Лекция 5
Язык векторов

▷Векторное и аффинное координатные пространства k^n ▷Системы линейных уравнений и подпространства ▷Модули, абелевы группы, векторные пространства ▷Образующие, линейная зависимость, базисы и координаты ▷Свободные модули, гомоморфизмы и соотношенгия ▷Теоремы о базисах конечномерных векторных пространств ▷Замены базисов и матрицы перехода ▷Задание гомоморфизмов матрицами ▷Ранг матрицы

§1. Координатные пространства

1.1. Алгебраизация основаниий геометрии. В этой лекции мы рассмотрим алгебраическую структуру, аксиоматизирующую геометрические представления о пространстве. Из школы Вам уже должны быть известны два пути для внедрения алгебры в геометрию: векторы и координаты. Оба дают возможность алгебраически вычислять с линейными геометрическими объектами: точками, прямыми, плоскостями и т. п. Векторы и координаты в школьном курсе обычно возникают на основе уже довольно далеко продвинутой геометрической техники, а их свойства в конечном итоге выводятся из Евклидовых аксиом планиметрии (или стереометрии). С алгебраической точки зрения намного удобнее обратить этот порядок, и с самого начала аксиоматизировать свойства векторов, взяв их за основу для дальнейшего построения геометрии.

В этих лекциях у нас не будет времени для подобного сравнения оснований геометрии по Евклиду и на основе аксиом векторнго пространства[1]. Тем не менее, мы настоятельно рекомендуем читателю следующие две вещи.

Во-первых, всюду далее при слове *вектор* черезвычайно полезно иметь в виду именно самый обычный школьный геометрический вектор, а *векторное пространство* представлять себе как множество "свободных векторов" (которые можно откладывать от любой точки), живущих в обычном школьном геометрическом пространстве.

Во-вторых, алгебраическое построение оснований геометрии позволяет геометризовать многие, на первый взгляд, негеометричные задачи, ибо на языке векторов и координат объяснить, что такое "n-мерная геометрия" или что такое "конечная геометрия над полем из q элементов" ничуть не сложнее, чем объяснить, что такое 3-мерное пространство Евклида.

1.2. Векторное и аффинное координатные пространства. Мы начнём с основного

[1] интересующиеся могут прочесть о нём в лекции 33 из книги: *М. М. Постников. Лекции по геометрии. 1-й семестр.* М., "Наука", 1986 (второе, "синее" издание).

модельного примера, непосредственно обобщающего школьные представления о координатах. Напомню, что если ввести в пространстве систему координат (скажем, декартовых) с центром в некоторой точке O, то каждой точке $P = (p_1, p_2, p_3)$ можно сопоставить радиус-вектор $\overrightarrow{OP}$, задав тем самым биекцию между точками пространства и векторами. При этом каждый вектор $p = \overrightarrow{OP}$ приобретет координаты — декартовы координаты своего конца (p_1, p_2, p_3). Хорошо известно, что действия над векторами легко описываются в терминах этих координат: при сложении векторов их соответственные координаты складываются, а при умножении на число — умножаются на это число. Обобщение этой конструкции напрашивается само собой.

1.3. Определение. *Множество всех матриц-столбцов высоты n с элементами из k вместе с операциями сложения векторов и умножением векторов на числа $\lambda \in k$:*

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \qquad \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \stackrel{\text{def}}{=} \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

называется координатным векторным пространством над полем k и обозначается k^n. Координатные столбцы $v \in k^n$ называются n-мерными векторами.

1.4. Определение. *То же самое множество всех матриц-столбцов высоты n с элементами из k называется n-мерным аффинным*[2] *координатным пространством $\mathbb{A}_n = \mathbb{A}_n(k)$ (а его элементы — точками) над полем k, если оно рассматривается вместе с операцией откладывания векторов $v \in k^n$ от точек $P \in \mathbb{A}_n$:*

$$+ : \mathbb{A}_n \times k^n \longrightarrow \mathbb{A}_n \ : \quad (P, v) = \left(\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}, \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right) \longmapsto P + v \stackrel{\text{def}}{=} \begin{pmatrix} p_1 + v_1 \\ p_2 + v_2 \\ \vdots \\ p_n + v_n \end{pmatrix} \in \mathbb{A}_n \quad .$$

Отметим, что хотя точки и векторы обозначаются одинаково (таково уж неприятное свойство координат), разница между ними та же, что и в школьной геометрии: с векторами можно вычислять, а из точек — составлять геометрические фигуры. Если в аффинном пространстве $\mathbb{A}_n$ зафиксировать какую-либо точку O (так называемое *начало отсчёта*), то можно установить взаимно-однозначное соответствие между точками и векторами, сопоставляя каждой точке $P \in \mathbb{A}_n$ её *радиус-вектор*

$$\overrightarrow{OP} \stackrel{\text{def}}{=} v \in k^n \quad \text{такой что} \quad O + v = P \ .$$

Это соответствие позволяет переводить геометрические построения с языка точек на язык векторов и наоборот.

