - \lambda\mathrm{Id})|_U\,, \quad \eta_W = (f + \lambda\mathrm{Id})|_W$$

нильпотентные составляющие оператора f на этих подпространствах. Поскольку f антисамосопряжён, $\eta^\times|_U = -\eta_U$, а $\eta^\times|_W = -\eta_W$. Так как оба пространства U, W изотропны, а форма β невырождена, задаваемое ею спаривание $\beta : U \times W \to \Bbbk$ невырождено, и

$$\beta(\eta_U^k u, w) = (-1)^k \beta(u, \eta_W^k w)$$

для всех $u \in U$, $w \in W$. Пусть $\eta_U^n, \eta_W^n = 0$, но $\eta_U^{(n-1)}, \eta_W^{(n-1)} \neq 0$. Форма β корректно задаёт невырожденное спаривание[3]

$$\overline{\beta} : \frac{U}{\ker \eta_U^{(n-1)}} \times \frac{W}{\ker \eta_W^{(n-1)}} \to \Bbbk\,, \quad \overline{\beta}([u],[w]) = \beta(\eta_U^{(n-1)} u, w) = (-1)^{n-1}\beta(u, \eta_W^{(n-1)} w)\,.$$

В частности, найдутся такие $u \in U$, $w \in W$, что $\beta(\eta_U^{(n-1)} u, w) = (-1)^{n-1}\beta(u, \eta_W^{(n-1)} w) = 1$. Так как

$$\beta(\eta_U^{(n-k)} u, \eta_W^{(n-\ell)} w) = (-1)^{n-\ell}\beta(\eta_U^{2n-(k+\ell)} u, w) = \begin{cases} 0 & \text{при } k+\ell \leqslant n \\ (-1)^{k-1} & \text{при } k+\ell = n+1\,, \end{cases}$$

[1] См. лем. 16.2 на стр. 295.
[2] Ср. с доказательством теор. 15.2 на стр. 285.
[3] См. упр. 15.16 на стр. 286.

матрица Грама векторов $\eta_U^{n-1}u, \dots, \eta_U u, u, \eta_W^{(n-1)}w, \dots, \eta_W w, w$ состоит из двух нижнеправотреугольных блоков с ненулевыми элементами на побочной диагонали:

$$\left(\begin{array}{ccc|ccc} & & & 0 & & * \\ & 0 & & & \iddots & \vdots \\ & & & * & \cdots & * \\ \hline 0 & & * & & & \\ & \iddots & \vdots & & 0 & \\ * & \cdots & * & & & \end{array}\right).$$

Тем самым, ограничение формы β на линейную оболочку L этих векторов невырождено и $V = L \oplus L^\perp$. Так как ЖНФ ограничения $f|_L$ состоит из двух жордановых клеток $J_n(\pm\lambda)$, это ограничение по предл. 16.3 изометрически изоморфно оператору (16-7).

Теперь рассмотрим случай, когда $V = K_0$ является нильпотентным корневым пространством. Пусть $f^{n-1} \neq 0$, а $f^n = 0$. Тогда на факторпространстве $V / \ker f^{n-1}$ корректно определена невырожденная билинейная форма $\overline{\beta}([u],[w]) \stackrel{\text{def}}{=} \beta(f^{n-1}u, w) = (-1)^{n-1}\beta(u, f^{n-1}w)$, симметричная при нечётном n и кососимметричная при чётном. В первом случае существует такой вектор $u \in V$, что $\beta(f^{n-1}u, u) = 1$ и матрица Грама векторов $f^{n-1}u, \dots, fu, u$ нижнеправотреугольная с ненулевыми элементами на побочной диагонали.

Упражнение 16.6. Убедитесь в этом.

Поэтому ограничение формы β на линейную оболочку L этой жордановой цепочки невырождено, и $V = L \oplus L^\perp$. По предл. 16.3 ограничение $f|_L$ изометрически изоморфно оператору (16-8).

Во втором случае существуют такие векторы $u, w \in V$, что $\beta(f^{n-1}u, w) = -\beta(u, f^{n-1}w) = 1$, а $\beta(f^{n-1}u, u) = \beta(f^{n-1}w, w) = 0$ в точности также, как в разобранном выше случае двух разных различающихся знаком собственных чисел. Мы заключаем, что $V = L \oplus L^\perp$, где $f|_L$ имеет две нильпотентные жордановы клетки одинакового чётного размера и по предл. 16.3 изометрически изоморфен оператору (16-7) с $\lambda = 0$ и чётным n. □

Замечание 16.2. Похожие рассуждения позволяют классифицировать с точностью до изометрического изоморфизма (анти)самосопряжённые операторы и на пространстве с невырожденной кососимметричной формой, а также изометрии невырожденных (косо)симметричных билинейных форм. Подробное изложение этих результатов можно прочитать в обстоятельном учебнике *А. И. Мальцев*, *Основы линейной алгебры*, или воссоздать самостоятельно при помощи зад. 16.7 на стр. 307 ниже.

16.4. Симплектические и гиперболические пространства. Допуская некоторую вольность, которая оправдывается теоремой Дарбу, мы будем далее называть любое пространство с невырожденной кососимметричной формой *симплектическим пространством*, а пространство, изометрически изоморфное гиперболическому пространству из прим. 15.2 на стр. 275, — *гиперболическим пространством*. Симплектические и гиперболические пространства имеют много общего. Удобной бескоординатной моделью обоих пространств является прямая сумма

$$W = U \oplus U^*,$$

где U — произвольное n-мерное векторное пространство. Симплектическая и гиперболическая формы на W задаются, соответственно, равенствами

$$\omega\big((u_1,\xi_1),(u_2,\xi_2)\big) \stackrel{\text{def}}{=} \langle u_1, \xi_2\rangle - \langle u_2, \xi_1\rangle, \tag{16-9}$$

$$\gamma\big((u_1,\xi_1),(u_2,\xi_2)\big) \stackrel{\text{def}}{=} \langle u_1, \xi_2\rangle + \langle u_2, \xi_1\rangle, \tag{16-10}$$

где $\langle u, \xi\rangle = \xi(u) = \mathrm{ev}_u(\xi)$ означает свёртку[1] векторов с ковекторами. В составленном из векторов двойственных друг другу базисов в U и U^* базисе $e_1,\dots,e_n,e_1^*,\dots,e_n^*$ пространства W формы ω и γ имеют матрицы Грама

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \quad \text{и} \quad H = \begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}. \tag{16-11}$$

Базис симплектического (соотв. гиперболического) пространства с матрицей Грама J (соотв. H) называется *симплектическим* (соотв. *гиперболическим*).

Предложение 16.4
В гиперболическом (соотв. симплектическом) пространстве V каждое изотропное подпространство $U \subset V$ содержится в некотором[2] гиперболическом (соотв. симплектическом) подпространстве $W \subset V$ размерности $\dim W = 2\dim U$, и любой базис пространства U дополняется[3] до симплектического базиса в W.

Доказательство. Выберем в U произвольный базис $u_1,\dots,u_m$, дополним его до базиса в V и рассмотрим первые m векторов $u_1^\vee,\dots,u_m^\vee$ двойственного (справа) базиса[4] относительно гиперболической (соотв. симплектической) формы β на V. Тогда

$$\beta(u_i,u_j^\vee) = \begin{cases} 1 & \text{при } i=j \\ 0 & \text{при } i\neq j, \end{cases} \tag{16-12}$$

и эти соотношения не нарушаются при добавлении к любому из векторов $u_j^\vee$ произвольной линейной комбинации векторов u_i. Заменим каждый из векторов $u_j^\vee$ на вектор

$$w_j = u_j^\vee - \sum_{\nu<j} \beta(u_j^\vee,u_\nu^\vee)\,u_\nu.$$

Векторы $w_1,\dots,w_m$ по прежнему удовлетворят равенствам (16-12), но порождают изотропное подпространство, так как для всех $i \geqslant j$ имеем $\beta(w_i,w_j) = \beta(u_i^\vee,u_j^\vee) - \beta(u_i^\vee,u_j^\vee)\beta(u_j,u_j^\vee) = 0$. Мы заключаем, что векторы $u_1,\dots,u_m,w_1,\dots,w_m$ составляют гиперболический (соотв. симплектический) базис своей линейной оболочки. □

Следствие 16.4
Следующие свойства пространства V с невырожденной симметричной билинейной формой эквивалентны друг другу:

[1] См. n° 7.4.2 на стр. 123.
[2] Не единственном.
[3] Вообще говоря, не единственным способом.
[4] См. n° 15.2.1 на стр. 276.

1) V изометрически изоморфно гиперболическому пространству

2) V является прямой суммой двух изотропных подпространств

3) $\dim V$ чётна, и в V имеется изотропное подпространство половинной размерности.

Доказательство. Импликация (1)⇒(2) очевидна. Пусть выполнено (2). Согласно предл. 15.2 на стр. 277 размерность каждого из из двух изотропных прямых слагаемых не превышает половины размерности V, что возможно только если обе эти размерности равны $\frac{1}{2}\dim V$. Тем самым, (2)⇒(3). По предл. 16.4 каждое изотропное подпространство размерности $\frac{1}{2}\dim V$ содержится в гиперболическом подпространстве размерности $\dim V$, которое таким образом совпадает со всем пространством V, что даёт импликацию (3)⇒(1). □

Предложение 16.5 (максимальные изотропные подпространства)
В $2n$-мерном гиперболическом (соотв. симплектическом) пространстве V для каждого n-мерного изотропного подпространства $L \subset V$ найдётся такое n-мерное изотропное подпространство $L' \subset V$, что $V = L \oplus L'$. При этом каждый базис $\boldsymbol{e}$ подпространства L однозначно достраивается некоторым базисом $\boldsymbol{e}'$ в L' до гиперболического (соотв. симплектического) базиса в V. Гиперболическая (соотв. симплектическая) форма β на V корректно задаёт невырожденное спаривание

$$\overline{\beta}\colon (V/L)\times L \to \Bbbk\,, \quad ([w],u)\mapsto \beta(w,u)\,, \tag{16-13}$$

и все дополнительные к L изотропные подпространства L' образуют аффинное пространство[1]: в гиперболическом случае — над векторным пространством

$$\operatorname{Hom}_-(V/L,L) \stackrel{\text{def}}{=} \{f\colon V/L\to L \mid \forall\, u,w\in V\ \overline{\beta}([u],f[w]) = -\overline{\beta}([w],f[u])\}$$

антисамосопряжённых относительно этого спаривания линейных операторов $f\colon L\to V/L$, а в симплектическом случае — над векторным пространством

$$\operatorname{Hom}_+(V/L,L) \stackrel{\text{def}}{=} \{f\colon V/L\to L \mid \forall\, u,w\in V\ \overline{\beta}([u],f[w]) = \overline{\beta}([w],f[u])\}$$

самосопряжённых операторов.

Доказательство. Корректность спаривания (16-13) обеспечивается изотропностью пространства L: $\beta(w+v,u)=\beta(w,u)$ для всех $u,v\in L$, $w\in V$. Невырожденность вытекает по лем. 7.2 на стр. 123 из невырожденности формы β на V и равенства размерностей $\dim L = \dim V/L$. В прим. 13.3 на стр. 236 мы видели, что множество всех дополнительных к L подпространств $L'\subset V$ является аффинным пространством над $\operatorname{Hom}(V/L,L)$, и результатом откладывания вектора $f\colon V/L\to L$ от точки L' является график $\Gamma_f = \{(v,f[v])\in L'\oplus L = V \mid v\in K\}$ линейного отображения $f\colon V/L\simeq L'\to L$. Этот график является изотропным подпространством в V если и только если $\beta(u+f[u],w+f[w])=0$ для всех $u,w\in L'$. Если подпространства L и L' изотропны, то это равенство переписывается как $\beta(u,f[w])\pm\beta(w,f[u])=0$, где знак «+» отвечает симметричной, а «−» — кососимметричной форме β. Остаётся заметить, что дополнительные к L изотропные подпространства L' существуют по предл. 16.4, и базис $\boldsymbol{e}'$ в таком подпространстве L', который дополняет данный базис $\boldsymbol{e}$ в L до симплектического базиса в V, — это прообраз двойственного к $\boldsymbol{e}$ относительно спаривания (16-13) базиса в V/L при изоморфизме $L'\xrightarrow{\sim} V/L$, $v\mapsto[v]$. □

[1] Ср. с прим. 13.3 на стр. 236.

Замечание 16.3. По традиции, изотропные подпространства максимальной размерности n в $2n$-мерном симплектическом пространстве W_{2n} называются *лагранжевыми* подпространствами.

16.5. Симплектическая группа. Линейные изометрии $f: W_{2n} \to W_{2n}$ симплектического пространства W_{2n} называются *симплектическими преобразованиями* и образуют группу[1], которая называется *симплектической группой* пространства W_{2n} и обозначается $\mathrm{Sp}(W_{2n})$. Сопоставление оператору его матрицы в симплектическом базисе изоморфно отображает группу $\mathrm{Sp}(W_{2n})$ на *группу симплектических матриц*

$$\mathrm{Sp}_{2n}(\Bbbk) \stackrel{\text{def}}{=} \{F \in \mathrm{Mat}_{2n}(\Bbbk) \mid F^t \cdot J \cdot F = J\}\,. \tag{16-14}$$

Если в соответствии с разложением $W_{2n} = U \oplus U^*$ записать матрицу F в блочном виде

$$F = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

где $A: U \to U$, $B: U^* \to U$, $C: U \to U^*$, $D: U^* \to U^*$, то равенство $F^t \cdot J \cdot F = J$ примет вид

$$\begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix} \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix},$$

что равносильно трём соотношениям

$$C^tA = A^tC\,, \quad D^tB = B^tD\,, \quad A^tD - C^tB = E\,. \tag{16-15}$$

В частности, группа изометрий лагранжевой плоскости $\mathrm{Sp}_2(\Bbbk) = \mathrm{SL}_2(\Bbbk)$ совпадает со специальной линейной группой, что и не удивительно, поскольку симплектическая форма на $\Bbbk^2$ изометрически изоморфна форме ориентированной площади

$$\det: \Bbbk^2 \times \Bbbk^2 \to \Bbbk\,, \quad u, w \mapsto \det(u, w)\,.$$

Обратите внимание, что изометрии гиперболической плоскости устроены совершенно иначе[2].

Упражнение 16.7. Напишите аналогичные (16-15) соотношения, описывающие группу изометрий $\mathrm{O}(H_{2n})$ гиперболического пространства H_{2n}.

Пример 16.2 (вложение $\mathrm{GL}(U) \hookrightarrow \mathrm{Sp}(W_{2n})$)
Соотношения (16-15) выполняются для блочно диагональных матриц с $AD = E$ и $D = C = 0$. Поэтому имеется инъективный гомоморфизм групп

$$\mathrm{GL}(U) \hookrightarrow \mathrm{Sp}(U \oplus U^*)\,, \quad G \mapsto \begin{pmatrix} G & 0 \\ 0 & G^{t-1} \end{pmatrix}. \tag{16-16}$$

На бескоординатном языке он сопоставляет оператору $g: U \to U$ прямую сумму

$$g \oplus g^{*-1}: U \oplus U^* \to U \oplus U^*\,, \quad (u, \xi) \mapsto (gu, g^{*-1}\xi)\,,$$

где $g^*: U^* \to U^*$ — двойственный[3] к g оператор. По определению двойственного оператора $\langle\, gu\,,\, g^{*-1}\xi\,\rangle = \langle\, g^{-1}gu\,,\, \xi\,\rangle = \langle\, u\,,\, \xi\,\rangle$, т. е. $g \oplus g^{*-1}$ сохраняет свёртку векторов с ковекторами и, тем самым, является изометрией формы (16-9).

[1] См. n° 8.1.4 на стр. 136.
[2] См. прим. 15.4 на стр. 277.
[3] См. n° 7.4.4 на стр. 127.

Упражнение 16.8. Убедитесь, что то же самое правило $g \mapsto g \oplus g^{*-1}$ задаёт вложение

$$\mathrm{GL}(U) \hookrightarrow \mathrm{O}_\gamma(U \oplus U^*)\,.$$

Предложение 16.6
Симплектическая группа $\mathrm{Sp}(W_{2n})$ транзитивно действует на изотропных и на симплектических подпространствах любой фиксированной размерности.

Доказательство. Если $2k$-мерные подпространства $V_1, V_2 \subset W_{2n}$ оба изометрически изоморфны W_{2k}, то их ортогоналы $V_1^\perp, V_2^\perp \subset W_{2n}$ оба изометрически изоморфны $W_{2(n-k)}$. Прямая сумма любых двух изометрических изоморфизмов $V_1 \xrightarrow{\sim} V_2$ и $V_1^\perp \xrightarrow{\sim} V_2^\perp$ даёт изометрический изоморфизм $W_{2n} = V_1 \oplus V_1^\perp \xrightarrow{\sim} V_2 \oplus V_2^\perp = W_{2n}$, переводящий V_1 в V_2.

Если k-мерные подпространства $K_1, K_2 \subset W_{2n}$ оба изотропны, то любой базис $\boldsymbol{u_1}$ в K_1 и любой базис $\boldsymbol{u_2}$ в K_2 дополняются по предл. 16.4 на стр. 299 до состоящих из $2k$ векторов наборов $\boldsymbol{v_1}$ и $\boldsymbol{v_2}$, являющихся симплектическими базисами в своих линейных оболочках V_1 и V_2. Отображая первый набор во второй, мы получаем изометрический изоморфизм $V_1 \xrightarrow{\sim} V_2$, переводящий K_1 в K_2. Беря, как и выше, прямую сумму этого автоморфизма с любым изометрическим изоморфизмом $V_1^\perp \xrightarrow{\sim} V_2^\perp$, получаем изометрический автоморфизм пространства W_{2n}, переводящий V_1 в V_2. □

Замечание 16.4. В сл. 17.1 на стр. 313 ниже мы увидим, что предл. 16.6 справедливо и для группы изометрий любой невырожденной симметричной билинейной формы. Однако доказательство потребует более глубокого изучения таких групп.

16.6. Грассмановы квадратичные формы и пфаффиан. Ненулевой однородный грассманов многочлен[1] второй степени $\omega \in \Lambda^2 V$, где V — конечномерное векторное пространство над произвольным полем $\Bbbk$, называется *грассмановой квадратичной формой*.

Предложение 16.7 (нормальная форма Дарбу)
Над произвольным полем любой характеристики всякая грассманова квадратичная форма в подходящем базисе $e_1, \ldots, e_n$ пространства V может быть записана в *нормальном виде Дарбу*

$$e_1 \wedge e_2 + e_3 \wedge e_4 + \ldots + e_{2r-1} \wedge e_{2r}\,. \tag{16-17}$$

Доказательство. Рассмотрим произвольный базис $u_1, \ldots, u_n$ и перенумеруем его векторы так, чтобы $\omega = u_1 \wedge (\alpha_2 u_2 + \ldots + \alpha_n u_n) + u_2 \wedge (\beta_3 u_3 + \ldots + \beta_n u_n) + (\text{члены без } u_1 \text{ и } u_2)$, где коэффициент α_2 и вектор $v_2 \stackrel{\text{def}}{=} \alpha_2 u_2 + \ldots + \alpha_n u_n$ оба ненулевые. Перейдём к новому базису $\boldsymbol{v}$ из векторов $v_i = u_i$ при $i \neq 2$ и вектора v_2.

Упражнение 16.9. Убедитесь, что это действительно базис.

Подставляя в предыдущую формулу $u_2 = \big(v_2 - \alpha_3 v_3 - \ldots - \alpha_n v_n\big)/\alpha_2$, получаем

$$\omega = v_1 \wedge v_2 + v_2 \wedge (\gamma_3 v_3 + \ldots + \gamma_n v_n) + (\text{члены без } v_1 \text{ и } v_2) = \\ = (v_1 - \gamma_3 v_3 - \ldots - \gamma_n v_n) \wedge v_2 + (\text{члены без } v_1 \text{ и } v_2)$$

для некоторых $\gamma_3, \ldots, \gamma_n \in \Bbbk$. Переходя к базису $\boldsymbol{w}$ из векторов $w_1 = v_1 - \gamma_3 v_3 - \ldots - \gamma_n v_n$ и $w_i = v_i$ при $i \neq 1$, получаем $\omega = w_1 \wedge w_2 + (\text{члены без } w_1 \text{ и } w_2)$, после чего процесс может быть продолжен по индукции. □

[1] См. n° 11.3 на стр. 192.

Следствие 16.5
Над полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ однородный грассманов многочлен $\omega \in \Lambda^2 V$ тогда и только тогда разложим в произведение $u \wedge w$ двух векторов $u, w \in V$, когда $\omega \wedge \omega = 0$.

Доказательство. Если $\omega = u \wedge w$, то $\omega \wedge \omega = u \wedge w \wedge u \wedge w = 0$. Чтобы получить обратное, выберем в V базис $\boldsymbol{e}$, в котором $\omega = e_1 \wedge e_2 + e_3 \wedge e_4 + \cdots$. Если в этой сумме есть хотя бы два слагаемых, то базисный моном $e_1 \wedge e_2 \wedge e_3 \wedge e_4$ войдёт в $\omega \wedge \omega$ с ненулевым коэффициентом 2, а значит, $\omega \wedge \omega \neq 0$. Таким образом, равенство $\omega \wedge \omega = 0$ влечёт равенство $\omega = e_1 \wedge e_2$. □

16.6.1. Поляризация грассмановой квадратичной формы. Напомню[1], что с каждым базисом $\boldsymbol{e} = (e_1, \ldots, e_n)$ пространства V связан базис в $\Lambda^2 V$, состоящий из $n(n-1)/2$ грассмановых мономов $e_{ij} = e_i \wedge e_j$ с $i < j$, и каждый однородный грассманов многочлен второй степени $\omega \in \Lambda^2 V$ однозначно представляется в виде

$$\omega = \sum_{i<j} \omega_{ij}\, e_{ij}\,, \quad \text{где} \quad \omega_{ij} \in \Bbbk\,, \tag{16-18}$$

и суммирование происходит по всем $1 \leqslant i < j \leqslant n$. Если $\operatorname{char}\Bbbk \neq 2$, то каждое слагаемое в (16-18) можно переписать в виде $\omega_{ij} e_{ij} = \omega'_{ij} e_i \wedge e_j + \omega'_{ji} e_j \wedge e_i$, где $\omega'_{ij} = -\omega'_{ji} = \omega_{ij}/2$. Составленная из чисел ω'_{ij} кососимметричная квадратная матрица $\Omega_{\boldsymbol{e}} = (\omega'_{ij}) \in \operatorname{Mat}_n(\Bbbk)$ называется *матрицей Грама* грассмановой квадратичной формы ω в базисе $\boldsymbol{e}$. В терминах матрицы Грама форма ω записывается в виде

$$\omega = \sum_{i,j=1}^{n} \omega'_{ij} e_i \wedge e_j = \left(\boldsymbol{e}\,\Omega_{\boldsymbol{e}}\right) \wedge \boldsymbol{e}^t\,, \tag{16-19}$$

где в отличие от (16-18) суммирование происходит по всем n^2 парам индексов i, j, а обозначение $A \wedge B$ для матриц A, B, элементами которых являются векторы, предписывает перемножить эти матрицы по обычному правилу, используя в качестве произведения матричных элементов грассманово произведение соответствующих векторов, т. е. в (i,j)-й позиции матрицы $A \wedge B$ стоит вектор $a_{i1} \wedge b_{1j} + a_{i2} \wedge b_{2j} + \cdots + a_{in} \wedge b_{nj}$.

При выборе в V другого базиса $\boldsymbol{f}$, через который базис $\boldsymbol{e}$ выражается по формуле $\boldsymbol{e} = \boldsymbol{f}\, C_{\boldsymbol{fe}}$, матрица Грамма $\Omega_{\boldsymbol{f}}$ грассмановой квадратичной формы ω в базисе $\boldsymbol{f}$ будет связана с матрицей Грама $\Omega_{\boldsymbol{e}}$ соотношением

$$\Omega_{\boldsymbol{e}} = C_{\boldsymbol{fe}} \Omega_{\boldsymbol{e}} C_{\boldsymbol{fe}}^t \tag{16-20}$$

поскольку $\omega = \left(\boldsymbol{e}\,\Omega_{\boldsymbol{e}}\right) \wedge \boldsymbol{e}^t = \left(\boldsymbol{f}\, C_{\boldsymbol{fe}} \Omega_{\boldsymbol{e}}\right) \wedge \left(C_{\boldsymbol{fe}}^t \boldsymbol{f}^t\right) = \left(\boldsymbol{f}\, C_{\boldsymbol{fe}} \Omega_{\boldsymbol{e}} C_{\boldsymbol{fe}}^t\right) \wedge \boldsymbol{f}^t$.

Пример 16.3 (нормальная форма Дарбу)
Если $\operatorname{char}\Bbbk \neq 2$, то существование базиса $\boldsymbol{e}$, в котором заданная грассманова квадратичная форма $\omega \in \Lambda^2 V$ имеет вид (16-17), вытекает из теоремы о приведении кососимметричной билинейной формы к нормальному виду Дарбу[2]. Действительно, доказывая эту теорему, мы установили, что для любой кососимметричной матрицы Ω существует такая обратимая матрица C, что все ненулевые элементы матрицы $C\Omega C^t$ сосредоточены в расположенных на главной диагонали 2×2-блоках вида $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Поэтому грассманова квадратичная форма, имеющая матрицу

[1] См. 11-8 на стр. 192.
[2] См. теор. 16.2 на стр. 293.

Грама Ω в некотором базисе $\boldsymbol{f}$, запишется в базисе $\boldsymbol{g} = \boldsymbol{f}\,C$ как

$$\omega = 2g_1 \wedge g_2 + 2g_3 \wedge g_4 + \ldots$$

Искомый базис $\boldsymbol{e}$ получается из $\boldsymbol{g}$ удвоением векторов с нечётными номерами:

$$e_{2i+1} = 2g_{2i+1}\,, \quad e_{2i} = g_{2i}\,.$$

16.6.2. Пфаффиан. Рассмотрим кососимметричную матрицу $A = (a_{ij})$ размера $(2n)\times(2n)$. Будем считать её элементы a_{ij} с $i < j$ независимыми коммутирующими переменными и обозначим через $\mathbb{Z}[a_{ij}]$ кольцо многочленов с целыми коэффициентами от этих $2n^2 - n$ переменных. Мы собираемся показать, что существует единственный такой многочлен $\mathrm{Pf}(A) \in \mathbb{Z}[a_{ij}]$, что

$$\mathrm{Pf}^2(A) = \det(A) \quad \text{и} \quad \mathrm{Pf}(J') = 1\,,$$

где J' — блочно диагональная матрица из n идущих по главной диагонали 2×2-блоков

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

как в теор. 16.2 на стр. 293. Многочлен $\mathrm{Pf}(A)$ называется *пфаффианом* кососимметричной матрицы A и явно выражается через матричные элементы по формуле

$$\mathrm{Pf}(A) = \sum_{\substack{\{i_1,j_1\}\sqcup\cdots\sqcup\{i_n,j_n\}=\\ =\{1,2,\ldots,2n\}}} \operatorname{sgn}\bigl(i_1,j_1,i_2,j_2,\ldots,i_n,j_n\bigr)\cdot a_{i_1j_1}a_{i_2j_2}\ldots a_{i_nj_n}\,, \tag{16-21}$$

где суммирование происходит по всем разбиениям множества $\{1,\ldots,2n\}$ в объединение n неупорядоченных непересекающихся двухэлементных множеств $\{i_\nu,j_\nu\}$, порядок внутри которых тоже не существен, а sgn означает знак указанной в его аргументе перестановки из симметрической группы S_{2n}.

Упражнение 16.10. Убедитесь, что этот знак не меняется при перестановках пар друг с другом, а вся правая часть (16-21) не меняется при перестановке элементов внутри любой из пар.

Например,

$$\det\begin{pmatrix} 0 & a_{12} \\ -a_{12} & 0 \end{pmatrix} = a_{12}^2\,, \quad \det\begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{pmatrix} = (a_{12}a_{23} - a_{13}a_{24} + a_{14}a_{23})^2\,.$$

Чтобы извлечь квадратный корень из $\det A$, интерпретируем A как матрицу Грама невырожденной кососимметричной формы в стандартном базисе координатного векторного пространства K^{2n} над полем $K = \mathbb{Q}(a_{ij})$ рациональных функций от переменных a_{ij} с коэффициентами в поле $\mathbb{Q}$. По теореме Дарбу[1] в K^{2n} есть базис, в котором эта форма имеет матрицу Грама J'. Поэтому $A = CJ'C^t$ для некоторой матрицы $C \in \mathrm{GL}_{2n}(K)$. Так как $\det J' = 1$, мы заключаем, что $\det(A) = \det^2(C)$. Чтобы убедиться в том, что $\det C$ является многочленом с целыми коэффициентами и вычисляется по формуле (16-21), рассмотрим ещё одну кососимметричную матрицу

[1] См. теор. 16.2 на стр. 293.

$B = \big(b_{ij}\big)$, наддиагональные элементы b_{ij} которой также будем считать независимыми коммутирующими переменными, и образуем грассманову квадратичную форму

$$\beta_B(\xi) \stackrel{\text{def}}{=} (\xi B) \wedge \xi^t = \sum_{ij} b_{ij}\xi_i \wedge \xi_j$$

от $2n$ переменных $\xi = (\xi_1, \dots, \xi_{2n})$ с коэффициентами в кольце $K[b_{ij}]$. Так как чётные мономы $\xi_i \wedge \xi_j$ лежат в центре грассмановой алгебры, n-тая грассманова степень формы β_B имеет вид

$$\begin{aligned}\beta_B(\xi)^{\wedge n} = \beta_B(\xi) \wedge \dots \wedge \beta_B(\xi) = \Big(\sum_{i_1 j_1} b_{i_1 j_1}\xi_{i_1} \wedge \xi_{j_1}\Big) \wedge \dots \wedge \Big(\sum_{i_n j_n} b_{i_n j_n}\xi_{i_n} \wedge \xi_{j_n}\Big) = \\ = 2^n n! \sum_{\substack{\{i_1,j_1\}\sqcup\dots\sqcup\{i_n,j_n\}=\\ =\{1,2,\dots,2n\}}} \operatorname{sgn}\big(i_1, j_1, \dots, i_n, j_n\big) b_{i_1 j_1} \dots\ b_{i_n j_n} \xi_1 \wedge \dots \wedge \xi_{2n} = \\ = 2^n n!\, \mathrm{Pf}(B)\, \xi_1 \wedge \dots \wedge \xi_{2n}\,,\end{aligned} \tag{16-22}$$

где суммирование в предпоследней строке идёт по всем разбиениям множества $\{1, \dots, 2n\}$ на непересекающиеся неупорядоченные пары элементов $\{i_\nu, j_\nu\}$, и $\mathrm{Pf}(B) \in \mathbb{Z}[b_{ij}]$ означает тот же самый многочлен, что и в формуле (16-21). Заменим в (16-22) грассмановы переменные ξ на новые грассмановы переменные η по формуле $\xi = \eta\, C$, где $C \in \mathrm{GL}_{2n}(K)$. В правой части (16-22) получим $2^n n!\, \mathrm{Pf}(B)\ \det C\, \eta_1 \wedge \dots \wedge \eta_{2n}$. Квадратичная форма $\beta_B(\xi)$ в самой левой части (16-22) превратится в $\beta_B(\xi) = (\xi\, B) \wedge \xi^t = (\eta\, CB) \wedge (\eta\, C)^t = (\eta\, CBC^t) \wedge \eta^t = \beta_{CBC^t}(\eta)$, а её n-тая грассманова степень — в $\beta_{CBC^t}(\eta)^{\wedge n} = 2^n n!\ \mathrm{Pf}(CBC^t)\, \eta_1 \wedge \dots \wedge \eta_{2n}$. Таким образом, для любой матрицы $C \in \mathrm{GL}_{2n}(K)$ в кольце многочленов $K[b_{ij}]$ выполняется равенство

$$\mathrm{Pf}(CBC^t) = \mathrm{Pf}(B)\ \det C\,. \tag{16-23}$$

Полагая в этом равенстве $B = J'$ и беря в качестве C такую матрицу, что $CJ'C^t = A$, получаем в поле $K = \mathbb{Q}(a_{ij})$ равенство $\mathrm{Pf}(A) = \det C$.

Упражнение 16.11. Убедитесь, что $\mathrm{Pf}(J') = 1$.

Это доказывает существование пфаффиана и формулу (16-21). Единственность пфаффиана вытекает из того, что многочлен $x^2 - \det A = \big(x - \mathrm{Pf}(A)\big)\big(x + \mathrm{Pf}(A)\big) \in \mathbb{Z}[a_{ij}][x]$ имеет в целостном кольце $\mathbb{Z}[a_{ij}]$ ровно два корня $x = \pm\,\mathrm{Pf}(A)$, и требование $\mathrm{Pf}(J') = 1$ однозначно фиксирует нужный знак.

Предложение 16.8
Каждая симплектическая матрица[1] $F \in \mathrm{Sp}_{W_{2n}}(\Bbbk)$ имеет $\det F = 1$ и[2] $\chi_F(t) = t^{2n}\chi_F(t^{-1})$.

Доказательство. Из равенства $F^t J\, F = J$ и форм. (16-23) на стр. 305 вытекает, что

$$\mathrm{Pf}(J) = \mathrm{Pf}(F^t J\, F) = \det(F)\, \mathrm{Pf}(J)\,,$$

[1] См. формулу (16-14) на стр. 301.

[2] Последнее равенство означает, что последовательность коэффициентов характеристического многочлена $\chi_F(t) = a_0 x^m + \dots + a_{m-1}x + a_m$ симметрична относительно своей середины, т. е. $a_k = a_{m-k}$ при всех k. Многочлены с таким свойством называются *возвратными*.

откуда $\det F = 1$, так как $\mathrm{Pf}(J) \neq 0$. Кроме того, из равенства $F^t J F = J$ вытекает, что $F^{-1} = J^{-1}F^tJ = -JF^tJ$, откуда

$$\chi_F(t) = \det(tE - F) = t^{2n}\det(F)\det(F^{-1} - t^{-1}E) = t^{2n}\det(t^{-1}J^2 - JF^tJ) = \\ = t^{2n}\det^2(J)\det(t^{-1}E - F^t) = t^{2n}\det(t^{-1}E - F) = t^{2n}\chi_F(t^{-1}),$$

что и требовалось. □

Задачи для самостоятельного решения к §16

Задача 16.1. Выясните, вырождено ли ограничение симметричной билинейной формы с матрицей Грама

$$\begin{pmatrix} 0 & -1 & 3 & -4 \\ -1 & -2 & 2 & -2 \\ 3 & 2 & -4 & 1 \\ -4 & -2 & 1 & 4 \end{pmatrix}$$

на пространство U решений системы линейных уравнений

$$\begin{cases} x_3 - x_4 = 0 \\ x_1 - x_2 - 2x_4 = 0 \end{cases}$$

в $\mathbb{Q}^4$, и если нет, найдите проекцию вектора $v = (14, -3, 10, 8)$ на $U^\perp$ вдоль U.

Задача 16.2. Выясните, вырождено ли ограничение кососимметричной формы на $\mathbb{Q}^4$ с матрицей Грама

$$\begin{pmatrix} 0 & -1 & -3 & 7 \\ 1 & 0 & -3 & 8 \\ 3 & 3 & 0 & 4 \\ -7 & -8 & -4 & 0 \end{pmatrix},$$

на подпространство U решений системы линейных уравнений

$$\begin{cases} x_1 + x_2 + 2x_3 - 2x_4 = 0 \\ x_1 + 2x_2 + 3x_3 - 5x_4 = 0 \end{cases}$$

и если нет, найдите проекцию вектора $(-10, 8, 7, 5)$ на $U^\perp$ вдоль U и на U вдоль $U^\perp$.

Задача 16.3 (полярные разложения). Покажите, что каждый невырожденный рефлексивный линейный оператор f на пространстве с невырожденной билинейной формой представляется (не единственным способом) в виде $f = g_1h_1 = h_2g_2$, где g_1, g_2 — изометрии, а h_1, h_2 — самосопряжены. Далее, для любого невырожденного линейного оператора f на вещественном евклидовом пространстве убедитесь в том, что оба самосопряжённых оператора $ff^\times$, $f^\times f$ имеют положительный спектр, и докажите, что полярные разложения $f = g_1h_1 = h_2g_2$, в которых самосопряжённые операторы h_1, h_2 имеют положительный спектр, единственны.

Задача 16.4. Найдите полярное разложение $f = gh$, где $g \in \mathrm{O}_3(\mathbb{R})$, а h самосопряжён и с положительным спектром, для оператора $f : \mathbb{R}^3 \to \mathbb{R}^3$, имеющего в стандартном ортонормальном базисе матрицу

$$\begin{pmatrix} -2/9 & -8/9 & 4/9 \\ 10/9 & -5/9 & -2/9 \\ -2/9 & 10/9 & 13/9 \end{pmatrix}.$$

Задача 16.5. Покажите, что два самосопряжённых оператора на евклидовом пространстве изометрически подобны если и только если у них одинаковые характеристические многочлены.

Задача 16.6 (нормальные операторы в евклидовом пространстве). Покажите, что следующие свойства невырожденного линейного оператора f на вещественном евклидовом пространстве V эквивалентны: (1) $ff^\times = f^\times f$ (2) $|fv| = |f^\times v|$ для всех $v \in V$ (3) компоненты разложения $f = f_+ + f_-$ в сумму самосопряжённого и антисамосопряжённого операторов коммутируют (4) компоненты полярного разложения $f = gh$, где g ортогонален, а h самосопряжён и с положительным спектром, коммутируют.

Задача 16.7 (дополнение к сл. 16.2 на стр. 296 и сл. 16.3 на стр. 297). Пусть V — конечномерное векторное пространство над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$, $\beta : V \times V \to \Bbbk$ невырожденная билинейная форма, а $f : V \to V$ — линейный оператор. Покажите, что

а) если форма β кососимметрична, а оператор $f : V \to V$ самосопряжён, то V является прямой ортогональной суммой чётномерных подпространств, в подходящем базисе каждого из которых матрица оператора и матрица Грама формы имеют вид

$$\begin{pmatrix} J_m(\lambda) & 0 \\ 0 & J_m(\lambda) \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix},$$

где E — единичная $m \times m$ матрица. В частности все жордановы клетки оператора f разбиваются на непересекающиеся пары вида $J_m(\lambda), J_m(\lambda)$.

б) если форма β кососимметрична, а оператор $f : V \to V$ антисамосопряжён, то V является прямой суммой чётномерных подпространств, в подходящем базисе каждого из которых матрица оператора и матрица Грама формы имеют вид

$$\begin{pmatrix} J_m(\lambda) & 0 \\ 0 & -J_m(\lambda) \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix},$$

где при $\lambda = 0$ размер блоков m обязательно нечётен, а также чётномерных подпространств, в подходящем базисе каждого из которых матрица оператора и матрица Грама формы имеют вид

$$J_m(0) \quad \text{и} \quad \begin{pmatrix} & & & & 1 \\ & 0 & & -1 & \\ & & \iddots & & \\ & 1 & & 0 & \\ -1 & & & & \end{pmatrix}.$$

В частности все жордановы клетки оператора f с ненулевыми собственными числами, а также нильпотентные клетки нечётного размера разбиваются на непересекающиеся пары вида $J_m(\lambda), J_m(-\lambda)$.

в) если форма β кососимметрична, а оператор f симплектический, то в его ЖНФ все клетки с собственными числами $\lambda \neq \pm 1$, а также клетки нечётного размера с собственными числами $\lambda = \pm 1$ разбиваются на непересекающиеся пары вида $J_m(\lambda)$, $J_m(\lambda^{-1})$, и все такие ЖНФ реализуются у симплектических преобразований формы β

г) если форма β симметрична, а оператор f изометрический, то в его ЖНФ все клетки с собственными числами $\lambda \neq \pm 1$, а также клетки чётного размера с собственными числами $\lambda = \pm 1$ разбиваются на непересекающиеся пары вида $J_m(\lambda)$, $J_m(\lambda^{-1})$, и все такие ЖНФ реализуются у изометрических преобразований формы β.

Задача 16.8. Приведите пример

а) симметричной матрицы с элементарными делителями t^2, t^3, $(t-2)^3$

б) кососимметричной матрицы с элементарными делителями t^2, t^2, t^3, $(t-2)^2$, $(t+2)^2$

в) ортогональной[1] матрицы с элементарными делителями $t-2$, $t-\frac{1}{2}$, $(t-1)^2$

г) симплектической матрицы с элементарными делителями $t+1$, $t+1$, $(t-1)^2$.

Задача 16.9. Постройте какой-нибудь симплектический базис для формы с матрицей Грама

а) $\begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \\ -1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 0 \end{pmatrix}$ б) $\begin{pmatrix} 0 & 1 & 0 & 2 \\ -1 & 0 & 3 & 0 \\ 0 & -3 & 0 & -2 \\ -2 & 0 & 2 & 0 \end{pmatrix}$.

Задача 16.10. Найдите ранги грассмановых квадратичных форм над полем $\mathbb{Q}$ и выясните, раскладываются ли они в произведение двух линейных множителей:

а) $\xi_2 \wedge \xi_5 - 2\xi_2 \wedge \xi_6 - 2\xi_3 \wedge \xi_5 + 3\xi_3 \wedge \xi_6 - 2\xi_4 \wedge \xi_5 + 3\xi_4 \wedge \xi_6 + 3\xi_5 \wedge \xi_6$

б) $\xi_2 \wedge \xi_3 + \xi_2 \wedge \xi_4 + 3\xi_2 \wedge \xi_5 + \xi_2 \wedge \xi_6 - \xi_3 \wedge \xi_4 + 2\xi_3 \wedge \xi_5 - 5\xi_4 \wedge \xi_5 - 2\xi_4 \wedge \xi_6 + \xi_5 \wedge \xi_6$.

Задача 16.11. Напишите явную формулу для пфаффиана 6×6.

Задача 16.12. Фиксируем любое $n \in \mathbb{N}$ и любое чётное $m \leqslant n$. Покажите, что для кососимметричной $n \times n$ матрицы A и произвольной матрицы C из m строк и n столбцов имеет место полиномиальное тождество[2]

$$\operatorname{Pf}(CAC^t) = \sum_{\#I=m} \operatorname{Pf}(A_I) \cdot \det(C_I)$$

где суммирование идёт по всем наборам $I = (i_1, \ldots, i_m)$ строго возрастающих индексов, а C_I и A_I обозначают квадратные подматрицы размера $m \times m$, образованные, соответственно, I-столбцами матрицы C и элементами, стоящими в пересечениях I-строк и I-столбцов матрицы A.

[1] Т. е. такой матрицы A, что $A^{-1} = A^t$.

[2] Т. е. равенство в кольце многочленов с целыми коэффициентами от независимых матричных элементов a_{ij} с $i \leqslant j$ и $c_{k\ell}$.

§17. Квадратичные формы

В этом параграфе мы по умолчанию считаем, что основное поле $\Bbbk$ имеет $\operatorname{char}\Bbbk \neq 2$, а все билинейные формы по умолчанию предполагаются симметричными.

17.1. Пространства с симметричным скалярным произведением. Всюду далее мы будем называть невырожденные симметричные формы *скалярными произведениями*, а пространства, оснащённые такими формами — *пространствами со скалярным произведением*.

17.1.1. Изотропные и анизотропные подпространства. Вектор $v \in V$ в пространстве со скалярным произведением β называется *изотропным*, если $\beta(v,v) = 0$. Подпространство $U \subset V$, целиком состоящее из изотропных векторов, изотропно в смысле n° 15.2.2 на стр. 276, т. е. $\beta(u,w) = 0$ для всех $u, w \in U$, так как $2\beta(u,w) = \beta(u+w,u+w) - \beta(u,u) - \beta(w,w) = 0$. Подпространство $U \subset V$ называется *анизотропным*, если в нём нет ненулевых изотропных векторов. Если анизотропно всё пространство V, то говорят, что форма β *анизотропна* на V. Например, евклидово скалярное произведение на вещественном векторном пространстве анизотропно. Так как анизотропная форма обладает свойствами (5,6) из предл. 15.1 на стр. 274, она автоматически невырождена. Поэтому для любого анизотропного подпространства $U \subset V$ имеет место ортогональное разложение $V = U \oplus U^\perp$ из предл. 15.4 на стр. 278.

Теорема 17.1
Каждое пространство V со скалярным произведением распадается в прямую ортогональную сумму[1] $V \simeq H_{2k} \dotplus A$, первое слагаемое которой гиперболическое и может быть нулевым или совпадать со всем пространством V, а второе слагаемое $A = H_{2k}^\perp$ анизотропно.

Доказательство. Индукция по $\dim V$. Если V анизотропно (что так при $\dim V = 1$), доказывать нечего. Если существует ненулевой изотропный вектор $e \in V$, то по предл. 16.4 на стр. 299 он лежит в некоторой гиперболической плоскости $H_2 \subset V$, и $V = H_2 \oplus H_2^\perp$, так как ограничение скалярного произведения на H_2 невырождено[2]. По индукции, $H_2^\perp = H_{2m} \oplus A$, где $A = H_{2m}^\perp$ анизотропно. Поэтому $V = H_{2m+2} \oplus A$ и $A = H_{2m+2}^\perp$. □

Замечание 17.1. В теор. 17.4 на стр. 312 ниже мы увидим, что разложение из теор. 17.1 единственно в следующем смысле: если $V \simeq H_{2k} \dotplus U \simeq H_{2m} \dotplus W$, где U и W анизотропны, то $k = m$ и существует изометрический изоморфизм $U \xrightarrow{\sim} W$.

17.1.2. Изометрии и отражения. Всякий анизотропный вектор $e \in V$ задаёт разложение пространства V в прямую ортогональную сумму $V = \Bbbk e \oplus e^\perp$. Линейный оператор $\sigma_e : V \to V$, тождественно действующий на гиперплоскости $e^\perp$ и переводящий вектор e в $-e$, называется *отражением* в гиперплоскости $e^\perp$, см. рис. 17⋄1 ниже. Произвольный вектор $v = v_e + v_{e^\perp} \in V$, где $v_e = e\,\beta(e,v)\,/\,\beta(e,e)$ — проекция вектора v на одномерное подпространство[3] $\Bbbk e$ вдоль гиперплоскости $e^\perp$, а $v_{e^\perp} = v - v_e \in e^\perp$, переходит при этом в вектор

$$\sigma_e(v) = -v_e + v_{e^\perp} = v - 2v_e = v - 2\,\frac{\beta(e,v)}{\beta(e,e)} \cdot e\,. \tag{17-1}$$

[1] См. n° 15.5 на стр. 283.
[2] См. n° 16.1.2 на стр. 292.
[3] Мы пользуемся тем, что $e^\vee = e/\beta(e,e)$ является двойственным к e относительно формы β базисным вектором одномерного пространства $\Bbbk e$ и по форм. (16-2) на стр. 292 ортогональная проекция произвольного вектора v на это подпространство равна $v_e = \beta(e,v)\,e^\vee$.

Упражнение 17.1. Убедитесь, что $\sigma_e \in \mathrm{O}_\beta(V)$ и $\sigma_e^2 = \mathrm{Id}_V$, и докажите для любых изометрии $f \in \mathrm{O}(V)$ и анизотропного вектора $e \in V$ равенство $f \circ \sigma_e \circ f^{-1} = \sigma_{f(e)}$.

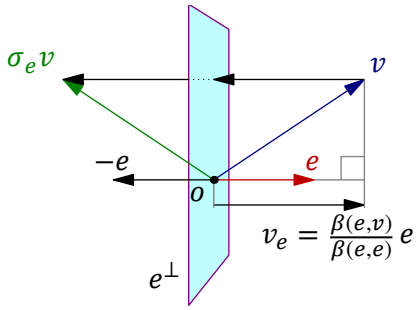


Рис. 17⋄1. Отражение σ_e.

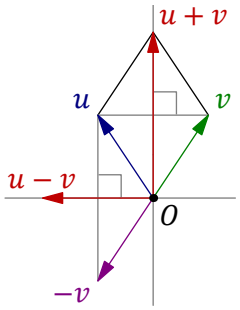


Рис. 17⋄2. Отражения в ромбе.

Лемма 17.1
В любом пространстве V со скалярным произведением β для каждой пары различных анизотропных векторов u, v с равными скалярными квадратами $\beta(u,u) = \beta(v,v) \neq 0$ существует отражение, переводящее u либо в v, либо в $-v$.

Доказательство. Если u и v коллинеарны, то искомым отражением является $\sigma_v = \sigma_u$. Если u и v не коллинеарны, то хотя бы одна из двух диагоналей $u+v$, $u-v$ натянутого на них ромба (см. рис. 17⋄2) анизотропна, поскольку эти диагонали ортогональны:

$$\beta(u+v, u-v) = \beta(u,u) - \beta(v,v) = 0\,,$$

и их линейная оболочка содержит анизотропные векторы u, v. Тем самым, хотя бы одно из отражений σ_{u-v}, σ_{u+v} определено. При этом $\sigma_{u-v}(u) = v$, а $\sigma_{u+v}(u) = -v$. □

Упражнение 17.2. Проверьте, последние два равенства.

Теорема 17.2
Всякая изометрия n-мерного пространства со скалярным произведением является композицией не более чем $2n-1$ отражений.

Доказательство. Индукция по n. Ортогональная группа одномерного пространства состоит из тождественного оператора E и отражения $-E$. Пусть $n > 1$ и $f : V \to V$ — изометрия. Выберем в V какой-нибудь анизотропный вектор v и обозначим через σ отражение, переводящее $f(v)$ в v или в $-v$. Композиция σf переводит v в $\pm v$, а значит, переводит в себя $(n-1)$-мерную гиперплоскость $v^\perp$. По индукции, действие σf на $v^\perp$ является композицией не более $2n-3$ отражений в гиперплоскостях внутри $v^\perp$. Продолжим их до отражений всего пространства V, добавив в зеркало каждого отражения вектор v. Композиция полученных отражений совпадает с σf на гиперплоскости $v^\perp$, а её действие на v либо такое же, как у σf (при $\sigma f(v) = v$), либо отличается от него знаком (при $\sigma f(v) = -v$). Поэтому σf, как оператор на всём пространстве V, есть композиция построенных $2n-3$ отражений и, возможно, ещё одного отражения в гиперплоскости $v^\perp$. Следовательно, $f = \sigma\sigma f$ это композиция не более $2n-1$ отражений. □

Упражнение 17.3. Покажите, что в анизотропном пространстве V в условиях лем. 17.1 всегда найдётся отражение, переводящее u в точности в v, и выведите отсюда, что любая изометрия n-мерного анизотропного[1] пространства является композицией не более n отражений.

[1] В частности, вещественного евклидова.

Пример 17.1 (изометрии евклидова пространства)
Согласно упр. 17.3 несобственная изометрия евклидовой плоскости является отражением, а собственная — композицией двух отражений, т. е. поворотом.

Упражнение 17.4. Убедитесь, что композиция $\sigma_a\sigma_b$ отражений евклидовой плоскости в ортогоналах к векторам b и a является поворотом на угол $2\measuredangle(b,a)$ в направлении от b к a.

Индукция по $\dim V$ показывает, что действие изометрического оператора φ на евклидовом пространстве V произвольной размерности описывается следующим образом. Если $\dim V = 2n$, то V можно так разложить в прямую сумму n попарно ортогональных двумерных f-инвариантных подпространств U_i, что если f несобственный, то он действует на плоскости U_1 отражением, а на всех остальных плоскостях U_i — поворотами на углы $\varphi_i \in [0,\pi]$, а если f собственный, то он действует поворотами во всех плоскостях U_i. Если же $\dim V = 2n+1$, то V раскладывается в сумму n ортогональных f-инвариантных плоскостей и ортогональной им всем прямой так, что f действует во всех плоскостях поворотами, а на прямой — тождественно, если f собственный, и умножением на -1, если f не собственный.

В самом деле, по прим. 12.5 на стр. 222 у f есть одномерное или двумерное инвариантное подпространство U. Так как f сохраняет скалярные произведения, ортогонал $U^\perp$ тоже f-инвариантен. По индукции, действие f на U и $U^\perp$ описывается так, как выше.

Упражнение 17.5. Убедитесь, что одномерные и/или несобственные компоненты действия f на U и $U^\perp$ всегда можно переразложить так, чтобы действие f имело нужный вид.

Легко видеть, что неупорядоченный набор[1] углов поворотов, которыми f действует на двумерных плоскостях, а также наличие и вид дополнительного к ним одно- или двумерного слагаемого не зависят от выбора такого разложения[2]. В самом деле, характеристический многочлен $\chi_f(t)$ является произведением характеристических многочленов матриц

$$\begin{pmatrix} \cos\varphi_i & -\sin\varphi_i \\ \sin\varphi_i & \cos\varphi_i \end{pmatrix}$$

всех поворотов, т. е. многочленов $t^2 - 2\cos\varphi_i + 1$, неприводимых в $\mathbb{R}[x]$ при $\varphi_i \neq 0,\pi$, а при $\varphi_i = 0,\pi$ равных $(t-1)^2$ и $(t+1)^2$ соответственно, а также множителя $(t+1)(t-1)$, или $t+1$, или $t-1$ в зависимости от дополнительного слагаемого. Таким образом, предыдущее описание однозначно задаёт разложение многочлена $\chi_f(t)$ на неприводимые множители в $\mathbb{R}[x]$ и столь же однозначно с него считывается.

Упражнение 17.6. Убедитесь в этом.

Теорема 17.3 (лемма Витта)
Пусть четыре пространства U_1, W_1, U_2, W_2 со скалярными произведениями таковы, что некоторые два из трёх пространств U_1, $U_1 \dotplus W_1$, W_1 изометрически изоморфны соответствующей паре пространств из тройки U_2, $U_2 \dotplus W_2$, W_2. Тогда оставшиеся третьи элементы троек тоже изометрически изоморфны.

Доказательство. Если есть изометрические изоморфизмы $f\colon U_1 \xrightarrow{\sim} U_2$ и $g\colon W_1 \xrightarrow{\sim} W_2$, то их прямая сумма $f \oplus g\colon U_1 \dotplus W_1 \to U_2 \dotplus W_2$, $(u,w) \mapsto (f(u), g(w))$, является требуемым изометрическим изоморфизмом. Оставшиеся два случая симметричны, и мы разберём один из них. Пусть

[1] Учитывающий кратности, т. е. каждый угол входит в набор столько раз, в скольких плоскостях происходит поворот на этот угол.

[2] А он, вообще говоря, не единствен.

имеются изометрические изоморфизмы

$$f\colon U_1 \xrightarrow{\sim} U_2 \quad \text{и} \quad h\colon U_1 \dotplus W_1 \xrightarrow{\sim} U_2 \dotplus W_2\,.$$

Изометрический изоморфизм $g\colon W_1 \xrightarrow{\sim} W_2$ строится индукцией по $\dim U_1 = \dim U_2$. Если пространство U_1 одномерно с базисом u, то вектор u анизотропен. Поэтому векторы $f(u)$ и $h(u,0)$ тоже анизотропны и имеют одинаковые скалярные квадраты. Обозначим через σ отражение пространства $U_2 \dotplus W_2$, переводящее $h(u,0)$ в $\bigl(\pm f(u),0\bigr)$. Композиция

$$\sigma h\colon U_1 \dotplus W_1 \xrightarrow{\sim} U_2 \dotplus W_2$$

изометрично отображает одномерное подпространство U_1 первой суммы на одномерное подпространство U_2 второй, а значит, изометрично отображает ортогональное дополнение к U_1 в первой сумме на ортогональное дополнение к U_2 во второй, что и даёт требуемый изоморфизм $\sigma h|_{W_1}\colon W_1 \xrightarrow{\sim} W_2$. Пусть теперь $\dim U_1 > 1$. Выберем в U_1 любой анизотропный вектор u и рассмотрим ортогональные разложения

$$U_1 \dotplus W_1 = \Bbbk u \dotplus u^\perp \dotplus W_1 \quad \text{и} \quad U_2 \dotplus W_2 = \Bbbk f(u) \dotplus f(u)^\perp \dotplus W_2\,,$$

в которых $u^\perp \subset U_1$ и $f(u)^\perp \subset U_2$ означают ортогональные дополнения к анизотропным векторам u и $f(u)$ внутри U_1 и U_2 соответственно. Так как пространства $\Bbbk u$ и $\Bbbk f(u)$ изометрически изоморфны, по уже доказанному существуют изометрии

$$f'\colon u^\perp \xrightarrow{\sim} f(u)^\perp \quad \text{и} \quad h'\colon u^\perp \dotplus W_1 \xrightarrow{\sim} f(u)^\perp \dotplus W_2\,,$$

к которым применимо индуктивное предположение. □

Теорема 17.4
Построенное в теор. 17.1 разложение пространства V со скалярным произведением в прямую ортогональную сумму гиперболического и анизотропного подпространств единственно в том смысле, что для любых двух таких разложений $V = H_{2k} \dotplus U = H_{2m} \dotplus W$ имеет место равенство $k = m$ и существует изометрический изоморфизм $U \simeq W$.

Доказательство. Пусть $m \geqslant k$, так что $H_{2m} = H_{2k} \dotplus H_{2(m-k)}$. Тождественное отображение $\mathrm{Id}\colon V \to V$ задаёт изометрический изоморфизм $H_{2k} \dotplus U \xrightarrow{\sim} H_{2k} \dotplus H_{2(m-k)} \dotplus W$. По лемме Витта существует изометрический изоморфизм $U \xrightarrow{\sim} H_{2(m-k)} \dotplus W$. Так как U анизотропно, $H_{2(m-k)} = 0$ (иначе в U будет ненулевой изотропный вектор), откуда $k = m$ и $U \simeq W$. □

Теорема 17.5
Если скалярное произведение на пространстве V невырожденно ограничивается на подпространства $U, W \subset V$ и существует изометрический изоморфизм $\varphi\colon U \xrightarrow{\sim} W$, то он продолжается (неоднозначно) до такого изометрического автоморфизма $f\colon V \xrightarrow{\sim} V$, что $f|_U = \varphi$.

Доказательство. Если есть хоть какой-нибудь изометрический изоморфизм $\psi\colon U^\perp \xrightarrow{\sim} W^\perp$, то изометрия $f = \varphi \oplus \psi\colon U \oplus U^\perp \xrightarrow{\sim} W \oplus W^\perp$, $(u,u') \mapsto \bigl(\varphi(h'),\psi(u')\bigr)$ является требуемым автоморфизмом пространства V. Поскольку тождественный автоморфизм пространства V является изометрией между $U \dotplus U^\perp \simeq V$ и $W \dotplus W^\perp \simeq V$, и по условию существует изометрия $U \xrightarrow{\sim} W$, из леммы Витта тоже изометрический изоморфизм. Так что по лемме Витта[1] ортогоналы $U^\perp$ и $W^\perp$ изометрически изоморфны. □

[1] См. теор. 17.3 на стр. 311.

Следствие 17.1
Для каждого натурального числа k в диапазоне $1 \leqslant k \leqslant \dim V/2$ группа изометрий $\mathrm{O}(V)$ транзитивно действует на k-мерных изотропных и $2k$-мерных гиперболических подпространствах в V.

Доказательство. Утверждение про гиперболические подпространства вытекает непосредственно из теор. 17.5, а про изотропные — получается из него применением предл. 16.4 на стр. 299 точно также, как в доказательстве предл. 16.6 на стр. 302. □

17.2. Квадратичные формы. Функция $q : V \to \Bbbk$ на n-мерном векторном пространстве V над полем $\Bbbk$ называется *квадратичной формой*, если она является однородным многочленом степени 2 от координат[1], т. е. существуют такие базис $\boldsymbol{e} = (e_1, \dots, e_n)$ в V и однородный многочлен второй степени $q_{\boldsymbol{e}} \in \Bbbk[x_1, \dots, x_n]$, что $q(\lambda_1 e_1 + \dots + \lambda_n e_n) = q_{\boldsymbol{e}}(\lambda_1, \dots, \lambda_n)$ для всех $(\lambda_1, \dots, \lambda_n) \in \Bbbk^n$. Если $\mathrm{char}(\Bbbk) \neq 2$, то многочлен $q_{\boldsymbol{e}}$ можно записать в виде

$$q_{\boldsymbol{e}}(x_1, \dots, x_n) = \sum_{i,j=1}^{n} q_{ij} x_i x_j \,, \tag{17-2}$$

где суммирование происходит по всем парам индексов $1 \leqslant i, j \leqslant n$, а коэффициенты q_{ij} симметричны по i и j, т. е. при $i \neq j$ число $q_{ji} = q_{ij}$ равно *половине*[2] фактического коэффициента при $x_i x_j$ в многочлене $q_{\boldsymbol{e}}$, возникающего после приведения подобных слагаемых в (17-2). Если организовать числа q_{ij} в симметричную матрицу $Q_{\boldsymbol{e}} = \bigl(q_{ij}\bigr)$, которую мы будем называть *матрицей Грама* многочлена $q_{\boldsymbol{e}}$, и обозначить через x и $x^t = (x_1, \dots, x_n)$ столбец и строку, составленные из переменных, то (17-2) можно переписать в виде

$$q(x_1, \dots, x_n) = \sum_{i,j=1}^{n} x_i q_{ij} x_j = x^t\, Q_{\boldsymbol{e}}\, x \,. \tag{17-3}$$

Сравнивая это с форм. (15-2) на стр. 272, мы заключаем, что $q(v) = \tilde{q}(v, v)$, где $\tilde{q} : V \times V \to \Bbbk$ — симметричная билинейная форма с матрицей Грама $Q_{\boldsymbol{e}}$ в базисе $\boldsymbol{e}$. Поскольку

$$q(u + w) - q(u) - q(w) = \tilde{q}(u + w, u + w) - \tilde{q}(u, u) - \tilde{q}(w, w) = 2\tilde{q}(u, w) \,,$$

симметричная билинейная форма $\tilde{q}$ со свойством $\tilde{q}(v, v) = q(v)$ однозначно определяется квадратичной формой q, если $\mathrm{char}\,\Bbbk \neq 2$. Симметричная билинейная форма $\tilde{q}$ называется *поляризацией* квадратичной формы q. Обратите внимание, что взаимно однозначное соответствие между квадратичными и симметричными билинейными формами

$$\begin{aligned} \tilde{q}(u, w) &\mapsto q(v) = \tilde{q}(v, v) \\ q(v) &\mapsto \tilde{q}(u, w) = \frac{1}{2}\bigl(q(u + w) - q(u) - q(w)\bigr) \end{aligned} \tag{17-4}$$

не зависят от базиса $\boldsymbol{e}$ в V. В частности, для любого базиса $\boldsymbol{f} = \boldsymbol{e}\, C_{\boldsymbol{ef}}$ в V значение $q(v)$ является однородным многочленом второй степени $q_{\boldsymbol{f}}$ от координат вектора v в базисе $\boldsymbol{f}$, причём матрица Грама этого многочлена, равная матрице Грама билинейной формы $\tilde{q}$ в базисе $\boldsymbol{f}$, будет равна[3] $Q_{\boldsymbol{f}} = C_{\boldsymbol{ef}}^t Q_{\boldsymbol{e}}\, C_{\boldsymbol{ef}}$.

[1] Т. е. $q \in S^2 V^*$ в обозначениях из n° 13.6 на стр. 248, где объяснялось, что это свойство не зависит от выбора координат.

[2] Обратите внимание, что над полем характеристики 2 многочлен $x_1 x_2$ не записывается в виде (17-2).

[3] См. формулу (15-1) на стр. 272.

Поскольку при переходе от базиса к базису определитель Грама умножается на квадрат определителя матрицы перехода, класс числа $\det Q_{\boldsymbol{e}} \in \Bbbk$ по модулю умножения на ненулевые квадраты из поля $\Bbbk$ не зависит от выбора базиса $\boldsymbol{e}$. Мы будем обозначать этот класс $\det q \in \Bbbk/\Bbbk^{*2}$ и называть его *определителем Грама* квадратичной формы q. Квадратичная форма q называется *вырожденной*, если $\det q = 0$. Формы с $\det q \neq 0$ называются *невырожденными*. Таким образом, невырожденность квадратичной формы q означает в точности то же, что невырожденность её поляризации[1] $\tilde{q}$. Под *рангом* квадратичной формы q мы понимаем ранг её поляризации $\tilde{q}$, равный рангу матрицы Грама $Q_{\boldsymbol{e}}$ в любом базисе $\boldsymbol{e}$. Также, как и для симметричных билинейных форм, мы будем называть ненулевой вектор $v \in V$ *изотропным* для квадратичной формы q, если $q(v) = 0$. Квадратичная форма называется *анизотропной*, если $q(v) \neq 0$ при $v \neq 0$.

Из доказанных выше результатов про симметричные билинейные формы немедленно получаются аналогичные результаты про квадратичные формы.

Следствие 17.2 (из теор. 17.1 на стр. 309)
Всякая квадратичная форма q над произвольным полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ в подходящих координатах записывается в виде $x_1x_{i+1} + x_2x_{i+2} + \ldots + x_ix_{2i} + \alpha(x_{2i+1}, x_{2i+2} \ldots, x_r)$, где $r = \operatorname{rk}(q)$ и $\alpha(x) \neq 0$ при $x \neq 0$. □

Следствие 17.3 (из теор. 16.1 на стр. 292)
Всякая квадратичная форма над произвольным полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ линейной обратимой заменой переменных приводится к виду $\sum a_i x_i^2$. □

Следствие 17.4 (из сл. 16.1 на стр. 293)
Два однородных многочлена второй степени $f, g \in \Bbbk[x_1, \ldots, x_n]$ над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ тогда и только тогда переводятся друг в друга линейными обратимыми заменами переменных, когда задаваемые им квадратичные формы $f, g : \Bbbk^n \to \Bbbk$ имеют одинаковый ранг. □

Пример 17.2 (квадратичные формы от двух переменных)
Согласно сл. 17.3, ненулевая квадратичная форма от двух переменных

$$q(\boldsymbol{x}) = a\,x_1^2 + 2\,b\,x_1x_2 + c\,x_2^2 = (x_1, x_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \tag{17-5}$$

подходящей линейной заменой координат приводятся либо к виду αt^2 с $\alpha \neq 0$, либо к виду

$$\alpha t_1^2 + \beta\, t_2^2\,, \quad \text{где} \quad \alpha\beta \neq 0\,.$$

Условимся писать $\xi \sim \eta$ для таких чисел $\xi, \eta \in \Bbbk$, что $\xi = \lambda^2\eta$ для какого-нибудь ненулевого $\lambda \in \Bbbk$. Тогда в первом случае $ac - b^2 \sim \det q \sim \alpha \cdot 0 = 0$, т. е. форма q вырождена, а во втором случае $ac - b^2 \sim \det q \sim \alpha\beta \neq 0$ и форма q невырождена. Тем самым, вырожденность ненулевой квадратичной формы (17-5) означает, что с точностью до постоянного множителя она является полным квадратом линейной формы $t \in V^*$. Такая форма q зануляется вдоль одномерного подпространства $\operatorname{Ann}(t) \subset V$ и отлична от нуля на всех остальных векторах.

[1] См. предл. 15.1 на стр. 274.

Если форма (17-5) невырождена, и у неё есть ненулевой изотропный вектор $v = (\vartheta_1, \vartheta_2)$, то из равенства $\alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$ вытекает, что $\vartheta_2 \neq 0$ и $-\det q \sim -\alpha\beta \sim -\beta/\alpha = (\vartheta_1/\vartheta_2)^2$ является квадратом в поле $\Bbbk$. В этом случае многочлен

$$\alpha t_1^2 + \beta\, t_2^2 = \alpha \left(t_1 + \frac{\vartheta_1}{\vartheta_2} t_2\right)\left(t_1 - \frac{\vartheta_1}{\vartheta_2} t_2\right)$$

раскладывается над полем $\Bbbk$ в произведение двух непропорциональных линейных форм. Поэтому квадратичная форма q, у которой $-\det q$ является ненулевым квадратом, тождественно зануляется на двух одномерных подпространствах и отлична от нуля на всех прочих векторах. Мы будем называть такие формы *гиперболическими*[1]. Если же $-\det q$ не квадрат, то форма q анизотропна. Число $-\det(q) = b^2 - ac$ часто обозначают через $D/4$ и называют D *дискриминантом* квадратичной формы (17-5).

17.3. Квадратичные формы над конечными полями. Пусть $q = p^m$, где $p > 2$. Зафиксируем какой-нибудь элемент $\varepsilon \in \mathbb{F}_q$, не являющийся квадратом.

Упражнение 17.7. Убедитесь, что ненулевые квадраты образуют в мультипликативной группе $\mathbb{F}_q^\times$ поля $\mathbb{F}_q$ подгруппу порядка $|\mathbb{F}_q^\times|/2 = (q-1)/2$, и что любой ненулевой элемент поля $\mathbb{F}_q$ умножением на подходящий ненулевой квадрат можно сделать равным либо 1, либо ε.

Лемма 17.2
При любых $a_1, a_2 \in \mathbb{F}_q^\times$ квадратичная форма $a_1x_1^2 + a_2x_2^2$ на двумерном координатном пространстве $\mathbb{F}_q^2$ принимает все значения из поля $\mathbb{F}_q$.

Доказательство. В силу упр. 17.7 при любых фиксированных $a_1, a_2 \in \mathbb{F}_q^\times$ и $b \in \mathbb{F}_q$ чисел вида $a_1x_1^2$ и чисел вида $b - a_2x_2^2$, где x_1, x_2 независимо пробегают $\mathbb{F}_q$, имеется ровно по

$$1 + \frac{q-1}{2} = \frac{q+1}{2}$$

штук. Следовательно эти два множества чисел имеют общий элемент $a_1x_1^2 = b - a_2x_2^2$. Тем самым, $a_1x_1^2 + a_2x_2^2 = b$. □

Предложение 17.1
Каждая квадратичная форма f ранга r над полем $\mathbb{F}_q$ в подходящих координатах записывается как $x_1^2 + \ldots + x_r^2$ или как $x_1^2 + \ldots + x_{r-1}^2 + \varepsilon x_r^2$, и эти две формы изометрически не изоморфны.

Доказательство. По теор. 16.1 форма f в подходящих координатах записывается в виде

$$a_1x_1^2 + \ldots + a_rx_r^2, \quad \text{где все } a_i \neq 0.$$

Согласно упр. 17.7, умножая базисные векторы на подходящие ненулевые константы, мы можем считать, что каждое a_i равно либо 1, либо ε. Если $a_i = a_j = \varepsilon$ при каких-то $i \neq j$, то в линейной оболочке U базисных векторов e_i, e_j по лем. 17.2 найдётся вектор v_i с $f(v_i) = 1$. Ортогональное дополнение к v_i в плоскости U одномерно, и форма f ограничивается на него невырождено. Пусть вектор v_j его порождает.

Упражнение 17.8. Покажите, что $f(v_j)$ является ненулевым квадратом в $\mathbb{F}_q$.

[1] Поскольку поляризация такой формы является гиперболическим скалярным произведением.

Заменяя e_i, e_j на v_i, $v_j / \sqrt{f(v_j)}$, мы сохраняем диагональный вид формы и уменьшаем на два количество коэффициентов, равных ε. Эту процедуру можно повторять, пока таких коэффициентов останется не более одного. Формы $f = x_1^2 + \ldots + x_r^2$ и $g = x_1^2 + \ldots + x_{r-1}^2 + \varepsilon x_r^2$ изометрически не изоморфны, поскольку индуцированные ими невырожденные квадратичные формы f_{red} и g_{red} на факторах $V/\ker \tilde{f}$ и $V/\ker \tilde{g}$ исходного пространства V, где были заданы формы, имеют разные определи Грама: $\det f_{\text{red}} = 1$ является квадратом, а $\det g_{\text{red}} = \varepsilon$ — нет. □

Предложение 17.2
Всякая квадратичная форма на пространстве размерности $\geqslant 3$ над полем $\mathbb{F}_q$ имеет ненулевой изотропный вектор.

Доказательство. По теор. 16.1 форма записывается в подходящем базисе как

$$a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + \ldots .$$

Если $a_1 = 0$ или $a_2 = 0$, то вектор $(1, 0, 0, \ldots)$ или вектор $(0, 1, 0, \ldots)$ изотропен. Если $a_1 a_2 \neq 0$, то по лем. 17.2 найдутся такие $\lambda, \mu \in \mathbb{F}_q$, что $a_1\lambda^2 + a_2\mu^2 = -a_3$. Тогда вектор $(\lambda, \mu, 1, 0, \ldots)$ изотропен. □

Предложение 17.3 (перечисление анизотропных форм)
Анизотропные формы над полем $\mathbb{F}_q$, где $q = p^m$ и $p > 2$, имеются только в размерностях 1 и 2. В размерности 2 квадратичная форма $x_1^2 + x_2^2$ анизотропна если и только если $q \equiv -1 \pmod 4$, а форма $x_1^2 + \varepsilon x_2^2$ анизотропна если и только если $q \equiv 1 \pmod 4$.

Доказательство. Из прим. 17.2 на стр. 314 вытекает, что форма $x_1^2 + x_2^2$ имеет изотропный вектор если и только если её $D/4 = -1$ является квадратом в $\mathbb{F}_q$. В этом случае вторая форма $x_1^2 + \varepsilon x_2^2$ анизотропна, так как $D/4 = -\varepsilon$ не является квадратом. Наоборот, если -1 не квадрат, то $-\varepsilon$ квадрат, и форма $x_1^2 + \varepsilon x_2^2$ имеет изотропный вектор. Остаётся убедиться, что -1 является квадратом в $\mathbb{F}_q$ если и только если $q \equiv 1 \pmod 4$. Для этого рассмотрим гомоморфизм мультипликативных групп $\gamma\colon \mathbb{F}_q^\times \to \mathbb{F}_q^\times, x \mapsto x^{\frac{q-1}{2}}$. Поскольку порядок $|\mathbb{F}_q^\times| = q - 1$, для каждого $x \in \mathbb{F}_q^\times$ выполняется равенство $x^{q-1} = 1$, из которого вытекает, что все ненулевые квадраты лежат в $\ker\gamma$, а все $x \in \operatorname{im}\gamma$ имеют $x^2 = 1$, откуда $\operatorname{im}\gamma \subset \{\pm 1\}$. Так как у уравнения $x^{\frac{q-1}{2}} = 1$ не более $(q-1)/2$ корней в поле $\mathbb{F}_q$, образ γ имеет порядок 2, а $\ker\gamma \subset \mathbb{F}_q^\times$ имеет индекс 2 и совпадает с группой квадратов, т. е. $x \in \mathbb{F}_q^\times$ является квадратом тогда и только тогда, когда $x^{\frac{q-1}{2}} = 1$. В частности, -1 квадрат если и только если $(q-1)/2$ чётно. □

17.4. Вещественные квадратичные формы. Из сл. 17.3 вытекает, что любая квадратичная форма на вещественном вектором пространстве V в подходящем базисе записывается в виде

$$q(x) = x_1^2 + x_2^2 + \ldots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \ldots - x_{p+m}^2 . \tag{17-6}$$

Для этого надо перейти к базису с диагональной матрицей Грама и поделить каждый базисный вектор e_i с $q(e_i) \neq 0$ на $\sqrt{|q(e_i)|}$. Числа p и m в представлении (17-6) называются *положительным* и *отрицательным индексами инерции*, упорядоченная пара (p, m) — *сигнатурой*, а разность $p - m$ — просто *индексом* вещественной квадратичной формы q.

Теорема 17.6
Числа p и m в представлении (17-6) не зависят от выбора базиса, в котором квадратичная форма имеет вид (17-6).

Доказательство. Будем считать, что $p \geqslant m$, поскольку противоположный случай сводится к этому заменой q на $-q$. Сумма $p+m = \operatorname{rk} q$ равна рангу билинейной формы $\tilde{q}$ и не зависит от выбора базиса. Линейная оболочка базисных векторов e_k с номерами $k > p+m$ является ядром билинейной формы $\tilde{q}$. Классы $[e_i]$ остальных базисных векторов по модулю $\ker \tilde{q}$ образуют базис факторпространства $W = V/\ker \tilde{q}$. По предл. 16.2 на стр. 291 форма $\tilde{q}$ корректно задаёт на W невырожденную симметричную билинейную форму $\tilde{q}_{\text{red}}([u],[w]) = \tilde{q}(u,w)$, которая в базисе из классов $[e_i]$ с $1 \leqslant i \leqslant p+m$ записывается той же самой формулой (17-6). Каждая пара базисных векторов $[e_i]$, $[e_{p+i}]$ порождает гиперболическую плоскость с гиперболическим базисом из векторов $\bigl([e_i] \pm [e_{p+i}]\bigr)/\sqrt{2}$. Поэтому форма $\tilde{q}_{\text{red}}$ является прямой ортогональной суммой гиперболического пространства H_{2m}, натянутого на классы $[e_i]$, $[e_{p+i}]$ с $1 \leqslant i \leqslant m$, и анизотропного пространства размерности $p-m$, натянутого на оставшиеся классы $[e_j]$ с $m < j \leqslant p$. По теор. 17.4 на стр. 312 размерности гиперболического и анизотропного слагаемых не зависят от выбора разложения пространства со скалярным произведением в ортогональную сумму гиперболического и анизотропного. Поэтому индекс $p-m$ и отрицательный индекс инерции m не зависят от выбора базиса, в котором форма q имеет вид (17-6). □

Следствие 17.5 (из доказательства теор. 17.6)
Для каждого n на пространстве $\mathbb{R}^n$ с точностью до изометрического изоморфизма имеются ровно два анизотропных скалярных произведения — евклидово и *антиевклидово*, получающееся из евклидова сменой знака. Вещественные квадратичные формы положительного индекса имеют ненулевое евклидово анизотропное слагаемое, а формы отрицательного индекса — ненулевое антиевклидово анизотропное слагаемое, размерности которых равны абсолютной величине индекса. Гиперболичность невырожденной вещественной квадратичной формы равносильна тому, что её индекс равен нулю. □

Следствие 17.6
Два однородных многочлена второй степени $f, g \in \mathbb{R}[x_1, \ldots, x_n]$ тогда и только тогда переводятся друг в друга линейными обратимыми заменами переменных, когда задаваемые ими квадратичные формы $f, g : \mathbb{R}^n \to \mathbb{R}$ имеют одинаковый ранг и индекс. □

17.4.1. Квадратичные формы на евклидовом пространстве. Если на вещественном векторном пространстве V имеется евклидова структура, то поляризацию $\tilde{q}$ любой квадратичной формы q на V можно единственным образом представить в виде $\tilde{q}(u,w) = (u, f_q w)$, где скобки в правой части означают евклидово скалярное произведение на V, а через $f_q : V \to V$ обозначен линейный оператор, отвечающий симметричной билинейной форме $\tilde{q}$ при задаваемом евклидовым скалярным произведением изоморфизме между формами и операторами[1]. В любом евклидово ортонормальном базисе пространства V матрица оператора f_q совпадает с матрицей Грама формы $\tilde{q}$ в этом базисе. В частности, она симметрична, а значит, оператор f_q евклидово самосопряжён. В прим. 16.1 на стр. 295 мы видели, что в пространстве V найдётся евклидово ортонормальный базис, в котором матрица оператора f_q диагональна. Диагональные элементы этой матрицы суть собственные числа оператора f_q учётом их кратностей. Мы получаем следующие полезные результаты.

Теорема 17.7 (теорема о нормальном базисе)
Для любой квадратичной формы q на евклидовом пространстве V существует евклидово ортонормальный базис, в котором матрица Грама формы q диагональна. Диагональные элементы

[1] См. n° 15.4 на стр. 279.

такой матрицы с точностью до перестановки не зависят от выбора указанного базиса и равны собственным числам того единственного линейного оператора $f : V \to V$, для которого

$$q(v) = (v, fv) \quad \text{при всех } v \in V.$$

Если все $\dim V$ собственных чисел различны, то ортонормальный базис, в котором матрица Грама формы q диагональна, единственен с точностью до перестановки базисных векторов и замены их направлений на противоположные. □

Следствие 17.7
Два однородных многочлена второй степени $f, g \in \mathbb{R}[x_1, \dots, x_n]$ тогда и только тогда переводятся друг в друга ортогональными[1] заменами переменных, когда их матрицы Грама в ортонормальном базисе имеют равные характеристические многочлены. □

17.4.2. Вычисление сигнатуры квадратичной формы на $\mathbb{R}^n$ можно осуществить несколькими способами.

Пример 17.3 (использование евклидовой структуры)
Согласно теор. 17.7 и предваряющему её рассуждению, положительный и отрицательный индексы инерции квадратичной формы на $\mathbb{R}^n$ равны количествам положительных и отрицательных собственных чисел (с учётом кратностей) матрицы Грама этой формы в любом ортонормальном для стандартной евклидовой структуры базисе пространства $\mathbb{R}^n$.

Пример 17.4 (метод Якоби – Сильвестра)
Обозначим через $V_k \subset \mathbb{R}^n$ линейную оболочку первых k базисных векторов $e_1, \dots, e_k$, а через Δ_k их определитель Грама, т. е. рассматриваемый с точностью до умножения на ненулевые положительные числа[2] главный угловой $k \times k$ минор матрицы Грама формы, сосредоточенный в первых k строках и столбцах. Если ограничение формы на подпространство V_k невырождено, то знак $\operatorname{sgn} \Delta_k = (-1)^{m_k}$, где показатель m_k равен отрицательному индексу инерции ограничения формы на V_k. Таким образом, когда все $\Delta_i \neq 0$, соседние миноры Δ_k, Δ_{k+1} различаются знаком если и только если отрицательный индекс инерции $m_{k+1} = m_k + 1$. Поэтому полный отрицательный индекс инерции $m = m_n$ в этом случае равен числу перемен знака в последовательности $1, \Delta_1, \dots, \Delta_n$.

Если некоторый $\Delta_k = 0$, но при этом Δ_{k-1} и Δ_{k+1} оба ненулевые, то ограничения формы на подпространства V_{k+1} и V_{k-1}, а также на двумерное ортогональное дополнение W к подпространству V_{k-1} внутри V_{k+1} невырождены, и в W имеется изотропный вектор, порождающий ядро ограничения формы на подпространство V_k, где она вырождена. Тем самым, $W \simeq H_2$ является гиперболической плоскостью с сигнатурой $(1,1)$, и из ортогонального разложения $V_{k+1} = V_{k-1} \dotplus W$ вытекает равенство $(p_{k+1}, m_{k+1}) = (p_{k-1} + 1, m_{k-1} + 1)$. Обратите внимание, что в этом случае Δ_{k-1} и Δ_{k+1} имеют противоположные знаки, т. е. при $\Delta_k = 0$ неравенство $\Delta_{k-1}\Delta_{k+1} > 0$ невозможно.

Если $\Delta_k = \Delta_{k+1} = 0$, но при этом $\Delta_{k-1}\Delta_{k+2} \neq 0$, то $V_{k+2} = V_{k-1} \dotplus W$, где W — трёхмерное ортогональное дополнение к V_{k-1} внутри V_{k+2}. Как и выше, ограничение формы на W невырождено, и в W есть изотропный вектор. Поэтому W имеет сигнатуру $(2,1)$ или $(1,2)$ и

$$(p_{k+2}, m_{k+2}) = (p_{k-1} + 2, m_{k-1} + 1), \quad \text{если } \Delta_{k-1}\Delta_{k+2} < 0,$$
$$(p_{k+2}, m_{k+2}) = (p_{k-1} + 1, m_{k-1} + 2), \quad \text{если } \Delta_{k-1}\Delta_{k+2} > 0.$$

[1] Т. е. сохраняющими стандартное евклидово скалярное произведение на $\mathbb{R}^n$
[2] Т. е. на ненулевые квадраты поля $\mathbb{R}$.

Итак, когда в последовательности $1, \Delta_1, \dots, \Delta_n$ не встречается более двух нулей подряд, прочтение её слева направо позволяет проследить за изменением сигнатуры (p_i, m_i) ограничения формы на пространства V_i с ненулевыми Δ_i и найти индекс.

Скажем, пусть $\Delta_1 < 0$, $\Delta_2 = 0$, $\Delta_3 > 0$, $\Delta_4 = 0$, $\Delta_5 = 0$, $\Delta_6 < 0$. Тогда

$$(p_1, m_1) = (0, 1), \quad (p_3, m_3) = (2, 1), \quad (p_6, m_6) = (4, 2).$$

Примером такой формы является форма с матрицей Грама

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Пример 17.5 (метод Гаусса)
Над любым полем $\Bbbk$ перейти от произвольного базиса $e_1, \dots, e_n$ к ортогональному базису заданной симметричной билинейной формы $\tilde{q}$ можно при помощи гауссовых элементарных преобразований базисных векторов[1]: перестановок каких-нибудь двух векторов e_i, e_j местами и замен одного из базисных векторов e_i на вектор $e_i' = e_i + \lambda e_j$, где $j \neq i$, а $\lambda \in \Bbbk$ произвольно, или на вектор $e_i' = \lambda e_i$, где $\lambda \in \Bbbk^*$ отлично от нуля. При перестановке местами векторов e_i, e_j в матрице Грама формы $\tilde{q}$ одновременно[2] переставляются друг с другом i-я и j-я строки, а также i-й и j-й столбцы. Обратите внимание, что диагональные элементы $\tilde{q}(e_i, e_i)$ и $\tilde{q}(e_j, e_j)$ при этом переставляются друг с другом, а элементы $\tilde{q}(e_i, e_j) = \tilde{q}(e_j, e_i)$ остаются без изменения, и матрица в целом остаётся симметричной. Например, перестановка первого и третьего базисного вектора действует на симметричную 3×3 матрицу так:

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \mapsto \begin{pmatrix} f & e & c \\ e & d & b \\ c & b & a \end{pmatrix}.$$

Если заменить вектора e_i на λe_i, то i-я строка и i-й столбец матрицы Грама умножатся на λ (всё равно в каком порядке). Обратите внимание, что диагональный элемент $\tilde{q}(e_i, e_i)$ при этом умножится на λ^2. Например, замена e_2 на $2e_2$ подействует на предыдущую матрицу так:

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \mapsto \begin{pmatrix} a & 2b & c \\ 2b & 4d & 2e \\ c & 2e & f \end{pmatrix}.$$

Наконец, замена e_i на $e_i' = e_i + \lambda e_j$ преобразует стоящие в i-й строке и i-м столбце недиагональные элементы $q_{ik} = \tilde{q}(e_i, e_k)$ и $q_{ki} = \tilde{q}(e_k, e_i)$ с $k \neq i$ в элементы $q_{ik}' = q_{ik} + \lambda q_{jk}$ и $q_{ki}' = q_{ki} + \lambda q_{kj}$ соответственно, а диагональный элемент $q_{ii} = \tilde{q}(e_i, e_i)$ — в $q_{ii}' = q_{ii} + \lambda q_{ij} + \lambda q_{ji} + \lambda^2 q_{jj}$, т. е. к i-й

[1] См. n° 9.2 на стр. 158.

[2] Точнее, i-я строка переставляется с j-й, а потом i-й столбец переставляется с j-м, либо в другой последовательности: сначала i-й столбец переставляется с j-м, а потом i-я строка переставляется с j-й, и результат не зависит от того, какая перестановка осуществляется первой, а какая второй.

строке матрицы Грама прибавится j-я, умноженная на λ, после чего *в получившейся матрице* к i-у столбцу матрицы прибавится j-й, умноженный на λ. Обратите внимание, что те же действия можно произвести в другой последовательности: сначала к i-у столбцу матрицы прибавить j-й, умноженный на λ, а потом в полученной матрице к i-у столбцу прибавить j-й, умноженный на λ, — результат получится тот же, и матрица в целом останется симметричной. Например, замена e_3 на $e_3 + 3e_2$ подействует на предыдущую матрицу так:

$$\begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix} \mapsto \begin{pmatrix} a & b & c+3b \\ b & d & e+3d \\ c+3b & e+3d & f+6e+9d \end{pmatrix}.$$

Метод Гаусса заключается в том, чтобы при помощи описанных трёх типов преобразований матрицы Грама превратить заданную симметричную матрицу в диагональную[1]. Для вещественной формы количества положительных и отрицательных чисел на диагонали итоговой матрицы — это в точности положительный и отрицательный индексы инерции.

Для иллюстрации вычислим методом Гаусса сигнатуру вещественной квадратичной формы с матрицей Грама

$$\begin{pmatrix} -1 & 2 & 0 & -3 \\ 2 & 2 & -1 & 0 \\ 0 & -1 & 0 & -2 \\ -3 & 0 & -2 & 0 \end{pmatrix}.$$

Сначала обнулим[2] 1-ю строку и 1-й столбец вне диагонали, добавляя к векторам e_2, e_4 соответственно векторы $2e_1$ и $-3e_1$:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 6 & -1 & -6 \\ 0 & -1 & 0 & -2 \\ 0 & -6 & -2 & 9 \end{pmatrix}.$$

Теперь обнулим вне диагонали 2-ю строку и 2-й столбец, добавляя к текущим векторам e_3, e_4 соответственно текущие векторы $e_1/6$ и e_1:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & -\frac{1}{6} & -3 \\ 0 & 0 & -3 & 3 \end{pmatrix}.$$

Наконец, обнулим вне диагонали 3-ю строку и 3-й столбец, добавляя к текущему вектору e_4 текущий вектор $-18e_3$:

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & -\frac{1}{6} & 0 \\ 0 & 0 & 0 & 57 \end{pmatrix}.$$

[1] Обратите внимание, что эта процедура похожа на ортогонализацию Грама – Шмидта из предл. 14.1 на стр. 256, только порядок действий предлагается таким, как в доказательстве теор. 16.1 на стр. 292: выбрать базисный вектор с ненулевым скалярным квадратом, спроектировать все остальные базисные векторы на ортогонал к нему, затем выбрать среди них вектор с ненулевым квадратом и т. д.

[2] Обратите внимание, что вычисления достаточно проделывать только для клеток, стоящих на главной диагонали и под нею — наддиагональная часть матрицы восстанавливается из соображений симметрии.

Таким образом, форма имеет сигнатуру $(2,2)$.

17.5. Проективные квадрики. Ненулевая квадратичная форма $q \in S^2V^*$ задаёт в проективном пространстве $\mathbb{P}(V)$ алгебраическую гиперповерхность[1]

$$Q = V(q) = \{v \in V \smallsetminus 0 \mid q(v) = 0\},$$

которая состоит из одномерных изотропных подпространств формы q и называется *проективной квадрикой*. Квадрика $V(q)$ называется *гладкой* или *неособой*, если невырождена квадратичная форма q. В противном случае квадрика называется *особой* или *вырожденной*.

17.5.1. Квадрики на $\mathbb{P}_1$. В прим. 17.2 на стр. 314 мы видели, что при $\dim V = 2$ вырожденность квадрики $V(q)$ означает обращение в нуль дискриминанта квадратичной формы q. В этом случае форма $q = \psi^2$ является квадратом ненулевой линейной формы $\psi \in V^*$, обращающейся в нуль в единственной точке $p = \mathbb{P}\operatorname{Ann}\xi \subset \mathbb{P}(V)$, и квадрика $V(q)$ называется *двойной точкой* p.

Гладкая квадрика имеет ненулевой дискриминант и либо состоит из двух различных точек, либо пуста. Первое происходит, когда $D/4 = -\det(q)$ является квадратом в $\Bbbk$, что всегда так, если поле $\Bbbk$ алгебраически замкнуто, второе — когда $D/4 = -\det(q)$ не квадрат, и над алгебраически замкнутым полем $\Bbbk$ такого не бывает.

Мы заключаем, что в проективном пространстве любой размерности произвольные квадрика Q и прямая ℓ пересекаются ровно одним из следующих четырёх способов: либо $\ell \subset Q$, либо $\ell \cap Q$ это одна двойная точка, либо $\ell \cap Q$ это две различные точки, либо $\ell \cap Q = \varnothing$, причём над алгебраически замкнутым полем последний случай невозможен.

17.5.2. Касательные прямые и касательное пространство. Прямая, проходящая через точку $a \in Q$, называется *касательной* к Q в точке a, если она лежит на Q или пересекает Q по двойной точке a. Объединение всех прямых, касающихся Q в a, обозначается T_aQ и называется *проективным касательным пространством* к квадрике Q в точке $a \in Q$. На языке формул прямая $(ab) \subset \mathbb{P}(V)$ касается квадрики $Q = V(q)$ в точке $a \in Q$ если и только если матрица Грама ограничения формы q на $\operatorname{span}(a,b) \subset V$ вырождена, т. е.

$$\det \begin{pmatrix} 0 & \tilde{q}(a,b) \\ \tilde{q}(a,b) & q(b) \end{pmatrix} = \tilde{q}(a,b)^2 = 0,$$

где $\tilde{q} : V \times V \to \Bbbk$ — поляризация[2] формы q. Мы заключаем, что

$$b \in T_aQ \quad \Longleftrightarrow \quad \tilde{q}(a,b) = 0. \tag{17-7}$$

Если $b \notin Q$, то ограничение формы q на одномерное подпространство $b \subset V$ невырождено и $V = b \oplus b^\perp$. Формула (17-7) утверждает, что видимый из точки $b \notin Q$ контур квадрики Q, т. е. ГМТ пересечения с квадрикой Q всевозможных касательных, опущенных на неё из точки b, высекается из квадрики Q не проходящей через точку b гиперплоскостью

$$\mathbb{P}(b^\perp) = \{x \mid \tilde{q}(x,b) = 0\}, \tag{17-8}$$

которая называется *полярой* точки b относительно квадрики Q. Из формулы (17-7) также следует, что касательное пространство

$$T_aQ = \mathbb{P}(a^\perp) = \{x \mid \tilde{q}(x,a) = 0\} \tag{17-9}$$

[1] См. n° 13.6.2 на стр. 249.
[2] См. n° 17.2 на стр. 313.

либо является гиперплоскостью в $\mathbb{P}(V)$, либо совпадает со всем пространством $\mathbb{P}(V)$. В первом случае точка $a \in Q$ называется *гладкой* или *неособой*, а во втором — *особой*. Последнее означает, что $\tilde{q}(v, a) = 0$ для всех $v \in V$, т. е. что a лежит в ядре корреляции[1] $q^\wedge : V \to V^*$, переводящей вектор $v \in V$ в линейную форму $w \mapsto \tilde{q}(w, v)$ на пространстве V. Подпространство $\ker q^\wedge$ изотропно и его проективизация

$$\operatorname{Sing} Q \stackrel{\text{def}}{=} \mathbb{P}(\ker q^\wedge) \subset Q$$

называется *пространством особых точек* или *вершинным пространством* квадрики Q. Вершинное подпространство непусто если и только если квадрика $Q = V(q)$ особа, т. е. $\det q = 0$.

Теорема 17.8
Пересечение особой квадрики Q с любым дополнительным к $\operatorname{Sing} Q$ проективным подпространством $L \subset \mathbb{P}(V)$ является гладкой (возможно пустой) квадрикой $Q' = L \cap Q$ в подпространстве L, и исходная квадрика Q является линейным соединением[2] Q' и $\operatorname{Sing} Q$.

Доказательство. Невырожденность ограничения формы q на подпространство L была доказана в предл. 16.1 на стр. 291. Каждая пересекающая $\operatorname{Sing} Q$ прямая, будучи касательной к квадрике Q, либо целиком лежит на квадрике Q, либо пересекает Q ровно в одной точке — точке своего пересечения с $\operatorname{Sing} Q$. Поэтому каждая прямая (a, b) с $a \in \operatorname{Sing} Q$, $b \in Q'$ целиком лежит на Q, т. е. $J(Q', \operatorname{Sing} Q) \subset Q$. По упр. 13.15 каждая не лежащая в L гладкая точка $c \in Q$ лежит на некоторой прямой, пересекающей и L, и $\operatorname{Sing} Q$. Поскольку эта прямая пересекает Q в точке $c \notin \operatorname{Sing} Q$, она целиком лежит на квадрике, а значит, пересекает L в точке, лежащей на квадрике Q'. Поэтому $Q \subset J(Q', \operatorname{Sing} Q)$. □

Упражнение 17.9. Покажите, что квадрика, имеющая хоть одну гладкую точку, не содержится в гиперплоскости.

Пример 17.6 (коники)
Квадрики на плоскости называются *ониками*. С гладкой коникой в $\mathbb{P}_2(\mathbb{R})$ мы встречались в прим. 13.11 на стр. 249.

Если $\operatorname{rk} q = 1$, то уравнение $q(x) = 0$ переписывается в ортогональном базисе как $x_0^2 = 0$. Такая коника $C = V(q)$ совпадает с $\operatorname{Sing} C$ и называется *двойной прямой*. В терминах теор. 17.8 коника C является линейным соединением прямой $\operatorname{Sing} C$ и пустой нульмерной квадрики[3].

Если $\operatorname{rk} q = 2$, то $\operatorname{Sing} q$ является проективизацией одномерного ядра формы q и состоит из одной точки s. По теор. 17.8 пересечение такой коники C с любой не проходящей через s прямой, будучи гладкой квадрикой на этой прямой, либо состоит из двух разных точек, либо пусто,и над алгебраически замкнутым полем последнее невозможно. В первом случае C является объединением двух различных прямых, пересекающихся в её особой точке s, и называется *распавшейся*, а форма $q = \psi_1\psi_2$ является произведением двух различных линейных форм. Во втором случае коника C называется *двойной точкой* и визуально совпадает со своей особой точкой. Например, над полем $\mathbb{R}$ уравнение $x_0^2 + x_1^2 = 0$ задаёт двойную точку $(0 : 0 : 1)$.

[1] См. n° 15.1.1 на стр. 272.
[2] Т. е. объединением всех прямых вида (ab) с $a \in Q'$ и $b \in \operatorname{Sing} Q$, ср. с упр. 13.16 на стр. 245.
[3] Дополнительным подпространством к прямой на плоскости является точка — проективизация одномерного векторного пространства, а невырожденная форма на одномерном пространстве автоматически анизотропна.

Невырожденная квадратичная форма q на трёхмерном векторном пространстве либо анизотропна, либо является прямой ортогональной суммой двумерной гиперболической и одномерной анизотропной форм. В первом случае $V(q) = \varnothing$, и над алгебраически замкнутым полем такое невозможно. Над полем $\mathbb{R}$ примером такой коники служит $x_0^2 + x_1^2 + x_2^2 = 0$. Во втором случае в подходящих координатах коника задаётся уравнением

$$x_1^2 = x_0 x_2\,. \tag{17-10}$$

Поскольку любые значения $x_0 = t_0$, $x_1 = t_1$ однозначно дополняются до тройки

$$(t_0 : t_1 : t_1^2/t_0) = (t_0^2 : t_0 t_1 : t_1^2)\,,$$

удовлетворяющей уравнению (17-10), коника (17-11) является образом *вложения Веронезе*

$$\mathbb{P}_1 \hookrightarrow \mathbb{P}_2\,, \quad (t_0 : t_1) \mapsto (t_0^2 : t_0 t_1 : t_1^2)\,. \tag{17-11}$$

Мы заключаем, что над любым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ имеется единственная с точностью до проективного преобразования непустая невырожденная коника. В подходящих координатах она задаётся уравнением (17-10) и допускает рациональную параметризацию (17-11).

17.5.3. Планарность гладкой квадрики. Размерность максимального по включению проективного пространства, целиком лежащего на гладкой квадрике $Q = V(q) \subset \mathbb{P}(V)$, называется *планарностью* квадрики Q. Планарность пустой квадрики, задаваемой анизотропной формой q, по определению полагается равной -1. Квадрики планарности 0 суть непустые квадрики, не содержащие прямых. Ортогональная группа $\mathrm{O}_q(V)$ невырожденной квадратичной формы q действует на $\mathbb{P}(V)$, переводя квадрику $Q = V(q)$ в себя, и согласно сл. 17.1 на стр. 313 это действие транзитивно на изотропных подпространствах любой фиксированной размерности и, в частности, на точках квадрики Q. Любое ортогональное преобразование, переводящее точку $p \in Q$ в точку $p' \in Q$, биективно отображает множество k-мерных подпространств $L \subset Q$, проходящих через p, в множество k-мерных подпространств $L' \subset Q$, проходящих через p'. Тем самым, через каждую точку m-планарной квадрики можно провести m-мерное проективное подпространство, целиком лежащее на квадрике, и мощность множества таких подпространств не зависит от точки, а никаких $(m+1)$-мерных проективных подпространств на m-планарной квадрике не лежит. По сл. 17.2 на стр. 314 уравнение гладкой m-планарной квадрики записывается в подходящих однородных координатах как

$$x_0 x_1 + x_2 x_3 + \cdots + x_{2m} x_{2m+1} = \alpha(x_{2m+2}, \ldots, x_n)\,, \tag{17-12}$$

где α — анизотропная квадратичная форма от $n - 2m - 1$ переменных. Число $2m + 2$ равно размерности гиперболического слагаемого в разложении пространства V в прямую ортогональную относительно формы $\tilde{q}$ сумму гиперболического и анизотропного подпространств, и максимум размерностей изотропных относительно формы $\tilde{q}$ векторных подпространств в V равен $m + 1$. При фиксированном n планарность m может принимать значение в пределах

$$-1 \leqslant m \leqslant (n-1)/2\,.$$

Квадрики (17-12) с разными m не переводятся одна в другую проективными преобразованиями.

Пример 17.7 (квадрики максимальной планарности)
Максимально возможная планарность квадрики $Q \subset \mathbb{P}_n$ равна $(n-1)/2$ при нечётном n и $(n-2)/2$ при чётном n. Над алгебраически замкнутым полем все невырожденные квадрики имеют максимальную планарность. Над любым полем уравнение квадрики максимальной планарности в $\mathbb{P}_n$ в подходящих однородных координатах записывается в виде

$$0 = x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} \text{ при } n = 2m+1\,, \tag{17-13}$$

$$x_0^2 = x_1x_{m+1} + x_2x_{m+2} + \cdots + x_mx_{2m} \text{ при } n = 2m\,. \tag{17-14}$$

Поэтому все квадрики максимальной планарности переводятся друг в друга проективными преобразованиями. Например, все непустые гладкие коники на $\mathbb{P}_2$ проективно конгруэнтны, как мы уже видели в прим. 17.6 на стр. 322.

Пример 17.8 (гладкие вещественные квадрики)
Над полем $\mathbb{R}$ при каждом $k \in \mathbb{N}$ есть единственная с точностью до изометрии и умножения на константу анизотропная форма от k переменных: $x_1^2 + \ldots + x_k^2$. Поэтому каждая гладкая вещественная квадрика размерности n, лежащая в $(n+1)$-мерном пространстве $\mathbb{P}_{n+1}(\mathbb{R})$, в подходящих однородных координатах задаётся уравнением

$$x_0x_1 + x_2x_3 + \ldots + x_{2m}x_{2m+1} = x_{2m+2}^2 + \ldots + x_{n+1}^2\,, \quad -1 \leqslant m \leqslant n/2\,. \tag{17-15}$$

При разных m эти уравнения задают квадрики разной планарности и тем самым являют собою полный список различных гладких вещественных квадрик с точностью до проективного преобразования.

Предложение 17.4
Сечение гладкой квадрики $Q \subset \mathbb{P}_n$ произвольной гиперплоскостью Π либо является гладкой квадрикой в этой гиперплоскости, либо имеет единственную особую точку $p \in \Pi \cap Q$. Последнее равносильно тому, что $\Pi = T_pQ$ касается квадрики в точке p, и в этом случае $Q \cap T_p$ является конусом с вершиной в p над гладкой квадрикой на единицу меньшей планарности и на два меньшей размерности, чем у Q, расположенной в $(n-2)$-мерной плоскости, дополнительной к p внутри T_pQ.

Доказательство. Пусть $\mathbb{P}_n = \mathbb{P}(V)$, $\Pi = \mathbb{P}(W)$ и $Q = V(q)$. Ядро ограничения оператора корреляции $\hat{q} : V \xrightarrow{\sim} V^*$ на подпространство $W \subset V$ является пересечением W с одномерным подпространством $W^\perp \subset V$. Это пересечение либо нулевое, либо является точкой $p \in \Pi$. В первом случае квадрика $Q \cap \Pi$ невырождена, а во втором имеет единственную особую точку p, причём $\Pi = \mathbb{P}(p^\perp)$ является касательным пространством[1] к Q в точке p. Согласно теор. 17.8 на стр. 322, особая квадрика $Q \cap \Pi$ в пространстве $\Pi \simeq \mathbb{P}_{n-1}$ является линейным соединением точки p и неособой квадрики, лежащей в любой не проходящей через p гиперплоскости $\mathbb{P}(U) \simeq \mathbb{P}_{n-2} \subset \Pi$. Так как ограничение квадратичной формы q на подпространство $U \subset V$ невырождено, имеется ортогональное разложение $V = U \oplus U^\perp$. Ограничение формы q на двумерное пространство $U^\perp$ невырождено, и в $U^\perp$ есть изотропная прямая $p \subset U^\perp$. Следовательно, $U^\perp \simeq H_2$ является гиперболической плоскостью, и размерность гиперболической составляющей ограничения $q|_U$ на два меньше, чем у самой формы q на V, т. е. планарность гладкой квадрики $Q \cap \mathbb{P}(U)$ на единицу меньше, чем у Q. □

[1] См. формулу (17-9) на стр. 321.

Задачи для самостоятельного решения к §17

Задача 17.1. Симметричная билинейная форма на $\mathbb{R}^5$ имеет в стандартном базисе матрицу Грама

$$\begin{pmatrix} -12 & 14 & -5 & -3 & 8 \\ 14 & -17 & 2 & 5 & -8 \\ -5 & 2 & -12 & 3 & 6 \\ -3 & 5 & 3 & -3 & 1 \\ 8 & -8 & 6 & 1 & -6 \end{pmatrix}$$

Найдите ранг и сигнатуру её ограничения на пространство решений системы

$$\begin{cases} 2x_1 + 2x_2 - 3x_3 - 4x_4 - 7x_5 = 0 \\ -x_1 - x_2 + 2x_3 + 2x_4 + 4x_5 = 0 \end{cases}$$

и напишите уравнение гиперплоскости, отражение в которой[1] переводит друг в друга прямые с направляющими векторами $(3, 0, 2, 3, 6)$ и $(0, 3, -11, -12, -18)$, а также найдите ортогональные проекции этих векторов на эту гиперплоскость.

Задача 17.2. Найдите ранг и сигнатуру ограничения квадратичной формы, имеющей в стандартных координатах на $\mathbb{R}^4$ вид

$$-4x_1^2 - 25x_2^2 - 2x_3^2 - 11x_4^2 + 20x_1x_2 + 4x_1x_3 - 6x_1x_4 - 10x_2x_3 + 16x_2x_4 + 2x_3x_4\,,$$

на ортогонал к вектору $v = (0, 3, 0, -7)$ относительно поляризации этой формы.

Задача 17.3. Существует ли на $\mathbb{R}^7$ квадратичная форма с главными угловыми минорами

а) $\Delta_1 > 0$, $\Delta_2 = 0$, $\Delta_3 > 0$, $\Delta_4 < 0$, $\Delta_5 = 0$, $\Delta_6 < 0$, $\Delta_7 > 0$

б) $\Delta_1 > 0$, $\Delta_2 = 0$, $\Delta_3 < 0$, $\Delta_4 > 0$, $\Delta_5 = 0$, $\Delta_6 < 0$, $\Delta_7 < 0$

в) $\Delta_1 > 0$, $\Delta_2 = 0$, $\Delta_3 = 0$, $\Delta_4 < 0$, $\Delta_5 = 0$, $\Delta_6 > 0$, $\Delta_7 < 0$

г) $\Delta_1 > 0$, $\Delta_2 = 0$, $\Delta_3 = 0$, $\Delta_4 > 0$, $\Delta_5 = 0$, $\Delta_6 < 0$, $\Delta_7 < 0$?

Если да, выясните, какой может быть её сигнатура, и предъявите явный пример такой матрицы Грама. Если нет, объясните, почему.

Задача 17.4. В последовательности главных левых верхних угловых миноров матрицы Грама квадратичной формы на $\mathbb{R}^{11}$ отличны от нуля лишь $\Delta_2 < 0, \Delta_5 > 0, \Delta_8 > 0, \Delta_{11} < 0$. Найдите ранг и сигнатуру ограничения этой формы на ортогонал (относительно неё же) к линейной оболочке первых 7 базисных векторов.

Задача 17.5. Для квадратичной формы $-5x_1^2 - 8x_2^2 - 21x_3^2 - 12x_1x_2 + 20x_1x_3 + 22x_2x_3$ на $\mathbb{Q}^3$:

а) укажите какой-нибудь ортогональный базис

б) разложите $\mathbb{Q}^3$ в прямую ортогональную сумму гиперболического и анизотропного подпространств

в) опишите все изотропные векторы.

Задача 17.6. Разложите в ортогональную прямую сумму гиперболической и анизотропной квадратичные формы[2]

а) $-x_1^2 + 2x_1x_2 + x_2^2 + 6x_2x_3 + 5x_3^2$

[1] Имеется в виду отражение в пространстве со скалярным произведением, которое является поляризацией заданной формы.

[2] Явно укажите гиперболический базис в какой-нибудь гиперболической плоскости и анизотропный вектор в ортогонале к ней

б) $-5x_1^2 - 18x_1x_2 - 16x_1x_3 - 17x_2^2 - 30x_2x_3 - 13x_3^2$
в) $-2x_1x_2 - 8x_1x_3 - 5x_2^2 - 22x_2x_3 - 7x_3^2$
г) $-13x_1^2 + 22x_1x_2 - 28x_1x_3 - 10x_2^2 + 24x_2x_3 - 15x_3^2$.

Задача 17.7. Существует ли (1) линейная обратимая (2) ортогональная[1] замена координат в $\mathbb{R}^3$, переводящая квадратичную форму
а) $x_1^2 - \frac{11}{9}x_2^2 + \frac{2}{9}x_3^2 + \frac{32}{9}x_1x_2 - \frac{16}{9}x_1x_3 + \frac{8}{3}x_2x_3$ в квадратичную форму

$$-\frac{1}{3}x_1^2 - \frac{2}{3}x_2^2 + x_3^2 - 4x_1x_2 - \frac{8}{3}x_1x_3 - \frac{4}{3}x_2x_3$$

б) $-\frac{1}{9}x_1^2 - \frac{7}{9}x_2^2 - \frac{1}{9}x_3^2 + \frac{8}{9}x_1x_2 - \frac{16}{9}x_1x_3 - \frac{8}{9}x_2x_3$ в квадратичную форму

$$\frac{1}{9}x_1^2 - \frac{14}{9}x_2^2 - \frac{5}{9}x_3^2 + \frac{4}{9}x_1x_2 - \frac{32}{9}x_1x_3 - \frac{28}{9}x_2x_3$$

в) $\frac{10}{9}x_1^2 + \frac{13}{9}x_2^2 + \frac{13}{9}x_3^2 - \frac{4}{9}x_1x_2 - \frac{4}{9}x_1x_3 + \frac{8}{9}x_2x_3$ в квадратичную форму

$$\frac{11}{9}x_1^2 - \frac{2}{9}x_2^2 - x_3^2 - \frac{8}{3}x_1x_2 + \frac{32}{9}x_1x_3 - \frac{16}{9}x_2x_3?$$

Задача 17.8. Докажите, что каждое собственное[2] изометрическое линейное преобразование евклидова пространства $\mathbb{R}^3$ является поворотом вокруг прямой (возможно, на нулевой угол), а каждое несобственное — композицией такого поворота с отражением в плоскости, перпендикулярной оси поворота.

Задача 17.9. В евклидовом пространстве $\mathbb{R}^n$ приведите к главным осям[3] квадратичные формы, имеющие в стандартных координатах вид а) $x_1^2 - 5x_2^2 + x_3^2 + 4x_1x_2 + 2x_1x_3 + 4x_2x_3$
б) $2x_1x_2 - 6x_1x_3 - 6x_2x_4 + 2x_2x_4$ в) $3x_1^2 - 3x_2^2 + 4x_3^2 + x_4^2 + 8x_1x_2 - 4x_3x_4$
г) $9x_1^2+5x_2^2+5x_3^2+8x_4^2+8x_2x_3-4x_2x_4+4x_3x_4$ д) $9x_1^2+5x_2^2+5x_3^2+8x_4^2+8x_2x_3-4x_2x_4+4x_3x_4$
и определите планарность соответствующих вещественных проективных квадрик.

Задача 17.10. Пусть в поле $\Bbbk$ уравнение $x^2 = a$ разрешимо относительно x при любом $a \in \Bbbk$. Покажите, что любая невырожденная квадратичная форма на $\Bbbk^n$ при $n \geqslant 2$ обладает
а) изотропным подпространством размерности $[n/2]$
б) двумя изотропными подпространствами размерности $[n/2]$ с нулевым пересечением.

Задача 17.11. Какими могут быть ранг и сигнатура ограничения невырожденной вещественной квадратичной формы сигнатуры (p, m) на векторное подпространство коразмерности 1?

Задача 17.12. Обозначим через W пространство однородных грассмановых многочленов степени 2 от четырёх переменных $\xi_1, \ldots, \xi_4$ и зададим на W билинейную форму $p\colon W \times W \to \Bbbk$ правилом

$$\omega_1 \wedge \omega_2 = p(\omega_1, \omega_2) \cdot \xi_1 \wedge \xi_2 \wedge \xi_3 \wedge \xi_4\,.$$

Напишите матрицу Грама формы p в базисе $\xi_{ij} = \xi_i \wedge \xi_j$ $(1 \leqslant i < j \leqslant 4)$ и убедитесь, что эта форма симметрична и невырождена. Какова её сигнатура над полем $\Bbbk = \mathbb{R}$?

[1] Т. е. замена стандартного евклидово ортонормального базиса на другой евклидово ортонормальный базис.

[2] Т. е. сохраняющее ориентацию, см. ?? на стр. ??.

[3] Укажите какой-нибудь ортонормальный базис, в котором матрица Грама диагональна, и саму эту матрицу.

Задача 17.13. Убедитесь, что функция $A \mapsto \det A$ является квадратичной формой на пространстве $\mathrm{Mat}_2(\Bbbk)$, и опишите такое линейное преобразование $Y \mapsto Y^?$ пространства $\mathrm{Mat}_2(\Bbbk)$, что поляризация формы det имеет вид $2\,\widetilde{\det}(X,Y) = \mathrm{tr}(XY^?)$. Является ли форма det гиперболической?

Задача 17.14. Зафиксируем в пространстве W квадратичных форм от переменных (x_0, x_1) базис x_0^2, $2x_0x_1$, x_1^2 и свяжем с каждой 2×2 матрицей A линейный оператор $S^2A : W \to W$, переводящий $f(x_0, x_1)$ в $f(y_0, y_1)$, где $(y_0, y_1) = (x_0, x_1)\,A$. Напишите его матрицу в выбранном базисе и выразите её след и определитель через $\mathrm{tr}\,A$ и $\det A$.

Задача 17.15. Для $X \in \mathrm{Mat}_n(\mathbb{R})$ пусть $\det(tE - X) = t^n - \sigma_1(X)\,t^{n-1} + \sigma_2(X)\,t^{n-2} - \ldots$. Убедитесь, что $\sigma_2(X)$ является квадратичной формой на пространстве $\mathrm{Mat}_n(\mathbb{R})$, и вычислите её ранг и сигнатуру. Если общий случай вызывает затруднения, решите задачу для $n = 2, 3, 4$.

Задача 17.16. Найдите сигнатуру квадратичной формы $\mathrm{tr}\left(A^2\right)$ на пространстве $\mathrm{Mat}_n(\mathbb{R})$. Если общий случай вызывает затруднения, решите задачу для $n = 2, 3, 4$.

Задача 17.17. Рассмотрим поле $\mathbb{F}_{27} = \mathbb{F}_3[x]/(x^3 - x + 1)$ как трёхмерное векторное пространство над полем $\mathbb{F}_3$. Напишите матрицу Грама симметричной билинейной формы[1] $\mathrm{tr}(ab)$ в базисе $[1]$, $[x]$, $[x^2]$ и опишите все изотропные векторы этой формы.

Задача 17.18 (проекция квадрики на гиперплоскость). Рассмотрим гладкую квадрику

$$Q = V(q) \subset \mathbb{P}(V),$$

точку $p \in Q$ и гиперплоскость $H = \mathbb{P}(U)$, не проходящую через p. Покажите, что проекция $\pi_p : \mathbb{P}(V) \smallsetminus p \twoheadrightarrow H$ из p на H задаёт биекцию $Q \smallsetminus T_pQ \xrightarrow{\sim} H \smallsetminus T_pQ$ между не лежащими в касательном пространстве T_pQ точками квадрики и аффинной картой в H, дополнительной к пересечению $T_pQ \cap H$, причём при этой биекции точка $x \in H$ соответствует точке $y \in Q \cap (px)$ с однородными координатами[2] $(-q(x) : 2\tilde{q}(p, x))$ в базисе p, x на прямой px.