1.5. Некоторые примеры из аффинной геометрии. Удобно представлять себе n-мерное аффинное пространство $\mathbb{A}_n$ вместе с системой координат с центром в нулевом столбце

[2] слово "аффинный", как показывает его орфография, не имеет ни малейшего отношения к Греции, а является всего лишь бесхитросной калькой с английского affine – "ассоциированный"

и координатными осями, каждая из которых напрвленна вдоль соответствующего базисного вектора e_i, у которого все координаты, кроме i-той, нулевые, а i-тая координата равна 1.

Задача 5.1. Сколько координатных "октантов" имеет описанная выше система координат?

Задача 5.2. Рассмотрим единичный стандартный 4-мерный куб в $\mathbb{A}_4(\mathbb{R})$ (натянутый на четыре базисных координатных вектора). Сколько у него:

а) i-мерных граней ($i = 0, 1, 2, 3$);

б) внутренних (т. е. не лежащих на гранях) диагоналей?

При помощи векторов нетрудно определить в $\mathbb{A}_n(k)$ линейные геометрические объекты: прямые, плоскости и т. п. Так *прямая*, проходящая через точку $P \in \mathbb{A}_n$ вдоль вектора $v \in k^n$ есть множество всех точек вида

$$Q(t) = P + tv \ ,$$

где p пробегает k (механическая аналогия: частица, движущаяся с постоянной скоростью v и в начальный момент времени $t = 0$ находящаяся в точке P, в произвольный момент времени t находится в точке $Q(t)$).

Задача 5.3. Докажите, что две прямые либо пересекаются по одной точке, либо совпадают, либо не пересекаются вообще.

Задача 5.4. Пусть $k = \mathbb{Z}/p\mathbb{Z}$ - конечное поле. Сколько всего имеется в $\mathbb{A}_n(k)$:

а) точек;

б) прямых, проходящих через фиксированную точку;

в) всего прямых?

(если общий случай вызывает затруднения, рассмотрите $n = 2.3.4$).

Аналогично, плоскость в $\pi \subset \mathbb{A}_n$ можно определить как множество точек вида

$$Q(s, t) = P + su + tv \ ,$$

где $P \in \pi$ — некоторая фиксированная начальная точка, $u, v \in k^n$ — фиксированная пара не пропорциональные друг другу векторов, параллельных плоскости, а s, t независимо пробегают k (их можно воспринимать как координаты на плоскости π).

Определения прямой и плоскости являются частными случаями более общего понятия *подпространства.*

1.6. Векторные подпространства и однородные линейные уравнения. Подмножество векторов $V \subset k^n$ называется *векторным подпространством*, если оно замкнуто относительно сложения векторов и умножения векторов на числа. Примером векторного подпространства является множество $W = W(v_1, v_2, \ldots, v_m)$, состоящее из всех векторов $w \in k^n$, представимых в виде $w = \sum t_i v_i$, где $(v_1, v_2, \ldots, v_n)$ есть фиксированный набор векторов из k^m, а числовые параметры $(t_1, t_2, \ldots, t_m)$ независимо пробегают k. Векторы $(v_1, v_2, \ldots, v_m)$ в этом случае называются *порождающими* подпространство W. Другой пример приходит из прошлой лекции

1.6.1. Предложение. *Пусть над полем k задана система из s однородных линейных уравнений от n неизвестных:*

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0 \ ,$$

где A — матрица размера $n \times s$ над полем k. Тогда множество её решений представляет собой векторное подпространство в k^n.

Доказательство. Действительно, если $a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$ и $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ — решения, то

$$\begin{aligned} A \cdot (a+b) &= A \cdot a + A \cdot b = (0) + (0) = (0) \\ A \cdot (\lambda a) &= \lambda A \cdot a = \lambda(0) = (0)\ , \end{aligned}$$

где через (0) обозначен нулевой вектор-столбец. Тем самым $a+b$ и λa — также решения.
□

Отметим, что описанный в прошлой лекции способ решения линейных систем над полем при помощи приведения их матрицы к ступенчатому виду доставляет алгоритм для отыскани порождающих векторов в подпространстве, заданном системой однородных линейных уравнений.

1.7. Аффинные подпространства и неоднородные линейные уравнения. Назовём *аффинным подпространством* в $\mathbb{A}_n$ всякое подмножество $\pi(P, W) \subset \mathbb{A}_n$, которое состоит из всех точек вида $P + v$, где $P \in \mathbb{A}_n$ —некоторая фиксированныя точка, а векторы v пробегают некоторое фиксированное векторное подпространство $W \subset k^n$. Говорят также, что $\pi(P, W)$ есть *аффинная (гипер)плоскость*, проходящая через точку P и параллельная подпространству W. Рассматривавшиеся выше прямые и плоскости доставляют примеры аффинных подпространств. Другие примеры вновь приходят из прошлой лекции.