Задача 17.19. Выведите из предыдущей задачи, что проекция непустой гладкой коники $C = V(q)$ из точки $p \in C$ на прямую $\ell \not\ni p$, доопределённая в самой точке p правилом $p \mapsto \ell \cap T_pC$, задаёт биекцию $C \xrightarrow{\sim} \ell$, причём прообразом точки $x \in \ell$ является точка $q(x, x)\,p - 2\tilde{q}(p, x)\,x$, и напишите рациональные параметризации коник с аффинными уравнениями[3]

а) $2x^2 + 3xy + y^2 + 7x + 6y + 6 = 0$

б) $5x^2 + 5xy - 9y^2 + 8x - 3y + 2 = 0$

в) $2x^2 + 15xy - 2y^2 - 4x - 4y + 1 = 0$.

Задача 17.20. Покажите, что гладкая проективная квадратичная поверхность $V(f) \subset \mathbb{P}_3(\mathbb{F}_q)$ имеет планарность 0 и состоит из $q^2 + 1$ точек, если $\det(f)$ не квадрат, и имеет планарность 1 и состоит $(q + 1)^2$ точек, если $\det(f)$ квадрат.

Задача 17.21. Из скольких точек состоит квадрика

$$6x_0^2 + 4x_0x_1 + 4x_0x_2 + x_0x_3 - 8x_1^2 + 3x_1x_2 + 3x_1x_3 - 8x_2^2 + 3x_2x_3 = 0$$

[1] След умножения на $ab : K \to K$, $x \mapsto ab\,x$.

[2] Подсказка: непропорциональный p изотропный вектор формы q в двумерном векторном пространстве $\mathrm{span}(p, x)$ является отражением $\sigma_x(p) \in Q$ изотропного вектора p в гиперплоскости $x^\perp$, ортогональной относительно формы $\tilde{q}$ анизотропному вектору x.

[3] О преобразовании локальных аффинных уравнений в глобальные однородные см. n° 13.6.3 на стр. 250.

в $\mathbb{P}_3(\mathbb{F}_{19})$?

Задача 17.22. Выясните, сколько решений имеет уравнение

а) $x_0x_1 - x_1x_2 + x_0x_2 = 0$ в поле $\mathbb{F}_9$

б) $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$ в поле $\mathbb{F}_9$

в) $-x_0x_1 + x_0x_2 + 3x_0x_3 - 3x_1^2 + x_1x_2 + x_1x_3 - 3x_2^2 - x_2x_3 + 2x_3^2 = 0$ в поле $\mathbb{F}_7$

г) $6x_0^2 + 4x_0x_1 + 4x_0x_2 + x_0x_3 - 8x_1^2 + 3x_1x_2 + 3x_1x_3 - 8x_2^2 + 3x_2x_3 = 0$ в поле $\mathbb{F}_{19}$.

Задача 17.23. Покажите, что на $\mathbb{P}_2(\Bbbk)$ пересечение непустой гладкой коники с любой кривой, заданной однородным степени d, либо совпадает с этой коникой, либо состоит из не более чем $2d$ точек.

Задача 17.24. Покажите, что через любые 5 точек плоскости проходит коника, причём если никакие 4 из точек не коллинеарны, такая коника единственна, а если никакие 3 не коллинеарны, то она гладкая.

Задача 17.25. Покажите, что через любые 9 точек в $\mathbb{P}_3$ проходит квадрика, и выведите отсюда, что любые три прямые в $\mathbb{P}_3$ лежат на некоторой квадрике, причём если прямые попарно не пересекаются, то это гладкая квадрика (максимальной) планарности 1.

Задача 17.26 (двойственная квадрика). Покажите, что касательные гиперплоскости к гладкой квадрике $Q \subset \mathbb{P}(V)$ образуют гладкую квадрику $Q^\times \subset \mathbb{P}(V^*)$, и что квадратичные формы, задающие квадрики Q и $Q^\times$, можно отскалировать так, чтобы их матрицы Грама в двойственных базисах пространств V и V^* стали обратны друг другу.

Задача 17.27. Покажите, что на проективной плоскости любые пять прямых, никакие три из которых не конкурентны, касаются единственной гладкой коники.

Задача 17.28 (полярное преобразование). Покажите, что каждая гладкая квадрика $Q \subset \mathbb{P}_n$ задаёт проективное преобразование

$$\pi_Q : \mathbb{P}_n \xrightarrow{\sim} \mathbb{P}_n^\times, \quad p \mapsto \operatorname{Ann}(p^\perp),$$

переводящее каждую точку $b \notin Q$ в её поляру[1], и убедитесь, что точка a лежит на поляре точки b если и только если точка b лежит на поляре точки a.

[1] См. формулу (17-8) на стр. 321.

§18. Примеры групп

18.1. Группы. Напомню[1], что множество G называется *группой*, если на нём задана операция *композиции* $G \times G \to G$, $(g_1, g_2) \mapsto g_1 g_2$ со свойствами:

$$\text{ассоциативность}: \quad \forall f, g, h \in G \quad (fg)h = f(gh) \tag{18-1}$$

$$\text{наличие единицы}: \quad \exists e \in G : \forall g \in G \quad eg = g \tag{18-2}$$

$$\text{наличие обратных}: \quad \forall g \in G \quad \exists g^{-1} \in G : g^{-1} g = e\,. \tag{18-3}$$

Группа называется *коммутативной* или *абелевой*, если дополнительно имеет место

$$\text{коммутативность}: \quad \forall f, g \in G \quad fg = gf\,. \tag{18-4}$$

Если группа G конечна, число элементов в ней обозначается $|G|$ и называется *порядком* группы G. Подмножество $H \subset G$ называется *подгруппой*, если оно образует группу относительно имеющейся в G композиции. Как мы видели в n° 8.1.4 на стр. 136, для этого достаточно, чтобы вместе с каждым элементом $h \in H$ в H лежал и обратный к нему элемент h^{-1}, а вместе с каждой парой элементов $h_1, h_2 \in H$ — их произведение $h_1 h_2$. Там же объяснялось, что левая единица e единственна и автоматически является правой единицей, а левый обратный к g элемент g^{-1} в (18-3) однозначно определяется элементом g и автоматически является правым обратным.

Пример 18.1 (группы преобразований)
Модельными примерами групп являются *группы преобразований*, обсуждавшиеся в n° 1.6. Все взаимно однозначные отображения произвольного множества X в себя образуют группу. Она обозначается $\operatorname{Aut} X$ и называется *группой автоморфизмов* множества X. Как правило, мы будем сокращать запись $g(x)$, где $g \in G$ и $x \in X$, до gx. Подгруппы $G \subset \operatorname{Aut} X$ называются *группами преобразований* множества X. Если множество X наделено той или иной дополнительной структурой, то биекции $g \in \operatorname{Aut} X$, сохраняющие эту структуру, образуют подгруппу в $\operatorname{Aut} X$, которая обычно называется группой автоморфизмов рассматриваемой структуры.

Пример 18.2 (линейные группы)
С n-мерным векторным пространством V связана группа линейных[2] автоморфизмов $V \xrightarrow{\sim} V$. Она обозначается $\mathrm{GL}(V)$ и называется *полной линейной группой* пространства V. Линейные автоморфизмы определителя[3] 1 составляют в ней подгруппу $\mathrm{SL}(V) \stackrel{\text{def}}{=} \{g \in \mathrm{GL}(V) \mid \det g = 1\}$, которая называется *специальной* линейной группой пространства V.

Упражнение 18.1. Убедитесь, что группа $\mathrm{SL}(V)$ состоит из всех линейных операторов $V \to V$, сохраняющих объёмы ориентированных n-мерных параллелепипедов[4].

Если зафиксировать в V базис и записать линейные операторы $V \to V$ матрицами в этом базисе, то возникнет биекция между элементами группы $\mathrm{GL}(V)$ и обратимыми матрицами в $\mathrm{Mat}_n(\Bbbk)$, при которой композиция операторов соответствует умножению матриц[5]. Согласно предл. 11.3 на стр. 198 обратимость матрицы $A \in \mathrm{Mat}_n(\Bbbk)$ равносильна тому, что $\det A \neq 0$. Такие матрицы называются *невырожденными*. Мультипликативная группа невырожденных $n \times n$ матриц

[1] См. n° 8.1.4 на стр. 136.
[2] См. n° 6.2 на стр. 102.
[3] Напомню, что *определителем* линейного оператора называется определитель его матрицы в каком-нибудь базисе, и он не зависит от выбора базиса, см. **??** на стр. **??**.
[4] См. n° 14.2 на стр. 258.
[5] См. n° 8.1.1 на стр. 131.

обозначается $\mathrm{GL}_n(\Bbbk) = \{A \in \mathrm{Mat}_n(\Bbbk) \mid \det A \neq 0\}$ и называется *полной линейной группой* над полем $\Bbbk$.

Упражнение 18.2. Убедитесь, что $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$.

Биекция $\mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(\Bbbk)$ отождествляет подгруппу $\mathrm{SL}(V) \subset \mathrm{GL}(V)$ с мультипликативной группой $\mathrm{SL}_n(\Bbbk) = \{A \in \mathrm{Mat}_n(\Bbbk) \mid \det A = 1\}$ матриц определителя 1, которая называется n-той *специальной линейной группой* над полем $\Bbbk$.

Упражнение 18.3. Найдите $|\mathrm{SL}_n(\mathbb{F}_q)|$.

Пример 18.3 (ортогональные группы)
Линейный эндоморфизм $f: V \to V$ евклидова пространства[1] V называется *изометрическим* или *ортогональным*, если он сохраняет длины векторов, т. е. $|fv| = |v|$ для всех $v \in V$. Ортогональные операторы образуют в $\mathrm{GL}(V)$ подгруппу, которая обозначается $\mathrm{O}(V)$ и называется *ортогональной группой* пространства V. Так как скалярное произведение выражается через длины по формуле $(u,w) = (|u+w|^2 - |u-w|^2)/4$, каждый ортогональный оператор f сохраняет скалярное произведения: $(fu, fw) = (u,w)$ для всех $u, w \in V$. Это условие равносильно тому, что какой-нибудь (а, значит, и любой) ортонормальный базис $\boldsymbol{e}$ пространства V переводится оператором f в ортонормальный базис $f\boldsymbol{e} = \boldsymbol{e}F_{\boldsymbol{e}}$, где $F_{\boldsymbol{e}}$ — матрица оператора f в базисе $\boldsymbol{e}$. Согласно форм. (14-7) на стр. 257 единичные матрицы Грама базисов $\boldsymbol{e}F_{\boldsymbol{e}}$ и $\boldsymbol{e}$ связаны соотношением $F_{\boldsymbol{e}}^t E F_{\boldsymbol{e}} = E$, означающим, что $F_{\boldsymbol{e}}^{-1} = F_{\boldsymbol{e}}^t$. Матрицы с таким свойством образуют в $\mathrm{GL}_n(\mathbb{R})$ подгруппу, которая обозначается $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^t\}$ и называется *группой ортогональных матриц* или вещественной *ортогональной группой*. Мы заключаем, что запись линейных операторов $V \to V$ матрицами в фиксированном ортонормальном базисе евклидова пространства V устанавливает изоморфизм $\mathrm{O}(V) \simeq \mathrm{O}_n(\mathbb{R})$.

Упражнение 18.4. Убедитесь, что $\det f = \pm 1$ для всех $f \in \mathrm{O}(V)$.

Ортогональные операторы определителя 1 сохраняют ориентацию[2] и называются *собственными*. Они образуют подгруппу *собственных* ортогональных преобразований $\mathrm{SO}(V) \subset \mathrm{O}(V)$. Мультипликативная группа их матриц обозначается $\mathrm{SO}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^t \text{ и } \det A = 1\}$ и называется n-той *специальной* или *собственной* ортогональной группой. Ортогональные операторы определителя -1 меняют ориентацию и называются *несобственными*.

Пример 18.4 (циклические подгруппы и порядки элементов)
В произвольной группе G наименьшая по включению подгруппа, содержащая заданный элемент $g \in G$, состоит из всевозможных целых степеней[3] g^m элемента g. Она называется *циклической подгруппой*[4], порождённой g, и обозначается $\langle g \rangle$. Группа $\langle g \rangle$ абелева и является образом сюръективного гомоморфизма абелевых групп $\varphi_g: \mathbb{Z} \twoheadrightarrow \langle g \rangle$, $m \mapsto g^m$, который переводит сложение в композицию.

Если $\ker \varphi_g \neq 0$, то $\ker \varphi_g = (n)$ и $\langle g \rangle \simeq \mathbb{Z}/(n)$, где $n \in \mathbb{N}$ — наименьшая степень, для которой $g^n = e$. Она называется *порядком* элемента g и обозначается $\mathrm{ord}(g)$. В этом случае $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$ имеет порядок $n = \mathrm{ord}\, g$, т. е. порядок элемента равен порядку порождённой им циклической подгруппы.

[1] См. n° 14.1 на стр. 255.
[2] См. **??** на стр. **??**.
[3] Где мы, как обычно, полагаем $g^0 \stackrel{\text{def}}{=} e$ и $g^{-n} \stackrel{\text{def}}{=} (g^{-1})^n$.
[4] Ср. с n° 3.5.1 на стр. 56.

Если $\ker \varphi_g = 0$, то $\varphi_g : \mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ является изоморфизмом и все степени g^m попарно различны. В этом случае говорят, что g имеет *бесконечный порядок* и пишут $\operatorname{ord} g = \infty$.

18.1.1. Симметрическая группа S_n. Группа всех автоморфизмов n-элементного множества $X = \{1, \dots, n\}$ называется n-той *симметрической группой* и обозначается S_n. Порядок $|S_n| = n!$. Чётные перестановки[1] образуют в S_n подгруппу, которая обозначается A_n и по историческим причинам часто называется *знакопеременной* группой. Порядок $|A_n| = n!/2$.

Перестановка $\tau \in S_n$ по кругу переводящая друг в друга m различных элементов[2]

$$i_1 \mapsto i_2 \mapsto \dots \mapsto i_{m-1} \mapsto i_m \mapsto i_1 \tag{18-5}$$

и оставляющая на месте все остальные элементы, называется *циклом* длины m.

Упражнение 18.5. Покажите, что k-тая степень цикла длины m является циклом если и только если $\text{нод}(k, m) = 1$.

Цикл (18-5) удобно обозначать $\tau = \big|i_1, \dots, i_m\big\rangle$, не смотря на то, что один и тот же цикл (18-5) допускает m *различных* таких записей, получающихся друг из друга циклическими перестановками элементов.

Упражнение 18.6. Сколько имеется в S_n различных циклов длины k?

Теорема 18.1
Каждая перестановка $g \in S_n$ является композицией $g = \tau_1 \dots \tau_k$ непересекающихся коммутирующих друг с другом циклов, и такое разложение единственно с точностью до перестановки циклов.

Доказательство. Поскольку множество $X = \{1, \dots, n\}$ конечно, в последовательности

$$x \overset{g}{\longmapsto} gx \overset{g}{\longmapsto} g^2x \overset{g}{\longmapsto} g^3x \overset{g}{\longmapsto} \dots, \tag{18-6}$$

возникающей при применении g к произвольной точке $x \in X$, случится повтор. Так как преобразование $g : X \xrightarrow{\sim} X$ биективно, первым повторившимся элементом будет стартовый элемент x. Таким образом, каждая точка $x \in X$ под действием g движется по циклу. В силу биективности g два таких цикла, проходящие через различные точки x и y, либо не пересекаются, либо совпадают. Таким образом, перестановка g является композицией непересекающихся циклов. Такие циклы перестановочны друг с другом, и их неупорядоченная совокупность однозначно определяется перестановкой g. □

Упражнение 18.7. Покажите, что два цикла $\tau_1, \tau_2 \in S_n$ перестановочны ровно в двух случаях: когда они не пересекаются или когда $\tau_2 = \tau_1^s$ и оба цикла имеют одинаковую длину, взаимно простую с s.

Определение 18.1 (цикловой тип перестановки)
Написанный в порядке нестрогого убывания набор длин непересекающихся циклов[3], в которые раскладывается перестановка $g \in S_n$, называется *цикловым типом* перестановки g и обозначается $\lambda(g)$.

[1] См. n° 11.1 на стр. 188.

[2] Числа $i_1, \dots, i_m$ произвольны, никаких свойств вроде «соседства» или «монотонности» не предполагается.

[3] Включая циклы длины один, отвечающие элементам, которые перестановка оставляет на месте.

Цикловой тип перестановки $g \in S_n$ удобно изображать n-клеточной диаграммой Юнга, а сами циклы записывать по строкам этой диаграммы. Например, перестановка

$$g = (6,\ 5,\ 4,\ 1,\ 8,\ 3,\ 9,\ 2,\ 7) = |1, 6, 3, 4\rangle\,|2, 5, 8\rangle\,|7, 9\rangle =$$

1	6	3	4
2	5	8	
7	9		

имеет цикловой тип  , т. е. $\lambda(6,\ 5,\ 4,\ 1,\ 8,\ 3,\ 9,\ 2,\ 7) = (4,\ 3,\ 2)$. Единственной перестановкой циклового типа $\lambda = (1, \dots, 1)$ (один столбец высоты n) является тождественная перестановка Id. Диаграмму $\lambda = (n)$ (одна строка длины n) имеют $(n-1)!$ циклов максимальной длины n.

Упражнение 18.8. Сколько перестановок в симметрической группе S_n имеют заданный цикловой тип, содержащий для каждого $i = 1, \dots, n$ ровно m_i циклов длины i?

Пример 18.5 (вычисление порядка и знака перестановки)
Порядок перестановки $g \in S_n$ равен наименьшему общему кратному длин непересекающихся циклов, из которых она состоит. Например, порядок перестановки

$$(3,\ 12,\ 7,\ 9,\ 10,\ 4,\ 11,\ 1,\ 6,\ 2,\ 8,\ 5) = |1,\ 3,\ 7,\ 11,\ 8\rangle\,|2,\ 12,\ 5,\ 10\rangle\,|4,\ 9,\ 6\rangle \in S_{12}$$

равен $5 \cdot 4 \cdot 3 = 60$. По правилу ниточек из прим. 11.1 на стр. 189 знак цикла длины ℓ равен $(-1)^{\ell-1}$. Поэтому перестановка чётна тогда и только тогда, когда у неё чётное число циклов чётной длины.

Упражнение 18.9. Найдите чётность $g = (6,\ 5,\ 4,\ 1,\ 8,\ 3,\ 9,\ 2,\ 7) \in S_9$ и вычислите g^{15}.

18.1.2. Группы фигур. Рассмотрим фигуру Φ в евклидовом[1] пространстве $\mathbb{R}^n$. Группа преобразований $\Phi \xrightarrow{\sim} \Phi$ задаваемых ортогональными[2] линейными операторами $\mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$, переводящими фигуру Φ в себя, называется *полной группой фигуры* Φ и обозначается O_Φ. Подгруппа $\mathrm{SO}_\Phi \subset \mathrm{O}_\Phi$, состоящая из биекций $\Phi \xrightarrow{\sim} \Phi$, задаваемых собственными[3] ортогональными преобразованиями, называется *собственной группой фигуры* Φ. Если фигура $\Phi \subset \mathbb{R}^n$ содержится в некоторой гиперплоскости $\Pi \subset \mathbb{R}^n$, то собственная группа фигуры Φ совпадает с полной: беря композицию любого несобственного движения из группы фигуры с отражением в плоскости Π, мы получаем собственное движение, которое действует на фигуру Φ точно также, как и исходное несобственное движение.

Упражнение 18.10. Изготовьте модели пяти *платоновых тел* — тетраэдра, октаэдра, куба, додекаэдра и икосаэдра, см. рис. 18⋄5 – рис. 18⋄8 на стр. 335.

Пример 18.6 (группы диэдров D_n)
Группа правильного плоского n-угольника, лежащего в пространстве $\mathbb{R}^3$ так, что его центр находится в нуле, обозначается D_n и называется *n-той группой диэдра*. Простейший диэдр — *двуугольник* — возникает при $n = 2$. Его можно представлять себе как вытянутую симметричную луночку с двумя сторонами, изображённую на рис. 18⋄1. Группа D_2 такой луночки совпадает с

[1] См. n° 14.1 на стр. 255.
[2] См. прим. 18.3 на стр. 330.
[3] Т. е. сохраняющими ориентацию или, что то же самое, с определителем 1.

группами описанного вокруг неё прямоугольника и вписанного в неё ромба[1]. Она состоит из тождественного отображения и трёх поворотов на 180° вокруг перпендикулярных друг другу осей, одна из которых проходит через вершины луночки, другая — через середины её сторон, а третья перпендикулярна плоскости луночки и проходит её центр.

Упражнение 18.11. Убедитесь, что $D_2 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

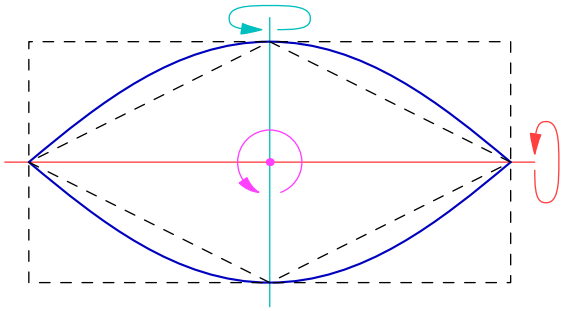


Рис. 18⋄1. Двуугольник D_2.

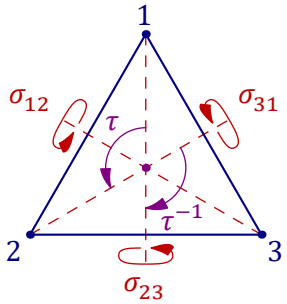


Рис. 18⋄2. Группа треугольника.

Следующая диэдральная группа — *группа треугольника* D_3 — состоит из шести движений: тождественного, двух поворотов τ, τ^{-1} на $\pm 120^\circ$ вокруг центра треугольника и трёх осевых симметрий σ_{ij} относительно его медиан (см. рис. 18⋄2). Так как движение плоскости однозначно задаётся своим действием на вершины треугольника, группа треугольника D_3 изоморфна группе перестановок S_3 его вершин. При этом повороты на $\pm 120^\circ$ отождествляются с циклическими перестановками $(2,\ 3,\ 1)$, $(3,\ 1,\ 2)$, а осевые симметрии — с транспозициями $\sigma_{23} = (1,\ 3,\ 2)$, $\sigma_{13} = (3,\ 2,\ 1)$, $\sigma_{12} = (2,\ 1,\ 3)$. Поскольку движение плоскости, переводящее в себя правильный n-угольник, однозначно определяется своим действием на аффинный репер, образованный какой-нибудь вершиной и примыкающей к ней парой сторон, группа диэдра D_n при каждом $n \geqslant 2$ состоит из $2n$ движений: выбранную вершину можно перевести в любую из n вершин, после чего одним из двух возможных способов совместить рёбра. Эти $2n$ движений суть n поворотов вокруг центра многоугольника на углы[2] $2\pi k/n$ с $k = 0, 1, \ldots, (n-1)$ и n осевых симметрий[3] относительно прямых, проходящих при нечётном n через вершину и середину противоположной стороны, а при чётном n — через пары противоположных вершин и через середины противоположных сторон (см. рис. 18⋄3).

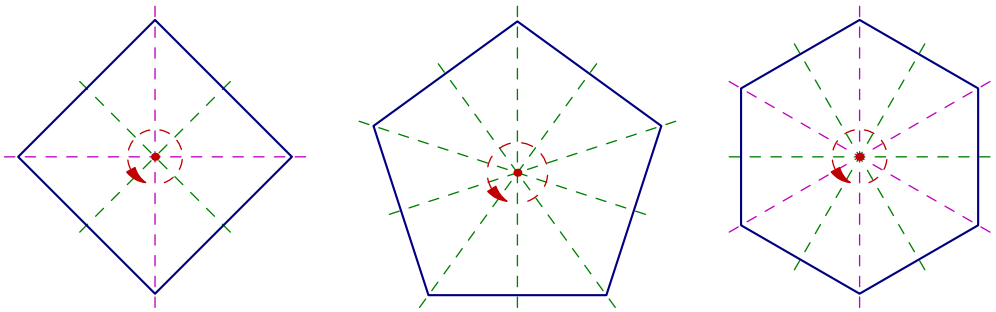


Рис. 18⋄3. Оси диэдров D_4, D_5 и D_6.

[1] Мы предполагаем, что луночка такова, что оба они не квадраты.

[2] При $k = 0$ получается тождественное преобразование.

[3] Или, что то же самое, поворотов на 180° в пространстве.

Упражнение 18.12. Составьте таблицы умножения в группах D_3, D_4 и D_5, аналогичные таблице из форм. (1-23) на стр. 14.

Пример 18.7 (группа тетраэдра)
Ортогональные преобразования $\mathbb{R}^3 \xrightarrow{\sim} \mathbb{R}^3$, переводящие в себя правильный тетраэдр с центром в нуле однозначно определяются своим действием на вершины и любая перестановка вершин задаёт ортогональный линейный оператор $\mathbb{R}^3 \xrightarrow{\sim} \mathbb{R}^3$. Поэтому полная группа такого тетраэдра изоморфна группе S_4 перестановок его вершин и состоит из 24 движений. Собственная группа состоит из $12 = 4 \cdot 3$ движений: поворот тетраэдра однозначно задаётся своим действием на аффинный репер, образованный какой-нибудь вершиной и тремя выходящими из неё рёбрами, и может переводить эту вершину в любую из четырёх вершин, после чего остаются ровно три возможности для совмещения рёбер, сохраняющего ориентацию пространства. Полный список всех собственных движений тетраэдра таков: тождественное, $4 \cdot 2 = 8$ поворотов на углы $\pm 120^\circ$ вокруг прямых, проходящих через вершину и центр противоположной грани, а также 3 поворота на 180° вокруг прямых, проходящих через середины противоположных рёбер. В несобственной группе, помимо перечисленных поворотов, имеется 6отражений σ_{ij} в плоскостях, проходящих через середину ребра $[i, j]$ и противоположное ребро, см. рис. 18⋄4. При изоморфизме с S_4 отражение σ_{ij} переходит в транспозицию букв i и j, повороты на $\pm 120^\circ$, представляющие собой всевозможные композиции $\sigma_{ij}\sigma_{jk}$ с попарно разными i, j, k, переходят в циклические перестановки букв i, j, k, три вращения на $\pm 180^\circ$ относительно осей, соединяющих середины противоположных рёбер, — в одновременные транспозиции непересекающихся пар букв: $\sigma_{12}\sigma_{34} = (2, 1, 4, 3)$, $\sigma_{13}\sigma_{24} = (3, 4, 1, 2)$, $\sigma_{14}\sigma_{23} = (4, 3, 2, 1)$.

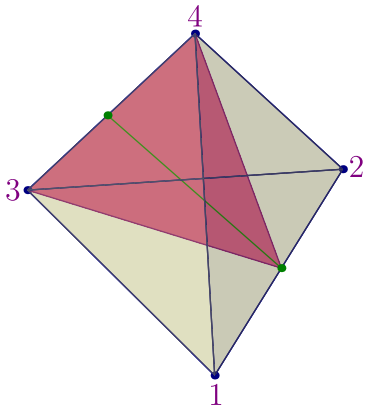


Рис. 18⋄4. Зеркало отражения σ_{12} и ось поворота на 180°.

Упражнение 18.13. Убедитесь, что вместе с тождественным преобразованием эти три поворота образуют группу двуугольника D_2.

Оставшиеся шесть несобственных преобразований тетраэдра отвечают шести циклическим перестановкам вершин $|1234\rangle$, $|1243\rangle$, $|1324\rangle$, $|1342\rangle$, $|1423\rangle$, $|1432\rangle$ и реализуются поворотами на $\pm 90^\circ$ относительно прямых, проходящих через середины противоположных рёбер с последующим отражением в плоскости, проходящей через центр тетраэдра и перпендикулярной оси поворота.

Упражнение 18.14. Выразите эти 6 движений через отражения σ_{ij}.

Пример 18.8 (группа додекаэдра)
Каждое вращение додекаэдра однозначно задаётся своим действием на аффинный репер, образованный вершиной и тремя выходящими из неё рёбрами, и может переводить эту вершину в любую из 20 вершин, а затем тремя способами совмещать рёбра с сохранением ориентации. Поэтому собственная группа додекаэдра (см. рис. 18⋄5) состоит из $20 \cdot 3 = 60$ движений: $6 \cdot 4 = 24$ поворотов на углы $2\pi k/5$, $1 \leqslant k \leqslant 4$, вокруг осей, проходящих через центры противоположных граней додекаэдра, $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi/3$ вокруг осей, проходящих через противоположные вершины, 15 поворотов на 180° вокруг осей, проходящих через середины

противоположных рёбер, и тождественного преобразования. Полная группа додекаэдра состоит из $20 \cdot 6 = 120$ движений и помимо перечисленных 60 поворотов содержит их композиции с центральной симметрией относительно центра додекаэдра.

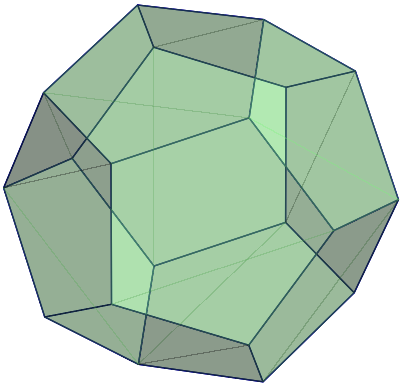


Рис. 18⋄5. Додекаэдр.

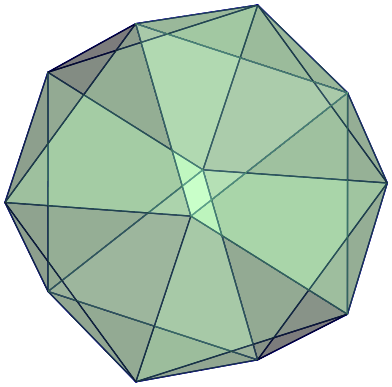


Рис. 18⋄6. Икосаэдр.

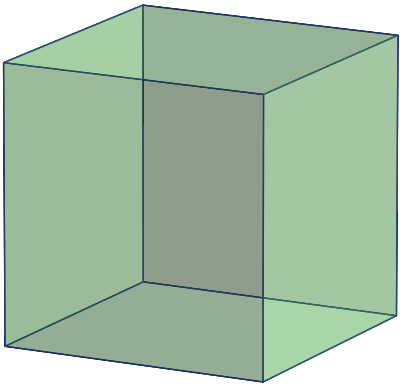


Рис. 18⋄7. Куб.

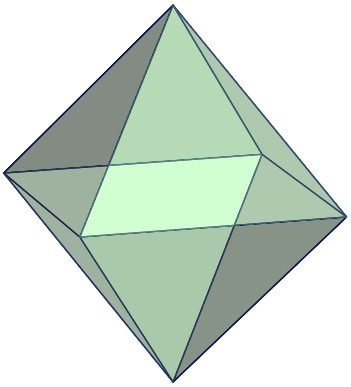


Рис. 18⋄8. Октаэдр.

Упражнение 18.15. Покажите что полные группы куба, октаэдра и икосаэдра состоят, соответственно из 48, 48 и 120 движений, а собственные — из 24, 24 и 60 поворотов.

18.2. Гомоморфизмы групп. Отображение групп $\varphi : G_1 \to G_2$ называется *гомоморфизмом*, если оно переводит композицию в композицию, т. е. для любых $g, h \in G_1$ в группе G_2 выполняется соотношение $\varphi(gh) = \varphi(g)\varphi(h)$. Термины *эпиморфизм*, *мономорфизм* и *изоморфизм* применительно к отображению групп всегда подразумевают по умолчанию, что это отображение является *гомоморфизмом* групп.

Упражнение 18.16. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

Каждый гомоморфизм групп $\varphi : G_1 \to G_2$ переводит единицу e_1 группы G_1 в единицу e_2 группы G_2: равенство $\varphi(e_1) = e_2$ получается из равенств $\varphi(e_1)\varphi(e_1) = \varphi(e_1 e_1) = \varphi(e_1)$ умножением правой и левой части на $\varphi(e_1)^{-1}$. Кроме того, для любого $g \in G$ выполняется равенство $\varphi(g^{-1}) = \varphi(g)^{-1}$, поскольку $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_1) = e_2$. Поэтому образ

$$\operatorname{im}\varphi \stackrel{\text{def}}{=} \varphi(G_1) \subset G_2$$

гомоморфизма групп является *подгруппой* группы G_2. Полный прообраз единицы $e_2 \in G_2$

$$\ker\varphi \stackrel{\text{def}}{=} \varphi^{-1}\left(e_2\right) = \left\{ g \in G_1 \;\middle|\; \varphi(g_1) = e_2 \right\} .$$

называется *ядром* гомоморфизма φ и является подгруппой в G_1, ибо из равенств $\varphi(g) = e_2$, $\varphi(h) = e_2$ вытекает равенство $\varphi(gh) = \varphi(g)\varphi(h) = e_2 e_2 = e_2$, а из равенства $\varphi(g) = e_2$ — равенство $\varphi(g^{-1}) = \varphi(g)^{-1} = e_2^{-1} = e_2$.

Предложение 18.1
Все непустые слои произвольного гомоморфизма групп $\varphi : G_1 \to G_2$ находится во взаимно однозначном соответствии его ядром $\ker\varphi$, причём $\varphi^{-1}\big(\varphi(g)\big) = g(\ker\varphi) = (\ker\varphi)g$, где

$$g(\ker\varphi) \stackrel{\text{def}}{=} \{gh \mid h \in \ker\varphi\} \quad \text{и} \quad (\ker\varphi)g \stackrel{\text{def}}{=} \{hg \mid h \in \ker\varphi\} .$$

Доказательство. Если $\varphi(t) = \varphi(g)$, то $\varphi(tg^{-1}) = \varphi(t)\varphi(g)^{-1} = e$ и $\varphi(g^{-1}t) = \varphi(g)^{-1}\varphi(t) = e$, т. е. $tg^{-1} \in \ker\varphi$ и $g^{-1}t \in \ker\varphi$. Поэтому $t \in (\ker\varphi)g$ и $t \in g(\ker\varphi)$. Наоборот, для всех $h \in \ker\varphi$ выполняются равенства $\varphi(hg) = \varphi(h)\varphi(g) = \varphi(g)$ и $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$. Тем самым, полный прообраз $\varphi^{-1}\big(\varphi(g)\big)$ элемента $\varphi(g)$ совпадает и с $(\ker\varphi)g$, и с $g(\ker\varphi)$, а $(\ker\varphi)g$ и $g(\ker\varphi)$ совпадают друг с другом. Взаимно обратные биекции

$$\ker\varphi \underset{g^{-1}t \leftarrow t}{\overset{h \mapsto gh}{\rightleftarrows}} g(\ker\varphi)$$

между ядром и слоем $\varphi^{-1}\big(\varphi(g)\big) = g(\ker\varphi)$ задаются левым умножением элементов ядра на g, а элементов слоя — на g^{-1}. □

Следствие 18.1
Для того, чтобы гомоморфизм групп $\varphi : G_1 \to G_2$ был инъективен, необходимо и достаточно, чтобы его ядро исчерпывалось единичным элементом. □

Следствие 18.2
Для любого гомоморфизма конечных групп $\varphi : G_1 \to G_2$ выполнено равенство

$$|\operatorname{im}(\varphi)| = |G_1| / |\ker(\varphi)| . \tag{18-7}$$

В частности, $|\ker\varphi|$ и $|\operatorname{im}\varphi|$ делят $|G_1|$. □

Пример 18.9 (знакопеременная группа)
Согласно сл. 11.2 на стр. 189 имеется мультипликативный гомоморфизм

$$\operatorname{sgn} : S_n \to \{\pm 1\} ,$$

сопоставляющий перестановке её знак. Ядром этого гомоморфизма является знакопеременная группа $A_n = \ker\operatorname{sgn}$, откуда $|A_n| = n!/2$.

Пример 18.10 (специальная линейная группа, продолжение прим. 18.2 на стр. 329)
В силу мультипликативности определителя[1], отображение

$$\det : \operatorname{GL}(V) \to \Bbbk^\times , \quad F \mapsto \det F . \tag{18-8}$$

[1] См. предл. 11.2 на стр. 194.

является гомоморфизмом полной линейной группы в мультипликативную группу $\Bbbk^\times$ поля $\Bbbk$. Ju сюрьективен, поскольку для любого $\lambda \in \Bbbk^\times$ диагонализуемый оператор F с собственными числами $(\lambda, 1, \dots, 1)$ лежит в GL имеет $\det F = \lambda$. Ядром гомоморфизма (18-8) является специальная линейная группа $\mathrm{SL}(V)$. Если $\Bbbk = \mathbb{F}_q$ состоит из q элементов и $\dim V = n$, то по упр. 18.2 на стр. 330 $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$. Мы заключаем, что

$$|\mathrm{SL}_n(\mathbb{F}_q)| = |\mathrm{GL}_n(\mathbb{F}_q)|/|\Bbbk^\times| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})/(q-1)\,.$$

Пример 18.11 (проективные группы)
С $(n+1)$-мерным векторным пространством V связана *проективная группа* $\mathrm{PGL}(V)$ проективных преобразований[1] $\mathbb{P}(V) \to \mathbb{P}(V)$ проективного пространства[2] $\mathbb{P}(V)$. По определению проективного преобразования имеется эпиморфизм

$$\pi:\ \mathrm{GL}(V) \twoheadrightarrow \mathrm{PGL}(V)\,, \quad F \mapsto \overline{F}\,, \tag{18-9}$$

который сопоставляет оператору $F \in \mathrm{GL}(V)$ его действие $\overline{F}: \mathbb{P}(V) \to \mathbb{P}(V)$ на множестве одномерных векторных подпространств в V. По сл. 13.4 на стр. 246 ядром гомоморфизма (18-9) является *группа гомотетий* $\Gamma = \{\lambda\mathrm{Id}: V \to V \mid \lambda \in \Bbbk^\times\} \simeq \Bbbk^\times$. Запись линейных отображений матрицами в фиксированном базисе пространства V задаёт изоморфизм группы $\mathrm{PGL}(V)$ с группой $\mathrm{PGL}_{n+1}(\Bbbk)$, которая состоит из классов пропорциональности невырожденных матриц и называется *проективной линейной группой*. Ограничивая эпиморфизм (18-9) на подгруппу $\mathrm{SL}(V) \subset \mathrm{GL}(V)$ получаем эпиморфизм $\mathrm{SL}(V) \twoheadrightarrow \mathrm{PSL}(V)$, образ которого называется *специальной проективной группой*, а ядро изоморфно конечной мультипликативной группе $\boldsymbol{\mu}_{n+1}(\Bbbk) \subset \Bbbk^\times$ содержащихся в поле $\Bbbk$ корней $(n+1)$-й степени из единицы. Соответствующая матричная группа $\mathrm{PSL}_{n+1}(\Bbbk)$ состоит из классов матриц, получающихся друг из друга умножениями на корни $(n+1)$-й степени из единицы.

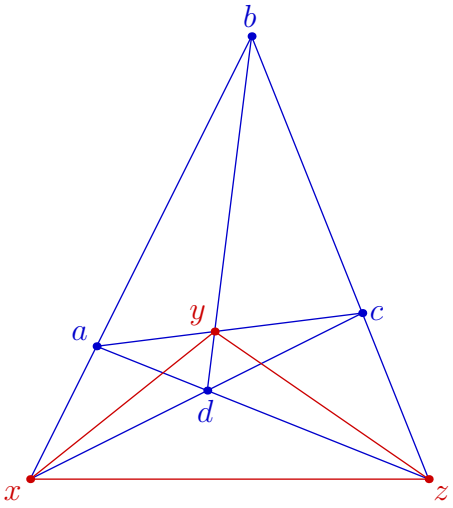


Рис. 18⋄9. Четырёхвешинник и ассоциированный треугольник.

Упражнение 18.17. Найдите $|\mathrm{PGL}_n(\mathbb{F}_q)|$ и $|\mathrm{PSL}_n(\mathbb{F}_q)|$.

Пример 18.12 (эпиморфизм $S_4 \twoheadrightarrow S_3$)
Плоская фигура, состоящая из шести изображённых на рис. 18⋄9 синих проективных прямых

$$(ab) \text{ и } (cd), \quad (ac) \text{ и } (bd), \quad (ad) \text{ и } (bc) \tag{18-10}$$

попарно соединяющих четыре точки $a, b, c, d \in \mathbb{P}_2(\Bbbk)$, никакие три из которых не коллинеарны, называется *четырёхвершинником* $abcd$. Пары прямых (18-10) называются *противоположными сторонами* четырёхвершинника. Красный треугольник xyz с вершинами в точках пересечения пар противоположных сторон

$$x = (ab) \cap (cd),\ y = (ac) \cap (bd),\ z = (ad) \cap (bc) \tag{18-11}$$

[1] См. n° 13.5 на стр. 245.
[2] См. n° 13.4 на стр. 241.

называется *ассоциированным* с четырёхвершинником $abcd$. Согласно теор. 13.2 на стр. 246 каждая перестановка вершин a, b, c, d однозначно задаёт проективное преобразование плоскости, что даёт вложение $S_4 \hookrightarrow \mathrm{PGL}_3(\Bbbk)$ в качестве подгруппы, состоящей из всех проективных преобразований, переводящих четырёхвершинник в себя. Все эти преобразования переводят в себя и ассоциированный треугольник, переставляя его вершины x, y, z согласно формулам (18-11). Например, 3-цикл $(b, c, a, d) \in S_4$ задаёт циклическую перестановку (y, z, x), а транспозиции (b, a, c, d), (a, c, b, d) и (c, b, a, d) дают транспозиции (x, z, y), (y, x, z) и (z, y, x) соответственно. Таким образом, имеется сюръективный гомоморфизм $S_4 \twoheadrightarrow S_3$. Его ядро имеет порядок $4!/3! = 4$ и состоит из тождественной перестановки и трёх пар независимых транспозиций (b, a, d, c), (c, d, a, b), (d, c, b, a). Эта группа называется 4-*группой Клейна* и обозначается $V_4 \subset A_4$.

Упражнение 18.18. Убедитесь, что $V_4 \simeq D_2 \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

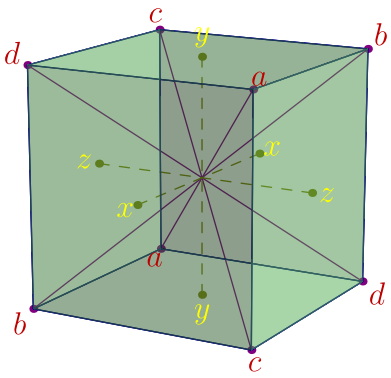


Рис. 18⋄10. От куба к четырёхвершиннику.

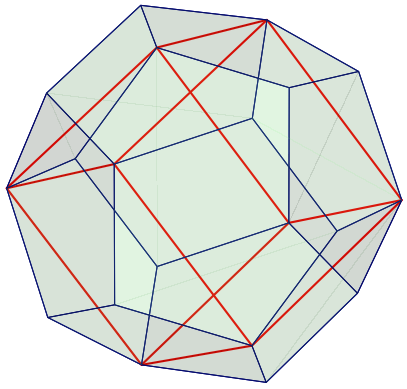


Рис. 18⋄11. Один из пяти кубов на додекаэдре.

Пример 18.13 (S_4 и собственная группа куба)
Линейные преобразования евклидова пространства $\mathbb{R}_3$, составляющие собственную группу куба с центром в нуле, действуют на четырёх прямых a, b, c, d, соединяющих противоположные вершины куба, а также на трёх прямых x, y, z, соединяющих центры его противоположных граней, см. рис. 18⋄10. На проективной плоскости $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$ эти 7 прямых становятся вершинами четырёхвершинника $abcd$ и ассоциированного с ним треугольника xyz, как на рис. 18⋄9. Поворот на 180° вокруг оси, соединяющей середины противоположных рёбер куба, меняет местами примыкающие к этому ребру диагонали и переводит в себя каждую их двух оставшихся диагоналей. Тем самым, вращения куба осуществляют транспозиции любых двух соседних диагоналей, и мы имеем сюръективный гомоморфизм $\mathrm{SO}_{\text{куб}} \to S_4$. Так как обе группы имеют порядок 24, это изоморфизм. Он переводит 6поворотов на $\pm 90°$ вокруг прямых x, y, z в 6циклов длины 4циклового типа $\square\square\square\square$, 3поворота на 180° вокруг тех же прямых — в 3пары независимых транспозиций циклового типа $\begin{smallmatrix}\square\square\\\square\square\end{smallmatrix}$, 8поворотов на $\pm 120°$ вокруг прямых a, b, c, d — в 8циклов длины 3циклового типа $\begin{smallmatrix}\square\square\square\\\square\end{smallmatrix}$, а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер — в 6простых транспозиций циклового типа $\begin{smallmatrix}\square\square\\\square\\\square\end{smallmatrix}$. Гомоморфизм $\mathrm{SO}_{\text{куб}} \to S_3$, возникающий из действия группы куба на прямых x, y, z, согласован с изоморфизмом $\mathrm{SO}_{\text{куб}} \xrightarrow{\sim} S_4$ и эпиморфизмом $S_4 \twoheadrightarrow S_3$ из предыдущего прим. 18.12. Его ядро состоит из собственных ортогональных преобразований евклидова пространства $\mathbb{R}^3$, переводящих в себя

каждую из декартовых координатных осей x, y, z в $\mathbb{R}^3$, и совпадает, таким образом, с группой двуугольника D_2 с осями x, y, z. Изоморфизм $\mathrm{SO}_{\text{куб}} \xrightarrow{\sim} S_4$ переводит её в ядро V_4 эпиморфизма $S_4 \twoheadrightarrow S_3$ из прим. 18.12.

Пример 18.14 (собственная группа додекаэдра и A_5)
Любая диагональ любой грани додекаэдра единственным образом достраивается до лежащего на поверхности додекаэдра куба, образованного диагоналями граней так, что в каждой грани рисуется ровно одна диагональ[1], как на рис. 18⋄11. Всего таких кубов на поверхности додекаэдра имеется ровно пять, и они биективно соответствуют пяти диагоналям какой-нибудь фиксированной грани. Собственная группа додекаэдра переставляет эти кубы друг с другом, что даёт гомоморфизм собственной группы додекаэдра в симметрическую группу S_5

$$\psi_{\text{дод}} : \mathrm{SO}_{\text{дод}} \to S_5 . \tag{18-12}$$

Глядя на модель додекаэдра, легко видеть, что образами $20 \cdot 3 = 60$ поворотов, из которых состоит группа $\mathrm{SO}_{\text{дод}}$ являются 60 чётных перестановок: тождественное преобразование додекаэдра задаёт тождественную перестановку кубов; $6 \cdot 4 = 24$ поворота на углы $2\pi k / 5$, $1 \leqslant k \leqslant 4$, вокруг осей, проходящих через центры противоположных граней, переходят во всевозможные циклы длины 5, т. е. в 24 перестановки циклового типа $\square\square\square\square\square$; $10 \cdot 2 = 20$ поворотов на углы $\pm 2\pi / 3$ вокруг осей, проходящих через противоположные вершины додекаэдра, переходят во всевозможные циклы длины 3, т. е. в 20 перестановок циклового типа $\begin{smallmatrix}\square\square\square\\\square\\\square\end{smallmatrix}$; 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, переходят во всевозможные пары независимых транспозиций, т. е. в 10 перестановок циклового типа $\begin{smallmatrix}\square\square\\\square\square\\\square\end{smallmatrix}$. Таким образом, гомоморфизм (18-12) является изоморфизмом собственной группы додекаэдра со знакопеременной подгруппой $A_5 \subset S_5$. В отличие от прим. 18.7 переход от собственной группы додекаэдра к полной не добавляет новых перестановок кубов, поскольку каждое несобственное движение является композицией собственного движения и центральной симметрии, которая переводит каждый из кубов в себя.

Упражнение 18.19. Покажите, что симметрическая группа S_5 не изоморфна полной группе додекаэдра.

18.3. Действие группы на множестве. Пусть G — группа, а X — множество. Обозначим через $\mathrm{Aut}(X)$ группу всех взаимно однозначных отображений из X в себя. Гомоморфизм

$$\varphi : G \to \mathrm{Aut}(X)$$

называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Отображение $\varphi(g) : X \to X$, отвечающее элементу $g \in G$ при действии φ часто бывает удобно обозначать через $\varphi_g : X \to X$. Тот факт, что сопоставление $g \mapsto \varphi_g$ является гомоморфизмом групп, означает, что $\varphi_{gh} = \varphi_g \circ \varphi_h$ для всех $g, h \in G$. Если понятно, о каком действии идёт речь, мы будем сокращать $\varphi_g(x)$ до gx. При наличии действия группы G на множестве X мы пишем $G : X$. Действие называется *транзитивным*, если любую точку множества X можно перевести в любую другую точку каким-нибудь преобразованием из группы G,

[1] Проще всего это увидеть на модели додекаэдра, которую я ещё раз настоятельно рекомендую изготовить — см. упр. 18.10 на стр. 332.

т. е. $\forall x, y \in X\ \exists g \in G : gx = y$. Более общим образом, действие называется *m-транзитивным*, если любые два упорядоченных набора из m различных точек множества X можно перевести друг в друга подходящими преобразованиями из G.

Упражнение 18.20. Убедитесь, что специальная проективная группа[1] $\mathrm{PSL}_{n+1}(\Bbbk)$ действует 2-транзитивно на $\mathbb{P}_n(\Bbbk)$ при всех $n \geqslant 1$.

Действие называется *свободным*, если каждый отличный от единицы элемент группы действует на X без неподвижных точек, т. е. равенство $gx = x$ для $x \in X$ возможно лишь при $g = e$. Действие $\varphi : G \to \operatorname{Aut} X$ называется *точным* (или *эффективным*), если $\ker \varphi = e$, т. е. действие каждого преобразования $g \neq e$ не тождественно. Точное представление отождествляет G с группой преобразований $\varphi(G) \subset \mathrm{Aut}(X)$ множества X. Любое свободное действие точно.

Если группа G действует на множестве X, то она действует и на подмножествах множества X: элемент $g \in G$ переводит подмножество $M \subset X$ в подмножество $gM = \{gm \mid m \in M\}$. При этом отображение $g : M \to gM$, $x \mapsto gx$ биективно, и обратным к нему является отображение $g^{-1} : gM \to g$, $\mapsto g^{-1}y$, ибо $g^{-1}gx = ex = x$. Говорят, что элемент $g \in G$ *нормализует*[2] подмножество $M \subset X$, если $gM = M$, т. е. $gx \in M$ для каждого $x \in M$. Каждый такой элемент задаёт биекцию $g|_M : M \to M$. Если эта биекция тождественна, т. е. $gx = x$ для всех $x \in M$, то говорят, что элемент g *централизует* подмножество M. Множество всех элементов $g \in G$, нормализующих (соотв. централизующих) данное подмножество $M \subset X$ обозначается $N(M)$ (соотв. $Z(M)$) и называется *нормализатором* (соотв. *централизатором*) подмножества $M \subset X$ при заданном действии группы G на X.

Упражнение 18.21. Убедитесь, что $Z(M) \subset N(M)$ являются подгруппами в G.

Нормализатор и централизатор одноточечного множества $M = \{x\}$ совпадают друг с другом. Эта подгруппа обозначаются $\mathrm{Stab}(x) \subset G$ и называется *стабилизатором* точки $x \in X$.

Пример 18.15 (регулярные действия)
Обозначим через X множество элементов группы G, а через $\mathrm{Aut}(X)$ — группу автоморфизмов этого *множества*[3]. Отображение $\lambda : G \to \operatorname{Aut} X$, переводящее элемент $g \in G$ в преобразование[4]

$$\lambda_g : x \mapsto gx$$

левого умножения на g является гомоморфизмом групп, поскольку

$$\lambda_{gh}(x) = ghx = \lambda_g(hx) = \lambda_g\left(\lambda_h(x)\right) = \lambda_g \circ \lambda_h(x).$$

Оно называется *левым регулярным действием* группы G на себе. Так как равенство $gh = h$ в группе G влечёт равенство $g = e$, левое регулярное действие свободно и, в частности, точно. Симметричным образом, *правое регулярное действие* $\varrho_g : G \to \mathrm{Aut}(X)$ сопоставляет элементу $g \in G$ преобразование $x \mapsto xg^{-1}$ правого умножения на обратный[5] к g элемент.

Упражнение 18.22. Убедитесь, что ϱ_g является свободным действием.

---

[1] См. прим. 18.11 на стр. 337.

[2] В этом случае также говорят, что подмножество $M \subset X$ является g-инвариантным.

[3] Возможно, не перестановочных с имеющейся в G композицией, т. е. не обязательно являющихся автоморфизмами *группы* G.

[4] Обратите внимание, что это преобразование множества X не является гомоморфизмом группы G, поскольку равенство $g(h_1h_2) = (gh_1)(gh_2)$, вообще говоря, не выполняется.

[5] Появление g^{-1} не случайно: проверьте, что сопоставление элементу $g \in G$ отображения правого умножения на g является не гомоморфизмом, а антигомоморфизмом (т. е. оборачивает порядок сомножителей в произведениях).

Тем самым, любая абстрактная группа G может быть реализована как группа преобразований некоторого множества. Например, левые регулярные представления числовых групп реализуют аддитивную группу $\mathbb{R}$ группой сдвигов $\lambda_v : x \mapsto x + v$ числовой прямой , а мультипликативную группу $\mathbb{R}^\times$ — группой гомотетий $\lambda_c : x \mapsto cx$ проколотой прямой $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$.

Пример 18.16 (присоединённое действие)
Отображение $\mathrm{Ad} : G \to \mathrm{Aut}(G)$, сопоставляющее элементу $g \in G$ автоморфизм *сопряжения* этим элементом

$$\mathrm{Ad}_g : G \to G\,, \quad h \mapsto ghg^{-1}\,, \tag{18-13}$$

называется *присоединённым действием* группы G на себе.

Упражнение 18.23. Убедитесь, что для каждого $g \in G$ сопряжение (18-13) является *гомоморфизмом* из G в G и что отображение $g \mapsto \mathrm{Ad}_g$ является гомоморфизмом из G в $\mathrm{Aut}\, G$.

Образ присоединённого действия $\mathrm{Ad}(G) \subset \mathrm{Aut}\, G$ обозначается $\mathrm{Int}(G)$ и называется группой *внутренних* автоморфизмов группы G. Не лежащие в $\mathrm{Int}(G)$ автоморфизмы группы G называются *внешними*. В отличие от левого и правого регулярных действий присоединённое действие, вообще говоря, не свободно и не точно. Например, если группа G абелева, все внутренние автоморфизмы (18-13) тождественные, и ядро присоединённого действия в этом случае совпадает со всей группой. В общем случае $\ker(\mathrm{Ad})$ состоит из всех таких $g \in G$, что $ghg^{-1} = h$ для всех $h \in G$. Последнее равенство равносильно равенству $gh = hg$ и означает, что g *коммутирует* со всеми элементами группы. Подгруппа элементов, перестановочных со всеми элементами группы G называется *центром* группы G и обозначается

$$Z(G) = \ker(\mathrm{Ad}) = \{g \in G \mid \forall\, h \in G\ gh = hg\}\ .$$

Стабилизатор заданного элемента $g \in G$ в присоединённом действии состоит из всех элементов группы, коммутирующих с g. Он называется *централизатором* элемента g и обозначается

$$Z(g) = \{h \in G \mid hg = gh\}\,.$$

18.3.1. Орбиты. Со всякой группой преобразований G множества X связано бинарное отношение $y \sim x$ на X, означающее, что $y = gx$ для некоторого $g \in G$. Это отношение рефлексивно, ибо $x = ex$, симметрично, поскольку $y = gx \iff x = g^{-1}y$, и транзитивно, т. к. из равенств $y = gx$ и $z = hy$ вытекает равенство $z = (hg)x$. Таким образом, это отношение является эквивалентностью. Класс эквивалентности точки $x \in X$ состоит из всех точек, которые можно получить из x, применяя всевозможные преобразования из группы G. Он обозначается

$$Gx = \{gx \mid g \in G\}$$

и называется *орбитой* точки x под действием G. Согласно n° 1.4 на стр. 11 множество X распадается в дизъюнктное объединение орбит. Множество всех орбит называется *фактором* множества X по действию группы G и обозначается X/G. С каждой орбитой Gx связано сюръективное отображение[1] множеств $\mathrm{ev}_x : G \twoheadrightarrow Gx$, $g \mapsto gx$, слой которого над точкой $y \in Gx$ состоит

[1] Являющееся некоммутативным аналогом *отображений вычисления* из прим. 5.3 на стр. 88 и из 8-5 на стр. 133.

из всех преобразований группы G, переводящих x в y. Он называется *транспортёром* x в y и обозначается $G_{yx} = \{g \in G \mid gx = y\}$. Слой над самой точкой x — это *стабилизатор*[1]

$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\} = G_{xx}$$

точки x в группе G. Если $y = gx$ и $z = hx$, то $hsg^{-1} \in G_{zy}$ для всех $s \in \mathrm{Stab}(x)$. Наоборот, если $fy = z$, то $h^{-1}fg \in \mathrm{Stab}(x)$. Таким образом, для любых трёх точек x, y, z из одной G-орбиты имеются взаимно обратные биекции:

$$\mathrm{Stab}(x) \underset{h^{-1}fg \leftarrow f}{\overset{s \mapsto hsg^{-1}}{\rightleftarrows}} G_{zy}\,. \tag{18-14}$$

Предложение 18.2
Стабилизаторы всех точек из одной орбиты равномощны и сопряжены:

$$y = gx \;\Rightarrow\; \mathrm{Stab}(y) = g\;\mathrm{Stab}(x)\,g^{-1} = \{ghg^{-1} \mid h \in \mathrm{Stab}(x)\}$$

Доказательство. Это получается из (18-14) при $z = y$ и $h = g$. □

Предложение 18.3 (формула для длины орбиты)
Длина орбиты произвольной точки x при действии на неё конечной группы преобразований G равна $|Gx| = |G| \,:\, |\mathrm{Stab}_G(x)|$. В частности, длины всех орбит и порядки стабилизаторов всех точек являются делителями порядка группы.

Доказательство. Группа G является дизъюнктным объединением множеств G_{yx} по всем $y \in Gx$. В силу (18-14) все эти множества состоят из $|\mathrm{Stab}(x)|$ элементов. □

Пример 18.17 (действие перестановок букв на словах)
Зафиксируем какой-нибудь k-буквенный алфавит $A = \{a_1, \dots, a_k\}$ и рассмотрим множество X всех n-буквенных слов w, которые можно написать с его помощью. Иначе X можно воспринимать как множество всех отображений $w : \{1, \dots, n\} \to A$. Сопоставим каждой перестановке $\sigma \in S_n$ преобразование $w \mapsto w\sigma^{-1}$, которое переставляет буквы в словах так, как предписывает[2] σ. Таким образом, мы получили действие симметрической группы S_n на множестве слов. Орбита слова $w \in X$ под действием этой группы состоит из всех слов, где каждая буква алфавита встречается столько же раз, сколько в слове w. Стабилизатор $\mathrm{Stab}(w)$ слова w, в котором буква a_i встречается m_i раз (для каждого $i = 1, \dots, k$), состоит из перестановок между собою одинаковых букв и имеет порядок $|\mathrm{Stab}(w)| = m_1! \dots m_k!$. Тем самым, длина орбиты такого слова равна мультиномиальному коэффициенту

$$|S_n w| = \frac{|S_n|}{|\mathrm{Stab}(w)|} = \frac{n!}{m_1! \dots m_k!} = \binom{n}{m_1 \dots m_k}.$$

Этот пример показывает, что разные орбиты могут иметь разную длину, и порядки стабилизаторов точек из разных орбит могут быть разными.

[1] См. определения перед и после упр. 18.21 на стр. 340.

[2] Т. е. переводит слово $w = a_{\nu_1} \dots a_{\nu_n}$ в слово $a_{\nu_{\sigma^{-1}(1)}} a_{\nu_{\sigma^{-1}(2)}} \dots a_{\nu_{\sigma^{-1}(n)}}$, на i-том месте которого стоит та буква, номер которой в исходном слове w переводится перестановкой σ в номер i.

Упражнение 18.24. Для каждого из пяти платоновых тел рассмотрите действие группы этого тела на его гранях и по формуле для длины орбиты найдите порядок собственной и несобственной группы каждого из платоновых тел.

Пример 18.18 (классы сопряжённости в симметрической группе)
Перестановка $\mathrm{Ad}_g(\sigma) = g\sigma g^{-1}$, сопряжённая перестановке $\sigma = (\sigma_1, \dots, \sigma_n) \in S_n$, для каждого $i = 1, 2, \dots, n$ переводит элемент $g(i)$ в элемент $g(\sigma_i)$. Поэтому при сопряжении цикла $\tau = |i_1, \dots, i_k\rangle \in S_n$ перестановкой $g = (g_1, \dots, g_n)$ получится цикл $g\tau g^{-1} = \left|g_{i_1}, \dots, g_{i_k}\right\rangle$. Если перестановка $\sigma \in S_n$ имеет цикловой тип λ и является произведением независимых циклов, записанных по строкам диаграммы λ, то действие на такую перестановку внутреннего автоморфизма Ad_g заключается в применении отображения g к заполнению диаграммы λ, т. е. в замене каждого числа i числом g_i.

Таким образом, орбиты присоединённого действия симметрической группы S_n на себе взаимно однозначно соответствуют n-клеточным диаграммам Юнга, и орбита, отвечающая диаграмме λ, состоит из всех перестановок циклового типа λ. Если диаграмма λ имеет m_i строк длины i для каждого $i = 1, \dots, n$, то централизатор любой перестановки σ циклового типа λ состоит из таких перестановок элементов заполнения диаграммы λ независимыми циклами перестановки σ, которые не меняют σ, т. е. циклически переставляют элементы вдоль строк или произвольным образом переставляют строки одинаковой длины между собой как единое целое. Тем самым, порядок стабилизатора перестановки циклового типа λ зависит только от λ и равен $z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot \ldots \cdot n^{m_n} \cdot m_n! = \prod_{i=1}^{n} m_i!\, i^{m_i}$. Количество перестановок циклового типа λ, т. е. длина соответствующей орбиты присоединённого действия, равна $n!/z_\lambda$.

18.3.2. Перечисление орбит. Подсчёт числа элементов в факторе X/G конечного множества X по действию конечной группы G наталкивается на очевидную трудность: поскольку длины орбит бывают разными, количества орбит «разных типов» придётся подсчитывать по отдельности, по ходу дела уточняя, что такое «тип орбиты». Одним махом преодолеть обе эти трудности позволяет

Теорема 18.2 (формула Полиа – Бернсайда)
Пусть конечная группа G действует на конечном множестве X. Для каждого $g \in G$ обозначим через $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \mathrm{Stab}(x)\}$ множество неподвижных точек преобразования g. Тогда $|X/G| = |G|^{-1} \sum_{g \in G} |X^g|$.

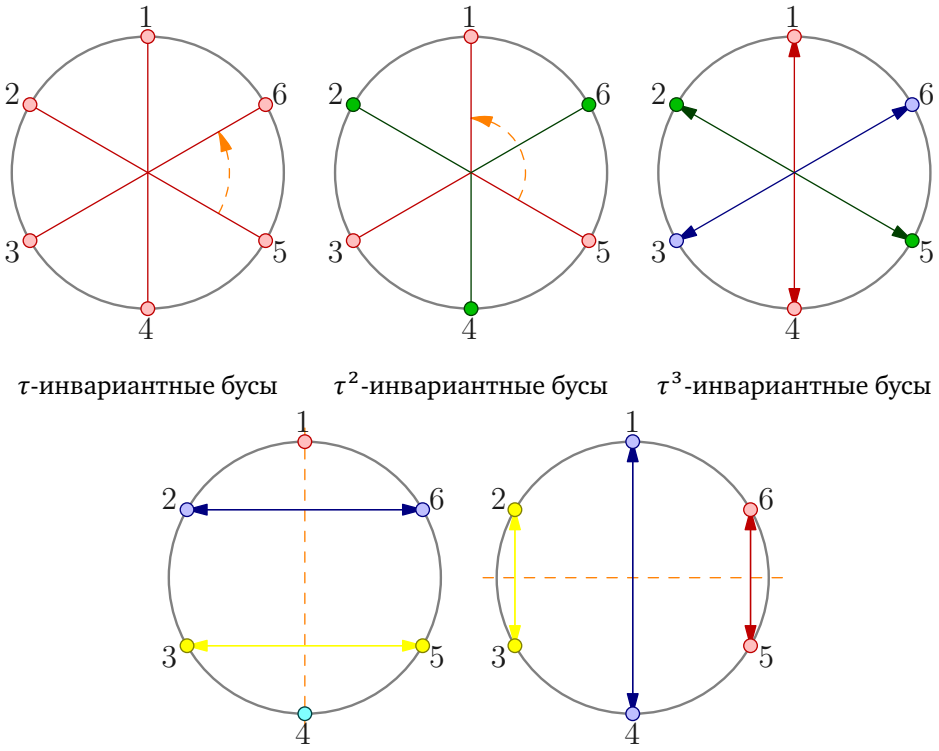
Доказательство. Обозначим через $F \subset G \times X$ множество всех таких пар (g, x), что $gx = x$. У этого множества есть ещё два описания

$$F = \bigsqcup\nolimits_{g \in G} X^g = \bigsqcup\nolimits_{x \in X} \mathrm{Stab}(x)\,.$$

Первое получается рассмотрением проекции $F \twoheadrightarrow G$, второе — из проекции $F \twoheadrightarrow X$. Согласно первому описанию, $|F| = \sum_{g \in G} |X^g|$, а из второго мы заключаем, что $|F| = |G| \cdot |X/G|$: стабилизаторы всех точек из одной орбиты имеют одинаковый порядок, суммируя эти порядки по всем точкам орбиты получаем произведение порядка стабилизатора на длину орбиты, т. е. $|G|$, что нужно умножить на количество орбит, т. е. на $|X/G|$. □

Пример 18.19 (ожерелья)
Пусть имеется неограниченный запас одинаковых по форме бусин n различных цветов. Сколько различных ожерелий можно сделать из 6 бусин? Ответом на этот вопрос является количество

орбит группы диэдра D_6 на множестве всех раскрасок вершин правильного шестиугольника в n цветов. Группа D_6 состоит из 12 элементов: тождественного преобразования e, двух поворотов $\tau^{\pm1}$ на $\pm60°$, двух поворотов $\tau^{\pm2}$ на $\pm120°$, центральной симметрии τ^3, трёх отражений σ_{14}, σ_{23}, σ_{36} относительно больших диагоналей и трёх отражений $\overline{\sigma}_{14}$, $\overline{\sigma}_{23}$, $\overline{\sigma}_{36}$ относительно срединных перпендикуляров к сторонам. Единица оставляет на месте все n^6 раскрасок. Раскраски, симметричные относительно остальных преобразований, показаны на рис. 18◇12. Беря на этих рисунках все допустимые сочетания цветов, получаем, соответственно, n, n^2, n^3, n^4 и n^3 раскрасок. По теор. 18.2 число 6-бусинных ожерелий равно $(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)/12$.



τ-инвариантные бусы τ^2-инвариантные бусы τ^3-инвариантные бусы

σ_{14}-инвариантные бусы $\overline{\sigma}_{14}$-инвариантные бусы

Рис. 18◇12. Симметричные ожерелья из шести бусин.

Упражнение 18.25. Подсчитайте количество ожерелий из 7, 8, 9, и 10 бусин.

Задачи для самостоятельного решения к §18

Задача 18.1. Докажите, что множество G с ассоциативной операцией $G \times G \to G$ тогда и только тогда является группой, когда для всех $a, b \in G$ уравнения $ax = b$ и $ya = b$ имеют единственные решения x и y.

Задача 18.2. Покажите, что любая подгруппа циклической группы тоже циклическая.

Задача 18.3. Докажите, что произведение $KH = \{kh \mid k \in K,\ h \in H\}$ двух подгрупп K, H является подгруппой если и только если $KH = HK$.

Задача 18.4 (порядки элементов). Напомню[1], что $\operatorname{ord} g = \min(n \in \mathbb{N} \mid g^n = e)$ называется *порядком* элемента $g \in G$.

а) Верно ли, что $\operatorname{ord}(g^n) = \operatorname{ord}(g)/\operatorname{нод}(n, \operatorname{ord}(g))$?

б) Чему может быть равен $\operatorname{ord}(fg)$, если $\operatorname{ord}(gf) = n$?

в) Убедитесь, что если $fg = gf$, то $\operatorname{нок}(\operatorname{ord}(f), \operatorname{ord}(g)) \vdots \operatorname{ord}(fg)$, и приведите пример, в котором $\operatorname{ord}(fg) \neq \operatorname{нок}(\operatorname{ord}(f), \operatorname{ord}(g))$.

Задача 18.5. Покажите, что группа, все элементы которой имеют порядок два, абелева.

Задача 18.6. Все ли элементы нечётного порядка являются квадратами?

Задача 18.7. Что можно сказать о чётности порядка произвольной нечётной перестановки?

Задача 18.8. Вычислите 2023-ю степень и знак перестановок: а) $(3, 5, 4, 1, 2)$
б) $(4, 5, 6, 1, 2, 3)$ в) $(4, 5, 12, 6, 7, 8, 9, 11, 2, 3, 1, 10)$
г) $(13, 4, 5, 12, 6, 14, 7, 8, 9, 11, 2, 3, 1, 15, 10)$.

Задача 18.9. Сколько элементов в S_6 неподвижны при сопряжении перестановками:
а) $(4, 5, 3, 6, 2, 1)$ б) $(4, 5, 6, 1, 2, 3)$ в) $(5, 6, 3, 4, 1, 6)$ г) $(4, 3, 2, 5, 6, 1)$?

Задача 18.10. В группах а) S_3 б) S_4 в) S_5 г) S_6 перечислите классы сопряжённости и порядки элементов и найдите количества элементов в каждом классе и каждого порядка.

Задача 18.11. Те же вопросы про группы а) A_4 б) A_5 в) A_6. Какие классы сопряжённости из S_n распадаются на несколько классов в A_n и как именно?

Задача 18.12. Сколько в A_{12} перестановок порядка 8? А сколько в S_9 перестановок порядка 3?

Задача 18.13. Сколько орбит имеет в S_9 оператор $\operatorname{Ad}_g : S_9 \to S_9$ сопряжения перестановкой

$$g = (1, 8, 5, 4, 9, 7, 2, 6, 3)\,?$$

Задача 18.14. Перестановка $\sigma \in S_n$ называется *инволюцией*, если $\sigma^2 = \mathrm{Id}$. Верно ли, что любой цикл $\tau \in S_n$ длины $\geqslant 3$ является композицией двух инволюций?

Задача 18.15 (Н. Н. Константинов). В городе N разрешаются лишь простые двусторонние обмены квартир[2], причём в течение одного дня каждому жителю разрешается сделать не более одного обмена. Можно ли за два дня осуществить любой, сколь угодно сложный обмен[3]?

Задача 18.16. Можно ли в игре «15» осуществить транспозицию фишек «1» и «2» так, чтобы все остальные фишки в результате оказались на своих исходных местах?

Задача 18.17. Перечислите все подгруппы в группах диэдров D_n с $n \leqslant 6$. Какие из них нормальны?

Задача 18.18. Во всякой ли группе чётного порядка есть элемент порядка два?

Задача 18.19. Постройте изоморфизмы: а) $\mathrm{PSL}_2(\mathbb{F}_2) \xrightarrow{\sim} S_3$ б) $\mathrm{PGL}_2(\mathbb{F}_3) \xrightarrow{\sim} S_4$ и $\mathrm{PSL}_2(\mathbb{F}_3) \xrightarrow{\sim} A_4$
в) $\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathrm{SL}_2(\mathbb{F}_4) \xrightarrow{\sim} A_5$ г*) $\mathrm{GL}_3(\mathbb{F}_2) \xrightarrow{\sim} \mathrm{PSL}_2(\mathbb{F}_7)$ д*) $\mathrm{PSL}_2(\mathbb{F}_9) \xrightarrow{\sim} A_6$.

Задача 18.20. Убедитесь, что *кватернионные единицы* $Q_8 = \{\pm e, \pm i, \pm j, \pm k\}$ с таким умножением, что e является единицей, «минус на минус даёт плюс», $i^2 = j^2 = k^2 = -e$ и $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, образуют группу. Изоморфна ли она D_4?

[1] См. прим. 18.4 на стр. 330 и° 3.5.1 на стр. 56.

[2] Когда A въезжает в квартиру, принадлежавшую B, а B — в квартиру, принадлежавшую A; все более сложные комбинации, скажем, когда A въезжает в квартиру, принадлежавшую B, B — в квартиру, принадлежавшую C, а уже C — в квартиру, принадлежавшую A, запрещены.

[3] Т. е. произвольную биекцию из множества квартир в себя.

Задача 18.21. Найдите все пары изоморфных групп в наборах: а) D_8, $D_4 \times \mathbb{Z}/(2)$, $Q_8 \times \mathbb{Z}/(2)$ б) S_4, D_{12}, $D_6 \times \mathbb{Z}/(2)$, $D_3 \times \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, $D_3 \times \mathbb{Z}/(4)$, $Q_8 \times \mathbb{Z}/(3)$, $D_4 \times \mathbb{Z}/(3)$.

Задача 18.22. При каких m и n группа диэдра D_{mn} изоморфна $D_m \times \mathbb{Z}/(n)$?

Задача 18.23. Пусть при каждом $k \in \mathbb{N}$ число элементов порядка k в конечных группах G и H одинаково. Верно ли, что $G \simeq H$?

Задача 18.24. Опишите группы автоморфизмов групп: а) $\mathbb{Z}/(n)$ б) D_3 в) D_4 г) Q_8 д) A_5. У каких из этих групп все автоморфизмы внутренние?

Задача 18.25. Найдите индекс подгруппы внутренних автоморфизмов в группе $\operatorname{Aut} A_5$.

Задача 18.26. У каких платоновых тел полная группа изоморфна прямому произведению собственной группы на группу знаков $\{\pm 1\}$?

Задача 18.27. Найдите длину орбиты и стабилизатор каждой точки каждого платонова тела под действием собственной и несобственной групп этого тела. Укажите все точки, орбиты которых короче максимума длин всех орбит.

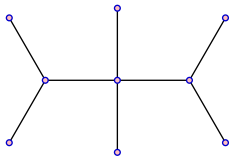
Задача 18.28. Собственная группа куба действует на множествах V и E вершин и рёбер этого куба. Опишите орбиты её диагонального[1] действия на а) $V \times V$ б) $V \times E$ в) $E \times E \times E$.

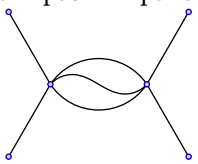
Задача 18.29. Найдите порядки собственной и несобственной групп правильных четырёхмерных а) куба[2] б) кокуба[3] в) симплекса[4] г) октаплекса[5].

Задача 18.30. Симметрическая группа S_n стандартно действует на множестве $X = \{1, \dots, n\}$. Опишите орбиты диагонального действия S_n на X^m при $m \leqslant n$ (начните с $m = 2, 3, \dots$).

Задача 18.31. Докажите, что собственная и полная группы правильного n-мерного симплекса изоморфны группам A_{n+1} и S_{n+1} соответственно.

Задача 18.32. Имеется неограниченный запас неразличимых по форме шнурочков n различных цветов. Сколько из них можно наделать разных фенечек вида

а) 

б) 

Задача 18.33. Каждую грань а) тетраэдра б) октаэдра в) икосаэдра случайным образом красят одним из n цветов. Сколько разных (т. е. не переводимых друг в друга вращением) безделушек получится? Как изменятся ответы, если красить не грани, а ребра? А если вершины?

Задача 18.34. Конечная группа транзитивно действует на множестве из не менее двух элементов. Всегда ли в ней есть элемент, действующий без неподвижных точек?

Задача 18.35. Пусть простое $p \mid |G|$. Рассмотрев действие группы $\mathbb{Z}/(p)$ циклическими перестановками элементов на множестве таких наборов $(g_1, \dots, g_p) \in G^p$, что $g_1 \dots g_p = 1$, покажите, что в G есть элемент порядка p.

---

[1] Если группа G действует на множествах $X_1, \dots, X_m$, то её *диагональное действие* на $X_1 \times \dots \times X_m$ происходит по правилу $g : (x_1, \dots, x_m) \mapsto (gx_1, \dots, gx_m)$.

[2] См. зад. 14.8 на стр. 269.

[3] См. зад. 14.10 на стр. 270.

[4] См. зад. 14.9 на стр. 270.

[5] См. зад. 14.11 на стр. 270.

§19. Подгруппы, факторгруппы и произведения

19.1. Смежные классы и факторизация. Каждая подгруппа $H \subset G$ задаёт на группе G два отношения эквивалентности, происходящие из левого и правого регулярного действия подгруппы H на группе G. Левое действие $\lambda_h : g \mapsto hg$ приводит к эквивалентности

$$g_1 \underset{L}{\sim} g_2 \iff g_1 = hg_2 \text{ для некоторого } h \in H, \tag{19-1}$$

разбивающей группу G в дизъюнктное объединение орбит вида $Hg \stackrel{\text{def}}{=} \{hg \mid h \in H\}$, называемых *правыми смежными классами* (или *правыми сдвигами*) подгруппы H в группе G. Множество правых смежных классов обозначается $H\backslash G$.

Упражнение 19.1. Покажите, что равенство $Hg_1 = Hg_2$ равносильно любому из эквивалентных друг другу включений $g_1^{-1}g_2 \in H$, $g_2^{-1}g_1 \in H$.

С правым действием $\varrho_h : g \mapsto gh^{-1}$ связано отношение эквивалентности

$$g_1 \underset{R}{\sim} g_2 \iff g_1 = g_2h \text{ для некоторого } h \in H, \tag{19-2}$$

разбивающее группу G в дизъюнктное объединение орбит $gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}$, которые называются *левыми смежными классами* (или *левыми сдвигами*) подгруппы H в группе G. Множество левых смежных классов обозначается G/H.

Поскольку и левое и правое действия подгруппы H на группе G свободны, все орбиты каждого из них состоят из $|H|$ элементов. Тем самым, число орбит в обоих действиях одинаково и равно $|G|/|H|$. Это число называется *индексом* подгруппы H в группе G и обозначается $[G : H] \stackrel{\text{def}}{=} |G/H|$. Следствием этих наблюдений является

Теорема 19.1 (теорема Лагранжа об индексе подгруппы)
Порядок и индекс любой подгруппы H в произвольной конечной группе G нацело делят порядок G и $[G : H] = |G| : |H|$. □

Следствие 19.1
Порядок любого элемента конечной группы нацело делит порядок группы.

Доказательство. Порядок элемента $g \in G$ равен порядку порождённой им циклической подгруппы $\langle g \rangle \subset G$. □

19.1.1. Нормальные погруппы. Подгруппа $H \subset G$ называется *нормальной* (или *инвариантной*) , если для любого $g \in G$ выполняется равенство $gHg^{-1} = H$ или, что то же самое, $gH = Hg$. Это означает, что левая и правая эквивалентности (19-1) и (19-2) совпадают друг с другом и $H\backslash G = G/H$. Если подгруппа $H \subset G$ нормальна, мы пишем $H \lhd G$.

Упражнение 19.2. Покажите, что любая подгруппа индекса два нормальна.

Пример 19.1 (ядра гомоморфизмов)
Ядро любого гомоморфизма групп $\varphi : G_1 \to G_2$ нормально в G_1, ибо $g(\ker\varphi) = (\ker\varphi)g$ по предл. 18.1 на стр. 336. Иначе в этом можно убедиться так: если $\varphi(h) = e$, то для любого $g \in G$

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e\,,$$

откуда $g(\ker\varphi)g^{-1} \subset \ker\varphi$.

Упражнение 19.3. Покажите, что если для любого $g \in G$ есть включение $gHg^{-1} \subset H$, то все эти включения — равенства.

Пример 19.2 ($V_4 \lhd S_4$)
Подгруппа Клейна $V_4 \subset S_4$ состоящая из перестановок циклового типа  и тождественной перестановки нормальна.

Пример 19.3 (внутренние автоморфизмы)
Подгруппа внутренних автоморфизмов $\mathrm{Int}(G) = \mathrm{Ad}(G)$ нормальна в группе $\mathrm{Aut}(G)$ всех автоморфизмов группы G, поскольку сопрягая внутренний автоморфизм $\mathrm{Ad}_g : h \mapsto ghg^{-1}$ произвольным автоморфизмом $\varphi : G \xrightarrow{\sim} G$, мы получаем внутренний автоморфизм $\varphi \circ \mathrm{Ad}_g \circ \varphi^{-1} = \mathrm{Ad}_{\varphi(g)}$.

Упражнение 19.4. Убедитесь в этом.

Пример 19.4 (нормализатор и централизатор, ср. с упр. 18.21 на стр. 340)
Если группа G действует на множестве X, то *централизатор*[1]

$$Z(M) \stackrel{\text{def}}{=} \{g \in G \mid \forall\, x \in M\ gx = x\}$$

любого подмножества $M \subset X$ является нормальной подгруппой в *нормализаторе*

$$N(M) \stackrel{\text{def}}{=} \{g \in G \mid \forall\, x \in M\ gx \in M\}$$

этого подмножества, поскольку является ядром действия $N(M) \to \mathrm{Aut}(M)$, индуцированного действием $G \to \mathrm{Aut}\, X$. Непосредственная проверка того, что $Z(M) \lhd Z(M)$, такова: если $g \in N(M)$, $h \in Z(M)$ и $x \in M$, то $g^{-1}x \in M$, откуда $h(g^{-1}x) = g^{-1}x$, а значит, $ghg^{-1}x = gg^{-1}x = x$, т. е. $ghg^{-1} \in Z(M)$ для всех $g \in N(M)$, $h \in Z(M)$.

19.1.2. Фактор группы. Попытка определить умножение на множестве левых смежных классов G/H неабелевой группы G формулой

$$(g_1H) \cdot (g_2H) \stackrel{\text{def}}{=} (g_1g_2)H\,, \tag{19-3}$$

вообще говоря, некорректна: различные записи $g_1H = f_1H$ и $g_2H = f_2H$ одних и тех же классов могут приводить к *различным* классам $(g_1g_2)H \neq (f_1f_2)H$.

Упражнение 19.5. Убедитесь, что для группы $G = S_3$ и подгруппы второго порядка $H \subset G$, порождённой транспозицией σ_{12}, формула (19-3) некорректна.

Предложение 19.1
Для того, чтобы правило $g_1H \cdot g_2H = (g_1g_2)H$ корректно определяло на G/H структуру группы, необходимо и достаточно, чтобы подгруппа H была нормальна в G.

Доказательство. Если формула (19-3) корректна, то она задаёт на множестве смежных левых классов G/H групповую структуру: ассоциативность композиции наследуется[2] из G, единицей служит класс $eH = H$, обратным к классу gH — класс $g^{-1}H$. Факторизация $G \twoheadrightarrow G/H$, $g \mapsto gH$, является гомоморфизмом групп с ядром H. Поэтому подгруппа H нормальна в силу прим. 19.1. Наоборот, если H нормальна и $f_1H = g_1H$, $f_2H = g_2H$, то в силу равенства $g_2H = Hg_2$

$$f_1f_2H = f_1g_2H = f_1Hg_2 = g_1Hg_2 = g_1g_2H\,.$$

□

[1] См. n° 18.3 на стр. 339.
[2] $(g_1H \cdot g_2H) \cdot g_3H = (g_1g_2)H \cdot g_3H = \big((g_1g_2)g_3\big)H = \big(g_1(g_2g_3)\big)H = g_1H \cdot (g_2g_3)H = g_1H \cdot (g_2H \cdot g_3H)$.

Определение 19.1
Множество смежных классов G/H нормальной подгруппы $H \lhd G$ с операцией

$$g_1H \cdot g_2H \stackrel{\text{def}}{=} (g_1g_2)H$$

называется *фактором* или *факторгруппой* группы G по нормальной подгруппе H. Гомоморфизм групп $G \twoheadrightarrow G/H$, $g \mapsto gH$, называется *гомоморфизмом факторизации*.

Следствие 19.2
Каждый гомоморфизм групп $\varphi\colon G_1 \to G_2$ является композицией эпиморфизма факторизации $G_1 \twoheadrightarrow G_1/\ker\varphi$ и мономорфизма $G_1/\ker\varphi \hookrightarrow G_2$, переводящего смежный класс $g\ker\varphi \in G_1/\ker\varphi$ в элемент $\varphi(g) \in G_2$. В частности, $\operatorname{im}\varphi \simeq G/\ker\varphi$.

Доказательство. Следствие утверждает, что слой $\varphi^{-1}\bigl(\varphi(g)\bigr)$ гомоморфизма φ над каждой точкой $\varphi(g) \in \operatorname{im}\varphi \subset G_2$ является левым сдвигом ядра $\ker\varphi$ на элемент g, что мы уже видели в предл. 18.1 на стр. 336. □

Предложение 19.2
Если подгруппа $H \subset G$ нормализует[1] подгруппу $N \subset G$, то множества

$$HN = \{hn \mid h \in H,\ n \in N\} \quad \text{и} \quad NH = \{nh \mid n \in N,\ h \in H\}$$

совпадают и образуют подгруппу в G, при этом $N \lhd HN$, $H \cap N \lhd H$ и $HN/N \simeq H/(H \cap N)$.

Доказательство. Равенство $NH = HN$ имеет место, поскольку для всех $n \in N$, $h \in H$

$$nh = h(h^{-1}nh) \in HN \quad \text{и} \quad hn = (hnh^{-1})h \in NH\,.$$

Это подгруппа, так как $(nh)^{-1} = h^{-1}n^{-1} \in HN = NH$ и

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2)h_2 = n_1(n_3h_3)h_2 = (n_1n_3)(h_3h_2) \in NH$$

(существование таких $n_3 \in N$ и $h_3 \in H$, что $h_1n_2 = n_3h_3$, вытекает из равенства $HN = NH$). Подгруппы $H \cap N \lhd H$ и $N \lhd HN$ нормальны, так как по условию $hNh^{-1} \subset N$ для всех $h \in H$. Отображение $\varphi\colon HN \to H/(H \cap N)$, переводящее произведение hn в смежный класс $h \cdot (H \cap N)$, корректно определено, поскольку при $h_1n_1 = h_2n_2$ элемент $h_1^{-1}h_2 = n_1n_2^{-1}$ лежит в $H \cap N$, и значит, $h_1 \cdot (H \cap N) = h_1 \cdot (h_1^{-1}h_2) \cdot (H \cap N) = h_2 \cdot (H \cap N)$. Это отображение сюръективно и является гомоморфизмом, поскольку $\varphi(h_1n_1h_2n_2) = \varphi(h_1h_2(h_2^{-1}n_1h_2)\,n_2) = h_1h_2 \cdot (H \cap N)$. Так как $\ker\varphi = eN = N$, из сл. 19.2 вытекает, что $H/(H \cap N) = \operatorname{im}\varphi \simeq HN/\ker\varphi = HN/N$. □

Упражнение 19.6. Пусть $\varphi\colon G_1 \twoheadrightarrow G_2$ — сюръективный гомоморфизм групп. Покажите, что полный прообраз $N_1 = \varphi^{-1}(N_2)$ любой нормальной подгруппы $N_2 \lhd G_2$ является нормальной подгруппой в G_1 и $G_1/N_1 \simeq G_2/N_2$.

[1] Т. е. $hNh^{-1} = N$ для всех $h \in H$.

19.2. Коммутант. В группе G произведение $(g,h) \stackrel{\text{def}}{=} ghg^{-1}h^{-1}$ называется *коммутатором*[1] элементов g, h. Название связано с тем, что $(g,h)hg = gh$. В частности, $gh = hg$ если и только если $(g,h) = e$. Очевидно, что $(g,h)^{-1} = (h,g)$ и $\mathrm{Ad}_f(g,h) = (\mathrm{Ad}_f g, \mathrm{Ad}_f h)$, где

$$\mathrm{Ad}_f : G \to G, \quad x \mapsto fxf^{-1},$$

автоморфизм сопряжения. Поэтому всевозможные конечные произведения коммутаторов элементов группы G образуют нормальную подгруппу, которая обозначается $G' \lhd G$ и называется *коммутантом* группы G. Так как $(g,h) = \mathrm{Ad}_g(h)h^{-1}$, коммутаторы элементов $g \in G$ с элементами h из любой нормальной подгруппы $N \lhd G$ лежат в N, т. е. $(G,N) = (N,G) \subset N$. В частности, $(G,G') \subset G'$. Всякий гомоморфизм $\varphi : G \to H$ ограничивается в гомоморфизм $\varphi|_{G'} : G' \to H'$, и если φ сюръективен, то сюръективен и $\varphi|_{G'}$.

Предложение 19.3 (универсальное свойство фактора по коммутанту)
Всякий гомоморфизм $\varphi : G \to A$ в абелеву группу A единственным образом пропускается через гомоморфизм факторизации $\pi : G \twoheadrightarrow G/G'$, т. е. существует единственный такой гомоморфизм $\varphi' : G/G' \to A$, что $\varphi = \varphi'\pi$.

Доказательство. Гомоморфизм φ' обязан действовать по правилу $gG' \mapsto \varphi(g)$. Оно корректно, так как $G' \subset \ker\varphi$, ибо в A все коммутаторы тривиальны. □

Следствие 19.3
Фактор группа G/N абелева если и только если $N \supseteq G'$.

Доказательство. Применяем предл. 19.3 к эпиморфизму $G \twoheadrightarrow G/N$. □

Пример 19.5 (коммутанты симметрических и знакопеременных групп)
Поскольку каждый коммутатор в S_n является чётной перестановкой, $S_n' \lhd A_n$. Так как $|A_3| = 3$ и группа S_3 не абелева, $S_3' = A_3$. Тем самым, при любом n коммутант S_n' содержит все 3-циклы.

Упражнение 19.7. Убедитесь, что группа A_n порождается 3-циклами.

Мы заключаем, что $S_n' = A_n$. Поскольку $|A_4/V_4| = 3$, группа $A_4/V_4 \simeq \mathbb{Z}/(3)$ абелева, откуда $A_4' \subseteq V_4$ по сл. 19.3. Так как группа A_4 не абелева, A_4' содержит пару независимых транспозиций, а значит, и все сопряжённые ей пары, т. е. $A_4' = V_4$. Отсюда вытекает, что при любом n коммутатор A_n' содержит все пары независимых транспозиций.

Упражнение 19.8. Убедитесь, что при $n \geqslant 5$ группа A_n порождается парами независимых транспозиций.

Мы заключаем, что $A_n' = A_n$ при $n \geqslant 5$.

Пример 19.6 (коммутанты линейных групп)
Пусть $\Bbbk$ — произвольное поле. Так как $\det(f,g) = 1$ для всех $f, g \in \mathrm{GL}_n(\Bbbk)$, мы заключаем, что $\mathrm{GL}_n'(\Bbbk) \trianglelefteq \mathrm{SL}_n(\Bbbk)$. Покажем, что $\mathrm{SL}_n'(\Bbbk) = \mathrm{SL}_n(\Bbbk)$ за исключением случаев $\mathrm{SL}_2(\mathbb{F}_2)$ и $\mathrm{SL}_2(\mathbb{F}_3)$.

Упражнение 19.9. Убедитесь, что $\mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ и $\mathrm{SL}_2(\mathbb{F}_3)/\{\pm E\} \simeq A_4$.

[1] Или *групповым коммутатором*, который не следует путать с коммутатором $[f,g] = fg - gf$ элементов ассоциативной алгебры.

Легко видеть, что любую матрицу из $\mathrm{SL}_n(\Bbbk)$ можно превратить в единичную элементарными преобразованиями, заключающимися в прибавлении к одной из строк другой строки, умноженной на произвольное число, т. е. в умножении матрицы слева на матрицу вида[1]

$$T_{ij}(\alpha) \stackrel{\text{def}}{=} E + \alpha E_{ij}\,. \tag{19-4}$$

Упражнение 19.10. Убедитесь в этом.

Коммутатор трансвекции (19-4) с диагональной матрицей $D(\beta_1, \ldots, \beta_n)$, где $\prod \beta_i = 1$, равен[2]

$$(E + \alpha E_{ij})(\beta_1 E_{11} + \ldots + \beta_n E_{nn})(E - \alpha E_{ij})(\beta_1^{-1} E_{11} + \ldots + \beta_n^{-1} E_{nn}) = \\ = (E + \alpha E_{ij})(E - \alpha\beta_i/\beta_j E_{ij}) = E + \alpha(1 - \beta_i/\beta_j)E_{ij}\,.$$

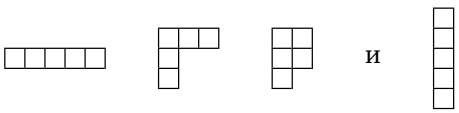
Если $n \geqslant 3$ или $\Bbbk \neq \{-1, 0, 1\}$ разность $1 - \beta_i/\beta_j$ можно сделать ненулевой[3]. Поэтому коммутант $\mathrm{SL}'_n(\Bbbk)$ содержит все трансвекции, и тем самым $\mathrm{GL}'_n(\Bbbk) = \mathrm{SL}'_n(\Bbbk) = \mathrm{SL}_n(\Bbbk)$ если $n \geqslant 3$ или $\Bbbk \neq \mathbb{F}_2, \mathbb{F}_3$.

Упражнение 19.11. Вычислите коммутанты $\mathrm{SL}'_2(\mathbb{F}_2)$ и $\mathrm{SL}'_2(\mathbb{F}_3)$.

19.3. Простые группы. Группа G называется *простой*, если она не содержит нормальных подгрупп, отличных от $\{e\}$ и G. Например, любая группа простого порядка проста, поскольку по теореме Лагранжа[4] вообще не содержит никаких подгрупп кроме $\{e\}$ и G. Согласно сл. 18.1 на стр. 336 простота группы G равносильна тому, что всякий гомоморфизм $G \to H$ либо инъективен, либо отображает всю группу G в единицу. Одним из выдающихся достижений математики XX века является перечисление всех конечных простых групп. Этот список состоит из нескольких бесконечных серий и 26 так называемых *спорадических групп*, не входящих в серии. Бесконечные серии делятся на три семейства: циклические группы $\mathbb{Z}/(p)$ простого порядка, знакопеременные группы A_n с $n \neq 4$ и простые линейные алгебраические группы над конечными полями[5], такие как $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSO}_n(\mathbb{F}_q)$, $\mathrm{PSp}_n(\mathbb{F}_q)$ и т. п. Описание конечных простых групп стало итогом сотен работ десятков авторов по различным, напрямую не связанным друг с другом направлениям математики. Никакой универсальной концепции, позволяющей единообразно классифицировать все конечные простые группы не известно.

Предложение 19.4
Знакопеременная группа A_5 проста.

Доказательство. Так как перестановки сопряжены если и только если у них одинаковый цикловой тип[6], классы сопряжённости чётных перестановок в S_5 состоят из перестановок цикловых типов



(19-5)

[1] Такие матрицы называются *трансвекциями*.

[2] См. формулу (8-4) на стр. 133.

[3] Обратите внимание, что при $n = 2$ разность $1 - \beta_i/\beta_j = 1 - \beta_i^2$ зануляется если $\Bbbk^\times \subset \{\pm 1\}$.

[4] См. теор. 19.1 на стр. 347.

[5] Описанию таких групп посвящены спецкурсы по линейным алгебраическим и арифметическим группам, например, см. книгу *Дж. Хамфри. Линейные алгебраические группы*. М., «Наука», 1980.

[6] См. прим. 18.18 на стр. 343.

(5-циклы, 3-циклы, пары независимых транспозиций и тождественное преобразование), коих имеется[1] соответственно $24 = 5!/5$, $20 = 5!/(3\cdot 2)$, $15 = 5!/(2^2\cdot 2)$ и 1.

Упражнение 19.12. Покажите, что класс сопряжённости чётной перестановки g в S_n либо совпадает с её классом сопряжённости в A_n, либо является объединением двух классов сопряжённости в A_n, причём второе происходит если и только если все циклы перестановки g имеют разные нечётные длины.

Мы заключаем, что 3-циклы, пары независимых транспозиций и тождественная перестановка являются классами сопряжённости в A_5, а 5-циклы разбиваются на два класса сопряжённости в A_5, состоящие из 12 циклов, сопряжённых $|1,2,3,4,5\rangle$, и 12 циклов, сопряжённых $|2,1,3,4,5\rangle$. Поскольку нормальная подгруппа $H \trianglelefteq A_5$ вместе с каждой перестановкой содержит и все ей сопряжённые, её порядок $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, где каждый ε_i равен либо 1, либо 0, при этом по теореме Лагранжа $|H|$ делит $|A_5| = 60 = 3\cdot 4\cdot 5$.

Упражнение 19.13. Убедитесь, что такое возможно ровно в двух случаях: когда все $\varepsilon_i = 1$ или когда все $\varepsilon_i = 0$.

Тем самым, в A_5 нет нетривиальных собственных нормальных подгрупп. □

Теорема 19.2
Все знакопеременные группы A_n с $n \geqslant 5$ просты.

Доказательство. Индукция по n. Случай $n = 5$ был разобран выше. Рассмотрим нормальную подгруппу $N \trianglelefteq A_n$. Так как стабилизатор элемента 1 в группе A_n изоморфен A_{n-1}, его пересечение с N, будучи нормальной подгруппой в A_{n-1}, либо совпадает с A_{n-1}, либо тривиально. Поскольку стабилизаторы всех элементов сопряжены, подгруппа N либо содержит стабилизаторы всех элементов, либо действует свободно[2]. В первом случае N содержит все 3-циклы и по упр. 19.7 на стр. 350 совпадает с A_n. Рассмотрим второй случай и допустим, что N содержит не тождественную перестановку g. Так как она действует без неподвижных точек, при $n \geqslant 6$ найдутся такие различные элементы $\{1,i,j,k,\ell,m\}$, что $g(1) = i$ и $g(j) = k$. Сопрягая g циклом $|k,\ell,m\rangle \in A_n$, получаем перестановку $h \in N$ с $h(1) = i$ и $h(j) = \ell \neq k$. Перестановка $gh^{-1} \in N$ не тождественна и оставляет 1 на месте. Противоречие. □

Теорема 19.3
Все специальные проективные группы[3] $\mathrm{PSL}_n(\Bbbk)$ просты, за исключением[4]

$$\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3 \quad \text{и} \quad \mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4\,.$$

Доказательство. Обозначим через $P \subset \mathrm{PSL}_n$ стабилизатор одномерного подпространства, порождённого первым вектором стандартного базиса $e_1, \ldots, e_n$ в $\Bbbk^n$. Группа P состоит из классов пропорциональных матриц вида

$$\left(\begin{array}{c|ccc} * & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right) \tag{19-6}$$

[1] См. упр. 18.8 на стр. 332.
[2] Т. е. никакой отличный от единицы элемент не имеет неподвижных точек, см. n° 18.3 на стр. 339.
[3] См. прим. 18.11 на стр. 337.
[4] См. упр. 19.9 на стр. 350.

с определителем 1 и содержит нормальную абелеву подгруппу $A \lhd P$ матриц, пропорциональных

$$\left(\begin{array}{c|ccc} 1 & \alpha_2 & \cdots & \alpha_n \\ \hline 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{array}\right) = E + \alpha_2 E_{12} + \ldots + \alpha_n E_{1n}\,,$$

которая является ядром гомоморфизма $P \to \mathrm{PGL}_{n-1}$, переводящего матрицу (19-6) в её правую нижнюю угловую подматрицу размера $(n-1)\times(n-1)$.

Упражнение 19.14. Убедитесь, что это и в самом деле гомоморфизм групп.

Так как подгруппа A содержит все трансвекции вида $T_{1j}(\alpha)$, сопряжённые ей подгруппы gAg^{-1}, где $g \in \mathrm{PSL}_n$, содержат вообще все трансвекции и порождают[1] PSL_n.

Упражнение 19.15. Убедитесь, что $T_{ij}(\alpha) = gT_{1j}(-\alpha)g^{-1}$, где $g \in \mathrm{SL}_n$ переводит e_1 в e_i, а e_i в $-e_1$, оставляя все остальные базисные векторы на месте.

Мы заключаем, что произведения элементов вида gag^{-1}, $a \in A$, $g \in \mathrm{PSL}_n$ исчерпывают PSL_n.

Рассмотрим теперь отличную от единичной нормальную подгруппу $N \trianglelefteq \mathrm{PSL}_n$. Пространство $\mathbb{P}_{n-1}$ является дизъюнктным объединением орбит подгруппы N, и в силу нормальности N каждый элемент $g \in \mathrm{PSL}_n$ переводит N-орбиту точки x в N-орбиту точки gx, ибо

$$y = hx \iff gy = (ghg^{-1})gx\,.$$

Таким образом, группа PSL_n, с одной стороны, не может перевести пару точек, лежащих в одной N-орбите, в пару точек, лежащих в разных N-орбитах, а с другой стороны, действует 2-транзитивно по упр. 18.20 на стр. 340. Такое возможно, только если N-орбита всего одна, т. е. для любого $g \in \mathrm{PSL}_n$ существует такое $h \in N$, что $ge_1 = he_1$, откуда $h^{-1}g \in P$ и $g \in hP$. Мы заключаем, что $\mathrm{PSL}_n = NP = PN$. Поскольку сопряжение элементами из P оставляет подгруппу $A \lhd P$ на месте, каждый элемент из PSL_n является произведением элементов вида hah^{-1} с $a \in A$, $h \in N$ и в силу равенства $AN = NA$ лежит в AN. В прим. 19.6 на стр. 350 мы видели, что все группы SL_n за исключением двух, указанных в условии теоремы, совпадают со своими коммутантами. Но коммутатор элементов вида ah с $a \in A$, $h \in N$ в силу абелевости A и нормальности N лежит в N.

Упражнение 19.16. Убедитесь в этом.

Поэтому $\mathrm{PSL}_n = \mathrm{PSL}_n' = N$ во всех случаях, кроме двух исключительных. □

19.4. Композиционные факторы. Конечная строго убывающая последовательность подгрупп

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \ldots \supsetneq G_{n-1} \supsetneq G_n = \{e\} \tag{19-7}$$

называется *композиционным рядом* или *рядом Жордана–Гёльдера* группы G, если при каждом i подгруппа G_{i+1} нормальна в G_i и фактор G_i/G_{i+1} прост. В этой ситуации неупорядоченный набор простых групп G_i/G_{i+1} (в котором возможны повторения) называется набором *композиционных факторов* (или *факторов Жордана–Гёльдера*) группы G, а число n называется *длиной* композиционного ряда (19-7).

[1] См. упр. 19.10 на стр. 351.

Пример 19.7 (композиционные факторы S_4)
Выше мы видели, что симметрическая группа S_4 имеет композиционный ряд

$$S_4 \rhd A_4 \rhd V_4 \rhd \mathbb{Z}/(2) \rhd \{e\}\,,$$

в котором $A_4 \lhd S_4$ — подгруппа чётных перестановок, $V_4 \lhd A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа $\square\!\square$, а

$$\mathbb{Z}/(2) \lhd V_4 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$$

любая из трёх циклических подгрупп второго порядка, порождённых неединичными элементами. Таким образом, симметрическая группа S_4 имеет композиционные факторы $\mathbb{Z}/(2) = S_4/A_4$, $\mathbb{Z}/(3) = A_4/V_4$, $\mathbb{Z}/(2) = V_4/\big(\mathbb{Z}/(2)\big)$ и $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$.

Упражнение 19.17. Убедитесь, что $A_4/V_4 \simeq \mathbb{Z}/(3)$.

Теорема 19.4 (теорема Жордана – Гёльдера)
Если группа G имеет конечный композиционный ряд, то неупорядоченный набор его факторов не зависит от выбора композиционного ряда. В частности, все ряды Жордана – Гёльдера имеют одинаковую длину.

Доказательство. Пусть у группы G есть два композиционных ряда

$$G = P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \ldots \supsetneq P_{n-1} \supsetneq P_n = \{e\} \tag{19-8}$$

$$G = Q_0 \supsetneq Q_1 \supsetneq Q_2 \supsetneq \ldots \supsetneq Q_{m-1} \supsetneq Q_m = \{e\}\,. \tag{19-9}$$

Мы собираемся вставить между последовательными членами этих рядов дополнительные цепочки нестрого убывающих подгрупп так, чтобы получившиеся удлинённые ряды стали равной длины, и установить между их последовательными факторами биекцию, при которой соответствующие друг другу факторы будут изоморфны. Для этого заменим каждое звено $P_i \rhd P_{i+1}$ верхней цепочки (19-8) цепочкой

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \ldots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}\,, \tag{19-10}$$

которая получается пересечением нижней цепочки (19-9) с подгруппой P_i и умножением всех полученных групп на нормальную в P_i подгруппу P_{i+1}. В предл. 19.2 на стр. 349 мы видели, что если подгруппа H нормализует подгруппу N, то $NH = HN$ тоже является подгруппой, причём $NH \rhd N$, $H \rhd (H \cap N)$ и $HN/N \simeq H/(H \cap N)$. Применяя это к подгруппам

$$H = Q_k \cap P_i \quad \text{и} \quad N = (Q_{k+1} \cap P_i)P_{i+1}\,,$$

мы получаем $HN = (Q_k \cap P_i)P_{i+1}$ и $H \cap N = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})$.

Упражнение 19.18. Убедитесь, что H нормализует N, и проверьте последние два равенства.

Таким образом, $(Q_k \cap P_i)P_{i+1} \trianglerighteq (Q_{k+1} \cap P_i)P_{i+1}$ и

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}\,. \tag{19-11}$$

Группа P_{i+1} является нормальной подгруппой во всех группах цепочки (19-10). Факторизуя по ней, получаем цепочку факторгрупп

$$\frac{P_i}{P_{i+1}} \trianglerighteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \trianglerighteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \trianglerighteq \ldots \trianglerighteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \trianglerighteq \{e\}\,, \tag{19-12}$$

в которой каждая подгруппа нормальна в предыдущей, а последовательные факторы

$$\frac{(Q_k \cap P_i)P_{i+1}/P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}/P_{i+1}} \simeq \frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}$$

совпадают с (19-11). Так как группа P_i/P_{i+1} проста, мы заключаем, что в цепочке (19-12) имеется ровно одно нестрогое включение, а все остальные включения — равенства. Тем самым, ровно один из факторов (19-11) отличен от единицы и изоморфен P_i/P_{i+1}.

Те же самые рассуждения с заменой P на Q позволяют вставить между последовательными группами $Q_k \rhd Q_{k+1}$ композиционного ряда (19-9) убывающую цепочку подгрупп

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \ldots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1}\,, \tag{19-13}$$

каждая из которых нормальна в предыдущей, а последовательные факторы имеют вид

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})} \tag{19-14}$$

и изоморфны соответствующим факторам (19-11). Таким образом, вставляя между последовательными элементами композиционного ряда (19-8) цепочки (19-10), а между последовательными элементами ряда (19-9) — цепочки (19-13), мы получим ряды одинаковой длины, в которых не все включения строгие, но факторы находятся в биективном соответствии, сопоставляющем друг другу изоморфные факторы (19-14) и (19-11). Поскольку Q_{k+1} является нормальной подгруппой всех групп цепочки (19-13), те же аргументы, что применялись выше к подгруппе P_{i+1} и цепочке (19-10), показывают, что при фиксированном k среди факторов (19-14) имеется ровно один отличный от единицы, и он изоморфен Q_k/Q_{k+1}. □

Замечание 19.1. Непростая группа может иметь несколько разных композиционных рядов с одинаковым набором факторов, а группы с одинаковыми наборами факторов Жордана-Гёльдера не обязательно изоморфны.

Предложение 19.5
Если группа G обладает конечным композиционным рядом, то все её подгруппы и факторгруппы тоже обладают конечными композиционными рядами, причём набор факторов каждого из них является поднабором в наборе композиционных факторов группы G.

Доказательство. Пересечение композиционного ряда группы G с подгруппой $H \subset G$ имеет вид

$$H \supseteq G_1 \cap H \supseteq \ldots \supseteq G_{n-1} \cap H \supseteq \{e\}\,, \tag{19-15}$$

где $(G_i \cap H) \rhd (G_{i+1} \cap H)$, так как $G_i \rhd G_{i+1}$, и $(G_i \cap H)/(G_{i+1} \cap H) \simeq (G_i \cap H)G_{i+1}/G_{i+1}$ по предл. 19.2 на стр. 349. Поскольку $G_i \supseteq (G_i \cap H)G_{i+1} \supseteq G_{i+1}$ и фактор G_i/G_{i+1} прост, одно включение строгое, другое — равенство. Если $(G_i \cap H)G_{i+1} = G_{i+1}$, то $(G_i \cap H)/(G_{i+1} \cap H) \simeq G_i/G_{i+1}$. Если

$(G_i \cap H)G_{i+1} = G_{i+1}$, то $(G_i \cap H) = (G_{i+1} \cap H)$. Таким образом, убирая из цепочки (19-15) все равенства, получаем ряд Жордана – Гёльдера, факторы которого содержатся среди композиционных факторов группы G. Аналогично, применяя к композиционному ряду группы G эпиморфизм $\pi\colon G \twoheadrightarrow Q$, получаем цепочку $Q \supseteq \pi(G_1) \supseteq \ldots \supseteq \pi(G_{n-1}) \supseteq \{e\}$, в которой $\pi(G_i) \rhd \pi(G_{i+1})$. Ограничим π на G_i и обозначим через $H = \pi|_{G_i}^{-1}(\pi(G_{i+1}))$ полный прообраз подгруппы $\pi(G_{i+1}) \subset \pi(G_i)$ относительно этого ограничения. Так как $G_i \supseteq H \supseteq G_{i+1}$ и фактор G_i / G_{i+1} прост, одно включение строгое, другое — равенство. Если $G_i = H$, то $\pi(G_i) = \pi(G_{i+1})$, а если $H = G_{i+1}$, то $\pi(G_i)/\pi(G_{i+1}) \simeq G_i/G_{i+1}$ по упр. 19.6 на стр. 349, применённому к $\varphi = \pi|_{G_i}$. □

Предложение 19.6
Пусть $N \lhd G$, $Q = G/N$, и группы N, Q обладают конечными композиционными рядами. Тогда у группы G тоже есть конечный композиционный ряд, и множество его факторов является дизъюнктным объединением композиционных факторов групп N и Q.

Доказательство. Пусть группы N и Q имеют композиционные ряды

$$N \rhd N_1 \rhd \ldots \rhd N_{n-1} \rhd \{e\}$$
$$Q \rhd Q_1 \rhd \ldots \rhd Q_{m-1} \rhd \{e\}\,.$$

Обозначим через $P_i = \pi^{-1}(Q_i)$ полный прообраз группы Q_i при гомоморфизме факторизации $\pi\colon G \twoheadrightarrow Q$ с ядром N. Цепочка подгрупп

$$G \rhd P_1 \rhd \ldots \rhd P_{m-1} \rhd N_1 \rhd \ldots \rhd N_{n-1} \rhd \{e\}$$

является рядом Жордана – Гёльдера с требуемыми свойствами. □

Следствие 19.4
Каждая конечная группа обладает конечным композиционным рядом. □

Упражнение 19.19. Постройте композиционный ряд аддитивной группы $\mathbb{Z}/(p^n)$, где p — простое.

19.5. Полупрямые произведения. Для пары подгрупп N, H группы G отображение

$$N \times H \to NH\,, \quad (x,h) \mapsto xh\,,$$

биективно если и только если $N \cap H = \{e\}$. В самом деле, при $x_1h_1 = x_2h_2$ элемент

$$x_2^{-1}x_1 = h_2h_1^{-1} \in N \cap H\,,$$

и если $N \cap H = \{e\}$, то $x_2 = x_1$ и $h_2 = h_1$, а если в $N \cap H$ есть элемент $z \neq e$, то разные пары (e,e), $(z,z^{-1}) \in N \times H$ перейдут в один и тот же элемент $e \in NH$. Будем называть подгруппы $N, H \subset G$ *дополнительными*, если $N \cap H = \{e\}$ и $NH = G$. В этом случае группа G как множество находится в биекции с прямым произведением $N \times H$. Если подгруппа $N \lhd G$ при этом нормальна, то композиция элементов $g_1 = x_1h_1$ и $g_2 = x_2h_2$ может быть выражена в терминах пар (x_1,h_1), $(x_2,h_2) \in N \times H$. А именно, поскольку

$$g_1g_2 = x_1h_1x_2h_2 = x_1(h_1x_2h_1^{-1}) \cdot h_1h_2 \quad \text{и} \quad h_1x_2h_1^{-1} \in N\,,$$

группу G можно *описать* как множество $N \times H$ с операцией

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 \operatorname{Ad}_{h_1}(x_2), h_1 h_2)\,, \tag{19-16}$$

где через $\operatorname{Ad}_h : N \xrightarrow{\sim} N$, $x \mapsto hxh^{-1}$, обозначено присоединённое действие элемента h на нормальной подгруппе N. В этой ситуации говорят, что группа G является *полупрямым произведением* нормальной подгруппы $N \lhd G$ и дополнительной к ней подгруппы $H \subset G$ и пишут $G = N \rtimes H$. Если сопряжение элементами из подгруппы H действует на подгруппе N тривиально, что равносильно перестановочности $xh = xh$ любых двух элементов $x \in N$ и $h \in H$, то полупрямое произведение называется *прямым*. В этом случае $(x_1, h_1) \cdot (x_2, h_2) = (x_1 x_2, h_1 h_2)$ для всех пар (x_1, h_1), $(x_2, h_2) \in N \times H$.

Пример 19.8 (диэдральная группа $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$)
Группа диэдра D_n содержит нормальную подгруппу поворотов, изоморфную аддитивной группе $\mathbb{Z}/(n)$. Подгруппа второго порядка, порождённая любым отражением, дополнительна к группе поворотов и изоморфна аддитивной группе $\mathbb{Z}/(2)$. Присоединённое действие отражения на группе поворотов меняет знак у угла поворота. При отождествлении группы поворотов с $\mathbb{Z}/(n)$ это действие превращается в умножение на -1. Таким образом, $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$ и в терминах пар $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$ композиция на группе диэдра задаётся правилом

$$\big(x_1, y_1\big) \cdot \big(x_2, y_2\big) = \big(x_1 + (-1)^{y_1} x_2, y_1 + y_2\big)\,, \quad x_1, x_2 \in \mathbb{Z}/(n)\,, \quad y_1, y_2 \in \mathbb{Z}/(2)\,.$$

Пример 19.9 (аффинная $\operatorname{Aff}(V) = V \rtimes \operatorname{GL}(V)$)
Помимо линейной и проективной групп $\operatorname{GL}(V)$ и $\operatorname{PGL}(V)$ с каждым векторным пространством V связана *аффинная группа* $\operatorname{Aff}(V)$ биективных аффинных преобразований[1] $\mathbb{A}(V) \xrightarrow{\sim} \mathbb{A}(V)$ аффинного пространства[2] $\mathbb{A}(V)$. Она содержит нормальную подгруппу сдвигов[3]

$$\tau_v : \mathbb{A}(V) \to \mathbb{A}(V)\,, \quad p \mapsto p + v\,,$$

которая (по второму из данных в n° 13.1 определений аффинного пространства) изоморфна аддитивной группе векторов пространства V и является ядром сюръективного гомоморфизма

$$D : \operatorname{Aff}(V) \twoheadrightarrow \operatorname{GL}(V)\,, \quad \varphi \mapsto D_\varphi\,, \tag{19-17}$$

сопоставляющего аффинному преобразованию $\varphi : \mathbb{A}(V) \to \mathbb{A}(V)$ его дифференциал

$$D_\varphi : V \to V\,, \quad \overrightarrow{pq} \mapsto \overrightarrow{\varphi(p)\varphi(q)}\,.$$

Если зафиксировать в $\mathbb{A}(V)$ какую-нибудь точку p, то ограничение гомоморфизма (19-17) на стабилизатор $\operatorname{Stab}_p \subset \operatorname{Aff}(V)$ задаст изоморфизм $D_p : \operatorname{Stab}_p \xrightarrow{\sim} \operatorname{GL}(V)$. Обратный изоморфизм сопоставляет линейному оператору $f : V \xrightarrow{\sim} V$ аффинное преобразование

$$\varphi_f : \mathbb{A}(V) \to \mathbb{A}(V)\,, \quad x \mapsto p + f(\overrightarrow{px})\,,$$

[1] См. n° 13.2 на стр. 238.
[2] См. прим. 13.4 на стр. 236.
[3] См. n° 13.1 на стр. 235.

оставляющее на месте точку p. Каждое преобразование $\varphi \in \mathrm{Aff}(V)$ однозначно раскладывается в композицию $\varphi = \tau_v \circ (\tau_{-v} \circ \varphi)$ параллельного переноса τ_v на вектор $v = \overrightarrow{p\varphi(p)}$ и преобразования $\tau_{-v} \circ \varphi \in \mathrm{Stab}(p)$. Поэтому

$$\mathrm{Aff}(V) = V \rtimes \mathrm{Stab}_p \simeq V \rtimes \mathrm{GL}(V) \tag{19-18}$$

Упражнение 19.20. Покажите, что $\varphi \circ \tau_v \circ \varphi^{-1} = \tau_{D_\varphi(v)}$ для всех $\varphi \in \mathrm{Aff}(V)$ и $v \in V$.

Мы заключаем, что композиция аффинных преобразований в терминах полупрямого разложения (19-18) задаётся правилом

$$(u, f) \cdot (w, g) = (u + f(w),\ fg)\,.$$

19.5.1. Полупрямое произведение групп. Предыдущую конструкцию можно применить к двум абстрактным группам N и H как только задано действие группы H на группе N, т. е. гомоморфизм группы H в группу автоморфизмов группы N:

$$\psi : H \to \mathrm{Aut}\, N\,, \quad h \mapsto \psi_h : N \xrightarrow{\sim} N\,, \tag{19-19}$$

По аналогии с форм. (19-16) на стр. 357 зададим на множестве $N \times H$ операцию правилом

$$(x_1, h_1) \cdot (x_2, h_2) \stackrel{\text{def}}{=} (x_1 \psi_{h_1}(x_2), h_1 h_2)\,. \tag{19-20}$$

Упражнение 19.21. Проверьте, что формула (19-20) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = \left(\psi_h^{-1}(x^{-1}), h^{-1}\right)$, где $\psi_h^{-1} = \psi_{h^{-1}}$ — автоморфизм, обратный к $\psi_h : N \xrightarrow{\sim} N$.

Полученная таким образом группа называется *полупрямым произведением* групп N и H по действию $\psi : N \to \mathrm{Aut}\, H$ и обозначается $N \rtimes_\psi H$. Подчеркнём, что результат зависит от ψ. Если действие тривиально, т. е. $\psi_h = \mathrm{Id}_N$ для всех $h \in H$, получится прямое произведение $N \times H$ с покомпонентными операциями.

Упражнение 19.22. Убедитесь, что подмножество $N' \stackrel{\text{def}}{=} \{(x, e) \mid x \in N\}$ является изоморфной группе N нормальной подгруппой в $G = N \rtimes_\psi H$ и фактор $G / N' \simeq H$, а подмножество $H' \stackrel{\text{def}}{=} \{(e, h) \mid h \in H\}$ (e, h) является изоморфной H и дополнительной к N' подгруппой в G, причём $G = N' \rtimes H'$ является полупрямым произведением своих подгрупп N' и H'.

Предложение 19.7
Для любых гомоморфизма $\psi : H \to \mathrm{Aut}(N)$, $h \mapsto \psi_h$, и автоморфизмов $\alpha : H \xrightarrow{\sim} H$ и $\beta : N \xrightarrow{\sim} N$ отображения $(n, h) \mapsto (n, \alpha^{-1} h)$ и $(n, h) \mapsto (\beta n, h)$ задают изоморфизмы полупрямых произведений $N \rtimes_\psi H \xrightarrow{\sim} N \rtimes_{\psi \circ \alpha} H$ и $N \rtimes_\psi H \xrightarrow{\sim} N \rtimes_{\mathrm{Ad}_\beta(\psi)} H$, где $\mathrm{Ad}_\beta(\psi) : H \to \mathrm{Aut}(N)$, $h \mapsto \beta \psi_h \beta^{-1}$.

Доказательство. Отображение $(n, h) \mapsto (n, \alpha^{-1} h)$ переводит сомножители из левой части равенства $(n_1, h_1)(n_2, h_2) = (n_1 \psi_{h_1} n_2, h_1 h_2)$ в $(n_1, \alpha^{-1} h_1)$ и $(n_2, \alpha^{-1} h_2)$, произведение которых в $N \rtimes_{\psi \circ \alpha} H$ равно $(n_1 \psi_{h_1} n_2, \alpha^{-1}(h_1 h_2))$. Отображение $(n, h) \mapsto (\beta n, h)$ переводит те же самые сомножители в $(\beta n_1, h_1)$ и $(\beta n_2, h_2)$. Их произведение в $N \rtimes_{\mathrm{Ad}_\beta(\psi)} H$ равно $(\beta(n_1 \psi_{h_1} n_2), h_1 h_2)$. □

Пример 19.10 (голоморф)
Группа автоморфизмов $\mathrm{Aut}\, G$ произвольной группы G тавтологически действует на G. Полупрямое произведение $\mathrm{Hol}\, G \stackrel{\text{def}}{=} G \rtimes \mathrm{Aut}\, G$ по этому действию называется *голоморфом* группы G. Вложение $G \hookrightarrow \mathrm{Hol}\, G$ замечательно тем, что любой автоморфизм группы G является сужением на G внутреннего автоморфизма объемлющей группы $\mathrm{Hol}\, G$.

Пример 19.11 (сплетение)
Для любых двух групп H, N множество N^H всех функций $f: H \to N$ имеет естественную структуру группы, в которой $f_1 f_2: H \to N$, $x \mapsto f_1(x) f_2(x)$. Эту группу можно воспринимать как прямое произведение одинаковых копий группы N, занумерованных элементами[1] $x \in H$. Группа H действует на N^H по следующему правилу: элемент $h \in H$ переводит функцию $f: H \to N$ в функцию $hf: x \mapsto f(xh)$.

Упражнение 19.23. Убедитесь, что $h(f_1 f_2) = (hf_1)(hf_2)$ и $(h_1 h_2)f = h_1(h_2 f)$.

Полупрямое произведение $N \wr H \stackrel{\text{def}}{=} N^H \rtimes H$ по этому действию называется *сплетением*[2] группы N с группой H. Сплетение замечательно тем, что любая группа G с нормальной подгруппой $N \lhd G$ и факторгруппой $H = G/N$ допускает гомоморфное *вложение Фробениуса* $\varphi: G \hookrightarrow N \wr H$. Чтобы задать его, зафиксируем какое-нибудь теоретико множественное сечение $\sigma: H \hookrightarrow G$ гомоморфизма факторизации $\pi: G \twoheadrightarrow H = G/N$, выбирающее в каждом классе $h \in G/N$ некоторый представитель $\sigma(h) \in G$. Тогда для любых $g \in G$ и $h \in H$ элемент $\sigma(h) g \sigma(h\pi(g))^{-1} \in N$, поскольку $\pi(\sigma(h) g \sigma(h\pi(g))^{-1}) = h\pi(g)(h\pi(g))^{-1} = e$. Рассмотрим функцию

$$\sigma_g: H \to N, \quad h \mapsto \sigma(h) g \sigma(h\pi(g))^{-1},$$

как элемент группы N^H и положим $\varphi_\sigma(g) = (\sigma_g, \pi(g)) \in N^H \rtimes H$.

Упражнение 19.24. Убедитесь, что $\varphi_\sigma(g_1 g_2) = \varphi_\sigma(g_1)\varphi_\sigma(g_2)$ в $N^H \rtimes H$ и что образы двух вложений $\varphi_\sigma, \varphi_\tau: G \hookrightarrow N \wr H$, построенных при помощи разных сечений $\sigma, \tau: H \hookrightarrow G$, сопряжены в группе $N \wr H$.

19.6. p-группы и теоремы Силова. Группа порядка p^n, где $p \in \mathbb{N}$ — простое, называется *p-группой*. Поскольку все нетривиальные подгруппы p-группы также являются p-группами, длина любой орбиты p-группы при любом её действии на любом множестве либо делится на p, либо равна единице. Мы получаем простое, но полезное

Предложение 19.8
Пусть p-группа G действует на конечном множестве X, число элементов в котором не делится на p. Тогда G имеет на X неподвижную точку. □

Предложение 19.9
Любая p-группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы является множеством одноточечных орбит этого действия. Так как число элементов в группе и длины всех неодноточечных орбит делятся на p, одноточечные орбиты не могут исчерпываться одной орбитой элемента e. □

Упражнение 19.25. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

Определение 19.2 (силовские подгруппы)
Пусть G — произвольная конечная группа. Запишем её порядок в виде $|G| = p^n m$, где p — простое, $n \geqslant 1$, и m взаимно просто с p. Всякая подгруппа $S \subset G$ порядка $|S| = p^n$ называется *силовской p-подгруппой* в G. Количество силовских p-подгрупп в G обозначается через $N_p(G)$.

[1] Ср. с n° 2.6 на стр. 36.
[2] По английски *wreath product*.

Теорема 19.5 (теорема Силова)
Для любого простого $p \mid |G|$ силовские p-подгруппы в G существуют. Все они сопряжены друг другу, и любая p-подгруппа в G содержится в некоторой силовской p-подгруппе.

Доказательство. Пусть $|G| = p^n m$, где m взаимно просто с p. Обозначим через $\mathcal{E}$ множество p^n-элементных подмножеств в G и рассмотрим действие G на $\mathcal{E}$, индуцированное левым регулярным действием G на себе. Стабилизатор точки $F \in \mathcal{E}$ состоит из всех элементов $g \in G$, левое умножение на которые переводит множество $F \subset G$ в себя: $\operatorname{Stab}(F) = \{g \in G \mid gF \subset F\}$. Так как $g_1 x \neq g_2 x$ при $g_1 \neq g_2$ в группе G, группа $\operatorname{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\operatorname{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\operatorname{Stab}(F)|$ и имеется следующая альтернатива: либо длина G-орбиты элемента $F \in \mathcal{E}$ делится на p, либо G-орбита элемента $F \in \mathcal{E}$ состоит из m элементов и $|\operatorname{Stab}(F)| = p^n$, т. е. подгруппа $\operatorname{Stab}(F) \subset G$ силовская. Во втором случае согласно предл. 19.8 каждая p-подгруппа $H \subset G$ (в частности, каждая силовская подгруппа), имеет на G-орбите элемента F неподвижную точку gF, а значит, содержится в силовской подгруппе $\operatorname{Stab}(gF) = g \operatorname{Stab}(F) g^{-1}$, сопряжённой к $\operatorname{Stab}(F)$ (и совпадает с ней, если H силовская). Таким образом, для доказательства теоремы остаётся убедиться, что в множестве $\mathcal{E}$ есть G-орбита, длина которой не делится на p. Это следует из лем. 19.1 ниже. □

Лемма 19.1
$|\mathcal{E}| = \binom{p^n m}{p^n} \equiv m \pmod{p}$ не делится на p.

Доказательство. Класс вычетов $\binom{p^n m}{p^n} \pmod{p}$ равен коэффициенту при x^{p^n}, возникающему при раскрытии бинома $(1+x)^{p^n m}$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Так как над $\mathbb{F}_p$ возведение в p-тую степень является аддитивным гомоморфизмом, $(1+x)^{p^n} = 1 + x^{p^n}$, откуда $(1+x)^{p^n m} = \left(1 + x^{p^n}\right)^m = 1 + m x^{p^n} +$ старшие степени. □

Следствие 19.5 (дополнение к теореме Силова)
В условиях теоремы Силова число N_p силовских p-подгрупп в G делит m и сравнимо с единицей по модулю p.

Доказательство. Обозначим множество силовских p-подгрупп в G через $\mathcal{S}$ и рассмотрим действие G на $\mathcal{S}$, индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathcal{S}| = |G| / |\operatorname{Stab}(P)|$, где $P \in \mathcal{S}$ — произвольно взятая силовская p-подгруппа. Поскольку $P \subset \operatorname{Stab}(P)$, порядок $|\operatorname{Stab}(P)|$ делится на $|P| = p^n$, а значит $|\mathcal{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что P, действуя сопряжениями на $\mathcal{S}$, имеет там ровно одну неподвижную точку, а именно, саму себя. Тогда порядки всех остальных P-орбит будут делиться на p, и мы получим $|\mathcal{S}| \equiv 1 \pmod{p}$.

Пусть силовская подгруппа $H \in \mathcal{S}$ неподвижна при сопряжении подгруппой P. Это означает, что $P \subset \operatorname{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. Поскольку $H \subset \operatorname{Stab}(H) \subset G$, порядок $|\operatorname{Stab}(H)| = p^n m'$, где $m' | m$ взаимно просто с p. Таким образом, и P, и H являются силовскими p-подгруппами в $\operatorname{Stab}(H)$, причём H нормальна в $\operatorname{Stab}(H)$. Так как все силовские подгруппы сопряжены, мы заключаем, что $H = P$, что и требовалось. □

Пример 19.12 (группы порядка pq с простыми $p > q$)
Пусть $|G| = pq$, где $p > q$ простые. Тогда в G есть ровно одна, автоматически нормальная силовская p-подгруппа $H_p \simeq \mathbb{Z}/(p)$. Рассмотрим любую силовскую q-подгруппу $H_q \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно n° 19.5 $G = \mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ для некоторого гомоморфизма $\psi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$.

Упражнение 19.26. Убедитесь, что $\mathrm{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)$.

Гомоморфизм $\psi : \mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^\times$ однозначно задаётся своим значением на образующей $[1]_q$, которая является элементом порядка q. Поэтому элемент $\eta = \psi([1]_q) \in \boldsymbol{\mu}_q(\mathbb{F}_p) \subset \mathbb{F}_p^\times$ является корнем q-й степени из 1 в поле $\mathbb{F}_p$. По упр. 6.7 на стр. 104 группа $\boldsymbol{\mu}_q(\mathbb{F}_p)$ циклическая порядка нод$(q, p-1)$. Мы заключаем, что если $q \nmid (p-1)$, то всякий гомоморфизм

$$\mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$$

тривиален, и единственной группой порядка pq в этом случае является $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$. Если же $q \mid (p-1)$, то существует нетривиальный гомоморфизм

$$\psi : \ \to \mathrm{Aut}(\mathbb{Z}/(p)), \quad [1]_q \mapsto \eta, \tag{19-21}$$

где $\eta \in \mathbb{F}_p^\times$ порождает мультипликативную группу $\boldsymbol{\mu}_q(\mathbb{F}_p)$. Гомоморфизм (19-21) сопоставляет каждому элементу $[y]_q \in \mathbb{Z}/(q)$ автоморфизм $\psi_y : \mathbb{Z}/(p) \xrightarrow{\sim} \mathbb{Z}/(p)$, $[x]_p \mapsto [\eta^y x]_p$, и задаёт полупрямое произведение $\mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ с операцией

$$\big([x_1]_p, [y_1]_q\big) \cdot \big([x_2]_p, [y_2]_q\big) = \big([x_1 + \eta^{y_1} x_2]_p, [y_1 + y_2]_q\big). \tag{19-22}$$

Любой другой нетривиальный гомоморфизм $\mathbb{Z}/(q) \to \mathrm{Aut}(\mathbb{Z}/(p))$ имеет вид $\psi^m : [1]_q \mapsto \eta^m$, где $1 \leqslant m \leqslant q-1$, и является композицией гомоморфизма (19-21) с автоморфизмом умножения на $m : \mathbb{Z}/(q) \xrightarrow{\sim} \mathbb{Z}/(q)$, $[y]_q \mapsto [my]_q$. Согласно предл. 19.7 на стр. 358

$$\mathbb{Z}/(p) \rtimes_{\psi \circ m} \mathbb{Z}/(q) \simeq \mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q).$$

Мы заключаем, что при $q \mid (p-1)$ кроме абелевой группы $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ существует единственная с точностью до изоморфизма неабелева группа порядка pq. Она изоморфна $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(q)$ с операцией (19-22). В частности, для простого $p > 2$ единственной с точностью до изоморфизма неабелевой группой порядка $2p$ является группа диэдра[1] D_p.

Задачи для самостоятельного решения к §19

Задача 19.1. Пусть две нормальные подгруппы пересекаются по единице. Покажите, что их элементы коммутируют друг с другом.

Задача 19.2. Пусть произведение любых двух левых смежных классов некоторой подгруппы H также является левым смежным классом подгруппы H. Верно ли, что H нормальна?

Задача 19.3. Приведите пример таких двух не изоморфных групп G_1, G_2 и их нормальных подгрупп $H_1 \lhd G_1$, $H_2 \lhd G_2$, что $H_1 \simeq H_2$ и $G_1/H_1 \simeq G_2/H_2$.

[1] См. прим. 19.8 на стр. 357.

Задача 19.4. Докажите, что ядро действия группы G левыми умножениями на множестве смежных классов G/H произвольной подгруппы $H \subset G$ является единственной максимальной по включению нормальной подгруппой $N \lhd G$, содержащейся в H.

Задача 19.5. Докажите, что при $n \geqslant 5$ индекс любой подгруппы $H \subsetneq A_n$ не меньше n.

Задача 19.6. Докажите, что неабелева простая группа, обладающая подгруппой индекса n, гомоморфно вкладывается в A_n.

Задача 19.7. Докажите, что любая подгруппа, индекс которой равен наименьшему делящему порядок группы простому числу, нормальна.

Задача 19.8. Перечислите левые и правые смежные классы группы $\mathrm{GL}_2(\mathbb{F}_2)$ по подгруппе верхнетреугольных матриц.

Задача 19.9. Для группы $\mathrm{GL}_2(\mathbb{F}_3)$ укажите а) все силовские подгруппы б) два разных композиционных ряда.

Задача 19.10. Вычислите коммутатор $T_{ij}(\alpha)T_{k\ell}(\beta)T_{ij}^{-1}(\alpha)T_{k\ell}^{-1}(\beta)$ двух трансвекций[1].

Задача 19.11. Вычислите коммутант группы а) обратимых верхнетреугольных б) унитреугольных матриц над произвольным полем.

Задача 19.12. Докажите, что: а) любая подгруппа, содержащая коммутант, нормальна б) коммутант нормальной подгруппы нормален.

Задача 19.13 (разрешимые группы). Докажите эквивалентность следующих двух свойств группы G: а) существует цепочка подгрупп $G = G_0 \rhd G_1 \rhd \ldots \rhd G_{n-1} \rhd G_n = e$ с абелевыми факторами G_i/G_{i+1} б) последовательные коммутаторы $G, G', G'', G''', \ldots$ тривиализуются на конечном шагу.

Задача 19.14. Пусть $N \lhd G$ и $H = G/N$. Верно ли, что если две из групп N, G, H разрешимы, то разрешима и третья?

Задача 19.15. Разрешимы ли при простых p, q, r все группы порядка а) pq б) pq^2 в) pqr?

Задача 19.16. Докажите, что любая p-группа разрешима[2].

Задача 19.17. Докажите, что все группы порядка < 60 разрешимы[3].

Задача 19.18. Докажите, что неразрешимая группа порядка 60 изоморфна[4] A_5.

Задача 19.19. Напишите два разных композиционных ряда для группы: а) S_4 б) D_6.

Задача 19.20. Предъявите три попарно не изоморфные группы порядка а) 2211 б) 6771 в) 22517, укажите их композиционные ряды и факторы Жордана – Гёльдера.

Задача 19.21. Разложите в полупрямое произведение собственных подгрупп группы а) S_n б) обратимых верхнетреугольных матриц в) подобий евклидовой плоскости.

Задача 19.22. Есть ли такое разложение у группы[5] Q_8?

Задача 19.23. Приведите пример неабелевой группы порядка а) 21 б) 27 и укажите какой-нибудь её композиционный ряд.

---

[1] См. формулу (19-4) на стр. 351.

[2] Подсказка: вложите её в S_n, а S_n — в $\mathrm{GL}_n(\mathbb{F}_p)$, и примените теорему Силова.

[3] Подсказка: $\exists\, p : N_p < 4$.

[4] Подсказка: рассмотрите её действие на силовских 5-подгруппах.

[5] См. зад. 18.20 на стр. 345.

Задача 19.24. Покажите, что группа $\mathbb{Z}/(3) \rtimes_\psi \mathbb{Z}/(4)$, где $\psi : \mathbb{Z}/(4) \to \mathrm{Aut}(\mathbb{Z}/(3))$ переводит $[1]_4$ в автоморфизм смены знака, не абелева и не изоморфна ни D_6, ни A_4.

Задача 19.25. Верно ли, что силовская p-подгруппа группы G

а) нормальна если и только если $N_p(G) = 1$

б) пересекает каждую подгруппу $H \subset G$ по силовской p-подгруппе в H

в) отображается в силовскую p-подгруппу при каждой факторизации $G \twoheadrightarrow G/N$?

Задача 19.26. Для простых $p \in \mathbb{N}$ найдите $N_p(S_p)$.

Задача 19.27. Перечислите все силовские подгруппы симметрических групп а) S_3 б) S_4 в) S_7.

Задача 19.28. Пусть $|D_n| = 2^m k$, где k нечётно. Докажите, что $N_2(D_n) = k$.

Задача 19.29. Верно ли, что p-группа G имеет нормальную подгруппу каждого делящего $|G|$ порядка?

Задача 19.30. Верно ли, что во всех группах порядка 12 есть нормальная подгруппа порядка 4?

Задача 19.31. Перечислите с точностью до изоморфизма все группы порядка:
а) 8 б) 12 в) $\leqslant 15$ г) 21 д) 45 е) 49 ж) 105 з) 2121.

Задача 19.32. Верно ли, что верхние унитреугольные матрицы составляют силовскую p-подгруппу в $\mathrm{GL}_n(\mathbb{F}_p)$? Сколько всего силовских p-подгрупп в $\mathrm{GL}_n(\mathbb{F}_p)$?

Задача 19.33. Опишите подгруппу, порождённую матрицами $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ и $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ в $\mathrm{SL}_2(\mathbb{F}_3)$, и перечислите все силовские подгруппы в $\mathrm{SL}_2(\mathbb{F}_3)$.

§20. Задание групп образующими и соотношениями

20.1. Свободные группы. С любым множеством M можно связать группу F_M, которая называется *свободной группой*, порождённой множеством M. Она состоит из классов эквивалентных слов, которые можно написать буквами x и x^{-1}, где $x \in M$, по наименьшему отношению эквивалентности, отождествляющему между собою слова, отличающиеся друг от друга вставкой или удалением[1] двубуквенного фрагмента xx^{-1} или $x^{-1}x$. Композиция определяется как приписывание одного слова к другому. Единицей служит пустое слово. Обратным к классу слова $w = x_1 \dots x_m$ является класс слова $w^{-1} = x_m^{-1} \dots x_1^{-1}$, где каждая из букв x_i равна x или x^{-1}, где $x \in M$, и $\left(x^{-1}\right)^{-1} \stackrel{\text{def}}{=} x$.

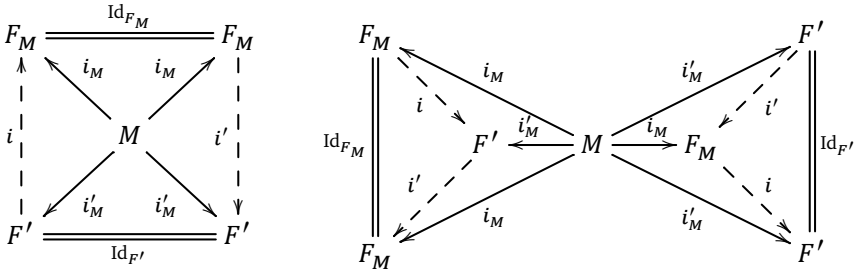
Упражнение 20.1. Убедитесь, что композиция корректно определена на классах эквивалентности слов и что в каждом классе содержится ровно одно *несократимое*[2] слово, которое одновременно является и самым коротким словом в своём классе.

Элементы множества M называются *образующими* свободной группы F_M. Свободная группа с k образующими обозначается F_k. Группа $F_1 \simeq \mathbb{Z}$ — это циклическая группа бесконечного порядка. Группа F_2 классов слов на четырёхбуквенном алфавите x, y, x^{-1}, y^{-1} уже трудно обозрима.

Упражнение 20.2. Постройте инъективный гомоморфизм групп $F_{\mathbb{N}} \hookrightarrow F_2$.

Предложение 20.1 (универсальное свойство свободной группы)
Отображение $i_M : M \to F_M$, переводящее элемент $x \in M$ в класс однобуквенного слова $x \in F_M$, обладает следующим свойством: для любых группы G и отображения множеств $\varphi_M : M \to G$ существует единственный такой гомоморфизм групп $\varphi : F_M \to G$, что $\varphi_M = \varphi \circ i_M$. Для любого обладающего этим свойством отображения $i'_M : M \to F'$ множества M в группу F' имеется единственный такой изоморфизм групп $i' : F_M \xrightarrow{\sim} F'$, что $i'_M = i' \circ i_M$.

Доказательство. Гомоморфизм φ единствен, так как обязан переводить слово $x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \in F_M$, где $x_\nu \in M$, $\varepsilon_\nu = \pm 1$, в произведение $\varphi_M(x_1)^{\varepsilon_1} \dots \varphi_M(x_m)^{\varepsilon_m} \in G$. С другой стороны, это правило корректно задаёт гомоморфизм групп, что доказывает первое утверждение. Если отображение $i' : M \to F'$ множества M в группу F' обладает универсальным свойством из предл. 20.1, то существуют единственные гомоморфизмы $i' : F_M \to F'$ и $i : F' \to F_M$, встраивающиеся в коммутативные диаграммы



Разложения вида $i_M = \varphi \circ i_M$, $i'_M = \psi \circ i'_M$ в силу их единственности возможны только с $\varphi = \mathrm{Id}_{F_M}$, $\psi = \mathrm{Id}_{F'}$. Поэтому $i' \circ i = \mathrm{Id}_{F'}$, $i \circ i' = \mathrm{Id}_{F_M}$. □

[1] В начале, в конце, или же между произвольными двумя последовательными буквами слова.
[2] Т. е. не содержащее двубуквенных фрагментов xx^{-1} и $x^{-1}x$.

20.2. Образующие и соотношения. Если гомоморфизм групп

$$\varphi : F_M \twoheadrightarrow G\,, \tag{20-1}$$

заданный отображением $\varphi_M : M \to G$ множества M в группу G, является сюръективным, то говорят, что группа G *порождается* элементами $g_m = \varphi_M(m)$, $m \in M$, а сами элементы g_m называются *образующими* группы G. В этом случае G исчерпывается всевозможными произведениями $g_1^{\varepsilon_1}\dots g_k^{\varepsilon_k}$, $\varepsilon = \pm 1$, образующих и обратных к ним элементов. Группа G называется *конечно порождённой*, если она допускает конечное множество образующих. Ядро $\ker\varphi \lhd F_M$ эпиморфизма (20-1) называется *группой соотношений* между образующими g_m. Набор слов $R \subset \ker\varphi$ называется набором *определяющих соотношений*, если $\ker\varphi$ — это наименьшая нормальная подгруппа в F_M, содержащая R. Это означает, что любое соотношение можно получить из слов множества R конечным числом умножений, обращений и сопряжений произвольными элементами из свободной группы F_M. Группа, допускающая конечное число образующих с конечным набором определяющих соотношений называется *конечно определённой*.

Всякую группу можно задать образующими и соотношениями, например, взяв в качестве M множество всех элементов группы. Удачный выбор образующих с простыми определяющими соотношениями может значительно прояснить устройство группы и её гомоморфизмов в другие группы. Однако в общем случае выяснить, изоморфны ли две группы, заданные своими образующими и определяющими соотношениями, или даже определить, отлична ли группа, заданная образующими и соотношениями, от тривиальной группы $\{e\}$, бывает очень непросто. Более того, обе эти задачи являются *алгоритмически неразрешимыми*[1] даже в классе конечно определённых групп.

Предложение 20.2
Пусть группа G_1 задана множеством образующих M и набором определяющих соотношений R, а G_2 — произвольная группа. Отображение $\varphi : M \to G_2$ тогда и только тогда корректно задаёт гомоморфизм групп $G_1 \to G_2$ правилом $x_1^{\varepsilon_1}\dots x_m^{\varepsilon_m} \mapsto \varphi(x_1)^{\varepsilon_1}\dots\varphi(x_m)^{\varepsilon_m}$, когда для каждого слова $y_1^{\varepsilon_1}\dots y_m^{\varepsilon_m} \in R$ в группе G_2 выполняется соотношение $\varphi(y_1)^{\varepsilon_1}\dots\varphi(y_m)^{\varepsilon_m} = 1$.

Доказательство. Отображения множеств $\varphi_M : M \to G_2$ биективно соответствуют гомоморфизмам групп $\varphi : F_M \to G_2$. Такой гомоморфизм φ факторизуется до гомоморфизма из группы $G_1 = F_M/N_R$, где $N_R \lhd F_M$ — наименьшая нормальная подгруппа, содержащая R, тогда и только тогда, когда $N_R \subset \ker\psi$. Так как $\ker\psi \lhd F_M$, для этого необходимио и достаточно включения $R \subset \ker\psi$. □

Пример 20.1 (образующие и соотношения группы диэдра)
Покажем, что группа диэдра D_n задаётся двумя образующими x_1, x_2 и соотношениями

$$x_1^2 = x_2^2 = (x_1x_2)^n = e\,. \tag{20-2}$$

Оси симметрии правильного n-угольника разбивают его на $2n$ конгруэнтных прямоугольных треугольников как на рис. 20⋄1 ниже. Обозначим один из них через e. Поскольку любое движение плоскости однозначно задаётся своим действием на треугольник e, треугольники разбиения находятся в биекции с движениями $g \in D_n$, и каждый из них можно однозначно пометить

[1] В формальном смысле, принятом в математической логике.

тем единственным преобразованием g, которое переводит треугольник e в этот треугольник. При этом каждое преобразование $h \in D_n$ переводит каждый треугольник g в треугольник hg.

Упражнение 20.3. Для любого движения F евклидова пространства $\mathbb{R}^n$ и отражения σ_π в произвольной гиперплоскости $\pi \subset \mathbb{R}^n$ докажите соотношения

$$\sigma_{F(\pi)} = F \circ \sigma_\pi \circ F^{-1} \quad \text{и} \quad \sigma_{F(\pi)} \circ F = F \circ \sigma_\pi \,. \tag{20-3}$$

Обозначим через ℓ_1 и ℓ_2 боковые стороны треугольника e, а отражения плоскости в этих сторонах обозначим через $\sigma_1 = \sigma_{\ell_1}$ и $\sigma_2 = \sigma_{\ell_2}$. Тогда по второму из равенств (20-3) треугольники, получающиеся из e последовательными отражениями в направлении часовой стрелки пометятся элементами

$$\begin{aligned}
\sigma_{\ell_1} &= \sigma_1\,,\\
\sigma_{\sigma_1(\ell_2)}\sigma_1 &= \sigma_1\sigma_2\,,\\
\sigma_{\sigma_1\sigma_2(\ell_1)}\sigma_1\sigma_2 &= \sigma_1\sigma_2\sigma_1\,,\\
\sigma_{\sigma_1\sigma_2\sigma_1(\ell_2)}\sigma_1\sigma_2\sigma_1 &= \sigma_1\sigma_2\sigma_1\sigma_2\,,\ \ldots
\end{aligned}$$

а треугольники, получающиеся из e последовательными отражениями против часовой стрелки пометятся элементами

$$\begin{aligned}
\sigma_{\ell_2} &= \sigma_2\,,\\
\sigma_{\sigma_2(\ell_1)}\sigma_2 &= \sigma_2\sigma_1\,,\\
\sigma_{\sigma_2\sigma_1(\ell_2)}\sigma_2\sigma_1 &= \sigma_2\sigma_1\sigma_2\,,\\
\sigma_{\sigma_2\sigma_1\sigma_2(\ell_1)}\sigma_2\sigma_1\sigma_2 &= \sigma_2\sigma_1\sigma_2\sigma_1\,,\ \ldots
\end{aligned}$$

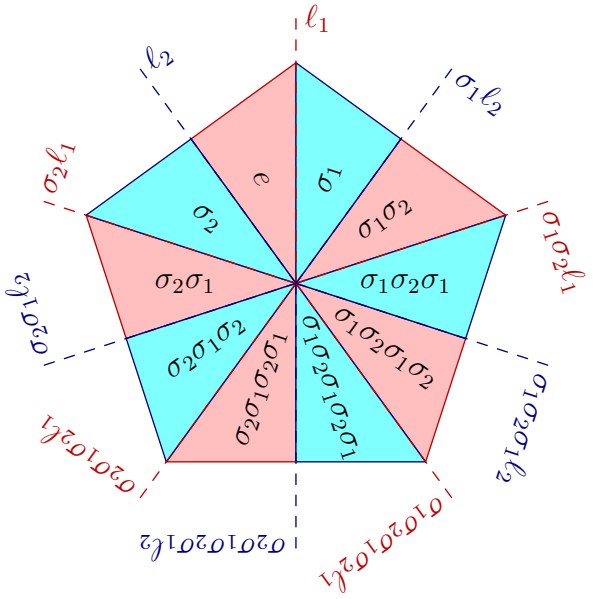


Рис. 20⋄1. Образующие группы диэдра.

В результате каждый треугольник пометится словом вида $\sigma_1\sigma_2\sigma_1\sigma_2\ldots$ или $\sigma_2\sigma_1\sigma_2\sigma_1\ldots$ Так как композиция $\sigma_1 \circ \sigma_2$ является поворотом на угол $2\pi/n$, в группе D_n выполняются соотношения

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e\,, \tag{20-4}$$

и правило $x_1 \mapsto \sigma_1$, $x_2 \mapsto \sigma_2$ корректно задаёт сюръективный гомоморфизм $\varphi : F_2/H \twoheadrightarrow D_n$ из фактора свободной группы F_2 с образующими x_1, x_2 по наименьшей нормальной подгруппе $H \lhd F_2$, содержащей слова x_1^2, x_2^2 и $(x_1x_2)^n$. Покажем, что он инъективен. Поскольку последнее соотношение в (20-2) равносильно равенству

$$\underbrace{\sigma_1\sigma_2\sigma_1\ldots}_{k} = \underbrace{\sigma_2\sigma_1\sigma_2\ldots}_{2n-k}\,, \tag{20-5}$$

каждое слово в алфавите $\{x_1, x_2, x_1^{-1}, x_2^{-1}\}$ записывается по модулю соотношений (20-2) словом

$$x_1x_2x_1\ldots \quad \text{или} \quad x_2x_1x_2\ldots \tag{20-6}$$

из не более n букв, причём два n-буквенных слова равны друг другу в F_2/H. Согласно предыдущему, все эти слова переводятся гомоморфизмом φ в разные треугольники, т. е. в разные элементы $g \in D_n$. Мы заключаем, что гомоморфизм $\varphi\colon F_2/H \xrightarrow{\sim} D_n$ биективен, а все слова (20-6), за исключением двух равных n-буквенных слов, различны по модулю H и являются самими короткими выражениями элементов группы D_n через образующие σ_1, σ_2.

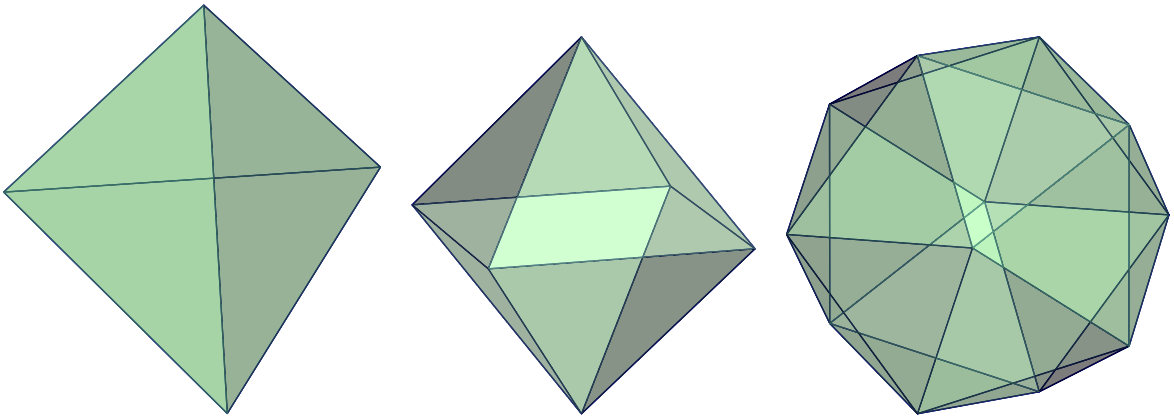


Рис. 20◇2. Тетраэдр, октаэдр и икосаэдр.

20.3. Образующие и соотношения групп платоновых тел. Обозначим через M платоново тело с треугольными гранями, т. е. правильный *тетраэдр*, *октаэдр* или *икосаэдр*, см. рис. 20◇2. Плоскости симметрии многогранника M задают *барицентрическое разбиение* каждой грани на 6 конгруэнтных друг другу треугольников с вершинами в центре грани, в середине ребра этой грани и в одном из концов этого ребра, см. рис. 20◇3. Обозначим, соответственно, через π_1, π_2, π_3 плоскости симметрии, высекающие противолежащие этим вершинам стороны в одном из треугольников, который пометим единичным элементом e группы O_M многогранника M. Двугранный угол между плоскостями π_i и π_j обозначим через

$$\pi/m_k = \measuredangle(\pi_i, \pi_j)\,, \quad \text{где} \quad k = \{1,2,3\} \smallsetminus \{i,j\}\,. \tag{20-7}$$

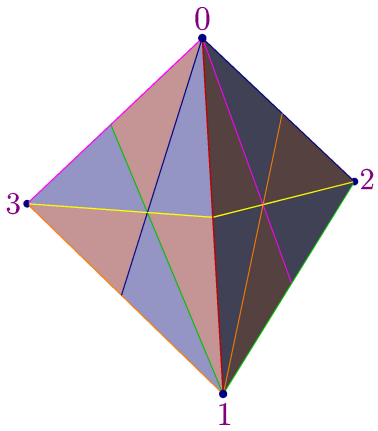


Рис. 20◇3. Барицентрическое разбиение тетраэдра плоскостями симметрии.

Числа m_i, а также число γ граней многогранника M и общее число треугольников $N = 6\gamma$ представлены в таблице[1]:

M	m_1	m_2	m_3	γ	N
тетраэдр	3	2	3	4	24
октаэдр	3	2	4	8	48
икосаэдр	3	2	5	20	120 .

Обозначим через σ_i отражение в плоскости π_i. Так как каждое преобразование из группы O_M однозначно определяется своим действием на тройку векторов с концами в вершинах треугольника e, каждый треугольник триангуляции является образом треугольника e под действием единственного преобразования $g \in \mathrm{O}_M$. Надпишем каждый треугольник этим преобразованием g,

[1] Обратите внимание, что помещённый в пространство n-угольный диэдр из прим. 20.1 тоже можно включить в этот список со значениями $m_1 = n$, $m_2 = 2$, $m_3 = 2$, $\gamma = 2$ и $N = 4n$, если условиться, что плоский диэдр имеет две двумерные грани: «верхнюю» и «нижнюю».

и пометим его стороны, высекаемые плоскостями $g(\pi_1)$, $g(\pi_2)$, $g(\pi_3)$ соответствующими номерами 1, 2, 3. Отметим, что каждое преобразование $h \in \mathrm{O}_M$ переводит каждый треугольник g в треугольник hg. На рис. 20⋄4 изображена стереографическая проекция картинки, которую 24 трёхгранных угла барицентрического разбиения тетраэдра с рис. 20⋄3 высекают на описанной около этого тетраэдра сфере. На каждом сферическом треугольнике написана композиция отражений $\sigma_1, \sigma_2, \sigma_3$, переводящая треугольник e в этот треугольник. Стороны треугольников, помеченные номерами 1, 2 и 3, изображены на рисунке в красным, зелёным и жёлтым цветом.

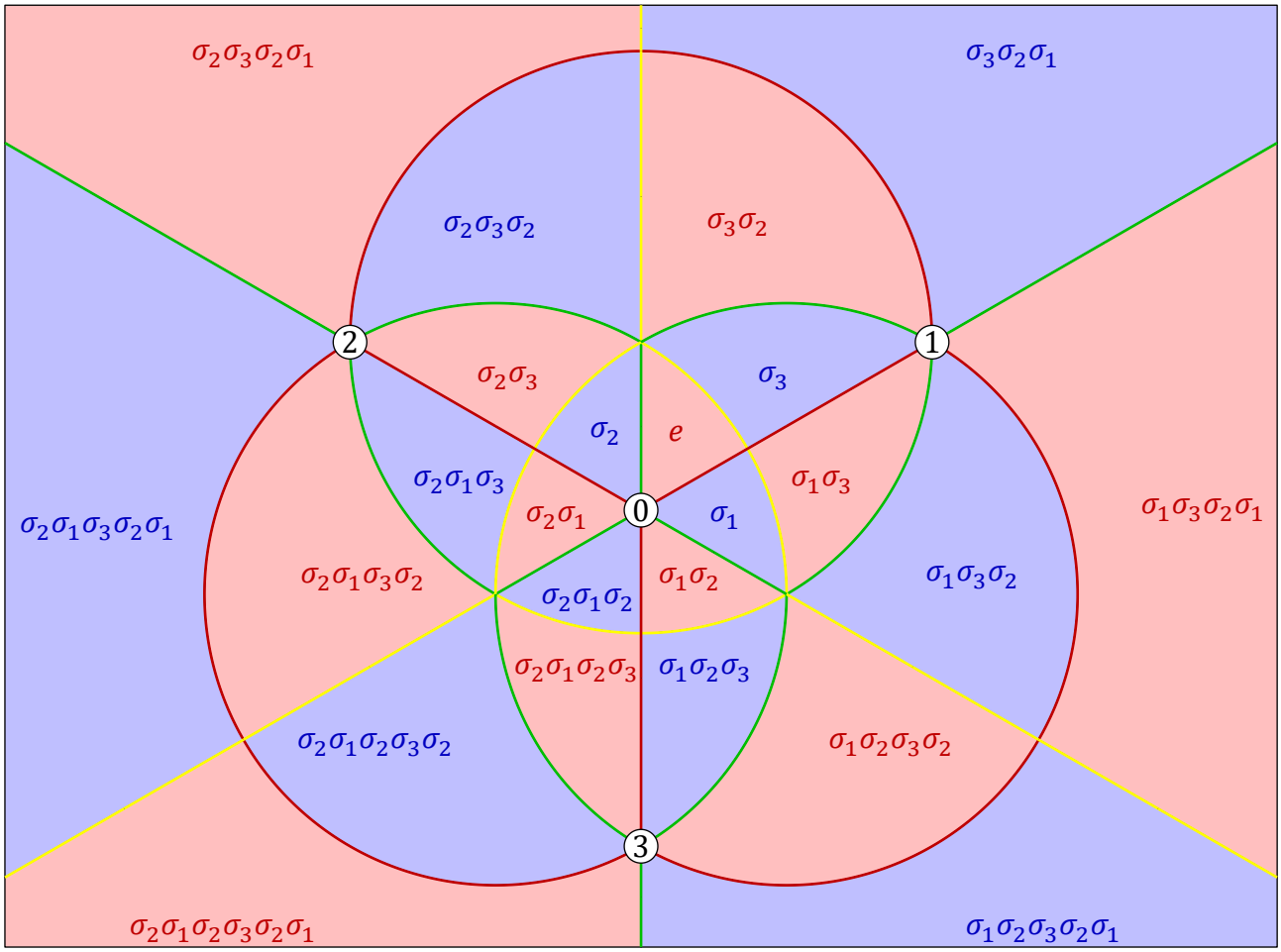


Рис. 20⋄4. Триангуляция описанной сферы плоскостями симметрии тетраэдра в стереографической проекции из диаметрально противоположного к вершине «0» полюса сферы на экваториальную плоскость, параллельную грани «123».

Чтобы явно написать композицию отражений $\sigma_1, \sigma_2, \sigma_3$, переводящую треугольник e в треугольник g, выберем внутри опирающихся на эти треугольники трёхгранных углов векторы u и w с концами на описанной около M сфере так, чтобы $w \neq -u$ и натянутая на них плоскость Π_{uw} не содержала линий пересечения плоскостей симметрии многогранника M. Пройдём из u в w по кратчайшей из двух дуг окружности, высекаемой плоскостью Π_{uw} на описанной около M сфере. Пусть мы при этом последовательно побываем в треугольниках

$$g_1 = e,\ g_2,\ g_3,\ \dots\ ,\ g_{m+1} = g\,.$$

Обозначим через $\nu_i \in \{1,2,3\}$ номер, надписанный на той стороне треугольника g_i, сквозь которую осуществляется проход из g_i в g_{i+1}. Это означает, что общая сторона треугольников g_i и g_{i+1} высекается плоскостью $g_i(\pi_{\nu_i})$, т. е. образом плоскости π_{ν_i} при отображении g_i. Тогда

$$g_2 = \sigma_{\nu_1}\,,\ g_3 = \sigma_{g_2(\pi_{\nu_2})}g_2 = \sigma_{\nu_1}\sigma_{\nu_2}\,,\ g_4 = \sigma_{g_3(\pi_{\nu_3})}g_3 = \sigma_{\nu_1}\sigma_{\nu_2}\sigma_{\nu_3}\,,\ \dots$$

по второму равенству из форм. (20-3) на стр. 366. Таким образом, последовательность индексов $\nu_i \in \{1,2,3\}$ в разложении $g = \sigma_{\nu_1}\dots\sigma_{\nu_m}$ состоит из выписанных по порядку номеров сторон, которые приходится пересекать по пути из $e = g_1$ в $g = g_{m+1}$ по дуге uw, как на рис. 20⋄5, где стороны с номерами 1, 2, 3 изображены соответственно красным, зелёным и жёлтым цветами. Отметим, что полученное нами разложение элемента $g \in \mathrm{O}_M$ в композицию отражений $\sigma_1, \sigma_2, \sigma_3$ не единственно и зависит от выбора векторов u и w внутри трёхгранных углов e и g. При изменении любого из этих векторов последовательность $\nu_1, \dots, \nu_m$ номеров зеркал, пересекаемых по дороге из u в w, не меняется до тех пор, пока натянутая на эти векторы плоскость Π_{uw} не натолкнётся на линию пересечения зеркал, а в момент пересечения такой линии в последовательности $\nu_1, \dots, \nu_m$ некоторый фрагмент вида $\sigma_i\sigma_j\sigma_i\sigma_j\dots$ длины m_k заменяется симметричным фрагментом $\sigma_j\sigma_i\sigma_j\sigma_i\dots$ той же самой длины m_k, как показано на рис. 20⋄5.

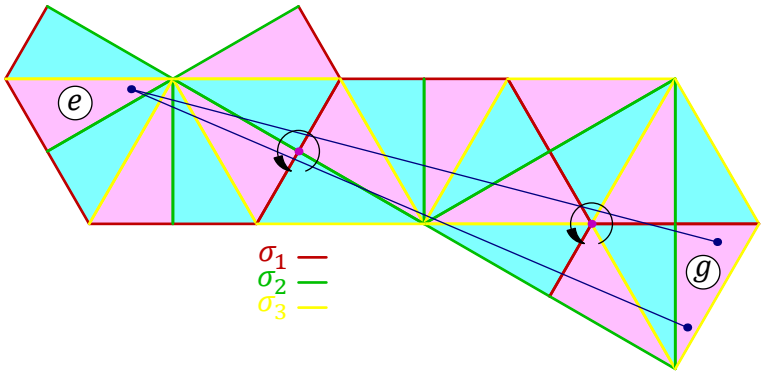


Рис. 20⋄5. $\sigma_2\sigma_3\sigma_2\sigma_3\boldsymbol{\sigma_1}\boldsymbol{\sigma}_2\sigma_3\sigma_2\sigma_3\sigma_2\boldsymbol{\sigma_3}\boldsymbol{\sigma_1}\boldsymbol{\sigma_3}\sigma_2 = g = \sigma_2\sigma_3\sigma_2\sigma_3\boldsymbol{\sigma_2}\boldsymbol{\sigma_1}\sigma_3\sigma_2\sigma_3\sigma_2\boldsymbol{\sigma_1}\boldsymbol{\sigma_3}\boldsymbol{\sigma_1}\sigma_2$.

Разложения, отвечающие верхней и нижней траекториям на рис. 20⋄5 отличаются друг от друга тем, что линии пересечения зеркал обходятся в противоположных направлениях. Композиции возникающих при этом отражений удовлетворяют соотношениям

$$\sigma_1\sigma_2 = \sigma_2\sigma_1 \quad \text{и} \quad \sigma_1\sigma_3\sigma_1 = \sigma_3\sigma_1\sigma_3$$

той же самой природы, что соотношения (20-4) в группе диэдра: так как композиция отражений $\sigma_i \circ \sigma_j$ является поворотом вокруг прямой $\pi_i \cap \pi_j$ на угол $2\pi/m_k$, равный удвоенному углу между плоскостями π_i и π_j, в группе O_M выполняются соотношения $\sigma_i^2 = e$ и $(\sigma_i\sigma_j)^{m_k} = e$, где $i = 1,2,3$, а тройка (i,j,k) пробегает три циклические перестановки номеров $(1,2,3)$.

Отсюда вытекает, во-первых, что длина представления $g = \sigma_{\nu_1}\dots\sigma_{\nu_m}$, считанного вдоль кратчайшей из двух дуг, соединяющих векторы u и w, не зависит от выбора этих векторов внутри трёхгранных углов, опирающихся на треугольники e и g, при условии, что плоскость Π_{uw} не проходит через линии пересечения зеркал, а во-вторых, что правило $x_i \mapsto \sigma_i$ задаёт сюръективный гомоморфизм $\varphi : F_3/H \twoheadrightarrow \mathrm{O}_M$ из фактора свободной группы F_3 с образующими x_1, x_2, x_3 по наименьшей нормальной подгруппе $H \lhd F_3$, содержащей шесть слов

$$x_i^2 \qquad \text{и} \qquad (x_ix_j)^{m_k}\,. \tag{20-8}$$

Для проверки его инъективности достаточно для каждого элемента $y \in F_3 / H$ убедиться в том, что последовательность номеров $\nu_1, \dots, \nu_k$, считанная с любой кратчайшей дуги, соединяющей треугольник e с треугольником $g = \varphi(y)$, как это объяснялось выше, даёт представление

$$y = x_{\nu_1} \dots x_{\nu_k}$$

минимально возможной по модулю соотношений (20-8) длины. Тогда каждый элемент $y \in F_3/H$ будет однозначно восстанавливаться по своему образу $g(y) \in \mathrm{O}_M$.

Воспользуемся индукцией по длине k кратчайшего по модулю соотношений (20-8) слова $x_{\nu_1} \dots x_{\nu_k}$, представляющего данный элемент $y \in F_3 / H$. Для представимых однобуквенными словами элементов $y = x_1, x_2, x_3$ утверждение очевидно. Пусть оно верно для всех $y \in F_3 / H$, представимых словами из $\leqslant k$ букв. Рассмотрим произвольный такой y и проверим утверждение для всех элементов yx_j, $j = 1, 2, 3$, которые по модулю соотношений (20-8) не представимы словами из $\leqslant k$ букв. Пусть $g = \varphi(y)$ и $h = \varphi(yx_j) = g\sigma_j$. Выберем в треугольниках e и g векторы $u \in e$ и $w \in g$ так, чтобы окружность, высекаемая из сферы плоскостью Π_{uw}, пересекала плоскость $H = g(\pi_j)$. Кротчайшая дуга этой окружности, ведущая из u в w либо не пересекает плоскость H, как на рис. 20⋄6, либо пересекает, как на рис. 20⋄7.

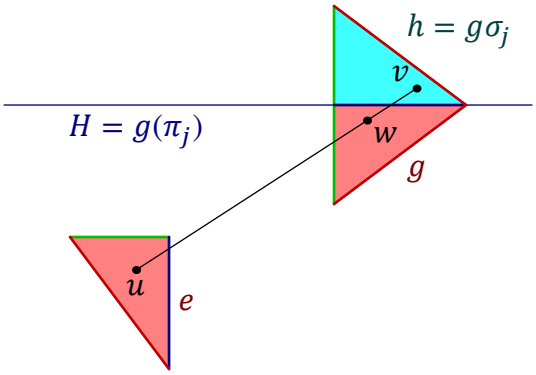


Рис. 20⋄6. H не разделяет e и g.

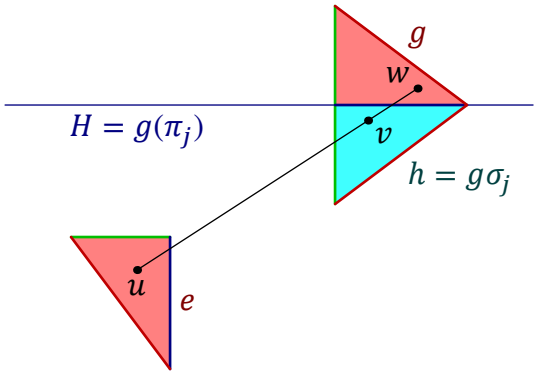


Рис. 20⋄7. H разделяет e и g.

Во втором случае обозначим через v какую-нибудь точку дуги $[u, w]$, лежащую в предыдущем треугольнике $\sigma_{g(\pi_j)} g = g\sigma_j g^{-1} g = g\sigma_j = h$. По предположению индукции, одно из минимальных по длине представлений $y = x_{\nu_1} \dots x_{\nu_m}$ имеет в качестве $\nu_1, \dots, \nu_m$ номера последовательных рёбер, которые приходится пересекать по пути из u в w по дуге $[u, w]$, и его длина $m \leqslant k$. В частности, последняя буква $x_{\nu_m} = x_j$. Поэтому элемент $yx_j = x_{\nu_1} \dots x_{\nu_{m-1}}$ записывается более коротким, чем y, словом из $< k$ букв, вопреки нашему предположению. Таким образом, имеет место первый случай, изображённый на рис. 20⋄6. Обозначим через $v \in h$ какой-нибудь вектор, лежащий на продолжении дуги $[u, w]$ за точку w. По предположению индукции, одно из минимальных по количеству букв представлений $y = x_{\nu_1} \dots x_{\nu_m}$ имеет в качестве $\nu_1, \dots, \nu_m$ номера последовательных рёбер, которые приходится пересекать по пути из u в w по дуге $[u, w]$, и его длина $m \leqslant k$. При этом $h = \varphi(yx_j) = g\sigma_j = \sigma_{i_1} \dots \sigma_{i_m} \sigma_j$, и представление $yx_j = x_{\nu_1} \dots x_{\nu_m} x_j$ по нашему предположению состоит, как минимум, из $k + 1$ букв. Мы заключаем, что $m = k$, представление $yx_j = x_{\nu_1} \dots x_{\nu_k} x_j$ является одним из кратчайших для элемента yx_j и считывается с дуги $[u, v]$, как и требуется. Мы получили следующий результат.

Предложение 20.3
Полная группа O_M платонова тела M с треугольными гранями порождается тремя элементами x_1, x_2, x_3, связанными шестью определяющими соотношениями $x_i^2 = e$ и $(x_i x_j)^{m_k} = e$. □

20.4. Образующие и соотношения симметрической группы. Обозначим числами от 0 до n концы стандартных базисных векторов $e_0, e_1, \dots, e_n$ в $\mathbb{R}^{n+1}$ и рассмотрим n-мерный правильный симплекс $\Delta \subset \mathbb{R}^{n+1}$ с вершинами в этих точках. Поскольку каждое аффинное преобразование n-мерной гиперплоскости $x_0 + x_1 + \dots + x_n = 1$, в которой лежит симплекс Δ, однозначно задаётся своим действием на вершины симплекса Δ, полная группа O_Δ симплекса Δ изоморфна симметрической группе S_{n+1} перестановок его вершин $0, 1, \dots, n$. Каждая k-мерная грань симплекса Δ является правильным k-мерным симплексом и представляет собою выпуклую оболочку каких-либо $k+1$ вершин симплекса Δ, и наоборот, выпуклая оболочка $[i_0, i_1, \dots, i_k]$ любых $k+1$ различных вершин $\{i_0, i_1, \dots, i_k\} \subset \{0, 1, \dots, n\}$ является k-мерной гранью симплекса Δ. Симплекс Δ симметричен относительно $n(n+1)/2$ гиперплоскостей π_{ij}, проходящих через середину ребра $[i, j]$ и противолежащую этому ребру грань коразмерности 2 с вершинами $\{0, 1, \dots, n\} \smallsetminus \{i, j\}$. Гиперплоскость π_{ij} перпендикулярна вектору $e_i - e_j$ и отражение $\sigma_{ij} \in \mathrm{O}_\Delta$ в этой гиперплоскости отвечает транспозиции элементов i и j в симметрической группе S_{n+1}.

Упражнение 20.4. Убедитесь, что гиперплоскости π_{ij} и π_{km} с $\{i, j\} \cap \{k, m\} = \varnothing$ ортогональны, а гиперплоскости π_{ij} и π_{jk} с различными i, j, k пересекаются под углом $\pi/3 = 60^\circ$.

Плоскости π_{ij} осуществляют *барицентрическое разбиение* симплекса Δ на $(n+1)!$ меньших симплексов с вершинами в центрах граней симплекса Δ и в центре самого симплекса. Если обозначить через $\langle i_0 i_1 \dots i_m \rangle$ центр m-мерной грани с вершинами в $i_0, i_1, \dots, i_m$, то каждый симплекс барицентрического разбиения будет иметь одну из вершин в какой-либо вершине $\langle i_0 \rangle$ симплекса Δ, следующую вершину — в центре $\langle i_0 i_1 \rangle$ какого-либо примыкающего к вершине i_0 ребра $[i_0, i_1]$, следующую вершину — в центре $\langle i_0 i_1 i_2 \rangle$ какой-либо примыкающей к ребру $[i_0, i_1]$ двумерной треугольной грани $[i_0, i_1, i_2]$ и т. д. вплоть до центра $\langle i_0 i_1 \dots i_n \rangle$ самого симплекса Δ. Эти симплексы находятся в естественной биекции с перестановками $g \in S_{n+1}$: симплекс

$$g = \big[\langle g_0 \rangle, \langle g_0, g_1 \rangle, \langle g_0, g_1, g_2 \rangle, \dots, \langle g_0 g_1 \dots g_{n-1} \rangle, \langle g_0 g_1 \dots g_n \rangle\big] \tag{20-9}$$

является образом начального симплекса

$$e = \big[\langle 0 \rangle, \langle 01 \rangle, \langle 012 \rangle, \dots, \langle 0, 1, \dots, n-1 \rangle, \langle 0, 1, \dots, n \rangle\big] \tag{20-10}$$

под действием единственной перестановки $g = (g_0, g_1, \dots, g_n) \in S_{n+1} = \mathrm{O}_M$. Спроектируем поверхность симплекса Δ из его центра на описанную сферу. Получим разбиение $(n-1)$-мерной сферы S^{n-1} на $(n+1)!$ конгруэнтных друг другу $(n-1)$-мерных симплексов, надписанных элементами $g \in S_{n+1}$. Грани этих симплексов высекаются из сферы гиперплоскостями π_{ij}. При $n = 3$ получится представленная на рис. 20⋄4 на стр. 368 триангуляция двумерной сферы S^2 двадцатью четырьмя сферическими треугольниками с углами $\pi/3$, $\pi/3$ и $\pi/2$. Помеченному тождественным преобразованием e начальному симплексу (20-10) отвечает сферический симплекс, высекаемый из сферы n гиперплоскостями $\pi_i \overset{\text{def}}{=} \pi_{i-1,i}$ с $1 \leqslant i \leqslant n$. Обозначим через $\sigma_i = \sigma_{i-1,i}$ отражения в этих гиперплоскостях. В симметрической группе S_{n+1} этим отражениям отвечают транспозиции $|i-1, i\rangle$ пар соседних элементов. По упр. 20.4 они удовлетворяют соотношениям[1]

$$\sigma_i^2 = e\,, \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \quad \text{и} \quad \sigma_i \sigma_j = \sigma_j \sigma_i\,, \quad \text{где} \quad |i-j| \geqslant 2\,. \tag{20-11}$$

[1] Соотношение $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ является более употребительной в данном контексте записью циклического соотношения $(\sigma_i \sigma_{i+1})^3 = e$ на поворот $\sigma_i \sigma_{i+1}$ на 120° вокруг $(n-2)$-мерного подпространства $\pi_i \cap \pi_{i+1}$.

Упражнение 20.5. Убедитесь напрямую, что транспозиции $\sigma_i = |i-1, i\rangle \in S_{n+1}$ удовлетворяют соотношениям (20-11).

В силу этих соотношений, гомоморфизм свободой группы F_n с образующими $x_1, \dots, x_n$, переводящий x_i в σ_i, корректно факторизуется до гомоморфизма $\varphi : F_n/H \to S_{n+1}$, где $H \lhd F_n$ — наименьшая нормальная подгруппа, содержащая слова

$$x_i^2\,, \quad (x_i x_{i+1})^3 \quad \text{и} \quad (x_i x_j)^2\,, \quad \text{где} \quad |i-j| \geqslant 2\,. \tag{20-12}$$

Чтобы убедиться в его сюръективности, выберем в симплексах e и g точки a и b так, чтобы они не были диаметрально противоположны и соединяющая их геодезическая[1] не пересекала граней коразмерности[2] 2. Пройдя из a в b по этой геодезической, мы получим разложение

$$g = \sigma_{i_1} \dots \sigma_{i_m}\,, \tag{20-13}$$

в котором каждое $i_\nu \in \{1, \dots, n\}$ равно номеру такого зеркала π_{i_ν}, что переход из ν-того встреченного по дороге симплекса g_ν в следующий симплекс[3] $g_{\nu+1}$ осуществляется через грань, высекаемую гиперплоскостью $g_\nu(\pi_{i_\nu})$. Дословно также, как и в n° 20.3, проверяется, что длина представления (20-13), полученного с помощью дуги $[a, b]$ не зависит от выбора её концов $a \in e$ и $b \in g$ при условии, что они не диаметрально противоположны и плоскость π_{ab} не проходит через пересечения зеркал π_{ij}: если при перемещении точек a и b внутри симплексов e и g дуга $[a, b]$ пройдёт через пересечение $g_k(\pi_i \cap \pi_j)$ перпендикулярных гиперграней $g_k(\pi_i)$, $g_k(\pi_j)$ с $|i-j| \geqslant 2$, или через пересечение $g_k(\pi_i \cap \pi_{i+1})$ гиперграней $g_k(\pi_i)$, $g_k(\pi_{i+1})$, пересекающихся под углом 60°, то в представлении $g = \sigma_1 \dots \sigma_m$ стоящий на k-том месте фрагмент $\sigma_i\sigma_j$ или $\sigma_i\sigma_{i+1}\sigma_i$ заменится, соответственно, равным ему в группе O_Δ фрагментом $\sigma_j\sigma_i$ или $\sigma_{i+1}\sigma_i\sigma_{i+1}$. В ортогональной проекции вдоль $(n-2)$-мерного подпространства $g_k(\pi_i \cap \pi_j)$ или $g_k(\pi_i \cap \pi_{i+1})$ на ортогональную ему двумерную плоскость мы при этом увидим картину вроде показанной на рис. 20⋄5 на стр. 369. Дословно такая же, как в n° 20.3, индукция по длине минимального по количеству букв выражения элемента $y \in F_n/H$ через образующие x_i показывает, что считанная с любой соединяющей симплекс e с симплексом $g = \varphi(y)$ дуги последовательность индексов $i_1, \dots, i_m$ даёт минимальное по количеству букв представление $y = x_{i_1} \dots x_{i_m}$ в группе F_n/H. Таким образом, симметрическая группа S_{n+1} порождается n образующими x_i, $1 \leqslant i \leqslant n$, связанными определяющими соотношениями (20-12).

Эту геометрическую картину нетрудно выхолостить до сугубо комбинаторного рассуждения, представленного в следующем разделе.

20.4.1. Порядок Брюа. Напомню[4], что *длиной* $\ell(g)$ перестановки $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ называется количество всех её инверсных пар[5]. Правое умножение перестановки g на транспозицию $\sigma_i = |i-1, i\rangle$ приводит к перестановке $g\sigma_i$, отличающейся от g транспозицией $(i-1)$-того и i-го символов g_{i-1} и g_i:

$$\big(g_0, \dots, g_{i-2}, \boldsymbol{g_{i-1}}, \boldsymbol{g_i}, g_{i+1}, \dots, g_n\big) \circ \sigma_i = \big(g_0, \dots, g_{i-2}, \boldsymbol{g_i}, \boldsymbol{g_{i-1}}, g_{i+1}, \dots, g_n\big)\,,$$

[1] Кратчайшая из двух дуг ab большой окружности, высекаемой из сферы двумерной плоскостью, проходящей через точки a, b и центр сферы.

[2] Т. е. пересечений всевозможных пар зеркал π_{ij}.

[3] Напомню, что при этом $g_\nu = \sigma_1 \dots \sigma_{\nu-1}$, f $g_{\nu+1} = \sigma_{g_\nu(\pi_{i_\nu})} g_\nu = g_\nu \sigma_{i_\nu}$.

[4] См. n° 11.1 на стр. 188.

[5] Т. е. таких пар $1 \leqslant i < j \leqslant n$, что $g_i > g_j$.

причём $\ell(g\sigma_i) = \ell(g) + 1$, если $g_{i-1} < g_i$, и $\ell(g\sigma_i) = \ell(g) - 1$, если $g_{i-1} > g_i$.

Упражнение 20.6. Убедитесь, что любая перестановка g длины $\ell(g) = m$ может быть записана таким словом $g = \sigma_{i_1} \dots \sigma_{i_m}$, что $\ell(\sigma_{i_1} \dots \sigma_{i_k}) = \ell(\sigma_{i_1} \dots \sigma_{i_{k-1}}) + 1$ при всех $2 \leqslant k \leqslant m$.

Частичный порядок на S_{n+1}, в котором $g < h$, если $h = g\sigma_{i_1} \dots \sigma_{i_s}$, где

$$\ell(g\sigma_{i_1} \dots \sigma_{i_k}) = \ell(g\sigma_{i_1} \dots \sigma_{i_{k-1}}) + 1 \text{ при всех } 1 \leqslant k \leqslant s\,,$$

называется *порядком Брюа*.

Слово $w = x_{i_1} \dots x_{i_m}$ в свободной группе F_n с образующими $x_1, \dots, x_n$ называется *минимальным словом* перестановки $g \in S_{n+1}$, если $m = \ell(g)$ и $g = \sigma_{i_1} \dots \sigma_{i_m}$. Начальные фрагменты минимального слова задают строго возрастающую в смысле порядка Брюа последовательность элементов $h_\nu = \sigma_{i_1} \dots \sigma_{i_\nu} \in S_{n+1}$. Перестановка g может иметь много разных минимальных слов, однако не может быть записана никаким более коротким словом.

Как и в предыдущем разделе, рассмотрим гомоморфизм $\varphi : F_n \to S_{n+1}$, $x_i \mapsto \sigma_i$.

Предложение 20.4
По модулю соотношений $x_i^2 = e$, $x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1}$ и $x_i x_j = x_j x_i$, где $|i - j| \geqslant 2$, каждое слово $w \in F_n$ эквивалентно некоторому минимальному слову перестановки $\varphi(w) \in S_{n+1}$, а все минимальные слова перестановки $\varphi(w)$ эквивалентны между собой.

Доказательство. Индукция по количеству букв в слове $w \in F_{n-1}$. Для $w = \varnothing$ утверждение очевидно. Пусть оно справедливо для всех слов из $\leqslant m$ букв. Достаточно для каждого m-буквенного слова w и каждой буквы x_ν проверить предложение для слова wx_ν. Если слово w не является минимальным словом элемента $g = \varphi(w)$, то оно эквивалентно более короткому минимальному слову. Тогда и wx_ν эквивалентно более короткому слову, и предложение справедливо по индукции. Поэтому мы будем далее считать, что слово w является минимальным словом элемента $g = \varphi(w) = (g_0, g_1, \dots, g_n)$. Возможны два случая: либо $g_{\nu-1} > g_\nu$, либо $g_{\nu-1} < g_\nu$. В первом случае у перестановки g есть минимальное слово вида ux_ν, по предположению индукции эквивалентное слову w. Тогда $wx_\nu \sim ux_\nu x_\nu \sim u$ и элемент $\varphi(wx_\nu) = \varphi(u)$ является образом более короткого, чем w слова u, эквивалентного слову wx_ν. По индукции, слово u эквивалентно минимальному слову элемента $\varphi(wx_\nu)$ и все такие слова эквивалентны друг другу. Поэтому то же верно и для эквивалентного u слова wx_ν.

Остаётся рассмотреть случай $g_{\nu-1} < g_\nu$. Здесь $\ell(g\sigma_\nu) = \ell(g) + 1$ и слово wx_ν является минимальным словом для элемента $\varphi(wx_\nu)$. Мы должны показать, что любое другое минимальное слово w' этого элемента эквивалентно wx_ν. Для самой правой буквы слова w' есть 3 возможности: либо она равна x_ν, либо она равна $x_{\nu\pm1}$ либо она равна x_μ с $|\mu - \nu| \geqslant 2$. В пером случае $w' = ux_\nu$, где u, как и w, является минимальным словом элемента g. По индукции $u \sim w$, а значит, и $w' = ux_k \sim wx_k$.

Пусть теперь $w' = ux_{\nu+1}$. Поскольку оба слова wx_ν и $ux_{\nu+1}$ минимальны для перестановки $h = \varphi(wx_\nu) = \varphi(ux_{\nu+1})$, в перестановке h на местах с номерами $\nu - 1, \nu, \nu + 1$ стоят числа $g_\nu > g_{\nu-1} > g_{\nu+1}$, а в перестановке $g = (g_0, g_1, \dots, g_n) = \varphi(w)$ на этих же местах — числа $g_{\nu-1} < g_\nu > g_{\nu+1}$, где $g_{\nu-1} > g_{\nu+1}$. Поэтому у перестановки h имеется минимальное слово вида $sx_{\nu+1}x_\nu x_{\nu+1}$, а у перестановки g — минимальное слово вида $tx_\nu x_{\nu+1}$. Перестановка $h' = \varphi(s) = \varphi(t)$ отличается от h тем, что числа на местах с номерами $\nu-1, \nu, \nu+1$ в ней возрастают и равны $g_{\nu+1} < g_{\nu-1} < g_\nu$. Поскольку $\ell(h') = \ell(h) - 3 = \ell(g) - 2$, оба слова t и s минимальны для h' и по индукции эквивалентны. Кроме того, по индукции $w \sim tx_\nu x_{\nu+1}$. Поэтому

$$wx_\nu \sim tx_\nu x_{\nu+1} x_\nu \sim sx_\nu x_{\nu+1} x_\nu \sim sx_{\nu+1} x_\nu x_{\nu+1}\,.$$

Но $sx_{\nu+1}x_\nu \sim u$, поскольку оба слова минимальны для одной и той же перестановки[1] длины $m = \ell(h) - 1$. Таким образом, $wx_\nu \sim ux_{\nu+1}$. Случай $w' = ux_{\nu-1}$ полностью симметричен.

Наконец, пусть $h = \varphi(wx_\nu) = \varphi(ux_\mu)$, где $|\mu - \nu| \geqslant 2$. Тогда в h есть два непересекающихся фрагмента $g_{\nu-1} > g_\nu$ и $g_{\mu-1} > g_\mu$. Поэтому у h есть минимальные слова вида $tx_\mu x_\nu$ и вида $sx_\nu x_\mu$, где t и s являются минимальными словами для перестановки $\varphi(t) = \varphi(s)$, отличающейся от h тем, что расматриваемые 2 фрагмента в ней имеют вид $g_\nu < g_{\nu-1}$ и $g_\mu < g_{\mu-1}$. Так как длина этой перестановки равна $\ell(h) - 2 = m - 1$, по индукции $t \sim s$. Поскольку tx_μ — минимальное слово для g, по индукции $w \sim tx_\mu$. Аналогично, т. к. sx_ν и u — минимальные слова для перестановки $\varphi(sx_\nu) = \varphi(u)$, отличающейся от h' транспозицией первого из двух фрагментов и потому имеющей длину $\ell(h) - 1 = m$, по индукции $sx_\nu \sim u$. Таким образом, $wx_\nu \sim tx_\mu x_\nu \sim sx_\mu x_\nu \sim sx_\nu x_\mu \sim ux_\mu$, что и требовалось. □

Упражнение 20.7. Убедитесь, что $h \leqslant g$ в смысле порядка Брюа если и только если в симплексах e, h, g из n° 20.4 можно выбрать такие точки a, b, c, что длина геодезической дуги $[ac]$ меньше π и $b \in [ac]$.

20.5. Группы отражений и системы корней. Конечная группа линейных ортогональных преобразований вещественного евклидова пространства называется *группой отражений* или *группой Коксетера*, если она порождается отражениями в гиперплоскостях[2]. Такая группа G однозначно задаётся указанием зеркал всех входящих в неё отражений[3] или, что равносильно, указанием для каждого зеркала пары перпендикулярных ему векторов $\pm e$ единичной длины. Эти векторы называются *корнями* группы G, а их совокупность — *системой корней* и обозначается $\Phi(G)$. Поскольку каждый элемент $g \in G$ переводит отражение $\sigma_e \in G$ в ортогонале к корню $e \in \Phi(G)$ в отражение $\sigma_{g(e)} = g\sigma_e g^{-1} \in G$ в ортогонале к вектору $g(e)$, система корней, равно как и объединение ортогональных корням зеркал, переводится в себя всеми преобразованиями из G. Наоборот, если имеется такой конечный набор Φ векторов единичной длины, что для каждого $e \in \Phi$

$$\Phi \cap \mathbb{R}\, e = \{\pm e\} \quad \text{и} \quad \sigma_e(\Phi) = \Phi\,, \tag{20-14}$$

то отражения в гиперплоскостях $e^\perp$, где $e \in \Phi$, порождают конечную группу отражений в евклидовом пространстве $\operatorname{span}\Phi$.

Упражнение 20.8. Убедитесь в этом.

Определение 20.1

Конечный набор Φ векторов единичной длины со свойствами (20-14) называется *коксетеровской системой корней*.

Замечание 20.1. Рассматриваемые нами коксетеровские системы корней отличаются от систем корней, возникающих в теории алгебр Ли и алгебраических групп[4], где *приведёнными системами корней* называют такие обладающие свойствами (20-14) наборы ненулевых векторов Φ,

[1] Она отличается от g, h и h' тем, что числа в позициях с номерами $\nu - 1, \nu, \nu + 1$ в ней упорядочены как $g_\nu > g_{\nu+1} < g_{\nu-1}$, где $g_\nu > g_{\nu-1}$.

[2] См. n° 17.1.2 на стр. 309.

[3] Обратите внимание, что композиция $\sigma_b\sigma_a$ отражений в ортогоналах к непропорциональным векторам a, b тождественна на подпространстве $a^\perp \cap b^\perp$ коразмерности 2, а в ортогональной ему плоскости $\operatorname{span}(a, b)$ действует поворотом на угол $2\measuredangle(a, b)$, т. е. группа отражений, вопреки названию, состоит не только из отражений. Она ими всего лишь порождается.

[4] Ср. с главой V части III книги Ж.-П. Серр, *Алгебры Ли и группы Ли*, М., «Мир», 1969.

в которых $2(a,b)/(a,a) \in \mathbb{Z}$ для всех $a, b \in \Phi$. Если заменить все векторы a приведённой системы корней единичными векторами $a/|a|$, то получится коксетеровская система корней, однако не все коксетеровские системы получаются из приведённых, а разные приведённые системы могут превратиться в одну и ту же коксетеровскую.

Пример 20.2 (система корней A_n)
Обозначим через V_n гиперплоскость $x_0 + x_1 + \cdots + x_n = 0$ в координатном пространстве[1] $\mathbb{R}^{n+1}$, а через $\sigma_{ij} = \sigma_{e_i - e_j} \colon \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$ — отражение в гиперплоскости, ортогональной вектору $e_i - e_j \in V_n$. Это отражение осуществляет транспозицию базисных векторов e_i, e_j, оставляя все остальные базисные векторы на месте, и группа, порождённая отражениями σ_{ij} изоморфна симметрической группе S_{n+1} перестановок базисных векторов пространства $\mathbb{R}^{n+1}$. Все эти перестановки оставляют на месте вектор $e = e_0 + e_1 + \ldots + e_n$ и переводят в себя подпространство $V_n = e^\perp$, действуя в нём полной группой правильного n-мерного симплекса $\Delta \subset V_n$ с центром в нуле и вершинами в ортогональных проекциях векторов e_i на V_n. Гиперплоскости $(e_i - e_j)^\perp \cap V_n$ суть гиперплоскости симметрии этого симплекса[2]. Единичные векторы $(e_i - e_j)/\sqrt{2}$ образуют в V_n коксетеровскую систему корней, которая обозначается A_n.

Пример 20.3 (система корней B_n)
Обозначим через $e_1, \ldots, e_n$ стандартный базис в $\mathbb{R}^n$. Отражения σ_{e_i} независимо меняют знаки координат и образуют группу, изоморфную $\bigl(\mathbb{Z}/(2)\bigr)^n$. Отражения $\sigma_{e_i - e_j}$ порождают группу S_n перестановок базисных векторов с системой корней A_{n-1} из прим. 20.2. Вторая группа нормализует первую: $g\sigma_{e_{i_1}} \ldots \sigma_{e_{i_k}} g^{-1} = \sigma_{e_{g(i_1)}} \ldots \sigma_{e_{g(i_k)}}$ для любой перестановки g базисных векторов. Их полупрямое произведение[3] $\bigl(\mathbb{Z}/(2)\bigr)^n \rtimes S_n$, в котором второй сомножитель действует на первом перестановками компонент, содержит и все отражения $\sigma_{e_i + e_j} = \sigma_{e_j}\sigma_{e_i - e_j}\sigma_{e_j}$.

Упражнение 20.9. Убедитесь, что векторы $\pm e_i$ и $\pm e_i \pm e_j$, где $1 \leqslant i < j \leqslant n$, исчерпывают множество всех векторов длины 1 и 2 с целыми координатами, а ортогональные им гиперплоскости суть гиперплоскости симметрии стандартного правильного кокуба[4]

$$C^n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \sum |x_i| \leqslant 1\}.$$

Мы заключаем, что полная группа правильного кокуба является группой отражений с коксетеровской системой корней из $2n + 2n(n-1) = 2n^2$ векторов $\pm e_i$ и $(\pm e_i \pm e_j)/\sqrt{2}$. Эта система корней обозначается B_n.

Пример 20.4 (система корней D_n)
Отражения $\sigma_{e_i - e_j}$ и $\sigma_{e_i + e_j}$ из прим. 20.3 порождают в группе кокуба подгруппу индекса 2, содержащую всевозможные перестановки координат и одновременные смены знака у любого *чётного* числа базисных векторов. Эта группа отражений изоморфна полупрямому произведению $\bigl(\mathbb{Z}/(2)\bigr)^{n-1} \rtimes S_n$, а её коксетеровская система корней состоит из $2n(n-1)$ векторов $(e_i \pm e_j)/\sqrt{2}$ и обозначается D_n.

[1] Обратите внимание, что координаты нумеруются с нуля.
[2] Ср. с n° 20.4 на стр. 371.
[3] См. n° 19.5 на стр. 356.
[4] Т. е. выпуклой оболочки концов векторов $\pm e_i$ в $\mathbb{R}^n$, см. зад. 14.10 на стр. 270.

20.5.1. Камеры Вейля. Пусть в n-мерном евклидовом пространстве V действует группа отражений G с системой корней $\Phi = \{a_1, \dots, a_m\}$. Обозначим через $\Sigma \stackrel{\text{def}}{=} \bigcup_{a\in\Phi} a^\perp$ объединение всех зеркал. Дополнение $C \stackrel{\text{def}}{=} V \smallsetminus \Sigma = C_1 \sqcup \dots \sqcup C_N$ является дизъюнктным объединением открытых конусов, которые называются *камерами Вейля* и представляют собою классы эквивалентности векторов из $V \smallsetminus \Sigma$ по отношению, объявляющему две точки эквивалентными, если они лежат в одном открытом полупространстве относительно всех гиперплоскостей $a_i^\perp$. Это отношение является пересечением более простых эквивалентностей, задаваемых каждым из векторов a_i.

Упражнение 20.10. Говорят, что векторы u, w лежат в одном полупространстве относительно гиперплоскости $a^\perp$, если $(a,u)(a,w) > 0$. Убедитесь, что это свойство является отношением эквивалентности и равносильно тому, что отрезок $[u,w] \stackrel{\text{def}}{=} \{\lambda u + \mu w \mid \lambda, \mu \geqslant 0 \ \&\ \lambda+\mu = 1\}$ не пересекает в гиперплоскости $a^\perp$.

Таким образом, каждая камера C_ν вместе с любыми двумя точками содержит соединяющий их отрезок, и две точки $u, w \in C$ лежат в одной камере если и только если отрезок $[u,w]$ не пересекает зеркал. Обозначим через Ψ_{ij} двумерную плоскость, порождённую корнями a_i, a_j. Ортогональным дополнением к ней является $(n-2)$-мерное пересечение зеркал $\Psi_{ij}^\perp = a_i^\perp \cap a_j^\perp$. Все проходящие через это пересечение зеркала группы G высекают в плоскости Ψ_{ij} двумерную конфигурацию прямых, составляющих зеркала некой диэдральной группы $D_{m_{ij}}$, как на рис. 20⋄1 на стр. 366. Целое число $m_{ij} \geqslant 2$ однозначно определяется группой G и корнями a_i, a_j как число всех зеркал группы G, проходящих через пересечение i-того и j-того зеркала. При этом наименьший из углов между всеми такими зеркалами равен π/m_{ij} (см. рис. 20⋄8). Таким образом, в любой группе отражений есть лишь следующие возможности для взаимного расположения произвольно выбранных i-того и j-того зеркал.

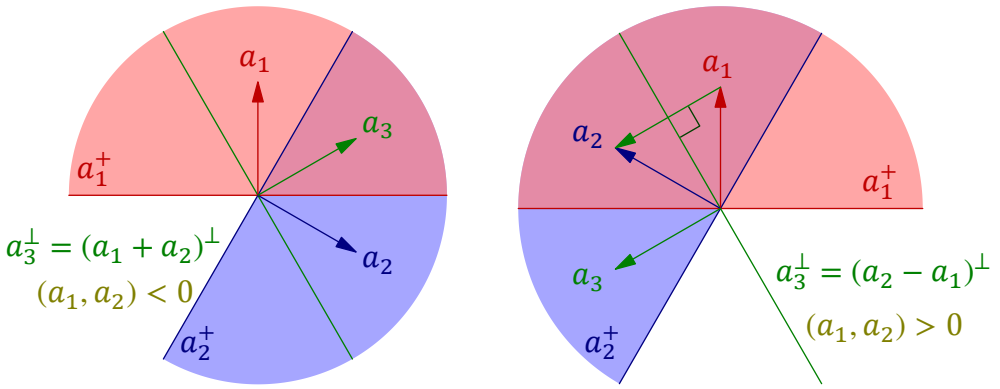


Рис. 20⋄8. Соседние и не соседние зеркала.

Лемма 20.1
Если двугранный угол $a_i^+ \cap a_j^+$, где $a^+ \stackrel{\text{def}}{=} \{v \in V \mid (a,v) > 0\}$, не пересекает зеркал группы G, то $(a_i, a_j) \leqslant 0$, и равенство равносильно тому, что $m_{ij} = 2$. При $(a_i, a_j) > 0$ в системе корней Φ имеется корень $a_k = \lambda a_i - \mu a_j$ с $\lambda, \mu > 0$, задающий зеркало проходящее между зеркалами $a_i^\perp$ и $a_j^\perp$, и разбивающее двугранный угол $a_i^+ \cap a_j^+$ на два непустых двугранных угла. При $(a_i, a_j) < 0$ в системе Φ_G есть корень $a_k = \lambda a_i + \mu a_j$ с $\lambda, \mu > 0$, задающий зеркало, относительно которого двугранный угол $a_i^+ \cap a_j^+$ расположен в одном полупространстве a_k^+. □

Упражнение 20.11. Докажите лемму, пользуясь рис. 20⋄8.

20.5.2. Положительные корни и стенки. Будем называть *i-той стенкой* часть i-того зеркала $a_i^\perp$, расположенную вне его пересечений с остальными зеркалами, т. е. множество

$$\Sigma_i \stackrel{\text{def}}{=} a_i^\perp \setminus \bigcup_{j\neq i} \Psi_{ij}^\perp .$$

Скажем, что зеркало $a_i^\perp$ *примыкает* к камере C_v, если существует отрезок $[x,y]$ с $x \in C_v$, $y \in \Sigma_i$, не пересекающий объединения зеркал Σ ни в каких других точках кроме y. Если выбрать в каждой паре противоположных корней $\pm a_i$ тот корень, относительно которого камера C_v лежит в положительном полупространстве a_i^+, мы получим (зависящее от камеры C_v) разбиение всей системы корней в дизъюнктное объединение двух центрально симметричных относительно нуля подмножеств

$$\Phi_v^+ \stackrel{\text{def}}{=} \{a \in \Phi \mid \forall\, v \in C_v\ (v,a) > 0\} \quad \text{и} \quad \Phi_v^- \stackrel{\text{def}}{=} \{a \in \Phi \mid \forall\, v \in C_v\ (v,a) < 0\},$$

элементы которых называются *положительными* и *отрицательными* корнями относительно камеры C_v.

Лемма 20.2
Стенка Σ_a, отвечающая корню $a \in \Phi$, тогда и только тогда примыкает к камере C_v, когда найдётся такая точка $y \in a^\perp$, что $(y,b) > 0$ для всех $b \in \Phi_v^+$. Если $a_i, a_j \in \Phi_v^+$ задают стенки, примыкающие к камере C_v, то $(a_i,a_j) \leqslant 0$, и равенство равносильно тому что $m_{ij} = 2$.

Доказательство. Пусть отрезок $[x,y]$ имеет $x \in C_v$, $y \in \Sigma_a$ и не пересекает ни одной гиперплоскости $b^\perp$, где $b \in \Phi_v^+$ отличен от a. Тогда каждая линейная функция $f_b(v) = (v,b)$ строго положительна на этом отрезке. В частности, $(y,b) > 0$ для всех $b \in \Phi_v^+$, $b \neq a$. Наоборот, если есть такая точка $y \in a^\perp$, что $(y,b) > 0$ для всех $b \in \Phi_v^+$, $b \neq a$, то $y \in \Sigma_a$, и для любой точки $x \in C_v$ отрезок $[x,y]$ не пересекает ни одного зеркала $b^\perp$ с $b \neq a$, а зеркало $a^\perp$ пересекает только в точке y, поскольку линейная функция $f_a(v) = (v,a)$ строго положительна на одном конце этого отрезка, зануляется на другом, а значит, строго положительна во всех внутренних точках отрезка. Последнее утверждение леммы вытекает из лем. 20.1, так как в плоскости Ψ_{ij} зеркала $a_i^\perp$ и $a_j^\perp$, которые примыкают к одной и той же камере C_v, должны быть соседними, т. е. образовывать минимальный двугранный угол. □

Упражнение 20.12. Строго докажите последнее утверждение.

Определение 20.2 (эффективность)
Конечная группа отражений G евклидова пространства V называется *эффективной*, если единственным неподвижным относительно всей группы вектором в V является нулевой вектор.

Упражнение 20.13. Убедитесь, что группа G эффективна если и только если её система корней Φ_G линейно порождает пространство V.

20.5.3. Простые корни. Зафиксируем какую-нибудь камеру C_v и будем последовательно выкидывать из множества положительных корней Φ_v^+ те корни, которые являются линейными комбинациями остальных с *положительными* коэффициентами. Оставшееся в результате множество корней обозначается через $\Delta_v \subset \Phi_v^+$, и его элементы называются *простыми корнями* (относительно камеры C_v), а задаваемые ими отражения — *простыми отражениями*.

Упражнение 20.14. Убедитесь, что ни один простой корень не является линейной комбинацией никаких других положительных корней с положительными коэффициентами.

Лемма 20.3
Если группа G эффективна, множество Δ_v является базисом в V и совпадает с множеством всех тех положительных корней, которые задают примыкающие к камере C_v стенки. В частности, Δ_v не зависит от произвола, имеющегося при его построении[1].

Доказательство. Каждый непростой корень $b \in \Phi_v^+ \setminus \Delta_v$ является положительной линейной комбинацией простых. Поэтому в гиперплоскости $b^\perp$ нет таких векторов v, что $(v, a) > 0$ для всех $a \in \Delta_v$. Согласно лем. 20.2 зеркало $b^\perp$ не содержит стенок, примыкающих к камере C_v.

Заметим, что для любых двух различных простых корней a_i, a_j выполняется неравенство $(a_i, a_j) \leqslant 0$, поскольку в противном случае по лем. 20.1 существовал бы положительный корень вида $\lambda a_i - \mu a_j$ с положительными λ, μ, и простой корень a_i был бы положительной линейной комбинацией положительных корней вопреки упр. 20.14.

Покажем теперь, что простые корни линейно независимы. Пусть между ними есть соотношение $\lambda_1 a_1 + \ldots + \lambda_r a_r = 0$, все коэффициенты которого ненулевые. Если они одного знака, можно считать их положительными. В таком случае, скалярно умножая левую часть на любой вектор $v \in C_v$, получаем строго положительное число, что невозможно, т. к. в правой части нуль. Если среди коэффициентов есть и положительные, и отрицательные, перенеся последние направо, получим соотношение $\lambda_{i_1} a_{i_1} + \ldots + \lambda_{i_s} a_{i_s} = \mu_{j_1} a_{j_1} + \ldots + \mu_{j_t} a_{j_t}$, в котором все коэффициенты положительны. Так как все $(a_i, a_j) \leqslant 0$, правая и левая части равны нулю по отдельности в силу идущего ниже упр. 20.15, и мы приходим к уже разобранному случаю.

Упражнение 20.15. Пусть векторы $a_1, \ldots, a_k$ и $b_1, \ldots, b_m$ таковы, что $(a_i, b_j) \leqslant 0$ для всех i, j. Покажите что равенство $\alpha_1 a_1 + \ldots + \alpha_k a_k = \beta_1 b_1 + \ldots + \beta_m b_m$ с неотрицательными коэффициентами α_i, β_j возможно если и только если обе его части равны нулю по отдельности, и $(a_i, b_j) = 0$ всякий раз, когда $\alpha_i \beta_j \neq 0$.

Поскольку группа G эффективна, положительные, а стало быть, и простые корни порождают всё пространство. Тем самым, простые корни $a \in \Delta_v$ составляют базис в V, а двойственные им линейные формы $g_a(v) = (v, a)$ образуют базис в V^*. Поэтому в пространстве V найдутся векторы, на которых одна из форм g_a нулевая, а все остальные положительны. По лем. 20.2 это означает, что все зеркала $a^\perp$ примыкают к камере C_v. □

Следствие 20.1
К каждой камере Вейля эффективной группы отражений пространства V примыкает ровно $\dim V$ зеркал, и их нормали составляют базис в V. Отличные от нуля коэффициенты разложения любого корня группы G по этому базису либо все положительны, либо все отрицательны. □

Упражнение 20.16. Убедитесь, что n векторов $(e_{i-1} - e_i)/\sqrt{2}$, где $1 \leqslant i \leqslant n$, являются простыми корнями системы A_n из прим. 20.2 на стр. 375, $n-1$ векторов $(e_{i-1} - e_i)/\sqrt{2}$, где $2 \leqslant i \leqslant n$, вместе с вектором e_n — простыми корнями системы B_n из прим. 20.3, а те же $n-1$ векторов $(e_{i-1} - e_i)/\sqrt{2}$ вместе с вектором $(e_{n-1} + e_n)/\sqrt{2}$ — простыми корнями системы D_n из прим. 20.4.

Теорема 20.1
Эффективная группа отражений G порождается простыми отражениями $\sigma_i \stackrel{\text{def}}{=} \sigma_{a_i}$ относительно зеркал $a_1^\perp, \ldots, a_n^\perp$, примыкающих к произвольно выбранной камере Вейля, и является факто-

[1] Т. е. порядка, в котором выкидываются лишние корни

ром свободной группы с n образующими x_i по наименьшей нормальной подгруппе, содержащей слова x_i^2 и $(x_i x_j)^{m_{ij}}$ для всех $i \neq j$, где m_{ij} — число зеркал группы G, проходящих через пересечение i-го и j-го зеркала[1]. Элементы группы G взаимно однозначно соответствуют камерам Вейля, и последние могут быть занумерованы элементами группы так, что $h(C_g) = C_{hg}$ для любых $g, h \in G$.

Доказательство. В n° 20.4 на стр. 371 мы уже доказали эту теорему для группы G правильного симплекса с системой корней A_n. То же самое рассуждение доказывает теорему и в общем случае. Зафиксируем «начальную» камеру Вейля C_1 и обозначим через a_i простые относительно неё корни, а через $\sigma_i = \sigma_{a_i}$ — соответствующие им простые отражения. Для каждой камеры C_μ выберем ненулевые векторы $u \in C_1$ и $w \in C_\mu$ единичной длины так, чтобы натянутая на них двумерная плоскость Π_{uw} не пересекалась с $(n-2)$-мерными пересечениями зеркал $\Psi_{ij}^\perp = a_i^\perp \cap a_j^\perp$ группы G. Пройдём из u в w по кратчайшей дуге окружности, высекаемой плоскостью Π_{uw} на единичной сфере с центром в нуле, последовательно отражая камеру C_1 относительно встречаемых стенок и записывая подряд номера $i_1, \dots, i_m \in \{1, \dots, n\}$ тех стенок камеры C_1 через образы которых мы проходим. Дословно также, как в n° 20.3 на стр. 367 проверяется, что $C_\mu = \sigma_{i_1} \dots \sigma_{i_m}(C_1)$, что сопоставление камере C_μ элемента $g_\mu = \sigma_{i_1} \dots \sigma_{i_m} \in G$ задаёт биекцию между камерами и элементами группы G, а соотношения $\big(\sigma_i \sigma_j\big)^{m_{ij}} = \mathrm{Id}$ выражают тот факт, что композиция отражений в паре зеркал, примыкающих к одной камере, является поворотом на угол $2\pi/m_{ij}$. □

20.6. Графы Коксетера. В этом разделе мы перечислим все конечные группы отражений. Назовём группу G отражений евклидова пространства V и её систему корней $\Phi = \Phi_G$ *разложимыми*, если V раскладывается в ортогональную прямую сумму $V = V_1 \oplus V_2$ так, что $\Phi = \Phi_1 \sqcup \Phi_2$, где $\Phi_i = \Phi \cap V_i$. В этом случае группа $G = G_1 \times G_2$ является прямым произведением двух своих подгрупп $G_1, G_2 \subset G$, действующих каждая на своём подпространстве V_i, оставляя дополнительное подпространство неподвижным. Каждая группа отражений пространства V является прямым произведением неразложимых подгрупп, эффективно действующих в попарно ортогональных подпространствах. Поэтому достаточно перечислить неразложимые группы отражений G.

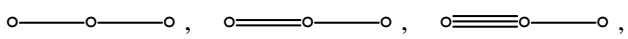
Размерность пространства, где эффективно действует неразложимая группа отражений G называется *рангом* этой группы. Выше мы видели, что ранг равен числу положительных простых корней $a_1, \dots, a_n$ группы G, и G полностью определяется попарными углами между этими корнями или — что то же самое — двугранными углами между стенками камеры Вейля, которые однозначно характеризуются целыми числами $m_{ij} \geqslant 2$ — количествами зеркал, проходящих через пересечение i-й и j-й стенки — и равны π/m_{ij}. Набор чисел m_{ij} принято кодировать неориентированным *графом Коксетера*, вершины которого биективно соответствуют стенкам камеры (или простым корням), и между i-й и j-й вершиной проводится $m_{ij} - 2$ рёбра. Таким образом, между ортогональными стенками рёбер нет, паре стенок, образующих угол $\pi/3$, отвечают вершины, соединённые одним ребром, стенкам с углом $\pi/4$ — вершины, соединённые двумя рёбрами, и т. д.

Упражнение 20.17. Убедитесь, что система корней неразложима если и только если её граф Коксетера связен.

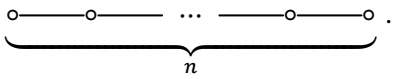
Например, диэдральная группа D_m из прим. 20.1 на стр. 365 имеет ранг 2 и граф Коксетера из двух вершин, соединённых $m-2$ рёбрами, а группы тетраэдра, октаэдра и икосаэдра из n° 20.3

[1] Эквивалентно, острый угол между i-м и j-м зеркалами равен π/m_{ij}.

на стр. 367 имеют ранг 3 и графы Коксетера

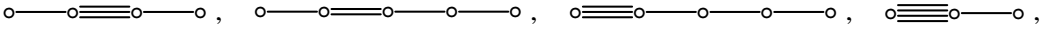


у которых число рёбер между i-й и j-й вершиной равно числу m_k из форм. (20-7) на стр. 367. Система корней A_n из прим. 20.2 на стр. 375, задающая группу правильного n-мерного симплекса, имеет граф Коксетера



Так как простые корни линейно независимы, их определитель Грама положителен. Поэтому связный граф без петель[1] имеет шанс быть графом Коксетера, только если определитель симметричной матрицы с недиагональными элементами $g_{ij} = g_{ji} = -\cos\left(\pi/m_{ij}\right)$ и $g_{ii} = 1$ положителен. При удалении из графа Коксетера любого набора вершин вместе со всеми приходящими в эти вершины рёбрами оставшийся граф тоже является графом Коксетера группы отражений, действующей в линейной оболочке U оставшихся простых корней и порождённой отражениями в пересечениях U с оставшимися зеркалами.

Упражнение 20.18. Покажите, что в графе Коксетера не может быть подграфов вида



указав в них пару векторов с не положительным определителем Грама. Убедитесь, что графов Коксетера, получающихся из нарисованных увеличением кратности имеющегося в них кратного ребра, тоже не существует.

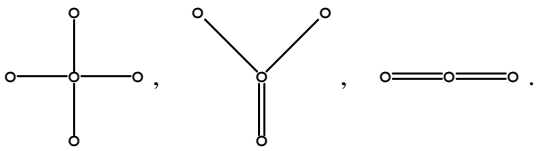
Лемма 20.4
Среди любых m вершин графа Костера рёбрами соединяется не более $m-1$ пар. В частности, в графе Коксетера нет циклов.

Доказательство. Выкинув все остальные вершины и примыкающие к ним рёбра, получаем граф Коксетера системы из m простых корней $a_1, \dots, a_m$. Поскольку $(a_i, a_j) \leqslant 0$ для всех $i \neq j$ по лем. 20.2 на стр. 377, для скалярного квадрата суммы всех этих корней[2] получаем неравенство

$$0 < \Big(\sum_{i=1}^{m} a_i, \sum_{i=1}^{m} a_i\Big) = m - 2\sum_{i<j} \cos\left(\pi/m_{ij}\right) \leqslant m-k\,,$$

где k равно числу таких пар $i<j$, что $m_{ij} \geqslant 3$. Тем самым, $k \leqslant m-1$. □

Лемма 20.5
В графе Коксетера нет подграфов вида



(20-15)

[1] Т. е. рёбер, начало которых совпадает с концом.

[2] Которая отлична от нуля поскольку простые корни линейно независимы.

Доказательство. Выкидывая остальные вершины вместе с примыкающими к ним рёбрами, получаем систему простых корней, в которой все крайние корни e_i образуют ортонормальный базис своей линейной оболочки U. Поскольку центральный корень $c \notin U$, его ортогональная проекция на U имеет длину $|c_U| < 1$. В наших трёх случаях координаты проекции

$$c_U = \sum_i (c, e_i) \cdot e_i = \begin{cases} (1/2, 1/2, 1/2, 1/2) & \text{в базисе } e_1,\ e_2,\ e_3,\ e_4 \\ (1/2, 1/2, \sqrt{3}/2) & \text{в базисе } e_1,\ e_2,\ e_3 \\ (\sqrt{3}/2, \sqrt{3}/2) & \text{в базисе } e_1,\ e_2 \end{cases}$$

и её длина $|c_U| \geqslant 1$. Противоречие. □

Лемма 20.6 (стягивание простых цепочек)
Если граф Коксетера содержит цепочку вида

(20-16)

крайние вершины которой могут быть соединены с какими-то другими вершинами графа, но во внутренние вершины больше не ведёт никаких рёбер, кроме нарисованных, то при замене всей цепочки на одну вершину, в которую входят все рёбра, ранее входившие в две крайних вершины цепочки (20-16), также получится граф Коксетера.

Доказательство. Пусть корни $a_1, \ldots, a_m$ соответствуют вершинам цепочки (20-16). Их сумма s имеет скалярный квадрат

$$(s, s) = \sum_{i=1}^{m} (a_i, a_i) + 2 \sum_{i=1}^{m-1} (a_i, a_{i+1}) = m - (m-1) = 1\,,$$

а скалярное произведение s с любым не входящим в цепочку корнем a_j равно

$$(s, a_j) = \sum_{i=1}^{m} (a_i, a_j) = (a_1, a_j) + (a_m, a_j)\,.$$

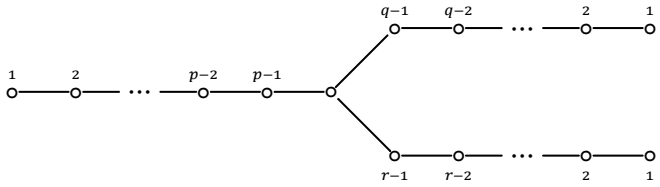
Поскольку в графе Коксетера нет петель, из двух произведений в правой части отлично от нуля может быть лишь одно. Следовательно, угол образуемый вектором s с корнем a_j либо такой же, как у a_1 с a_j, либо такой же как у a_m с a_j, т. е. имеет вид $\pi(1 - m^{-1})$ для целого $m \geqslant 2$. Следовательно, вектор s вместе со всеми остальными корнями a_j, не входящими в цепочку (20-16), образует систему простых корней с графом Коксетера, который получается из исходного графа стягиванием цепочки (20-16) в одну точку. □

Следствие 20.2 (отсутствие двух кратных объектов)
В связном графе Коксетера не может быть ни двух вершин валентности $\geqslant 3$, ни двух пар кратных рёбер[1], ни вершины валентности $\geqslant 3$ вместе с кратным ребром (не обязательно идущим в эту вершину).

Доказательство. Стягивая цепочку вида (20-16), связывающую друг с другом пару нежелательных нам объектов, мы получаем один из трёх подграфов, запрещённых по лем. 20.5. □

[1] Т. е. пар вершин, соединённых между собою более, чем одним ребром.

Лемма 20.7 (перечисление мерседесов)
Пусть граф Коксетера имеет трёхвалентную вершину, в которую ведут цепочки из $p-1$, $q-1$ и $r-1$ последовательных рёбер



(20-17)

(так что всего в рассматриваемом подграфе $p+q+r-2$ вершин). Тогда тройка чисел (p,q,r) с точностью до перестановки имеет вид $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ или $(2,2,m)$ с любым целым $m \geqslant 2$.

Доказательство. Обозначим центральный корень через e, а остальные — через a_i, b_i и c_i, занумеровав их от окраины к центру, как показано на графе (20-17). Положим

$$a \stackrel{\text{def}}{=} a_1 + 2a_2 + 3a_3 + \cdots + (p-1)\cdot a_{p-1}$$
$$b \stackrel{\text{def}}{=} b_1 + 2b_2 + 3b_3 + \cdots + (q-1)\cdot b_{p-1}$$
$$c \stackrel{\text{def}}{=} c_1 + 2c_2 + 3c_3 + \cdots + (r-1)\cdot c_{r-1}\,.$$

Векторы a, b, c образуют ортогональный базис в своей линейной оболочке U и имеют скалярные квадраты $(a,a) = p(p-1)/2$, $(b,b) = q(q-1)/2$, $(c,c) = r(r-1)/2$, поскольку

$$\Big(\sum_{k=1}^{p-1} ka_k, \sum_{k=1}^{p-1} ka_k\Big) = \sum_{k=1}^{p-1} k^2 - \sum_{k=1}^{p-2} k(k+1) = (p-1)^2 - \frac{(p-2)(p-1)}{2} = \frac{p(p-1)}{2}$$

и аналогично для векторов b и c. Так как вектор $e \notin U$, длина его ортогональной проекции

$$e_U = \frac{(e,a)}{(a,a)}\cdot a + \frac{(e,b)}{(b,b)}\cdot b + \frac{(e,c)}{(c,c)}\cdot c$$

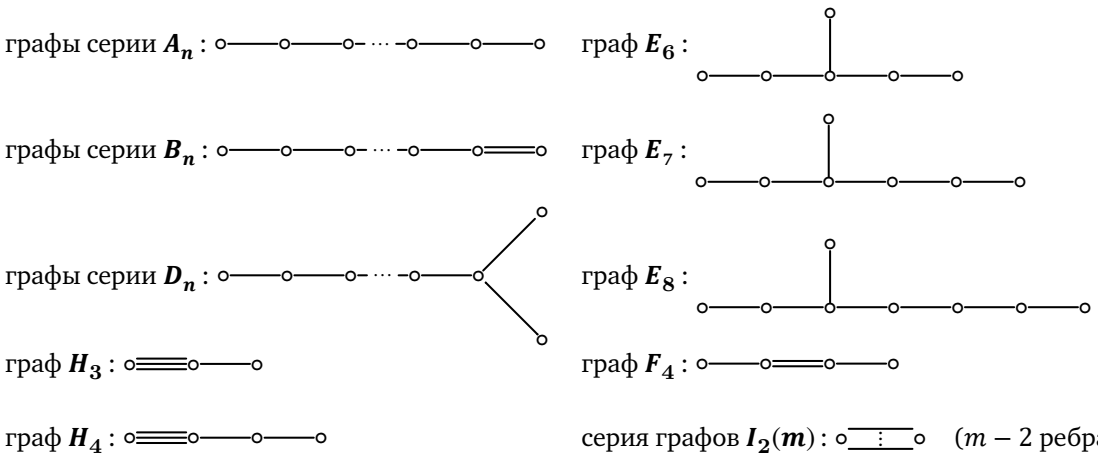
на подпространство U строго меньше единицы, откуда

$$1 > (e_U, e_U) = \frac{(e,a)^2}{(a,a)} + \frac{(e,b)^2}{(b,b)} + \frac{(e,c)^2}{(c,c)} = \frac{p-1}{2p} + \frac{q-1}{2q} + \frac{r-1}{2r} = \frac{3}{2} - \frac{1}{2p} - \frac{1}{2q} - \frac{1}{2r}\,.$$

Все решения неравенства $p^{-1} + q^{-1} + r^{-1} > 1$ в натуральных числах $p, q, r > 1$ как раз и перечислены в лем. 20.7. □

Упражнение 20.19. Удостоверьтесь в этом.

Теорема 20.2
Полный список связных графов Коксетера таков (нижний индекс равен числу вершин):



Доказательство. Из предыдущих лемм вытекает, что все связные графы Коксетера содержатся в указанном списке, так что остаётся лишь предъявить соответствующие системы корней. Серии A_n, B_n и D_n отвечают одноимённым системам корней из прим. 20.2, прим. 20.3 и прим. 20.4 на стр. 375. Граф H_3 отвечает группе икосаэдра, а графы $I_2(m)$ — диэдральным группам D_m.

Чтобы построить систему корней E_8, рассмотрим в $\mathbb{Z}^8 \subset \mathbb{R}^8$ подрешётку E, образованную всеми векторами с чётной суммой координат, и обозначим через $L \subset \mathbb{R}^8$ подрешётку, порождённую решёткой E и вектором $w = \frac{1}{2}\sum e_i$, где $e_1, \dots, e_8$ — стандартный базис в $\mathbb{R}^8$. Таким образом, L образована всевозможными линейными комбинациями $z_1 u + z_2 w$ с $u \in E$ и $z_1, z_2 \in \mathbb{Z}$.

Упражнение 20.20. Проверьте, что скалярные квадраты всех векторов $v \in L$ являются чётными целыми числами.

Система корней Φ с графом E_8 состоит из векторов $u/\sqrt{2}$, где u пробегает все векторы минимально возможной длины $|u| = \sqrt{2}$ в L. Таких векторов $240 = 112 + 128$: двучленные суммы $\pm e_i \pm e_j$ с $1 \leqslant i < j \leqslant 8$ и восьмичленные полусуммы $\frac{1}{2}\sum_{i=1}^{8} \pm e_i$ с чётным числом плюсов.

Упражнение 20.21. Убедитесь, что отражения относительно всех этих векторов переводят множество Φ в себя, выведите отсюда, что эти отражения порождают конечную группу, и проверьте, что векторы $(e_1 + e_8 - \sum_{i=2}^{7} e_i)/2\sqrt{2}$, $(e_1 + e_2)/\sqrt{2}$ и $(e_{i-1} - e_{i-2})/\sqrt{2}$ с $3 \leqslant i \leqslant 8$ образуют систему простых корней с графом E_8.

Системы корней E_6 и E_7 получаются из E_8 ограничением на линейную оболочку первых шести и семи простых корней.

Системы корней с графами F_4 и H_4 имеют полные группы двух четырёхмерных правильных многогранников в пространстве кватернионов $\mathbb{H} \simeq \mathbb{R}^4$, вершины которых находятся в кватернионах, образующих так называемые *бинарные группы* тетраэдра и икосаэдра, с которыми мы познакомимся в прим. 4.2 и прим. 4.3 на стр. 61 части II. □

Задачи для самостоятельного решения к §20

Задача 20.1. Порождается ли

а) S_n циклами $|1,2\rangle$ и $|1,2,3,\ \dots\ ,n\rangle$? б) A_n циклами $|1,2,3\rangle$, $|1,2,4\rangle$, $\dots$, $|1,2,n\rangle$?

Задача 20.2. Сколько элементов в группе

а) порождённой x_1, x_2 с соотношениями $x_1^2 = x_2^3 = (x_1x_2)^2 = e$

б) порождённой x_1, x_2, x_3 с соотношениями $x_1^3 = x_2^3 = x_3^3 = (x_1x_2)^2 = (x_2x_3)^2 = (x_3x_1)^2 = e$? Каким из известных Вам групп изоморфны эти группы?

Задача 20.3 (2-группа Гейзенберга). Обозначим через H группу, порождённую $4n+4$ образующими ± 1, $\pm u_1$, $\dots$, $\pm u_{2n+1}$ с соотношениями $u_i^2 = -1$, $u_iu_j = -u_ju_i$ и «минус на минус даёт плюс». Покажите, что

а) H состоит из 2^{2n+2} элементов $\pm u_I = \pm u_{i_1}u_{i_2}\dots u_{i_k}$, где $I = \{i_1, \dots, i_k\}$ пробегает всевозможные упорядоченные подмножества в $\{1,\ 2,\ \dots\ ,\ (n+1)\}$ и $u_\varnothing = 1$

б) элементы $\pm u_I$, отвечающие индексам I чётной длины, образуют в H подгруппу (она называется *группой Гейзенберга* H_2^n)

в) H_2^1 изоморфна группе кватернионных единиц $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

г) Опишите центр и классы сопряжённости группы H_2^n

Задача 20.4*. Постройте изоморфизмы $\mathrm{PGL}_2(\mathbb{F}_5) \xrightarrow{\sim} S_5$, рассмотрев: а) действие $\mathrm{PGL}_2(\mathbb{F}_5)$ сопряжениями на множестве нелинейных[1] инволюций без неподвижных точек на $\mathbb{P}_1(\mathbb{F}_5)$ б) вложение $\mathrm{PGL}_2(\mathbb{F}_5) \hookrightarrow S_6$ и действие $\mathrm{PGL}_2(\mathbb{F}_5)$ левыми умножениями на $S_6/\mathrm{PGL}_2(\mathbb{F}_5)$.

Задача 20.5*. Постройте внешний автоморфизм группы S_6 и докажите, что $\mathrm{Aut}\, S_6/\mathrm{Int}\, S_6 \simeq \mathbb{Z}/(2)$.

Задача 20.6*. Докажите, что $\mathrm{Aut}\, S_n = \mathrm{Int}\, S_n$ при всех[2] $n \neq 6$.

Задача 20.7. Покажите, что свободная группа F_2 на алфавите x_1, x_2 вкладывается в $\mathrm{SL}_2(\mathbb{Z})$ по правилу

$$x_1 \mapsto \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix},\ x_2 \mapsto \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix},\ \text{где целое } z \geqslant 2\,.$$

Задача 20.8. Рассмотрим подгруппу $G \subset \mathrm{SL}_2(\mathbb{C})$, порождённую матрицами $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ и $\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$, где $i^2 = \omega^2 + \omega = -1$. Найдите $|G|$, разложите группу G в полупрямое произведение собственных подгрупп и задайте её образующими и соотношениями.

Задача 20.9. Докажите, что конечная группа, порождённая двумя различными нетривиальными инволюциями, изоморфна группе диэдра.

Задача 20.10. Задайте двумя образующими и тремя соотношениями неабелеву группу порядка а) 355 б) 417 в) 689 и найдите её коммутант.

---

[1] Т. е. не лежащих в $\mathrm{PGL}_2(\mathbb{F}_5)$. На шеститочечном множестве $\mathbb{P}_1(\mathbb{F}_5)$ имеется 15 инволюций без неподвижных точек, и ровно 10 из них лежат в $\mathrm{PGL}_2(\mathbb{F}_5)$ — это полярные преобразования, задаваемые гладкими пустыми квадриками на $\mathbb{P}_1(\mathbb{F}_5)$ (т. е. корреляции анизотропных квадратичных форм на $\mathbb{F}_5^2$, рассматриваемые с точностью до пропорциональности).

[2] Подсказка: автоморфизм S_n внутренний если и только если он переводит транспозиции в транспозиции.

Задача 20.11. Докажите[1], что конечные подгруппы $G \subset \mathrm{SO}_3(\mathbb{R})$ с точностью до сопряжения исчерпываются циклическими и диэдральными группами и собственными группами тетраэдра, октаэдра и икосаэдра.

Задача 20.12 (правильные многогранники). Многогранник[2] M в n-мерном евклидовом пространстве V называется *правильным*, если его группа O_M транзитивно действует на его *флагах* — последовательностях вида

$$M = F^0 \supsetneq F^1 \supsetneq F^2 \supsetneq \ldots \supsetneq F^{n-1} \supsetneq F^n \supsetneq F^{n+1} = \varnothing\,, \tag{20-18}$$

где F^1 — гипергрань[3] в M, F_2 — гипергрань в F_1 (являющаяся гранью коразмерности 2 в M) и т. д., а при чтении справа налево F^n — вершина, F^{n-1} — примыкающее к ней ребро, F^{n-2} — примыкающая к нему двумерная грань и т. д.

а) (фундаментальный конус) С каждым флагом правильного многогранника связана последовательность $c_0, c_1, \ldots, c_n$ центров[4] составляющих этот флаг граней (в ней $c_0 = 0$ — центр всего многогранника, а $c_n = F^n$). Конус с вершиной в c_0 и направляющими векторами $c_1, \ldots, c_n$ называется *фундаментальным*. Его гиперграни высекаются гиперплоскостями

$$H_j = \operatorname{span}(c_\nu \mid \nu \neq j)\,, \quad \text{где} \quad j = 1, \ldots, n\,.$$

Убедитесь, что каждая из них содержит все грани F^k с $k > j$ и перпендикулярна всем граням F^i с $i < j$, а отражение σ_j в гиперплоскости H_j переводит M в себя.

б) Постройте биекцию между элементами группы O_M и фундаментальными конусами флагов в M, аналогичную той, что была построена в n° 20.3 на стр. 367 для многогранников в $\mathbb{R}^3$, и докажите, что группа O_M порождается отражениями $\sigma_1, \ldots, \sigma_n$ в гиперплоскостях $H_1, \ldots, H_n$, высекающих один из фундаментальных конусов.

в) (символ) Сопоставим флагу (20-18) правильного многогранника M набор чисел[5]

$$(p^1, \ldots, p^{n-1})\,,$$

в котором p^k равно количеству граней коразмерности k, содержащих заданную грань F^{k+2} и содержащихся в заданной грани F^{k-1} фиксированного флага (20-18), последнее число p^{n-1} равно числу рёбер двумерной грани многогранника M. Убедитесь, что этот набор не зависит от выбора флага, а его поднабор $(p^1, \ldots, p^{n-2})$ является символом $(n-1)$-мерного правильного многогранника[6], высекаемого из M гиперплоскостью, проходящей через все вершины многогранника M, соединённые ребром с заданной вершиной F^n. Напишите символы пяти

[1] Подсказка: покажите, что если в G есть повороты с разными осями, то G является сохраняющей ориентацию подгруппой индекса два в конечной группе, порождённой отражениями в плоскостях, проходящих через пары разных осей поворотов из G.

[2] Точные определения используемых здесь геометрических терминов (многогранник, грань и т. п.) можно посмотреть в разделе 12.4 на стр. 161 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_12.pdf.

[3] Т. е. грань коразмерности 1.

[4] *Центром* многогранника называется центр тяжести (равновесный барицентр) его вершин.

[5] Выписанный в обратном порядке набор $(p_1, \ldots, p_{n-1}) \overset{\text{def}}{=} (p^{n-1}, \ldots, p^1)$ называется *символом Шлефли* многогранника M.

[6] Он называется *звездой* многогранника M.

платоновых тел, правильных n-мерных куба[1], кокуба[2] и симплекса[3], а также (если получится) четырёхмерного октаплекса[4].

г) Покажите, что правильный многогранник восстанавливается по своему символу однозначно с точностью до подобия.

д) Покажите, что $(\sigma_i\sigma_{i+1})^{p_i} = e$ и это определяющие соотношения между образующими σ_i группы O_M.

е) Покажите, что графы Коксетера групп O_M исчерпываются линейными[5] графами $G_2(m)$, A_n, B_n, H_3, F_4, H_4 из теор. 20.2 на стр. 382, и для каждой из этих групп имеются, с точностью до подобия, один или два правильных многогранника с такой группой: символ первого имеет $p^i = m_i + 2$, где m_i-число рёбер, ведущих из i-й слева вершины графа в $(i+1)$-ю, а символ второго получается из него прочтением справа налево.

ж*) Для трёх отличных от куба, кокуба и симплекса четырёхмерных многогранников найдите количество граней каждой размерности и выясните, какие платоновы тела являются их гипергранями.

Задача 20.13* (системы Штейнера). Набор S из k-элементных подмножеств n-элементного множества X называется *системой Штейнера* $S(t,k,n)$, если каждое t-элементное подмножество в X содержится ровно в одном множестве из S. Например, множество аффинных прямых на координатной плоскости над полем $\mathbb{F}_5$ является системой $S(2,5,25)$.

а) По системе Штейнера $S(t,k,n)$ постройте систему $S(t-1,k-1,n-1)$.

б) Для всех $q = p^k$, где p — простое, постройте системы $S(2,q,q^2)$ и $S(2,q+1,q^2+q+1)$.

в) Покажите, что образы множества квадратов $\{0,1,4,9,3,5\}$ поля $\mathbb{F}_{11}$ под действием группы $\mathrm{PGL}_2(\mathbb{F}_{11})$ дробно линейных преобразований проективной прямой $\mathbb{P}_1(\mathbb{F}_{11}) = \{0,1,\dots,10,\infty\}$ составляют систему Штейнера $S(5,6,12)$.

г) Постройте систему Штейнера $S(5,8,24)$.

Задача 20.14*. Для системы Штейнера $S = S(t,k,n)$ положим $\mathrm{Aut}\, S \stackrel{\text{def}}{=} \{g \in S_n \mid \forall\, Y \in S\ g(Y) \in S\}$. Постройте изоморфизмы:

а) $\mathrm{PGL}_3(\mathbb{F}_4)$ с $\mathrm{Aut}\, S(2,5,21)$ б) A_6 с коммутантом $\mathrm{Aut}'\, S(3,4,10)$.

Задача 20.15*. Найдите порядки *спорадических простых групп Матьё*[6]:

а) $M_{11} \stackrel{\text{def}}{=} \mathrm{Aut}\, S(4,5,11)$ б) $M_{12} \stackrel{\text{def}}{=} \mathrm{Aut}\, S(5,6,12)$ в) $M_{22} \stackrel{\text{def}}{=} \mathrm{Aut}\, S(3,6,22)$

г) $M_{23} \stackrel{\text{def}}{=} \mathrm{Aut}\, S(4,7,23)$ д) $M_{24} \stackrel{\text{def}}{=} \mathrm{Aut}\, S(5,8,24)$.

Задача 20.16*. Покажите, что M_{11}, M_{22} и M_{23} суть стабилизаторы точек тавтологических действий M_{12}, M_{23} и M_{24} на соответствующих системах Штейнера.

[1] См. зад. 14.8 на стр. 269.
[2] См. зад. 14.10 на стр. 270.
[3] См. зад. 14.9 на стр. 270.
[4] См. зад. 14.11 на стр. 270.
[5] Т. е. без трёхвалентных вершин.
[6]

ответы: 7920, 95 040, 443 520, 10 200 960, 244 823 040.

Ответы и указания к некоторым упражнениям

Упр. 1.1. Ответ: 2^n.

Упр. 1.2. Ответ на второй вопрос — нет. Пусть $X = \{1, 2\}$, $Y = \{2\}$. Все их парные пересечения и объединения суть $X \cap Y = Y \cap Y = Y \cup Y = Y$ и $X \cup Y = X \cup X = X \cap X = X$, и любая формула, составленная из X, Y, $\cap$, $\cup$, даст на выходе или $X = \{1, 2\}$, или $Y = \{2\}$, тогда как $X \setminus Y = \{1\}$.

Упр. 1.3. В первом случае имеется 6 наложений и ни одного вложения, во втором — 6 вложений и ни одного наложения.

Упр. 1.5. Если X конечно, то инъективное или сюръективное отображение $X \to X$ автоматически биективно. Если X бесконечно, то в X есть подмножество, изоморфное $\mathbb{N}$. Инъекция $\mathbb{N} \hookrightarrow \mathbb{N}$, $n \mapsto (n + 1)$, и сюръекция $\mathbb{N} \twoheadrightarrow \mathbb{N}$, $n \mapsto \max(1, (n - 1))$, обе не биективны и продолжаются до точно таких же отображений $X \to X$ тождественным действием на $X \setminus \mathbb{N}$.

Упр. 1.6. Ответ: нет. Воспользуйтесь «диагональным трюком» Кантора: пусть все биекции $\mathbb{N} \to \mathbb{N}$ занумерованы натуральными числами; глядя на этот список, постройте биекцию, которая при каждом $k = 1, 2, 3, \ldots$ отображает некоторое число $n_k \in \mathbb{N}$ не туда, куда его отображает k-тая биекция из списка.

Упр. 1.7. Ответ: $\binom{n+m-1}{m-1} = \binom{n+m-1}{n} = \frac{(n+m-1)!}{n!(m-1)!}$. Указание: слагаемых столько же, сколько имеется упорядоченных наборов неотрицательных целых чисел $(k_1, \ldots, k_m)$ с суммой $\sum k_i = n$. Такой набор можно закодировать словом, составленным из $(m - 1)$ букв 0 и n букв 1: сначала пишем k_1 единиц, потом нуль, потом k_2 единиц, потом нуль, и т. д. (слово кончится k_m единицами, стоящими следом за последним, $(m - 1)$-м нулём) .

Упр. 1.8. Ответ: $\binom{n+k}{k}$. Каждая такая диаграмма представляет собою ломаную, ведущую из левого нижнего угла прямоугольника в правый верхний. В такой ломаной ровно n горизонтальных звеньев и ровно k вертикальных.

Упр. 1.9. Пусть $[x']_n = [x]_n$ и $[y']_n = [y]_n$, т. е. $x' = x + nk$, $y' = y + n\ell$ с некоторыми $k, \ell \in \mathbb{Z}$. Тогда $x' + y' = x + y + n(k + \ell)$ и $x'y' = xy + n(\ell x + ky + k\ell n)$ сравнимы по модулю n с $x + y$ и xy соответственно, т. е. $[x' + y']_n = [x + y]_n$ и $[x'y']_n = [xy]_n$.

Упр. 1.10. Положим $x \sim y$, если существует конечная последовательность точек

$$x = z_0, z_1, z_2, \ldots, z_n = y$$

как в условии задачи. Проверьте, что это отношение эквивалентности и что оно содержится в любой эквивалентности $S \subset X \times X$, содержащей R.

Упр. 1.11. Рефлексивность и симметричность очевидны. Транзитивность: если $(p, q) \sim (r, s)$ и $(r, s) \sim (u, w)$, т. е. $ps - rq = 0 = us - rw$, то $psw - rqw = 0 = usq - rwq$, откуда $s(pw - uq) = 0$, и $pw = uq$, т. е. $(p, q) \sim (u, w)$.

Упр. 1.12. Если прямые ℓ_1 и ℓ_2 пересекаются в точке O под углом $0 < \alpha \leqslant \pi / 2$, то отражение относительно ℓ_1, за которым следует отражение относительно ℓ_2, это поворот вокруг точки O на угол 2α в направлении от первой прямой ко второй. Таким образом, отражения относительно пересекающихся прямых коммутируют тогда и только тогда, когда прямые перпендикулярны.

Упр. 1.14. Таблица композиций gf в симметрической группе S_3:

$g \diagdown f$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	$(3,2,1)$	$(2,1,3)$	$(2,3,1)$	$(3,1,2)$
$(1,3,2)$	$(1,3,2)$	$(1,2,3)$	$(3,1,2)$	$(2,3,1)$	$(2,1,3)$	$(3,2,1)$
$(3,2,1)$	$(3,2,1)$	$(2,3,1)$	$(1,2,3)$	$(3,1,2)$	$(1,3,2)$	$(2,1,3)$
$(2,1,3)$	$(2,1,3)$	$(3,1,2)$	$(2,3,1)$	$(1,2,3)$	$(3,2,1)$	$(1,3,2)$
$(2,3,1)$	$(2,3,1)$	$(3,2,1)$	$(2,1,3)$	$(1,3,2)$	$(3,1,2)$	$(1,2,3)$
$(3,1,2)$	$(3,1,2)$	$(2,1,3)$	$(1,3,2)$	$(3,2,1)$	$(1,2,3)$	$(2,3,1)$

Упр. 1.15. Отношение $n \mid m$ на множестве $\mathbb{Z}$ не кососимметрично: $n \mid m$ и $m \mid n$ если и только если $m = \pm n$. Фактор множества $\mathbb{Z}$ по этому отношению эквивалентности можно отождествить с множеством $\mathbb{Z}_{\geqslant 0}$ неотрицательных целых чисел, на котором отношение $n \mid m$ является частичным порядком (обратите внимание, что нуль является нижней гранью этого множества, т. е. делит все элементы.)

Упр. 1.16. Пусть множество $S \subset W$ состоит из всех таких элементов $z \in W$, что утверждение $\Phi(z)$ ложно. Если $S \neq \varnothing$, то в нём есть начальный элемент $s_* \in S$. Поскольку утверждение $\Phi(w)$ истинно для всех $w < s_*$, утверждение $\Psi(s_*)$ тоже истинно, т. е. $s_* \notin S$. Противоречие.

Упр. 1.17. Обозначим через x_I начальный элемент дополнения $W \smallsetminus I$. Начальный интервал $[x_I) \subset W$ является объединением начальных интервалов $[y) \subset W$ по всем $y < x_I$. Так как I содержит все интервалы $[y)$ с $y < x_I$, мы заключаем, что $I \supseteq [x_I)$, откуда $I = [x_I)$.

Упр. 1.18. Пусть соотношение $U \geqslant W$ не выполняется. Покажем, что любой начальный отрезок $[u) \subset U$ изоморфен некоторому начальному отрезку $[w) \subset W$, где $w = w(u)$ однозначно восстанавливается по u. Это верно для пустого начального отрезка $\varnothing = [u_*)$, где $u_* \in U$ — минимальный элемент. Пусть это верно для всех начальных отрезков $[y) \subset U$ с $y < u$. Тогда $[u) = \bigcup_{y<u}[y)$ изоморфен объединению вложенных отрезков $\bigcup_{y<u}[w(y)) \subset W$. Если это объединение исчерпывает всё множество W, то $W \simeq [y)$, т. е. $W \leqslant U$ вопреки предположению. Положим $w(u) \in W$ равным минимальному элементу, не содержащемуся в $\bigcup_{y<u}[w(y))$. Проверьте, что $\bigcup_{y<u}[w(y)) = [w(u))$ и что отображение $u \mapsto w(u)$ устанавливает изоморфизм множества U либо со всем множеством W, либо с некоторым его начальным отрезком.

Упр. 1.19. Пусть рекурсивные подмножества $W_1, W_2 \subset P$ имеют общий начальный элемент. Рассмотрим подмножество $Z \subseteq W_1$, состоящее из всех таких $z \in W_1$, что начальный интервал $[z)_1$ в множестве W_1 совпадает с начальным интервалом $[z)_2$ в множестве W_2. Множество Z не пусто, поскольку содержит общий начальный элемент множеств W_1 и W_2. В силу рекурсивности W_1 и W_2 множество Z содержится в $W_1 \cap W_2$, являясь, по упр. 1.17 на стр. 19, начальным интервалом как в W_1, так и в W_2. Если $Z \neq W_1$ и $Z \neq W_2$, то точные верхние грани Z в W_1 и W_2, с одной стороны, не лежат в Z и поэтому различны, а с другой стороны обе равны $\varrho(Z)$ в силу рекурсивности W_1 и W_2. Тем самым, $Z = W_1$ или $Z = W_2$.

Упр. 1.20. Каждое подмножество $S \subset U$ имеет непустое пересечение с каким-нибудь рекурсивным вполне упорядоченным подмножеством $W \subset P$ с начальным элементом $\varrho(\varnothing)$. По упр. 1.19 подмножество W является начальным интервалом всех содержащих W рекурсивных вполне упорядоченных подмножеств с начальным элементом $\varrho(\varnothing)$. Поэтому начальный элемент пересечения $S \cap W$ не зависит от выбора такого W, что $W \cap S \neq \varnothing$, и является начальным элементом подмножества S. Каждый начальный интервал $[u) \subset U$ является начальным интервалом любого содержащего u множества W из цепи. В силу рекурсивности W элемент $\varrho[u) = u$.

Упр. 1.21. Пользуясь аксиомой выбора, зафиксируем для каждого $W \in \mathcal{W}(P)$ какую-нибудь верхнюю грань $b(W) \in P$. Если $f(x) > x$ для всех $x \in P$, то отображение $\beta : \mathcal{W}(P) \to P, W \mapsto f(b(W))$ противоречит лем. 1.2 на стр. 19.

Упр. 1.22. Обозначим через $\mathcal{S}(X)$ множество всех непустых подмножеств данного множества X, включая само X. При помощи аксиомы выбора постройте такое отображение $\mu : \mathcal{S}(X) \to X$, что $\mu(Z) \in Z$ для всех $Z \in \mathcal{S}(X)$. Обозначим через $\mathcal{W}(X)$ множество всех $W \in \mathcal{S}(X)$, которые можно вполне упорядочить так, что $\mu(X \smallsetminus [w)) = w$ для всех $w \in W$. Вдохновляясь лем. 1.2 на стр. 19 покажите, что $\mathcal{W}(X) \neq \varnothing$, и убедитесь, что $X \in \mathcal{W}(X)$.

Упр. 1.23. Убедитесь, что множество всех цепей, содержащих данную цепь, является полным чумом относительно отношения включения, и примените лемму Цорна.

Упр. 2.2. Ответы: $1 + x$ и $xy + x + y$.

Упр. 2.3. Если умножить числитель и знаменатель любой дроби в левой части равенств (2-11) на c, числитель и знаменатель правой части также умножится на c. Отсюда следует корректность. Проверка аксиом бесхитростна.

Упр. 2.5. Пусть $ax_0 + by_0 = k$. Тогда $a(x_0 + n\beta) + b(y_0 - n\alpha) = ax_0 + by_0 + n(a\beta - b\alpha) = k$ при всех $n \in \mathbb{Z}$. Если $ax + by = k$, то $a(x - x_0) = -b(y - y_0)$ делится на нок$(ab) = \alpha\beta d$. Тем самым, число $n = (x - x_0)/\beta = -(y - y_0)/\alpha \in \mathbb{Z}$, и $x = x_0 + n\beta$, а $y = y_0 - n\alpha$.

Упр. 2.6. Пусть числа таблицы $\begin{pmatrix} m & x & y \\ n & s & t \end{pmatrix}$ удовлетворяют равенствам $m = xa + by$, $n = as + bt$ и $xt - ys = 1$. Прибавляя к 1-й строке 2-ю, умноженную на k, получаем таблицу $\begin{pmatrix} m' & x' & y' \\ n & s & t \end{pmatrix}$, в которой $m' = m + nk$, $x' = x + ks$, $y' = t + kt$. Тогда

$$m' = ax + by + k(as + bt) = ax' + by'$$
$$x't - y's = xt - ys + kst - kst = 1\,.$$

Упр. 2.7. Подставьте в это равенство $x = y = 0$.

Упр. 2.8. Существование разложения. Если число n простое, то оно само и будет своим разложением. Если n составное, представим его в виде произведения строго меньших по абсолютной величине чисел, каждое из которых в свою очередь или просто или является произведением строго меньших по абсолютной величине чисел и т. д. Поскольку модуль целого числа нельзя бесконечно долго уменьшать, мы в конце концов получим требуемое разложение.

Единственность разложения. Для любого простого числа p и любого целого z имеется альтернатива: либо нод$(z, p) = |p|$, и тогда z делится на p, либо нод$(z, p) = 1$, и тогда z взаимно прост с p. Пусть в равенстве $p_1 \ldots p_k = q_1 \ldots q_m$ все сомножители просты. Так как $\prod q_i$ делится на p_1, число p_1 не может быть взаимно просто с каждым q_i в силу лем. 2.3 на стр. 29. Согласно упомянутой альтернативе, хотя бы один из множителей q_i (будем считать, что q_1) делится на p_1. Поскольку q_1 прост, $q_1 = \pm p_1$. Сокращаем первые множители и повторяем рассуждение.

Упр. 2.9. При любом $k \in \mathbb{N}$ умножение на класс $[x]^{-1}[y]$ переводит класс $[a^k x]$ в класс $[a^k y]$, а умножение на класс $[x][y]^{-1}$ переводит класс $[a^k y]$ назад в $[a^k x]$.

Упр. 2.11. Класс $\binom{mp^n}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему после раскрытия скобок и приведения подобных слагаемых в биноме $(1 + x)^{mp^n}$ над полем $\mathbb{F}_p$. Последовательно

применяя формулу форм. (2-24) на стр. 31, получаем

$$(1+x)^{p^n m} = \bigl((1+x)^p\bigr)^{p^{n-1}m} = \bigl(1+x^p\bigr)^{p^{n-1}m} = \bigl((1+x^p)^p\bigr)^{p^{n-2}m} = \bigl(1+x^{p^2}\bigr)^{p^{n-2}m} = \cdots$$
$$\cdots = \bigl(1+x^{p^n}\bigr)^m = 1 + mx^{p^n} + \text{ старшие степени}$$

Упр. 2.13. Если число $\alpha \in \Bbbk$ является корнем многочлена $f(x)$, то $f(x)$ делится на $(x-\alpha)$ (разделите $f(x)$ на $(x-\alpha)$ с остатком и подставьте $x=\alpha$).

Упр. 2.14. По малой теореме Ферма[1] каждый элемент $x \in \operatorname{im}\psi$ удовлетворяет уравнению $x^2 = 1$.

Упр. 2.16. Ненулевой гомоморфизм полей инъективен, переводит единицу в единицу и перестановочен со сложением, вычитанием, умножением и делением[2]. Простое подполе состоит из элементов вида $\pm(1+\cdots+1)/(1+\cdots+1)$, каждый из которых остаётся на месте. Если имеется ненулевой гомоморфизм $\Bbbk \to \mathbb{F}$, то равенство или неравенство нулю суммы некоторого количества единиц в поле $\Bbbk$ влечёт точно такое же равенство или неравенство в поле $\mathbb{F}$, откуда $\operatorname{char}\Bbbk = \operatorname{char}\mathbb{F}$.

Упр. 2.17. Воспользуйтесь тем, что $\mathbb{R}$ является множеством дедекиндовых сечений линейно упорядоченного множества $\mathbb{Q}$.

Упр. 3.3. Ответ: $(y^n - x^n)/(y-x) = y^{n-1} + y^{n-2}x + y^{n-3}x^2 + \ldots + yx^{n-2} + x^{n-1}$.

Упр. 3.5. $\bigl(a_0 + a_1x + a_2x^2 + \ldots\bigr)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots = a_0 + a_1x^p + a_2x^{2p} + \ldots$ (первое равенство справедливо, поскольку возведение в p-тую степень перестановочно со сложением, второе — по малой теореме Ферма).

Упр. 3.6. Если $f(x) = \sum a_k x^k$, то $f(x+t) = \sum\limits_{k,\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu}t^\nu = \sum\limits_\nu t^\nu \cdot f_\nu(x)$, где

$$f_\nu(x) = \sum_{k\geqslant\nu} a_k \binom{k}{\nu} \cdot x^{k-\nu} = \frac{1}{\nu!}\frac{d^k}{dx^k}\sum_{k\geqslant 0} a_k x^k\,.$$

Упр. 3.7. Годятся дословно те же аргументы, что и в упр. 2.8.

Существование. Если f неприводим, то сам он и является своим разложением. Если f приводим, то он раскладывается в произведение многочленов строго меньшей степени, которые в свою очередь или неприводимы или являются произведениями многочленов строго меньшей степени и т. д. Поскольку степень не может бесконечно уменьшаться, в конце концов получится требуемое разложение.

Единственность. Для приведённого неприводимого $p \in \Bbbk[x]$ и любого $g \in \Bbbk[x]$ имеется следующая альтернатива: либо $\text{нод}(p,g) = p$, и тогда g делится на p, либо $\text{нод}(p,g) = 1$, и тогда g взаимно прост с p. Пусть все сомножители в равенстве $p_1 \ldots p_k = q_1 \ldots q_m$ неприводимы. Деля p_1 на старший коэффициент, мы можем считать, что он приведён. Поскольку $\prod q_i$ делится на p_1, многочлен p_1, не может быть взаимно прост с каждым q_i в силу лем. 2.3. Согласно упомянутой выше альтернативе найдётся q_i, делящийся на p_1. После надлежащей перенумерации можно считать, что это q_1. Так как q_1 неприводим, $q_1 = \lambda p_1$, где λ — ненулевая константа. Сокращаем первый множитель и повторяем рассуждение.

[1] См. сл. 2.1 на стр. 32.

[2] См. n° 2.5.4 на стр. 34.

Упр. 3.8. При умножении любой из строк таблицы $\begin{pmatrix} p & r & s \\ q & u & w \end{pmatrix}$ на ненулевую константу равенства $p = rf + sg$, $q = uf + wg$ сохраняются, а многочлен $rw - us$ умножается на эту константу. Если заменить любую строку таблицы на её сумму с другой строкой, умноженной на любой многочлен, равенства $p = rf + sg$, $q = uf + wg$ сохранятся, а многочлен $rw - us$ вообще не поменяется (ср. с упр. 2.6 на стр. 28). Пусть в итоговой таблице

$$\begin{pmatrix} d' & h_1 & h_2 \\ 0 & m_1 & m_2 \end{pmatrix}$$

$h_1m_2 - h_2m_1 = \delta \in \Bbbk^\times$. Умножая это равенство на f и на g и пользуясь тем, что $d' = fh_1 + gh_2$, а $fm_1 = -gm_2$, получаем

$$\delta f = fh_1m_2 - fh_2m_1 = fh_1m_2 + gh_2m_2 = d'm_2$$
$$\delta g = gh_1m_2 - gh_2m_1 = -fh_1m_1 - gh_2m_1 = -d'm_1\,.$$

Поэтому $f = d'm_2\delta^{-1}$ и $g = -d'm_1\delta^{-1}$ делятся на d'. Для любого $q = fs = gt$ из равенства

$$\delta q = qh_1m_2 - qh_2m_1 = gth_1m_2 - fsh_2m_1 = -c'(th_1 + sh_2)\,,$$

где $c' = fm_1 = -gm_2$, заключаем, что $q = -c'(th_1 + sh_2)\delta^{-1}$ делится на c'.

Упр. 3.9. Если многочлен степени $\leqslant 3$ приводим, то у него есть делитель первой степени, корень которого будет корнем исходного многочлена.

Упр. 3.11. См. упр. 1.9 на стр. 13.

Упр. 3.12. Вложение $\varphi\colon \Bbbk \hookrightarrow \Bbbk[x]/(x-\alpha)$ в качестве констант сюръективно, поскольку число $\alpha \in \Bbbk$ переходит в класс$[x]$, и значит, для любого $g \in \Bbbk[x]$ число $g(\alpha)$ переходит в класс $[g]$.

Упр. 3.13. Обратным элементом к произвольному ненулевому $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ является $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$. Кольцо в (а) содержит делители нуля: $[t+1]\cdot[t^2-t+1] = [0]$ и, тем самым, не является полем. Кольцо в (б) является полем: многочлен $p = \vartheta^3 + 2$ не имеет корней в $\mathbb{Q}$, и значит, не делится в $\mathbb{Q}[x]$ ни на какой многочлен первой или второй степени; следовательно, p взаимно прост со всеми $g \in \mathbb{Q}[x]$, не делящимися на p, т. е. для любого $[g] \neq [0]$ существуют $h_1, h_2 \in \mathbb{Q}[x]$, такие что $h_1g + h_2p = 1$; тем самым, $[h_1] = [g]^{-1}$.

Упр. 3.14. Ответ: $(1+\vartheta)^{-1} = -\vartheta$.

Упр. 3.16. Число $\zeta = \cos(2\pi/5) + i\cdot\sin(2\pi/5)$ является корнем многочлена

$$z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)\,.$$

Уравнение $z^4 + z^3 + z^2 + z + 1 = 0$ можно решить в радикалах, деля обе части на z^2 и вводя новую переменную $t = z + z^{-1}$.

Упр. 3.17. Пусть $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$ — первообразный корень с наименьшим положительным аргументом, и $\xi = \zeta^k$. Так как равенство $\zeta^m = \xi^x$ означает, что $m = kx + ny$ для некоторого $y \in \mathbb{Z}$, среди целых степеней корня ξ встречаются те и только те степени первообразного корня ζ, которые делятся на нод(k,n).

Упр. 3.18. См. листок $2\frac{1}{2}$.

Упр. 3.21. Проще всего воспользоваться известным из курса линейной алгебры и геометрии понятием *векторного пространства*[1]. Конечное поле $\mathbb{F}$ характеристики p является векторным пространством над своим простым подполем[2] $\mathbb{F}_p \subset \mathbb{F}$, и в нём имеются такие векторы $v_1, \ldots, v_m$, что любой вектор $w \in \mathbb{F}$ линейно выражается через них в виде $w = x_1 v_1 + \ldots + x_m v_m$, где все $x_i \in \mathbb{F}_p$. Удаляя из набора $v_1, \ldots, v_m$ все векторы, которые линейно выражаются через оставшиеся, мы получим такой набор векторов $\{e_1, \ldots, e_n\} \subset \{v_1, \ldots, v_m\}$, через который каждый вектор $w \in \mathbb{F}$ выражается единственным способом, поскольку равенство $x_1 e_1 + \ldots + x_n e_n = y_1 e_1 + \ldots + y_n e_n$, в котором $x_i \neq y_i$ для какого-нибудь i, позволяет выразить e_i через остальные векторы как $e_i = \sum_{\nu \neq i} e_\nu (y_\nu - x_\nu)/(x_i - y_i)$, что уже невозможно. Так как каждый элемент поля $\mathbb{F}$ однозначно записывается в виде $x_1 e_1 + \ldots + x_n e_n$, где каждый коэффициент x_i независимо принимает p значений, мы заключаем, что $|\mathbb{F}| = p^n$.

Не опирающееся на курс геометрии решение этой задачи вытекает из теор. 3.4 на стр. 57.

Упр. 3.22. См. доказательство теоремы Эйлера из прим. 2.6 на стр. 31.

Упр. 3.23. $b^m = a^{mk} = 1$ если и только если $n \mid mk$. При нод$(n,k) = 1$ такое возможно только когда $m \mid n$, а значит, $\operatorname{ord} b \geqslant n$ и b — образующая. Если же $n = n_1 d$ и $k = k_1 d$, где $d > 1$, то $b^{n_1} = a^{kn_1} = a^{nk_1} = e$ и $\operatorname{ord} b \leqslant n_1 < n$.

Упр. 3.24. Отображение $\mathrm{ev}_\zeta \colon \mathbb{F}_p[x] \to \mathbb{F}$, $f \mapsto f(\zeta)$, является гомоморфизмом колец. Поскольку поле $\mathbb{F}$ конечно, а кольцо многочленов $\mathbb{F}_p[x]$ бесконечно, у этого гомоморфизма ненулевое ядро. Многочлен g — это приведённый многочлен минимальной степени в $\ker \mathrm{ev}_\zeta$. Если $g(x) = h_1(x)\, h_2(x)$, то $h_1(\zeta) = 0$ или $h_2(\zeta) = 0$, что по выбору g невозможно при $\deg h_1, \deg h_2 < \deg g$. Пусть $f(\zeta) = 0$ для $f = gh + r$, где $\deg r < \deg g$ или $r = 0$. Подставляя $x = \zeta$, получаем $r(\zeta) = 0$, откуда $r = 0$.

Упр. 4.1. Воспользуйтесь лем. 4.1.

Упр. 4.2. По теор. 4.1 на стр. 63 эпиморфизм $\pi \colon K = \mathbb{Z}/(30) \twoheadrightarrow \mathbb{Z}/(15)$, $[n]_{30} \mapsto [n]_{15}$, раскладывается в композицию гомоморфизма $\iota_S \colon K \to KS^{-1}$ и гомоморфизма

$$\pi_S \colon KS^{-1} \twoheadrightarrow \mathbb{Z}/(15), \quad [m]_{30}/[2^k]_{30} \mapsto [m]_{15}[2^k]_{15}^{-1},$$

сюръективного в силу сюръективности π. Если $[m]_{30}/[2^k]_{30} \in \ker \pi_S$, то $[m]_{15} = 0$, а значит, $[m]_{30}/[2^k]_{30} = [2m]_{30}/[2^{k+1}]_{30} = 0$ в KS^{-1}. Тем самым, $\ker \pi_S = 0$ и π_S инъективен.

Упр. 4.4. По правилу дифференцирования композиции $\left(f^m\right)' = m f^{m-1} f'$, откуда

$$\frac{d}{dx}(1-x)^{-m} = \frac{d}{dx}\left(\frac{1}{1-x}\right)^m = m(1-x)^{-(m+1)}.$$

Нужная формула получается отсюда по индукции.

Упр. 4.5. Первое равенство вытекает и правила дифференцирования сложной функции[3], второе доказывается дифференцированием обеих частей.

Упр. 4.9. Ответы: $a_1 = \frac{1}{2}$, $a_2 = \frac{1}{6}$, $a_3 = 0$, $a_4 = -\frac{1}{30}$, $a_5 = 0$, $a_6 = \frac{1}{42}$, $a_7 = 0$, $a_8 = -\frac{1}{30}$, $a_9 = 0$,

[1] Если Вы не знакомы с этим понятием, см. n° 7.1 на стр. 114 ниже.

[2] См. n° 2.5.6 на стр. 35.

[3] См. формулу (3-8) на стр. 43.

$a_{10} = \frac{5}{66}$, $a_{11} = 0$, $a_{12} = -\frac{691}{2730}$,

$$S_4(n) = n(n+1)(2n+1)(3n^2+3n-1)/30$$
$$S_5(n) = n^2(n+1)^2(2n+1)(2n^2+2n-1)/12$$
$$S_{10}(1000) = 91\,409\,924\,241\,424\,243\,424\,241\,924\,242\,500\,.$$

Упр. 4.10. Подставьте $t = 1$ в $(m+1)\,S_m(t) = (a^{\downarrow}+t)^{m+1} - a_{m+1}$.

Упр. 4.13. Если звено Z соединяет точки $(0, m)$ и $(1, 0)$, то его вектор нормали $(m, 1)$, откуда $\varepsilon = m \in \mathbb{N}$. Младшая форма $f_m(t, x) = \alpha t^m + \beta x$ имеет $\alpha\beta \neq 0$, откуда $c = -\alpha/\beta$. Заменяя x на $t^m(x - \alpha/\beta)$ заключаем, что $f_m(t, t^m(x-\alpha/\beta))/t^m = \beta x$, т. е. возникающий на следующем шагу многочлен содержит ненулевой моном βx. Это означает, что его ломаная Ньютона проходит через точку $(1, 0)$.

Упр. 4.14. Подставляя в многочлен $(-t^3 + t^4) - 2t^2\,x - t\,x^2 + 2t\,x^4 + x^5$ ряд $x(t) = \sum_{k\geqslant 1} a_k t^{\frac{k}{2}}$, где $a_1 = -1, a_2 = 1$, и приравнивая к нулю коэффициент при $t^{\frac{n}{2}}$ получаем при $n \neq 6, 8$ соотношение

$$-2a_{m-4} - \sum_{i_1+i_2=m-2} a_{i_1}a_{i_2} + 2\sum_{i_1+\ldots+i_4=m-2} a_{i_1}\ldots a_{i_4} + \sum_{i_1+\ldots+i_5=m} a_{i_1}\ldots a_{i_5} = 0$$

(при $m = 6$ и $m = 8$ к левой части надо добавить -1 и $+1$ соответственно). Из этих соотношений линейно входящий во второе слагаемое и не присутствующий в остальных слагаемых коэффициент a_{m-3} полиномиально выражается через предыдущие коэффициенты по формуле

$$2a_{m-3} = -2a_{m-4} - \sum_{i=2}^{m-4} a_i a_{m-2-i} + 2\sum_{i_1+\ldots+i_4=m-2} a_{i_1}\ldots a_{i_4} + \sum_{i_1+\ldots+i_5=m} a_{i_1}\ldots a_{i_5}\,.$$

Упр. 4.15. Заменяя в форм. (4-33) на стр. 79 переменные t и x соответственно на t^2 и $t(x-1)$ и деля результат на t^2, получаем

$$\begin{gathered}F_3(t,x) = f_2(1,x) + t^2 f_4(1,x) + t^3 f_5(1,x) + t^4 f_6(1,x) + t^5 f_7(1,x) + t^6 f_8(1,x) + t^7 f_9(1,x) = \\ = -x^2 - 2x + t^2 - 3t^3(x-1) + 2t^4(x-1)^2 + 2t^5(x-1)^3 - 3t^6(x-1)^4 + t^7(x-1)^5 = \\ = (t^2 + 3t^3 + 2t^4 - 2t^5 - 3t^6 - t^7) + (2 - 3t^3 - 4t^4 + 6t^5 + 12t^6 + 5t^7)\,x + \\ +(-1 + 2t^4 - 6t^5 - 18t^6 - 10t^7)\,x^2 + (2t^5 + 12t^6 + 10t^7)\,x^3 + (-3t^6 - 5t^7)\,x^4 + t^7 x^5.\end{gathered}$$

Упр. 5.1. Импликации (а)⇒(б)⇒(в) очевидны. Если I содержит обратимый элемент, то среди его кратных есть единица, кратные которой исчерпывают всё кольцо.

Упр. 5.2. Первое утверждение очевидно, второе вытекает из того, что все суммы вида $b_1a_1 + \ldots + b_ma_m$, где $a_1, \ldots, a_m \in M$, $b_1, \ldots, b_m \in K$, лежат во всех идеалах,, содержащих множество M.

Упр. 5.3. Если a и b являются старшими коэффициентами многочленов $f(x)$ и $g(x)$ из идеала I, причём $\deg f = m$ и $\deg g = n$, где $m \geqslant n$, то $a + b$ либо нуль, т. е. является старшим коэффициентом нулевого многочлена, либо является старшим коэффициентом многочлена $f(x) + x^{m-n}\cdot g(x) \in I$ степени m. Аналогично, для любого $\alpha \in K$ произведение αa является старшим коэффициентом многочлена $\alpha f(x) \in I$ степени m.

Упр. 5.4. Повторите доказательство теор. 5.1, следя за младшими коэффициентами вместо старших.

Упр. 5.6. Обозначим через I_0 идеал, образованный всеми аналитическими функциями[1], обращающимися в нуль на множестве $\mathbb{Z} \subset \mathbb{C}$, а через I_k — идеал всех функций, обращающихся в нуль на множестве $\mathbb{Z} \smallsetminus \{1,\ 2,\ \ldots\ ,\ k\}$. Убедитесь, что $\sin(2\pi z)/\prod\limits_{\alpha=1}^{k}(z-\alpha) \in I_k \smallsetminus I_{k-1}$, откуда $I_k \subsetneq I_{k+1}$.

Упр. 5.7. Из того, что I является абелевой подгруппой в K немедленно вытекает, что отношение $a_1 \equiv a_2 \pmod I$ рефлексивно, транзитивно и симметрично. Корректность операций проверяется так же, как в упр. 1.9: если $[a']_I = [a]_I$ и $[b']_I = [b]_I$, т. е. $a' = a + x$, $b' = b + y$ с некоторыми $x, y \in I$, то $a' + b' = a + b + (x + y)$ и $a'b' = ab + (ay + bx + xy)$ сравнимы по модулю I с $a + b$ и ab соответственно, поскольку суммы в скобках лежат в I (именно в этот момент мы пользуемся тем, что идеал вместе с каждым элементом содержит и все его кратные); таким образом, $[a' + b']I = [a + b]_I$ и $[a'b']_I = [ab]_I$.

Упр. 5.8. Возьмите в качестве J^* объединение всех идеалов из M.

Упр. 5.9. В (а) всякий идеал в $\mathbb{C}[x]$ является главным. Если факторкольцо $\mathbb{C}[x]/(f)$ не имеет делителей нуля, то многочлен f неприводим. Над полем $\mathbb{C}$ неприводимые многочлены исчерпываются линейными, поэтому $f(x) = x - p$ для некоторого $p \in \mathbb{C}$ и $(f) = (x - p) = \ker \mathrm{ev}_p$. В (б) с помощью леммы о конечном покрытии докажите, что для любого идеала I в кольце непрерывных функций $[0, 1] \to \mathbb{R}$ найдётся точка $p \in [0, 1]$, в которой все функции из I обращаются в нуль, что даст включение $I \subset \ker \mathrm{ev}_p$. В (в) подойдёт главный идеал $\mathfrak{m} = (x^2 + 1)$.

Упр. 5.11. Если в каждом идеале I_k есть элемент $x_k \in I_k \smallsetminus \mathfrak{p}$, то произведение этих элементов $x_1 \ldots x_m \in \bigcap I_k \subset \mathfrak{p}$, что противоречит простоте $\mathfrak{p}$.

Упр. 5.12. Рассмотрим эпиморфизм факторизации $\pi\colon K \twoheadrightarrow K/I$. Полный прообраз $\pi^{-1}(J)$ любого идеала $J \subset K/I$ является идеалом в K. Классы элементов, порождающих этот идеал в K порождают идеал J в K/I.

Упр. 5.13. В (в) и (г) для любого $z \in \mathbb{C}$ в рассматриваемом кольце существует такой элемент w, что $|z - w| < 1$. Взяв такой w для $z = a/b$, заключаем, что $|a - bw| < |b|$.

Упр. 5.14. Если $\exists\ b^{-1}$, то $\nu(ab) \leqslant \nu(abb^{-1}) = \nu(a)$. Наоборот, если $\nu(ab) = \nu(a)$, то деля a на ab с остатком, получаем $a = abq + r$, где либо $\nu(r) < \nu(ab) = \nu(a)$, либо $r = 0$. Из равенства $r = a(1 - bq)$ вытекает, что либо $\nu(r) \geqslant \nu(a)$, либо $1 - bq = 0$. С учётом предыдущего, такое возможно только при $1 - bq = 0$ или $r = 0$. Во втором случае $a(1 - bq) = 0$, что тоже влечёт $1 - bq = 0$. Следовательно $bq = 1$ и b обратим.

Упр. 5.15. Если $b = ax$ и $a = by = axy$, то $a(1 - xy) = 0$, откуда $xy = 1$.

Упр. 5.16. Многочлены x и y не имеют в $\mathbb{Q}[x, y]$ никаких общих делителей, кроме констант. Общими делителями элементов 2 и x в $\mathbb{Z}[x]$ являются только ± 1.

Упр. 5.17. По аналогии с комплексными числами, назовём *сопряжённым* к числу $\vartheta = a + b\sqrt{5}$ число $\overline{\vartheta} = a - b\sqrt{5}$, а целое число $||\vartheta|| \stackrel{\text{def}}{=} \vartheta \cdot \overline{\vartheta} = a^2 - 5b^2$ назовём *нормой* числа ϑ. Легко видеть, что $\overline{\vartheta_1\vartheta_2} = \overline{\vartheta}_1 \cdot \overline{\vartheta}_2$, откуда $||\vartheta_1\vartheta_2|| = \vartheta_1\vartheta_2\overline{\vartheta}_1\overline{\vartheta}_2 = ||\vartheta_1|| \cdot ||\vartheta_2||$. Поэтому $\vartheta \in \mathbb{Z}[\sqrt{5}]$ обратим тогда и только тогда, когда $||\vartheta|| = \pm 1$, и в этом случае $\vartheta^{-1} = \pm\overline{\vartheta}$. Поскольку $||2|| = 4$, а $||1 \pm \sqrt{5}|| = -4$, разложение этих элементов в произведение xy с необратимыми x и y возможно только при $||x|| = ||y|| = \pm 2$. Но элементов нормы ± 2 в $\mathbb{Z}[\sqrt{5}]$ нет, так как равенство $a^2 - 5b^2 = \pm 2$ при редукции по модулю 5 превращается в равенство $a^2 = \pm 2$ в поле $\mathbb{F}_5$, где числа ± 2 не являются квадратами.

[1] Функция $\mathbb{C} \to \mathbb{C}$ называется *аналитической*, если она задаётся сходящимся всюду в $\mathbb{C}$ степенным рядом из $\mathbb{C}[\![z]\!]$.

Упр. 5.18. Из равенства $z_1 z_2 = 1$ вытекает равенство $|z_1| \cdot |z_2| = 1$. Так как $|z|^2 \in \mathbb{N}$ для всех $z \in \mathbb{Z}[i]$, гауссово число z может быть обратимо только если $|z| = 1$.

Упр. 5.19. Пусть $n = p_1^{\alpha_1} \dots p_s^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}$, где $p_i, q_j \in \mathbb{N}$ — попарно разные простые числа, причём p_i представляются в виде суммы двух квадратов, а q_j — нет, т. е. все $q_j \equiv 3 \pmod 4$, а все p_i — нет. Тогда разложение n на простые множители в области $\mathbb{Z}[i]$ имеет вид $n = \prod_i (x_i + iy_i)^{\alpha_i} (x_i - iy_i)^{\alpha_i} \prod_j q_j^{\beta_j}$. Если все β_j чётные, то $n = (a+ib)(a-ib) = a^2 + b_2$ для $a + ib = \prod_i (x_i + iy_i)^{\alpha_i} \prod_j q_j^{\beta_j/2} \in \mathbb{Z}[i]$. Наоборот, если $n = a^2 + b_2 = (a+ib)(a-ib)$ для некоторого $a + ib \in \mathbb{Z}[i]$, который раскладывается на простые множители как $a + bi = \prod_k \ell_k^{\gamma_k}$, то разложение n на простые множители в $\mathbb{Z}[i]$ имеет вид $\prod_k \ell_k^{\gamma_k} \overline{\ell}_k^{\gamma_k}$, и тем самым все вещественные простые множители входят в него в чётных степенях.

Упр. 5.22. Это следует из равенства $a_0 q^n + a_1 q^{n-1} p + \dots + a_{n-1} q p^{n-1} + a_n p^n = 0$

Упр. 5.23. Ответ: $(x^2 - 2x + 2)(x^2 + 2x + 2)$.

Упр. 6.1. Пусть $0\,v = w$. Тогда $w + v = 0v + 1\,v = (0+1)\,v = 1\,v = v$. Прибавляя к обеим частям этого равенства $-v$, получаем $w = 0$. Из равенства $0\,v = 0$ вытекает, что $x\,0 = x(0\,v) = (x\,0)\,v = 0\,v = 0$. Наконец, равенство $(-1)\,v + v = (-1)\,v + 1\,v = ((-1)+1)\,v = 0\,v = 0$ означает, что $(-1)\,v = -v$.

Упр. 6.2. Ядро и образ любого гомоморфизма абелевых групп являются абелевыми подгруппами согласно n° 2.5 на стр. 32. Если гомоморфизм K-линеен, то обе эти подгруппы выдерживают умножение на элементы из K, поскольку $x\varphi(u) = \varphi(xu)$ и $\varphi(u) = 0 \Rightarrow \varphi(xu) = x\varphi(u) = 0$.

Упр. 6.4. Прямая проверка: если φ и ψ K-линейны, то $\varphi\psi(xu+yw) = \varphi(x\psi(u)+y\psi(w)) = x\varphi\psi(u)+y\varphi\psi(w)$ для любых скаляров x, y и векторов u, w.

Упр. 6.5. Сложите равенства $\varphi(\lambda u + \mu w) = \lambda\varphi(u) + \mu\varphi(w)$ и $\psi(\lambda u + \mu w) = \lambda\psi(u) + \mu\psi(w)$, а также умножьте первое из них на x.

Упр. 6.6. $[z_1]_m = [z_2]_m$ если и только если $z_1 = z_2 + km$, и в этом случае $\varphi(z_1) = z_1 w = z_2 x + kmx = z_2 x \varphi(z_2)$.

Упр. 6.7. Пусть $m = d\mu$, $n = d\nu$, где $d = \text{нод}(m,n)$ и $\text{нод}(\mu,\nu) = 1$. Тогда $mx \vdots n$ если и только если $x \vdots \nu$. Различные целые кратные вычета $[\nu]_n$ суть $[0]_n, [\nu]_n, [2\nu]_n, \dots, [(d-1)\nu]_n$, и они образуют в $\mathbb{Z}/(n)$ подмодуль, изоморфный $\mathbb{Z}/(d)$.

Упр. 6.8. Сопоставьте семейству гомоморфизмов $\varphi_\mu : N \to M_\mu$ отображение $\bigoplus_{\mu\in\mathcal{M}} \varphi_\mu : N \to \bigoplus_{\mu\in\mathcal{M}} M_\mu$, переводящее вектор $u \in N$ в семейство векторов $\big(\varphi_\mu(u)\big)_{\mu\in\mathcal{M}}$.

Упр. 6.9. Пусть $A \not\subseteq B$ — две подгруппы в абелевой группе. Выберем $a \in A \smallsetminus B$. Если $A \cup B$ является подгруппой, то $\forall\, b \in B\ a + b \in A \cup B$, но $a + b \notin B$, поскольку $a \notin B$. Следовательно, $a + b \in A$, откуда $b \in A$, т. е. $B \subseteq A$.

Упр. 6.10. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с упр. 5.7 на стр. 88).

Упр. 6.12. Так как каждый вектор $w \in M$ имеет единственное представление в виде $w = w_N + w_L$ с $w_N \in N$ и $w_L \in L$, корректно определены K-линейные сюръекции $\pi_N : M \twoheadrightarrow N$ и $\pi_L : M \twoheadrightarrow L$, переводящие $w_N + w_L$ соответственно в w_N и в w_L. Так как $\ker \pi_N = L$ и $\ker \pi_L = N$ отображения $\iota_{\pi_N} : M/L \xrightarrow{\sim} N$ и $\iota_{\pi_L} : M/N \xrightarrow{\sim} L$ из n° 6.5.1 на стр. 107 являются искомыми изоморфизмами.

Упр. 6.14. Каждый вектор $w \in M$ имеет вид $w = \sum_{u\in Z} x_u u$, где $x_u \in K$ и лишь конечное число из них отлично от нуля. Поэтому $\varphi(w) = \sum_{u\in Z} x_u \varphi(u) = \sum_{u\in Z} x_u \psi(u) = \psi(w)$.

Упр. 7.1. Базисом являются, например, все одноточечные подмножества[1]. Нулевым вектором является пустое подмножество.

Упр. 7.2. Линейность f вытекает из того, что отображение дифференцирования

$$d/dx\colon \Bbbk[x] \to \Bbbk[x], \quad g \mapsto g',$$

и все отображения вычисления $\mathrm{ev}_a\colon \Bbbk[x] \to \Bbbk$, $g \mapsto g(a)$, где $a \in \Bbbk$, линейны и композиция линейных отображений тоже линейна. Если $g \in \ker f$, то каждое число $a_i \in \Bbbk$ является как минимум (m_i+1)-кратным корнем многочлена g, и g делится на $\prod_i (x-a_i)^{m_i+1}$, что невозможно при $g \neq 0$, поскольку степень этого произведения равна $m+1 > \deg g$.

Упр. 7.3. Очевидно, что E вкладывается в B_E, а B_E вкладывается в множество $\mathbb{N}\times E$ — дизъюнктное объединение счётного множества копий множества E, которое равномощно E, так как E бесконечно. Тем самым, B_E вкладывается в E. Остаётся применить теорему Кантора – Бернштейна.

Упр. 7.4. Линейное отображение G действует на каждый вектор $v = \sum_{e\in E} x_e e$ по правилу $G(v) = \sum_{e\in E} x_e g(e)$, и для любого отображения множеств $g\colon E \to W$ это правило задаёт линейное отображение $G\colon V \to W$.

Упр. 7.6. Достаточно убедиться, что векторы $v_1, \ldots, v_n$ линейно независимы. Применяя к обеим частям соотношения $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$ функционал ξ_i, получаем $\lambda_i = 0$, и так для каждого $i = 1, \ldots, n$.

Упр. 7.7. Ядро $\ker \mathrm{ev} = \{v \in V \mid \forall\, \varphi \in V^* \ \varphi(v) = 0\} = 0$, поскольку для любого ненулевого вектора $v \in V$ существует такой линейный функционал $\varphi\colon V \to \Bbbk$, что $\varphi(v) \neq 0$. Например, можно дополнить вектор v до базиса пространства V и взять в качестве φ функционал, сопоставляющий вектору его координату в направлении базисного вектора vотносительно этого базиса.

Упр. 7.8. Подсказка: $\langle\, x^k\,,\, [D^\ell]\,\rangle = k!$ при $k = \ell$ и нуль при $k \neq \ell$.

Упр. 7.9. Покажите, что множество конечных последовательностей элементов бесконечного множества равномощно этому множеству, а множество функций на любом множестве X со значениями в множестве, содержащем хотя бы два разных элемента, более мощно, чем X. Поэтому множество многочленов, т. е. конечных последовательностей коэффициентов из $\mathbb{Q}$ счётно, а множество рядов, т. е. множество бесконечных последовательностей коэффициентов или, что то же самое, функций $\mathbb{N} \to \mathbb{Q}$ не счётно.

Упр. 7.10. Пусть $x_1 \mathrm{ev}_{\alpha_1} + \ldots + x_n \mathrm{ev}_{\alpha_m} = 0$. Согласно прим. 7.3 на стр. 116 для каждого $i = 1, \ldots, m$ в $\Bbbk[x]$ имеется многочлен f, принимающий значение 1 в точке α_i и зануляющийся во всех остальных точках α_j. Вычисляя левую часть на этом многочлене, заключаем, что $\lambda_i = 0$.

Упр. 7.11. Если линейная форма зануляется на каком-то множестве векторов, то она зануляется и всех линейных комбинациях этих векторов.

Упр. 7.12. Ковекторы $w_1^*, \ldots, w_m^*$ лежат в $\mathrm{Ann}\, U$ и линейно независимы, так как являются частью базиса в V^*. Поскольку координатами каждого линейного функционала $\varphi \in V^*$ в базисе

$$u_1^*, \ldots, u_k^*, w_1^*, \ldots, w_m^*$$

являются значения $\varphi(u_1), \ldots, \varphi(u_k), \varphi(w_1), \ldots, \varphi(w_m)$, ковектор $\varphi \in \mathrm{Ann}\, U$ если и только если он является линейной комбинацией ковекторов $w_1^*, \ldots, w_m^*$. Тем самым, эти ковекторы линейно порождают $\mathrm{Ann}\, U$.

[1] Обратите внимание, что если множество X бесконечно, то одноточечные подмножества не образуют базиса в пространстве подмножеств.

Упр. 7.13. По упр. 7.11 на стр. 125 $\operatorname{Ann} N = \operatorname{Ann}\operatorname{span} N$, откуда $\operatorname{Ann}\operatorname{Ann} N = \operatorname{Ann}\operatorname{Ann}\operatorname{span} N = \operatorname{span} N$.

Упр. 7.15. Оператор $F^{**}\colon U^{**} \to W^{**}$ переводит функционал вычисления $\mathrm{ev}_u\colon U^* \to \Bbbk$ в композицию $\mathrm{ev}_u \circ F^*\colon W^* \to \Bbbk$, которая в свою очередь переводит ковектор $\xi\colon W \to \Bbbk$ в число $\mathrm{ev}_u(F^*\xi) = F^*\xi(u) = \xi(Fu) = \mathrm{ev}_{Fu}(\xi)$. Таким образом, $F^{**}(\mathrm{ev}_v) = \mathrm{ev}_{F(v)}$. Отождествления $U^{**} \simeq U$ и $W^{**} \simeq W$ переводят функционалы вычисления $\mathrm{ev}_u\colon U^* \to \Bbbk$ и $\mathrm{ev}_w\colon W^* \to \Bbbk$ в векторы $u \in U$ и $w \in W$, на которых эти вычисления производятся. Формула $F^{**}(\mathrm{ev}_v) = \mathrm{ev}_{F(v)}$ утверждает, что при этом действие оператора F^{**} на функционалы вычисления превращается в действие F на векторы.

Упр. 8.3. Ответ:

$$[E_{ij}, E_{k\ell}] \stackrel{\text{def}}{=} E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} E_{ii} - E_{jj} & \text{при } j = k \text{ и } i = \ell \\ E_{i\ell} & \text{при } j = k \text{ и } i \neq \ell \\ -E_{kj} & \text{при } j \neq k \text{ и } i = \ell \\ 0 & \text{в остальных случаях.} \end{cases}$$

Упр. 8.5. Прямая проверка:

$$(AB)^\vee = \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right)^\vee = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{21} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{21} + a_{22}b_{22} \end{pmatrix}^\vee =$$
$$= \begin{pmatrix} a_{21}b_{21} + a_{22}b_{22} & -a_{11}b_{21} - a_{12}b_{22} \\ -a_{21}b_{11} - a_{22}b_{21} & a_{11}b_{11} + a_{12}b_{21} \end{pmatrix} = \begin{pmatrix} b_{22} & -b_{12} \\ -b_{21} & b_{11} \end{pmatrix}\begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} = B^\vee A^\vee$$

Упр. 8.7. Если e' и e'' — единичные элементы, то $e' = e'e'' = e''$. Если $fg = e$ и $gh = e$, то $f = fe = f(gh) = (fg)h = eh = h$.

Упр. 8.13. Оба равенства проверяются прямым вычислением.

Упр. 9.1. $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \frac{1}{\Delta}\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ как мы видели в прим. 8.5 на стр. 134.

Упр. 9.3. Если матрица D диагональна, то матрица DA (соотв. AD) получается из матрицы A умножением её i-й строки (соотв. i-го столбца) на диагональный элемент d_{ii} матрицы D. Поэтому равенство $AD = DA = E$ равносильно тому, что $a_{ii}d_{ii} = 1$ и $a_{ij} = 0$ при всех $i \neq j$.

Упр. 9.4. Последовательно заменяя в данном столбце пары ненулевых элементов a, b по лем. 9.1 на стр. 149 парами $\text{нод}(a, b), 0$, получаем столбец в котором отличен от нуля ровно один элемент $d \in K$, равный нод элементов исходного столбца. Если матрица A обратима, то её столбцы $(a_1, \ldots, a_n)$ образуют базис в K^n, причём $a_j = de_i$, где $(e_1, \ldots, e_n)$ — стандартный базис в K^n. Пусть стандартный базисный вектор e_i выражается через столбцы матрицы A по формуле $e_i = \sum x_\nu a_\nu$. Тогда $a_j - \sum dx_\nu a_\nu = 0$, и вектор a_j входит в эту линейную комбинацию с коэффициентом $1 - dx_j$, откуда $dx_j = 1$.

Упр. 9.6. Если матрица координат векторов $u_1, \ldots, u_r$ содержит единичную $r \times r$ матрицу в столбцах с номерами $j_1, \ldots, j_r$, то при j_i-я координата вектора $\lambda_1 u_1 + \ldots + \lambda_r u_r$ равна λ_i каждом $i = 1, \ldots, r$. Поэтому такой вектор зануляется только когда все $\lambda_i = 0$.

Упр. 9.7. Пусть базисными являются столбцы с номерами $j_1, \ldots, j_r$. Тогда в любом другом столбце могут быть отличны от нуля только числа, стоящие в первых r строках. Если они равны

$\alpha_1, \dots, \alpha_r$, то сам столбец является линейной комбинацией $\alpha_1 c_1 + \dots + \alpha_r c_r$ базисных столбцов $c_1, \dots, c_r$.

Упр. 9.8. Если отнять из произвольной такой матрицы матрицу E_J, имеющую единичную $r \times r$ подматрицу в столбцах с номерами $j_1, \dots, j_r$ и нули в остальных местах, то получится матрица, у которой равны нулю все элементы в столбцах с номерами $j_1, \dots, j_r$, а также, при каждом $i = 1, \dots, r$, все элементы i-й строки в клетках с 1-й по j_i-ю включительно. Ну а остальные $r^2 + \sum_{\nu=1}^{r}(i_\nu - \nu + 1)$ элементов могут принимать любые значения. Тождество выражает собою равенство количества r-мерных векторных подпространств в n-мерном координатном пространстве над полем $\mathbb{F}_q$ из q элементов количеству приведённых ступенчатых матриц с r ненулевыми строками в $\mathrm{Mat}_{r\times n}(\mathbb{F}_q)$.

Упр. 10.1. Векторы w_1, w_2 — это первые два вектора набора $\boldsymbol{w} = \boldsymbol{a}R$, где матрица $R = R_1R_2R_3R_4$ задаёт совершённые в прим. 10.2 на стр. 171 преобразования столбцов:

$$R_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

делает четвёртый столбец первым,

$$R_2 = \begin{pmatrix} 1 & 2 & -3 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

прибавляет ко 2-у и 3-у столбцам 1-й, умноженный на 2 и на -3,

$$R_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

записывает во 2-й столбец сумму к 3-го и 4-го, а в 3-й столбец — бывший 2-й,

$$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -8 & -3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

отнимает из 3-го и 4-го столбцов 2-й, умноженный на 8 и на 3. Вычисляя произведение[1], получаем

$$R = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & -8 & -3 \\ 0 & 1 & -8 & -2 \\ 1 & -3 & 26 & 9 \end{pmatrix},$$

откуда $w_1 = a_4$ и $w_2 = a_2 + a_3 - 3a_4$.

[1] Или, что тоже самое, применяя указанные четыре преобразования к единичной матрице 4×4.

Упр. 10.2. Если $x_1 w_1 = 0$ и $x_2 w_2 = 0$ для ненулевых $x_1, x_2 \in K$, то $x_1 x_2 (w_1 \pm w_2) = 0$ и $x_1 x_2 \neq 0$, так как в K нет делителей нуля, и $x_1(y w_1) = x_2(y w_2) = 0$ для всех $y \in K$.

Упр. 10.3. Если $p^{k_1} w_1 = 0$ и $p^{k_2} w_2 = 0$, то $p^{k_1+k_2}(w_1 \pm w_2) = 0$ и $p^{k_1} y w_1 = 0$ для всех $y \in K$. Равенство $p^{k_1}[w] = [0]$ в $M / \operatorname{Tors}_p(M)$ означает, что $p^{k_1} w \in \operatorname{Tors}_p(M)$, т. е. $p^{k_2} p^{k_1} w = 0$ для некоторого $k_2 \in \mathbb{N}$, откуда $p^{k_1+k_2} w = 0$ и $w \in \operatorname{Tors}_p(M)$, т. е. $[w] = [0]$. Если $w \in \operatorname{Tors}_p(M) \setminus N$, то класс $[w] \in M/N$ является ненулевым элементом p-кручения.

Упр. 10.4. Класс $[p^{m-k}x] \in K/(p^m)$ лежит в $\ker \varphi^k$, поскольку $p^k[p^{m-k}x] = [p^m x] = [0]$. Если $x' = x + py$, то $p^{m-k}x' = p^{m-k}x + p^{m-k+1}y$ и класс $[p^{m-k+1}y] \in K/(p^m)$ лежит в $\ker \varphi^{k-1}$, так как $p^{k-1}[p^{m-k+1}y] = [p^m y] = [0]$. Линейность отображения очевидна. Оно сюръективно, поскольку каждый класс $[y] \in K/(p^m)$, такой что $[p^k y] = [0]$, имеет $y = p^{m-k}x$ для некоторого $x \in K$ в силу того, что $p^k x$ делится на p^m в факториальном кольце K если и только если x делится на p^{m-k}. Ядро отображения нулевое по той же причине: если класс $[p^{m-k}x] \in K/(p^m)$ лежит в $\ker \varphi^{k-1}$, то $p^{k-1}p^{m-k}x = p^{m-1}x$ делится на p^m, а значит $x \vdots p$ и класс $[x] \in K/(p)$ нулевой.

Упр. 10.5. В $\mathbb{Z}/(4)$ есть элемент порядка 4, а в $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ такого элемента нет.

Упр. 10.6. Имеется ровно три таких подгруппы. Они порождаются элементами $(1, [0]_3)$, $(1, [1]_3)$ и $(1, [-1]_3)$.

Упр. 10.7. Каждая ненулевая собственная подгруппа в $\mathbb{Z}$ имеет вид $(n) = \{x \in \mathbb{Z} \mid x \vdots n\}$, где $n \geqslant 2$, а каждая ненулевая собственная подгруппа в $\mathbb{Z}/(p^m)$ имеет вид $(p^k) = \{[x] \in \mathbb{Z}/(p^m) \mid x \vdots p^k\}$, где $1 \leqslant k \leqslant m$.

Упр. 10.8. Так как любой вектор $b \in B$ представляется в A как $b = v + c + u$, где $u \in U$, $c \in$, $u \in U$, выполняется равенство $b = \pi(b) = \pi(v + c + u) = v + \pi(u)$. Поэтому $B = V + W$. Если $b \in V \cap W$, то $b = \pi(u)$ для некоторого $u \in U$, и $\pi(b - u) = b - \pi(u) = 0$. Поэтому $b - u \in \ker \pi = C$, что возможно только при $b = u = 0$.

Упр. 10.10. Умножая $\mathbb{Q}$-линейную комбинацию векторов на общий знаменатель всех её коэффициентов, получаем $\mathbb{Z}$-линейную комбинацию тех же векторов.

Упр. 11.1. $\max \ell(g) = n(n-1)/2$ достигается на единственной перестановке $(n, n-1, \ldots, 1)$.

Упр. 11.2. Индукция по n. Каждая перестановка $g = (g_1, \ldots, g_n)$ является композицией $g = \sigma \circ g'$ транспозиции σ, переставляющей между собою элементы n и g_n, и перестановки $g' = \sigma \circ g$, оставляющей элемент n на месте. По индукции, g' раскладывается в композицию транспозиций, не затрагивающих элемент n.

Упр. 11.3. Когда все точки пересечения двойные и трансверсальные, две нити, идущие из i и из j пересекаются между собою нечётное число раз, если пара (i, j) инверсна, и чётное, если не инверсна[1]. Для тасующей перестановки $(i_1, \ldots, i_k, j_1, \ldots, j_m)$ нити, выходящие из $i_1, \ldots, i_k$ верхней строки не пересекаются между собою и пересекают, соответственно, $i_1 - 1, i_2 - 2, \ldots, i_k - k$ начинающихся левее нитей, выходящих из j-точек верхней строки, причём все эти нити не пересекаются между собою.

Упр. 11.4. Если g является композицией транспозиций $\sigma_k \sigma_{k-1} \ldots \sigma_1$, то $g^{-1} = \sigma_1 \ldots \sigma_k$ является произведением тех же транспозиций в противоположном порядке.

Упр. 11.6. При чётном n центр алгебры $K\langle \xi_1, \ldots, \xi_n \rangle$ линейно порождается мономами чётных степеней, при нечётном n — мономами чётных степеней и старшим мономом $\xi_1 \wedge \ldots \wedge \xi_n$, имеющим в этом случае нечётную степень.

[1] На самом деле картинку всегда можно нарисовать так, чтобы количества точек пересечения в этих двух случаях равнялись 1 и 0 соответственно

Упр. 11.8. Беря определители в равенстве $C \cdot C^{-1} = E$, получаем $\det(C) \cdot \det(C^{-1}) = \det E = 1$.

Упр. 11.9. Это следует из равенств $\det A = \det A^t$ и $(AB)^t = B^t A^t$.

Упр. 11.10. Если все $A_{ij} = 0$, положим $A = 0$, если, скажем, $A_{12} \neq 0$, положим

$$A = \begin{pmatrix} 1 & 0 & -A_{23}/A_{12} & -A_{24}/A_{12} \\ 0 & A_{12} & A_{13} & A_{14} \end{pmatrix}.$$

Обратите внимание, что равенство

$$A_{34} = \det \begin{pmatrix} -A_{23}/A_{12} & -A_{24}/A_{12} \\ A_{13} & A_{14} \end{pmatrix}$$

эквивалентно соотношению Плюккера из форм. (11-20) на стр. 197.

Упр. 11.11. Если стоящие в левых частях уравнений (11-25) линейные формы

$$\alpha_i = \left(a_{i,0},\, a_{i,1}, \ldots, a_{i,n}\right) \in \Bbbk^{n+1*}$$

линейно независимы, то по лемме о замене[1] ими можно заменить подходящие n ковекторов стандартного базиса в $\Bbbk^{n+1*}$. Пусть это будут последние n базисных ковекторов. Коль скоро ковектор $(1,\, 0, \ldots, 0)$ и ковекторы $\alpha_1, \ldots, \alpha_n$ образуют базис, определитель, составленный из строк их координат, отличен от нуля. Раскладывая его по строке $(1,\, 0, \ldots, 0)$, видим, что он равен A_0, откуда $A_0 \neq 0$. Если же строки матрицы A линейно зависимы, то все $A_i = 0$.

Упр. 11.12. Это вытекает из прим. 11.6 на стр. 197. Полагая в форм. (11-21) на стр. 197 $x = 1$, $y = t$ и $B = E$, получаем разложение

$$\det(tE + A) = t^n + \sum_{m=1}^{n} t^{n-m} \sum\nolimits_{\#I=m} a_{II} = \\ = t^n + t^{n-1} \sum\nolimits_i a_{ii} + t^{n-1} \sum\nolimits_{i<j} (a_{ii}a_{jj} - a_{ij}a_{ji}) + \ldots + t \sum\nolimits_i a_{\overline{ii}} + \det A\,,$$

где коэффициент при t^{n-k} равен сумме определителей всех $k \times k$ подматриц в A с главной диагональю, содержащейся в главной диагонали матрицы A.

Упр. 11.13. $f(C)g(C) = \sum_{k=0}^{m+n} \sum_{i+j=k} C^i A_i C^j B_j = \sum_{k=0}^{m+n} \sum_{i+j=k} C^{i+j} A_i B_j = \sum_{k=0}^{m+n} C^k \sum_{i+j=k} A_i B_j = = \sum_{k=0}^{m+n} C^k H_k = h(C)$.

Упр. 11.14. Если $f = h\varphi$, $g = h\psi$, где $\deg h > 0$, то $\deg \varphi < n$, $\deg \psi < m$ и $f\psi - g\varphi = 0$. Если же f и g взаимно просты, то из равенства $fh_1 = -gh_2$ вытекает, что $g \mid h_1$, а $f \mid h_2$, что невозможно для ненулевых h_1, h_2 с $\deg h_1 < m$ и $\deg h_2 < n$.

Упр. 12.1. Если отождествить $\mathbb{R}[t]/(t^2+1)$ с полем $\mathbb{C}$, отправив классы $[1]$ и $[t]$ в 1 и i соответственно, умножение на класс $[t]$ превратится в умножение на i, т. е. в поворот на угол $\pi/2$, который не переводит никакое одномерное векторное подпространство в себя.

Упр. 12.2. Пусть $\Bbbk[t]/\left(t^n\right) = U \oplus W$, где U и W переводятся в себя умножением на $[t]$. Оба этих подпространства не могут целиком содержаться в образе оператора умножения на $[t]$, так как иначе их сумма тоже бы в нём содержалась. Поэтому в одном из них, пусть это будет U, имеется класс $[g]$ многочлена g с ненулевым свободным членом. Тогда классы $[t^{n-1}g], \ldots, [tg], [g] \in U$

[1] См. лемму 4.2 на стр. 48 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_04.pdf.

выражаются через базис $[1], [t], \dots, [t^{n-1}]$ пространства $\Bbbk[t]/(t^n)$ при помощи верхнетреугольной матрицы, на диагонаи которой всюду стоит ненулевой свободный член многочлена g. Следовательно, эти классы тоже образуют базис в $\Bbbk[t]/(t^n)$, и значит, содержащее их подпространство U совпадает со всем пространством $\Bbbk[t]/(t^n)$.

Упр. 12.3. Разложите каждое пространство $(F|_{U_i}, U_i)$ по форм. (12-1) на стр. 207. В силу единственности такого разложения прямая сумма полученных разложений является разложением исходного пространства (F, V).

Упр. 12.4. Коэффициенты $g_i \in \Bbbk^n$ неполного частного $g(t)$ от деления $h(t)$ на $tE - A$ вычисляются рекурсивно по формулам $g_{m-1} = h_m$, $g_{i-1} = h_i + Ag_i$ при $i \leqslant m-1$. Остаток $r = h(t) - (tE - A)\,g(t) \in \Bbbk^n$ не зависит от t. Подставляя $t = A$, что законно, ибо A коммутирует[1], заключаем, что $r = h(A)$.

Упр. 12.5. $\det(tE - C^{-1}AC) = \det(tC^{-1}EC - C^{-1}AC) = \det\bigl(C^{-1}(tE-A)C\bigr) = \det C^{-1} \cdot \det(tE-A) \cdot \det C = \det(tE - A)$.

Упр. 12.6. Пусть $f = t^n + a_1 t^{n-1} + \dots + a_n$. Напишите матрицу F оператора умножения на класс $[t]$ в факторкольце $\Bbbk[x]/(f)$ в базисе $[t^{n-1}], [t^{n-2}], \dots, [t], [1]$ и разложите $\det(tE - F)$ по первому столбцу.

Упр. 12.7. Пусть $f(t) = \mu_{v,F}(t)g(t) + r(t)$, где либо $r = 0$, либо $\deg r < \deg \mu_{v,F}$. Если $f(F) = 0$, то $r(F)v = 0$, что невозможно для ненулевого r с $\deg r < \deg \mu_{v,F}$ по определению многочлена $\mu_{v,F}$. Поэтому $r = 0$.

Упр. 12.8. Если оператор $q(F)$ аннулирует все векторы из какого-нибудь линейного порождающего V множества, то он аннулирует любой вектор из V.

Упр. 12.12. Так как любой вектор $h \in H$ представляется в V как $h = u + q + r$ с $u \in U$, $q \in Q$, $r \in R$, в U выполняется равенство $h = \pi(h) = \pi(u) + \pi(r)$, в котором $\pi(u) = u \in U$ и $\pi(r) \in W$, т. е. $U + W = H$. Если $u \in U \cap W$, то $u = \pi(r)$ для некоторого $r \in R$, и $\pi(u - r) = \pi(u) - \pi(r) = u - u = 0$, откуда $u - r \in \ker \pi = Q$, что возможно только при $u = r = 0$. Поэтому $U \cap W = 0$.

Упр. 12.13. Если $\lambda \in \operatorname{Spec} F$ и $g(\lambda) \neq 0$, то $g(F)$ действует на ненулевом собственном подпространстве V_λ умножением на ненулевое число $g(\lambda)$. Тем самым, $g(F) \neq 0$.

Упр. 12.14. Над алгебраически замкнутым полем всякий многочлен имеющий только один корень 0 равен t^m. Поэтому $\chi_F(t) = t^m$ и по теореме Гамильтона – Кэли $F^m = 0$.

Упр. 12.17. Разложение характеристического многочлена оператора F в виде произведения степеней попарно разных линейных форм $\chi_F(t) = \prod\limits_{\lambda \in \operatorname{Spec} F} (t-\lambda)^{N_\lambda}$ удовлетворяет условиям теор. 12.3 с $q_i = (t - \lambda)^{N_\lambda}$, а корневые подпространства $K_\lambda = \ker(\lambda \operatorname{Id} - F)^{N_\lambda}$.

Упр. 12.18. Над полем $\mathbb{C}$ можно применить предл. 12.5. Над произвольным полем $\Bbbk$ оператор F с матрицей $J_n(\lambda)$ имеет вид $\lambda\mathrm{Id} + N$, где $N^n = 0$, но $N^{n-1} \neq 0$. Обратный оператор

$$F^{-1} = (\lambda\mathrm{Id} + N)^{-1} = \lambda^{-1}(\mathrm{Id} + N/\lambda)^{-1} = \lambda^{-1} - \lambda^{-2}N + \lambda^{-3}N^2 - \dots + (-1)^{n-1}\lambda^{-n}N^{n-1}$$

имеет вид $\lambda^{-1}\mathrm{Id} + M$, где оператор $M = -\lambda^{-2}N(1 - \lambda^{-1}N + \dots)$ тоже имеет $M^n = 0$, а $M^{n-1} = \lambda^{2(1-n)}N^{n-1} \neq 0$. Таким образом, ЖНФ оператора F^{-1} это одна клетка $J_n\left(\lambda^{-1}\right)$.

Упр. 12.20. В $\Bbbk[\![x]\!]$ квадрат ряда $\sqrt{1+x}$ равен $1 + x$, а коэффициенты при x^k для $0 \leqslant k \leqslant n$ у квадрата ряда $\sqrt{1+x}$ такие же, как и у квадрата многочлена из условия.

[1] См. **??** на стр. **??**.

Упр. 12.21. Если $a^n = 0$, $b^m = 0$ и $ab = ba$, то $(a-b)^{m+n-1} = 0$ по формуле Ньютона.

Упр. 13.1. Первое следует из того, что по правилу треугольника $\overrightarrow{aa} + \overrightarrow{ab} = \overrightarrow{ab}$ для любого вектора $\overrightarrow{ab} \in V$, второе — из того, что $\overrightarrow{pq} + \overrightarrow{qp} = \overrightarrow{pp} = 0$, третье — из того, что при $\overrightarrow{ab} = \overrightarrow{dc}$ имеем $\overrightarrow{bc} = \overrightarrow{ba} + \overrightarrow{ad} + \overrightarrow{dc} = -\overrightarrow{ab} + \overrightarrow{ad} + \overrightarrow{dc} = \overrightarrow{ad}$.

Упр. 13.2. Пусть $\tau_0(p) = q$ и $\tau_v(q) = p$. Тогда $\tau_v(q) = \tau_0(\tau_v(q)) = \tau_0(p) = q$, откуда $q = p$, а значит, $\tau_0 = \mathrm{Id}$. Наоборот, если $\tau_0 = \mathrm{Id}$, то для каждого $v \in V$ преобразования τ_v и τ_{-v} обратны друг другу в силу равенств $\tau_v \circ \tau_{-v} = \tau_{-v} \circ \tau_v = \tau_{v+(-v)} = \tau_0 = \mathrm{Id}$, а значит, оба биективны.

Упр. 13.4. Равенства $x_1(u_1, \varphi(u_1)) + x_2(u_2, \varphi(u_2)) = (x_1u_1 + x_2u_2, \varphi(x_1u_1 + x_2u_2))$ и $x_1\varphi(u_1) + x_2\varphi(u_2) = \varphi(x_1u_1 + x_2u_2)$ эквивалентны.

Упр. 13.5. Покажите, что лежащие в одной плоскости прямые $p + ut$ и $q + wt$ не пересекаются если и только если векторы u, w пропорциональны, а вектор $\overrightarrow{pq}$ им не пропорционален. Таким образом, в параллелограмме $abcd$ выполняются соотношения: $\overrightarrow{dc} = \lambda\overrightarrow{ab}$ и $\overrightarrow{bc} = \mu\overrightarrow{ad}$, а векторы $\overrightarrow{ab}$ и $\overrightarrow{ad}$ образуют базис в направляющем векторном пространстве плоскости. Из равенств

$$\overrightarrow{ac} = \overrightarrow{ab} + \overrightarrow{bc} = \overrightarrow{ab} + \mu\overrightarrow{ad}$$
$$\overrightarrow{ac} = \overrightarrow{ad} + \overrightarrow{dc} = \lambda\overrightarrow{ab} + \overrightarrow{ad}$$

вытекает, что $\lambda = \mu = 1$ и условия (1) – (3) в параллелограмме выполнены. Рассуждая как в упр. 13.1 на стр. 235, убедитесь, что условия (1) – (3) равносильны друг другу. Из них вытекает, что точка c лежит в плоскости (abc), а $(ab) \cap (dc) = \varnothing$ и $(ad) \cap (bc) = \varnothing$ в силу сделанного в самом начале замечания.

Упр. 13.6. Отображение $D_{\varphi\circ\psi} : U \to W$ переводит вектор $\overrightarrow{pq} \in U$ в

$$\overrightarrow{\varphi(\psi(p))\varphi(\psi(q))} = D_\varphi(\overrightarrow{\psi(p)\psi(q)}) = D_\varphi\big(D_\psi(\overrightarrow{pq})\big) \in W$$

и является композицией $D_\varphi D_\psi$ линейных отображений D_φ и D_ψ. Поэтому оно тоже линейно.

Упр. 13.7. Покажите, что в каждом параллелограмме $abcd$ прямые (ac) и (bd) пересекаются. Пусть $o = (ac) \cap (bd)$, а $a'b'c'd' = \varphi(abcd)$. Так как преобразование φ биективно и переводит прямые в прямые, $o' = \varphi(o) = (a'c') \cap (b'd')$. Из этого вытекает, что $a'b'c'd'$ лежит в одной плоскости. Ещё раз пользуясь тем, что φ биективно и переводит прямые в прямые, заключаем, что $(a'b') \cap (c'd') = \varnothing$ и $(a'd') \cap (b'c') = \varnothing$.

Упр. 13.8. Пусть $\xi(x) = 1$ для всех x из аффинной гиперплоскости $\Pi = p + U$, где $U \subset V$ — векторное подпространство коразмерности 1. Тогда $\xi \in \operatorname{Ann} U$, ибо $1 = \xi(p + u) = \xi(p) + \xi(u) = 1 + \xi(u)$. Каждый функционал $\xi \in \operatorname{Ann} U$ принимает на Π постоянное значение $\xi(p)$, ненулевое, так как $0 \notin \Pi$. Так как $\dim \operatorname{Ann} U = 1$, существует единственный такой $\xi \in \operatorname{Ann} U$, что $\xi(\Pi) = 1$.

Упр. 13.9. В правой части стоит геометрическая прогрессия $q^n + q^{n-1} + \cdots + q + 1$, а слева — количество ненулевых векторов в $(n+1)$-мерном пространстве, делённое на количество ненулевых векторов в одномерном пространстве, т. е. $(q^{n+1} - 1)/(q - 1)$.

Упр. 13.11. Это следует из соотношения $(s : 1) = (x_0 : x_1) = (1 : t)$.

Упр. 13.12. Ср. с прим. 13.3 на стр. 236

Упр. 13.13. Пусть $K = \mathbb{P}(W)$. Векторное подпространство $W \subset V$ имеет размерность $k + 1$ и либо содержится в гиперплоскости $\operatorname{Ann}(\xi)$, либо пересекается с нею по k-мерному векторному пространству $W' = \operatorname{Ann}(\xi|_W) \subset W$. В первом случае K не пересекается с картой U_ξ, во втором

случае пересечение $K \cap U_\xi$ представляет собою аффинное пространство над векторным пространством $W \cap \operatorname{Ann} \xi = W'$.

Упр. 13.15. Если $v = u + w$, где $u \in U$, $w \in W$ и $v \notin U \cup W$, то u и w линейно независимы, и $v \in (u, w)$. Если отвечающая вектору v точка проективного пространства лежит на какой-то ещё прямой (ab) с $a \in U$ и $b \in W$, то $v = \lambda a + \mu b$ для некоторых ненулевых $\lambda, \mu \in \Bbbk$, причём $\lambda a = u$ и $\mu b = w$ в силу единственности разложения вектора v. Поэтому a и u, так же как b и w, суть совпадающие точки проективного пространства. В частности, $(uw) = (ab)$.

Упр. 13.17. При замене однородных координат все определители в правой части формулы (13-8) умножаются на определитель матрицы замены координат, что не меняет правой дроби. Средняя дробь всегда равна правой в силу вычисления (13-7). Последнее утверждение проверяется выкладкой

$$\frac{\det(a,c)}{\det(a,d)} \cdot \frac{\det(b,d)}{\det(b,c)} = \frac{\det(a,b+\gamma a)}{\det(a,b+\delta a)} \cdot \frac{\det(b,b+\delta a)}{\det(b,b+\gamma a)} = \frac{\delta}{\gamma}\,.$$

Упр. 13.19. Если основное поле $\Bbbk = \mathbb{F}_q$ состоит из q элементов, алгебра функций $\mathbb{F}_q^n \to \mathbb{F}_q$ состоит из q^{q^n} элементов, и гомоморфизм бесконечной алгебры многочленов в конечную алгебру функций не может быть инъективен. Зато он сюръективен, поскольку для любого конечного набора точек в $\Bbbk^n$ существует многочлен $f \in \Bbbk[x_1, \dots, x_n]$, принимающий в этих точках любые наперёд заданные значения (убедитесь в этом). Над бесконечным полем $\Bbbk$ множество функций $\Bbbk^n \to \Bbbk$ строго мощнее, чем $\Bbbk^n$, а пространство многочленов равномощно $\Bbbk$. Поэтому гомоморфизм из алгебры многочленов в алгебру функций не может быть сюръективным. Инъективность доказывается индукцией по $n = \dim V$. При $n = 1$ это утверждение о том, что ненулевой многочлен от одной переменной не может иметь бесконечно много корней. Записывая многочлен от n переменных как многочлен от x_n с коэффициентами из $\Bbbk[x_1, \dots, x_{n-1}]$: $f(x_1, \dots, x_n) = \sum_{\nu=0}^{d} \varphi_\nu(x_1, \dots, x_{n-1}) \cdot x_n^{d-\nu}$ и вычисляя коэффициенты φ_ν в произвольной точке $(p_1, \dots, p_{n-1}) \in \Bbbk^{n-1}$, мы получаем многочлен от x_n с постоянными коэффициентами, задающий тождественно нулевую функцию на прямой, состоящей из точек вида $(p_1, \dots, p_{n-1}, t)$, где $t \in \Bbbk$, в $\Bbbk^n$. По уже доказанному, он нулевой. Следовательно, все многочлены φ_ν являются тождественно нулевыми функциями на $\Bbbk^{n-1}$. По предположению индукции, они являются нулевыми многочленами.

Упр. 14.2. Билинейность вытекает из свойств интеграла, положительность — из того, что ненулевая непрерывная функция отлична от нуля сразу на некотором интервале.

Упр. 14.4. Значение линейной формы g_{v_j} на базисном векторе v_i равно (v_i, v_j), т. е. столбец координат этой формы в двойственном базисе $\boldsymbol{v}^*$ состоит из произведений (v_i, v_j).

Упр. 15.2. $B_{\boldsymbol{uw}} = \boldsymbol{u}^t \boldsymbol{w} = \left(\boldsymbol{e} C_{\boldsymbol{eu}}\right)^t \left(\boldsymbol{f} C_{\boldsymbol{fw}}\right) = C_{\boldsymbol{eu}}^t \boldsymbol{e}^t \boldsymbol{f} C_{\boldsymbol{fw}} = C_{\boldsymbol{eu}}^t B_{\boldsymbol{ef}} C_{\boldsymbol{fw}}$.

Упр. 15.5. Линейная оболочка векторов $e_\nu + i e_{n+\nu}$ с $1 \leqslant \nu \leqslant n$.

Упр. 15.6. Если матрица $B \in \operatorname{Mat}_n(\Bbbk)$ кососимметрична, то при нечётном n

$$\det B = \det B^t = \det(-B) = (-1)^n \det B = -\det B\,,$$

откуда $\det B = 0$ если $\operatorname{char} \Bbbk \neq 2$.

Упр. 15.7. Пусть $v = \sum x_i e_i$. Скалярно умножая v слева на ${}^\vee e_i$, получаем $\beta({}^\vee e_i, v) = x_i$. Скалярно умножая v справа на $e_i^\vee$, получаем $\beta(v, e_i^\vee) = x_i$, и т. д.

Упр. 15.10. ${}^\vee\left(f^\vee\right) = \left(\beta^*\right)^{-1} \left((\beta)^{-1} f^* \beta\right)^* \beta^* = f^{**} = f$.

Упр. 15.11. Полагая $w = g^{-1}v$ в равенстве $\beta(u,w) = \beta(gu,gw)$, заключаем, что $\beta(gu,v) = \beta(u,g^{-1}v)$ для всех $u, v \in V$.

Упр. 15.12. Это переформулировка упр. 15.10.

Упр. 15.15. Двумерное симплектическое пространство неразложимо, поскольку все его одномерные подпространства изотропны. Пространство U_n неразложимо, поскольку его канонический оператор неразложим. Форма $W_n\ \big((-1)^{n-1}\big)$ изометрически изоморфна биортогональной прямой сумме $U_n \oplus U_n$, так как у них подобные канонические операторы — оба имеют две жордановы клетки с собственным числом $(-1)^{n-1}$.

Упр. 15.16. Корректность вытекает из того, что для всех $u \in U$ и $w \in \ker \eta_W^{(n-1)}$ выполняется равенство $\beta(\eta_U^{(n-1)}u, w) = \beta(u, \eta_U^{\times(n-1)}w) = (-1)^{(n-1)}\beta(u, \eta_U^{(n-1)}w) = 0$. Невырожденность: если $\beta(\eta_U^{(n-1)}u, w) = 0$ для всех $w \in W$, то $\eta_U^{(n-1)}u = 0$ в силу невырожденности спаривания $\beta : U \times W \to \Bbbk$.

Упр. 16.2. Это размерности пространств симметричных и кососимметричных $n\times n$ матриц, равные $n(n+1)/2$ и $n(n-1)/2$ соответственно.

Упр. 16.3. Если $f^\times = f$ и $g^\times = g$ или $f^\times = -f$ и $g^\times = -g$ это очевидно. Если $f^\times = f^{-1}$ и $g^\times = g^{-1}$, то равенство имеет вид $g^{-1} = \varphi^{-1\times} f^{-1} \varphi^\times$, и надо взять обратные к обеим частям.

Упр. 16.4. Билинейная форма $\beta_f(u,w) = \beta(u, fw)$ имеет в этом базисе матрицу

$$Z_n J_n(\lambda) = \begin{pmatrix} 0 & & & \lambda \\ & & \ddots & 1 \\ & \ddots & \ddots & \\ \lambda & 1 & & 0 \end{pmatrix}$$

и тем самым симметрична. Поэтому f самосопряжён.

Упр. 16.5. Билинейная форма $\beta_f(u,w) = \beta(u, fw)$ имеет в этих случаях матрицы

$$\begin{pmatrix} 0 & -J_n'(\lambda) \\ J_n'(\lambda) & 0 \end{pmatrix},\ \text{где } J_n'(\lambda) = \begin{pmatrix} 0 & & & \lambda \\ & & \ddots & 1 \\ & \ddots & \ddots & \\ \lambda & 1 & & 0 \end{pmatrix},\quad \text{и} \quad \begin{pmatrix} & & & 0 \\ & & \iddots & -1 \\ & \iddots & \iddots & \\ 0 & 1 & & \end{pmatrix}.$$

Последнее утверждение вытекает из предл. 16.3 на стр. 296

Упр. 16.6. $\beta(f^{(n-k)}u, f^{(n-\ell)}u) = (-1)^{n-\ell}\beta(f^{2n-(k+\ell)}u, u) = \begin{cases} 0 & \text{при } k+\ell \leqslant n \\ (-1)^{k-1} & \text{при } k+\ell = n+1. \end{cases}$

Упр. 16.7. $C^tA = -A^tC$, $D^tB = -B^tD$, $A^tD + C^tB = E$.

Упр. 16.10. Перестановка одной пары с другой как единого целого чётная (это пара транспозиций). Перестановка между собою элементов из ν-й пары меняет $\operatorname{sgn}(i_1, j_1, \ldots, i_n, j_n)$, но одновременно заменяет матричный элемент $a_{i_\nu j_\nu}$ элементом $a_{j_\nu i_\nu} = -a_{i_\nu j_\nu}$.

Упр. 17.4. Посмотрите куда переходят векторы скоростей прямых.

Упр. 17.5. Ортогональная сумма плоскостей, на которых f действует отражениями, является ортогональной суммой двух других плоскостей, на которых f действует поворотами на углы 0 и π. Ортогональная сумма двух прямых, на которых f действует отражениями, является плоскостью, на которой f действует поворотом на угол π. И т. д.

Упр. 17.6. Пусть $\chi_f(t) = (t-1)^p(t+1)^q \prod_{\varphi_i \neq 0,\pi}(t^2 - 2\cos\varphi_i + 1)$. Если p и q оба чётны, то $\det f > 0$, и кроме «настоящих» поворотов на углы $\varphi_i \neq 0, \pi$ имеются $p/2$ и $q/2$ поворотов на углы 0 и π соответственно. Если p чётно, а q нет, то $\det f < 0$, и к настоящим поворотам добавляются $p/2$ и $(q-1)/2$ поворотов на углы 0 и π, а также отражение в одномерном подпространстве. Если p нечётно, а q чётно, то $\det f > 0$, то добавляются $(p-1)/2$ и $q/2$ поворотов на углы 0 и π, а также одномерное подпространство, на котором f действует тождественно. Наконец, если p и q оба нечётны, то $\det f < 0$, и добавятся $(p-1)/2$ и $(q-1)/2$ поворотов на углы 0 и π, а также плоскость, в которой f действует отражением.

Упр. 17.7. Ненулевые квадраты составляют образ гомоморфизма мультипликативных групп

$$\mathbb{F}_q^\times \to \mathbb{F}_q^\times, \quad x \mapsto x^2 .$$

Так как уравнение $x^2 = 1$ имеет в поле $\mathbb{F}_q$ ровно два корня $x = \pm 1$, ядро этого гомоморфизма состоит из двух элементов, а значит, образ является подгруппой порядка $(q-1)/2$.

Упр. 17.8. Исходный базис (e_i, e_j) плоскости U имеет определитель Грама ε^2, а определитель Грама базиса (v_i, v_j) равен $f(v_j)$.

Упр. 17.9. Для нульмерной квадрики на $\mathbb{P}_1$ утверждение очевидно. Пусть при $n \geqslant 2$ квадрика $Q \subset \mathbb{P}_n$ содержится в гиперплоскости $H \subset \mathbb{P}_n$ и имеет гладкую точку $a \in Q$. Тогда каждая проходящая через a и не содержащаяся в H прямая пересекает Q ровно в одной точке a, т. е. лежит в T_pQ. Поэтому $\mathbb{P}_n = H \cup T_pQ$. Если $H = V(\xi)$, $T_pQ = V(\eta)$ для каких-то ненулевых ковекторов $\xi, \eta \in V^*$, то квадратичная форма $q(v) = \xi(v)\eta(v)$ тождественно зануляется на векторном пространстве V. Но тогда и оба сомножителя ξ, η должны быть нулевыми. Противоречие.

Упр. 18.1. Пусть $\omega : V \times \ldots \times V \to \Bbbk$ — ненулевая форма объёма, и векторы $\boldsymbol{v} = (v_1, \ldots, v_n)$ образуют в V базис. По теор. 14.1 на стр. 259

$$\omega(fv_1, \ldots, fv_n) = \det(f) \cdot \omega(v_1, \ldots, v_n),$$

ибо $(fv_1, \ldots, fv_n) = (v_1, \ldots, v_n)F_v$ и $\det f = \det F_v$. Мы заключаем, что объём ω не меняется если и только если $\det f = 1$. Так как все формы объёма на V пропорциональны друг другу по той же теор. 14.1, то f сохраняет каждую из них, если сохраняет какую-нибудь одну ненулевую.

Упр. 18.2. Для выбора первого столбца имеется $|V| - 1 = q^n - 1$ возможностей, для выбора второго — $q^n - q$ возможностей, для выбора третьего — $q^n - q^2$ и т. д.

Упр. 18.3. Ответ: $|\mathrm{GL}_n(\mathbb{F}_q)|/(q-1)$, см. прим. 18.10 на стр. 336.

Упр. 18.5. Пусть $k = dr$, $m = \mathrm{ord}(\tau) = ds$, где $\mathrm{нод}(r, s) = 1$. Если $d > 1$, то τ^d является произведением d независимых циклов длины s, и $\tau^k = \left(\tau^d\right)^r$ будет произведением s-тых степеней этих циклов. Остаётся показать, что когда $\mathrm{ord}(\tau) = m$ взаимно прост с k, то τ^k тоже цикл длины m. Если для какого-то элемента a цикла τ выполняется равенство $\left(\tau^k\right)^r(a) = a$, то kr делится на m, что при $\mathrm{нод}(k, m) = 1$ возможно только когда r делится на m. Поэтому $r \geqslant m$, т. е. длина содержащего a цикла перестановки τ^k не меньше m.

Упр. 18.6. Ответ: $n(n-1)\ldots(n-k+1)/k$ (в числителе дроби k сомножителей).

Упр. 18.7. Непересекающиеся циклы коммутируют. Если коммутирующие циклы τ_1 и τ_2 пересекаются по элементу a, то $\tau_1(a)$ является элементом цикла τ_2, поскольку в противном случае $\tau_2\tau_1(a) = \tau_1(a)$, а $\tau_1\tau_2(a) \neq \tau_1(a)$, так как $\tau_2(a) \neq a$. По той же причине $\tau_2(a)$ является элементом цикла τ_1, и значит, оба цикла состоят из одних и тех же элементов. Пусть $\tau_1(a) = \tau_2^s(a)$.

Любой элемент b, на который оба цикла реально действуют имеет вид $b = \tau_2^r(a)$, и цикл τ_1 действует на него как τ_2^s:

$$\tau_1(b) = \tau_1\tau_2^r(a) = \tau_2^r\tau_1(a) = \tau_2^r\tau_2^s(a) = \tau_2^s\tau_2^r(a) = \tau_2^s(b)\,.$$

Второе утверждение следует из упр. 18.5.

Упр. 18.8. Ответ: $n!\,/\prod_{i=1}^n i^{m_i}m_i!$ (ср. с форм. (1-11) на стр. 11). Решение: сопоставим каждому заполнению диаграммы циклов λ неповторяющимися числами от 1до n произведение независимых циклов, циклически переставляющих элементы каждой строки слева направо; получаем сюръективное отображение множества заполнений на множество всех перестановок циклового типа λ; прообраз каждой перестановки состоит из $\prod_{i=1}^n i^{m_i}m_i!$ заполнений, получающихся друг из друга независимыми циклическими перестановками элементов в каждой строке и произвольными перестановками строк одинаковой длины между собою как единого целого.

Упр. 18.9. $|1,6,3,4\rangle^{15}\cdot|2,5,8\rangle^{15}\cdot|7,9\rangle^{15} = |1,6,3,4\rangle^{-1}\cdot|7,9\rangle = (4,\ 2,\ 6,\ 3,\ 5,\ 1,\ 9,\ 8,\ 7)$

Упр. 18.14. Ответ: $|1,2,3,4\rangle = \sigma_{12}\sigma_{23}\sigma_{34}$, $|1,2,4,3\rangle = \sigma_{12}\sigma_{24}\sigma_{34}$, $|1,3,2,4\rangle = \sigma_{13}\sigma_{23}\sigma_{24}$, $|1,3,4,2\rangle = \sigma_{13}\sigma_{34}\sigma_{24}$, $|1,4,2,3\rangle = \sigma_{24}\sigma_{23}\sigma_{13}$, $|1,4,3,2\rangle = \sigma_{34}\sigma_{23}\sigma_{12}$.

Упр. 18.15. Подсчёт для группы куба дословно тот же, что и для группы додекаэдра. Группы октаэдра и икосаэдра изоморфны группам куба и додекадра с вершинами в центрах граней октаэдра и икосаэдра соответственно.

Упр. 18.17. $|\operatorname{PGL}_n(\mathbb{F}_q)| = |\operatorname{GL}_n(\mathbb{F}_q)|/|\Bbbk^\times| = |\operatorname{SL}_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})/(q-1)$, а $|\operatorname{PSL}_n(\mathbb{F}_q) = |\operatorname{SL}_n(\mathbb{F}_q)|/\text{нод}(n,q-1)$, так как решения уравнения $x^n = 1$ в циклической мультипликативной группе $\mathbb{F}_q^\times$ находятся в биекции с решениями уравнения $nx = 0$ в аддитивной группе $\mathbb{Z}/(q-1)$, коих имеется нод$(n,q-1)$, см. упр. 6.7 на стр. 104.

Упр. 18.19. Подсказка: центральная симметрия коммутирует со всеми элементами полной группы додекаэдра; покажите, что единственная перестановка в S_5, коммутирующая со всеми перестановками из S_5 — это тождественное преобразование.

Упр. 18.20. Чтобы перевести одномерные подпространства, порождённые непропорциональными векторами e_1, e_2, в одномерные подпространства, порождённые непропорциональными векторами v_1, v_2, дополним эти пары векторов до базисов $\boldsymbol{e} = (e_1,\dots,e_n)$ и $\boldsymbol{v} = (v_1,\dots,v_n)$. Матрица перехода $C_{\boldsymbol{ee}}$ имеет ненулевой определитель δ. Умножая её первый столбец на δ^{-1} получаем матрицу $F \in \operatorname{SL}_n$. Оператор $x \mapsto Fx$ переводит e_1 в $\delta^{-1}v_1$, а e_2 в v_2.

Упр. 18.24. Проиллюстрируем рассуждение на примере икосаэдра. И собственная и полная группы транзитивно действуют на 20 его треугольных гранях. Стабилизатор грани в собственной и полной группах представляет собой собственную и полную группу треугольника на плоскости, состоящую, соответственно из 3 и из 6 преобразований. По формуле для длины орбиты получаем $|\operatorname{SO}_{\text{ико}}| = 20\cdot 3 = 60$ и $|\operatorname{O}_{\text{ико}}| = 20\cdot 6 = 120$.

Упр. 19.1. Равенство $h_1g_1 = h_2g_2$ влечёт равенства $g_2g_1^{-1} = h_2^{-1}h_1 \in H$ и $g_1g_2^{-1} = h_1^{-1}h_2 \in H$. С другой стороны, если один из обратных друг другу элементов $g_1^{-1}g_2$ и $g_2^{-1}g_1$ лежит в H, то в H лежит и второй, и $Hg_1 = H(g_2g_1^{-1})g_2 = Hg_2$.

Упр. 19.2. Есть ровно 2 смежных класса: H и $G\smallsetminus H$, оба являются одновременно и левым, и правым.

Упр. 19.3. Включение $gHg^{-1} \subset H$ влечёт включение $H \subset g^{-1}Hg$. Если это так для всех $g \in G$, то заменяя g на g^{-1} мы получаем обратное к исходному включение $gHg^{-1} \supset H$.

Упр. 19.4. $\varphi\circ\operatorname{Ad}_g\circ\varphi^{-1}\colon\ h \mapsto \varphi\bigl(g\,\varphi^{-1}(h)\,g^{-1}\bigr) = \varphi(g)\,h\,\varphi(g)^{-1}$.

Упр. 19.6. Если $\varphi(x) \in N_2$, то $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in N_2$ в силу нормальности $N_2 \lhd G_2$. Поэтому $N_1 = \varphi^{-1}(N_2) \lhd G_1$. Композиция сюръективных гомоморфизмов $G_1 \twoheadrightarrow G_2 \twoheadrightarrow G_2/N_2$ является сюръективным гомоморфизмом с ядром N_1.

Упр. 19.7. Поскольку S_n порождается транспозициями, подгруппа A_n порождается парами транспозиций. Но $|ij\rangle|jk\rangle = |ijk\rangle$ и $|ij\rangle|k\ell\rangle = |ijk\rangle|jk\ell\rangle$ при различных i, j, k, ℓ.

Упр. 19.8. Воспользуйтесь равенством $|ij\rangle|jk\rangle = |ij\rangle|\ell m\rangle|jk\rangle|\ell m\rangle$ для различных i, j, k, ℓ, m.

Упр. 19.9. Первый изоморфизм задаётся действием группы $\mathrm{SL}_2(\mathbb{F}_2) \simeq \mathrm{GL}_2(\mathbb{F}_2)$ на трёх ненулевых векторах координатной плоскости $\mathbb{F}_2^2$, второй — действием группы $\mathrm{PSL}_2(\mathbb{F}_3) \stackrel{\text{def}}{=} \mathrm{SL}_2(\mathbb{F}_3)/\{\pm E\}$ на четырёх одномерных векторных подпространствах в $\mathbb{F}_3^2$ или, что то же самое, действием дробно линейных преобразований $t \mapsto (at+b)/(ct+d)$, где $a, b, c, d \in \mathbb{F}_3$ и $ad \neq bc$, на четырёх точках проективной прямой $\mathbb{P}_1(\mathbb{F}_3) = \{-1, 0, 1, \infty\}$.

Упр. 19.11. Так как $\mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) = S_3$, коммутант $\mathrm{SL}_2' = \{E, T, T^2\} \simeq A_3$, где

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{и} \quad T^2 = T^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

циклически переставляют ненулевые векторы $(1,0), (0,1), (1,1)$ пространства $\mathbb{F}_2^2$. При факторизации $\mathrm{SL}_2(\mathbb{F}_3) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$ по подгруппе $\{\pm E\} \subset \mathrm{SL}_2(\mathbb{F}_3)$ коммутант $\mathrm{SL}_2'(\mathbb{F}_3)$ сюръективно отображается на группу Клейна $V_4 = A_4'$, состоящую независимых транспозиций двух пар точек проективной прямой $\mathbb{P}_1(\mathbb{F}_3) = \{(1:0), (0:1), (1:1), (1:-1)\}$, которые задаются следующими матрицами из $\mathrm{SL}_2(\mathbb{F}_3)$ с точностью до знака

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Убедитесь, что $I^2 = J^2 = K^2 = -E$ и $IJ = -JI = K$, $JK = -KJ = I$, $KI = -IK = J$. Таким образом, при любом выборе знаков у трёх матриц $\pm I, \pm J, \pm K$ эти три матрицы порождают группу *кватернионных единиц* $Q_8 \stackrel{\text{def}}{=} \{\pm E, \pm I, \pm J, \pm K\}$ порядка 8, и $\mathrm{SL}_2(\mathbb{F}_3)' = Q_8$.

Упр. 19.12. Пусть $g \in A_n$, $h \in S_n \smallsetminus A_n$. Всякая перестановка, сопряжённая g в S_n, сопряжена в A_n либо g, либо $\mathrm{Ad}_h g$. Равенство $\mathrm{Ad}_p g = \mathrm{Ad}_h g$ равносильно равенству $\mathrm{Ad}_{p^{-1}h} g = g$. Поэтому существование чётной перестановки p удовлетворяющей первому равенству равносильно существованию нечётной перестановки $p^{-1}h$, коммутирующей с g, т. е. класс сопряжённости перестановки g в S_n не распадается на два класса сопряжённости в A_n если и только если централизатор $Z(g)$ содержит нечётную перестановку. Когда в цикловом типе g есть строка чётной длины или две строки одинаковой нечётной длины, то такая перестановка есть, а если g является произведением попарно разных циклов нечётной длины, то — нет.

Упр. 19.13. Правая часть равенства $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, приведённая по модулям 3, 4 и 5, равна, соответственно, $1 - \varepsilon_3$, $1 - \varepsilon_4$ и $1 + 2(\varepsilon_1 + \varepsilon_2)$. Она может делиться на 3 или на 4 только если $\varepsilon_3 = 1$ или $\varepsilon_4 = 1$. В обоих случаях $|H| \geqslant 16$, так что $|H|$ не может быть ни 3, ни 4, ни $3 \cdot 4$, ни $3 \cdot 5$. Если $|H|$ делится на 5, то $\varepsilon_1 = \varepsilon_2 = 1$ и $|H| \geqslant 25$, так что $|H|$ не может быть ни 5, ни $4 \cdot 5$. Остаются ровно две возможности: $|H| = 1$ и $|H| = 3 \cdot 4 \cdot 5$.

Упр. 19.16. $a_1 n_1 a_2 n_2 n_1^{-1} a_1^{-1} n_2^{-1} a_2^{-1} = (a_1 n_1 a_1^{-1})(a_1 a_2 n_2 n_1^{-1} a_1^{-1} a_2^{-1})(a_2 n_2^{-1} a_2^{-1})$. Так как N нормальна, а A абелева, заключённые в скобки слагаемые лежат в N.

Упр. 19.17. При эпиморфизме S_4 на группу треугольника из прим. 18.12 на стр. 337 подгруппа чётных перестановок $A_4 \subset S_4$ переходит в группу вращений треугольника.

Упр. 19.18. Не вполне очевидно, разве что последнее равенство

$$(Q_k \cap P_i) \cap ((Q_{k+1} \cap P_i)P_{i+1}) = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})\,.$$

Левая часть содержит правую, поскольку $Q_{k+1}Q_k \subset Q_k$ и $P_iP_{i+1} \subset P_i$. Правая часть содержит левую, так как если элемент $c \in Q_k \cap P_i$ имеет вид $c = ab$, где $a \in Q_{k+1} \cap P_i$, $b \in P_{i+1}$, то $b = a^{-1}c$ лежит в Q_k, а значит, и в $Q_k \cap P_{i+1}$.

Упр. 19.19. $\mathbb{Z}/(p^n) \supsetneq A_1 \supsetneq \ldots \supsetneq A_{n-1} \supsetneq 0$, где $A_k = \{[zp^{k-1}] \in \mathbb{Z}/(p^n) \mid z \in \mathbb{Z}\}$.

Упр. 19.21. Проверка ассоциативности:

$$\big((x_1,h_1)\cdot(x_2,h_2)\big)\cdot(x_3,h_3) = \big(x_1\psi_{h_1}(x_2)\,,\ h_1h_2\big)\cdot(x_3,h_3) = \big(x_1\psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)\,,\ h_1h_2h_3\big)$$
$$(x_1,h_1)\cdot\big((x_2,h_2)\cdot(x_3,h_3)\big) = (x_1,h_1)\cdot\big(x_2\psi_{h_2}(x_3)\,,\ h_2h_3\big) = \Big(x_1\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big)\,,\ h_1h_2h_3\Big)\,.$$

Но $\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big) = \psi_{h_1}(x_2)\psi_{h_1} \circ \psi_{h_2}(x_3) = \psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)$. Существование единицы:

$$(x,h)\cdot(e,e) = (x,\psi_h(e),he) = (x,h)\,,$$

поскольку $\psi_h(e) = e$ в силу того, что ψ_h гомоморфизм. Существование обратного:

$$\big(\psi_h^{-1}(x^{-1})\,,\ h^{-1}\big)\cdot(x,h) = \big(\psi_h^{-1}(x^{-1})\psi_h^{-1}(x^{-1})\,,\ h^{-1}h\big) = (e,e)\,.$$

Упр. 19.22. Так как $\psi\colon\ H \to \operatorname{Aut} N$ — гомоморфизм, $\psi_e = \mathrm{Id}_N$ и

$$(x_1,e)\cdot(x_2,e) = (x_1\psi_e(x_2),e) = (x_1x_2,e)\,,$$

т. е. элементы (x,e) образуют подгруппу, изоморфную N. Она нормальна, поскольку

$$(y,h)\cdot(x,e)\cdot\big(\psi_h^{-1}(y^{-1}),h^{-1}\big) = (y\psi_h(x),h)\cdot\big(\psi_h^{-1}(y^{-1}),h^{-1}\big) = \big(y\psi_h(x)y^{-1},e\big)\ .$$

Элементы (e,h) очевидно образуют дополнительную подгруппу, изоморфную H, и

$$\mathrm{Ad}_{(e,h)}(x,e) = (\psi_h(x),e)\,.$$

Упр. 19.25. Пусть центр $Z(G) = C$. Если $|C| = p$, то $C \simeq \mathbb{Z}/(p) \simeq G/C$. Пусть $a \in C$ — образующая центра, а $b \in G$ — такой элемент, что смежный класс bC является образующей в G/C. Тогда любой элемент группы имеет вид b^ka^m. Так как a централен, любые два таких элемента коммутируют.

Упр. 19.26. Аддитивные автоморфизмы группы $\mathbb{Z}/(p)$ суть линейные автоморфизмы одномерного векторного пространства над полем $\mathbb{F}_p$. Они образуют группу $\mathrm{GL}_1(\mathbb{F}_p) \simeq \mathbb{F}_p^\times$ ненулевых элементов поля $\mathbb{F}_p$ по умножению. Как и всякая конечная мультипликативная подгруппа поля, она циклическая[1].

Упр. 20.1. Первое очевидно, второе вытекает из того, что при вставке фрагмента $x^\varepsilon x^{-\varepsilon}$ в произвольное слово w получится такое слово, в котором сокращение любого фрагмента вида $y^\varepsilon y^{-\varepsilon}$ приведёт либо обратно[2] к слову w, либо к слову, получающемуся из w сначала сокращением *того же самого фрагмента* $y^\varepsilon y^{-\varepsilon}$, а уже затем вставкой $x^\varepsilon x^{-\varepsilon}$ в *то же самое место*, что и в w.

[1] См. сл. 3.3 на стр. 56.

[2] Обратите внимание, что такое происходит *не только* при сокращении того же самого фрагмента $x^\varepsilon x^{-\varepsilon}$, который был перед этим вставлен, но и при сокращении одной из букв $x^{\pm\varepsilon}$ с её соседкой.

Упр. 20.2. Отобразите $n \in \mathbb{N}$ в $x^n y x^n \in F_2$ и воспользуйтесь предл. 20.1 на стр. 364.

Упр. 20.3. Поскольку отображение $F\colon \mathbb{R}^n \to \mathbb{R}^n$ биективно, достаточно убедиться, что отображения $\sigma_{F(\pi)}$ и $F \circ \sigma_\pi \circ F^{-1}$ одинаково действуют на точку вида $F(p)$ с произвольным $p \in \mathbb{R}^n$.

Упр. 20.4. Обозначим через v_i вектор, идущий из центра симплекса Δ в вершину i. Вектор $n_{ij} = v_i - v_j$ ортогонален гиперплоскости π_{ij}, поскольку для любого $k \neq i, j$ скалярное произведение $\big(n_{ij}, v_k - (v_i + v_j)/2\big) = (v_i, v_k) - (v_j, v_k) + (v_i, v_i)/2 - (v_j, v_j)/2 = 0$, т. к. все произведения (v_i, v_j) с $i \neq j$ и все скалярные квадраты (v_i, v_i) одинаковы. Аналогичная выкладка показывает, что при $\{i, j\} \cap \{k, m\} = \varnothing$ векторы n_{ij} и n_{km} ортогональны. Векторы $v_i - v_k$ и $v_k - v_j$ образуют в натянутой на них двумерной плоскости стороны правильного треугольника с вершинами в концах векторов v_i, v_j и v_k, и угол между ними равен 60°.

Упр. 20.8. Эта группа является подгруппой группы перестановок корней.

Упр. 20.11. Минимальный угол между зеркалами не может быть тупым, и прямой он только когда есть всего два ортогональных зеркала. Если угол $\measuredangle(a_i, a_j)$ тупой, векторы a_i, a_j разделяются зеркалом. Нормальный вектор этого зеркала можно выбрать лежащим внутри угла с направляющими векторами a_i и $-a_j$, т. е. имеющим вид $\alpha a_i - \beta a_j$, где $\alpha, \beta > 0$. Если угол $\measuredangle(a_i, a_j)$ острый, то угол между векторами a_i и $-a_j$ тупой, а значит, между ними есть зеркало с направляющим вектором, лежащим между векторами a_i, a_j, т. е. имеющим вид $\alpha a_i + \beta a_j$, где $\alpha, \beta > 0$.

Упр. 20.12. Пусть точки $x \in a_i^\perp$, $y \in a_j^\perp$ таковы, что $(a_k, x) > 0$ для всех $a_k \in \Phi_v^+$ с $k \neq_i$ и $(a_k, y) > 0$ для всех $a_k \in \Phi_v^+$ с $k \neq_i$. Тогда их ортогональные проекции на плоскость Ψ_{ij} лежат на сторонах $a_i^\perp$, $a_j^\perp$ угла $a_i^+ \cap a_j^+$, и проекция отрезка $[x, y]$ не пересекает ни одной прямой $a_k^\perp$ с $k \neq i, j$.

Упр. 20.13. Совпадение линейной оболочки корней a_i со всем пространством V равносильно равенству $\bigcap a_i^\perp = 0$. С другой стороны, множество неподвижных относительно всей группы G векторов пространства V тоже является пересечением этих зеркал.

Упр. 20.14. Пусть $a_r = \sum\limits_{i<r} \lambda_i a_i + \sum\limits_{j>r} \lambda_j a_j$, где все $\lambda_i \leqslant 0$ и некоторые из них строго положительны. Выражая векторы a_j через векторы a_i с положительными коэффициентами, получим равенство вида $\mu a_r = \sum\limits_{i<r} \mu_i a_i$, в котором все $\mu_i \geqslant 0$ и некоторые из них строго положительны. Скалярно умножая обе части на произвольный вектор $v \in C_e$, получим справа строго положительное число. Поэтому $\mu \cdot (v, a_r) > 0$, и $\mu > 0$, так как $(v, a_r) > 0$. Тем самым, вектор a_r линейно выражается с положительными коэффициентами через векторы $a_1, \ldots, a_{r-1}$, и мы должны были бы его выкинуть.

Упр. 20.15. Скалярный квадрат стоящего в обоих частях вектора

$$\Big(\sum_\alpha \lambda_{i_\alpha} a_{i_\alpha}, \sum_\beta \mu_{j_\beta} a_{j_\beta}\Big) = \sum_{\alpha,\beta} \lambda_{i_\alpha} \mu_{j_\beta} \left(a_{i_\alpha}, a_{j_\beta}\right) \leqslant 0$$

в силу неравенств $(a_i, b_j) \leqslant 0$. Поэтому и этот вектор, и все слагаемые в предыдущей формуле нулевые.

Упр. 20.17. Связные компоненты графа как раз и отвечают взаимно ортогональным подмножествам корней.

Упр. 20.18. Выкинем из графов все остальные вершины вместе с приходящими в них рёбрами и обозначим через a_1, a_2, a_3, … корни, отвечающие вершинам оставшегося графа, прочитанным слева направо. Для первого графа матрица Грама векторов $u = a_1 + 2a_2$, $w = 2a_3 + a_4$

имеет

$$\det\begin{pmatrix} 5+4(a_1,a_2) & 4(a_2,a_3) \\ 4(a_2,a_3) & 5+4(a_3,a_4) \end{pmatrix} = \det\begin{pmatrix} 3 & -4\cos\left(\frac{\pi}{m}\right) \\ -4\cos\left(\frac{\pi}{m}\right) & 3 \end{pmatrix} = 9 - 16\cos^2\left(\frac{\pi}{m}\right) < 0$$

при[1] $m \geqslant 5$, где $m-2$ — число рёбер между второй и третьей вершинами. Для остальных трёх графов нулевой или отрицательный определитель Грама будут иметь векторы

$$\begin{aligned} u &= a_1 + 2a_2 \quad & w &= 2a_3 + a_4 + a_5\,, \\ u &= a_1 & w &= 2a_2 + a_3 + a_4 + a_5\,, \\ u &= a_1 & w &= 2a_2 + a_3\,. \end{aligned}$$

Упр. 20.20. Если $u = \sum x_i e_i \in E$, то $(u,u) = \sum x_i^2 = \left(\sum x_i\right)^2 - 2\sum_{i<j} x_i x_j$ чётно, а $(u,w) = \sum x_i/2 \in \mathbb{Z}$. Поэтому $(z_1u + z_2w, z_1u + z_2w) = z_1^2(u,u) + 2z_1z_2(u,w) + 2z_2^2$ чётно.

[1] Напомню, что $\cos(\pi/5) = (1+\sqrt{5})/4$.