1.7.1. Предложение. *Множество решений неоднородной системы $Ax = b$ из s линейных уравнений с n неизвестными либо пусто, либо является аффинной гиперплоскостью вида $\pi(a, W)$, где $a \in \mathbb{A}_n$ – какое-либо одно решение неоднородной системы, а $W \subset k^n$ есть векторное подпространство решений однородной системы $Ax = (0)$ с той же матрицей A.*

Доказательство. Пусть $a \in \mathbb{A}_n$ — решение системы $Ax = b$. Поскольку равенство $Aa' = b$ равносильно тому, что $a' = a + w$, где $w \in k^n$ удовлетворяет равенству $Aw = Aa' - Aa = b - b = 0$, откладывание векторов $w \in k^n$, являющихся решениями однородной системы $Ax = (0)$, от точки a задает биекцию между множеством решений системы $Ax = b$ и множеством решений системы $Ax = 0$.
□

Отметим, что описанное в прошлой лекции решение неоднородных систем вновь может восприниматься как переход от неявного задания аффинной гиперплоскости к явному её заданию.

> Задача 5.5. Выясните, как устроены сечения 4-мерного куба из зад.5.2 3-мерными плоскостями $x_1 + x_2 + x_3 + x_4 = d$, где $0 \le d \le 4$.

§2. Модули

2.1. Определение модуля. Пусть K – коммутативное кольцо с единицей. *K-модулем* называется всякое множество V (элементы которого называются *векторами*), наделенное бинарной операцией сложения векторов

$$+ : V \times V \longrightarrow V \quad : \qquad (v, w) \longmapsto v + w \in V$$

и операцией умножения векторов на числа из K:

$$\cdot : K \times V \longrightarrow V \quad : \qquad (\lambda, v) \longmapsto \lambda v \in V \ ,$$

так что выполнены аксиомы:

Аксиомы K-модуля

1) Аксиомы сложения векторов

   а) коммутативность: $a + b = b + a \quad \forall a, b \in V$

   б) ассоциативность: $a + (b + c) = (a + b) + c \quad \forall a, b, c \in V$

   в) существование нуля: $\exists 0 \in V : \ a + 0 = a \quad \forall\, a \in k$

   г) существование противоположного: $\forall a \in V \quad \exists (-a) \in V : \quad a + (-a) = 0$

2) Аксиомы умножения векторов на числа

   а) ассоциативность: $\lambda(\mu a) = (\lambda\mu)a \quad \forall\, a \in V \ , \ \forall\, \lambda, \mu \in K$

   б) дистрибутивность по отношению к сложению чисел:

$$(\lambda + \mu)a = \lambda a + \mu a \qquad \forall\, a \in V \ , \ \forall\, \lambda, \mu \in K$$

   в) дистрибутивность по отношению к сложению векторов:

$$\lambda(a + b) = \lambda a + \lambda b \qquad \forall\, \lambda \in K \ , \ \forall\, a, b \in K$$

   г) умножение на единицу $1 \in K$: $\quad 1 \cdot a = 1 \qquad \forall\, a \in V$.

2.1.1. Частный случай: векторные пространства. Если $K = k$ — поле, то k-модули называются *векторными пространствами* над k, и термин “k-модуль” в этой ситуации практически не употребляется.

Задача 5.6. Проверьте, что координатное пространство k^n удовлетворяет аксиомам векторного пространства.

2.1.2. Частный случай: абелевы группы. Если на множестве A задана бинарная операция сложения

$$+ : A \times A \longrightarrow A \quad : \qquad (a, b) \longmapsto a + b \in A \ ,$$

которая удовлетворяет всем четырем аксиома сложения векторов, то A называют *абелевой группой*. Иначе говоря, абелева группа — это векторное пространство, в котором “исключили из рассмотрения” умножение на числа.

Тем не менее, абелевы группы являются частными случаями модулей, а именно, модулями над кольцом $K = \mathbb{Z}$, ибо умножение на *целые* числа есть внутреннее свойство абелевой группы: всегда можно считать по определению, что

$$n \cdot a \overset{\text{def}}{=} \begin{cases} \underbrace{a + a + \cdots + a}_{n} \ , & \text{при} \quad n \geq 0 \\ \underbrace{-a - a - \cdots - a}_{-n} , & \text{при} \quad n < 0 \end{cases} \qquad \forall\, n \in \mathbb{Z} \ , \ \forall\, a \in A \ .$$

Задача 5.7. Проверьте выполнение аксиом $\mathbb{Z}$-модуля.

Приведённый выше список аксиом, как обычно, можно дополнить несколькими интуитивно ожидаемыми свойствами векторов, формально вытекающими из аксиом:

Задача 5.8. Докажите, что в любой абелевой группе 0 единственен, а противоположный элемент $(-a)$ к элементу a однозначно определяется по a.

Задача 5.9. Докажите, что в любом K-модуле V справедливы равенства:
а) $0 \cdot v = 0 \in V \quad \forall v \in V$;
б) $\lambda \cdot 0 = 0 \quad \forall \lambda \in K$;
в) $(-1) \cdot v = (-v) \in V \quad \forall v \in V$.

2.2. Определение. *Отображение $\varphi\colon\ V_1 \longrightarrow V_2$ между двумя K-модулями V_1 и V_2 называется* ***гомоморфизмом*** *K-модулей (или* ***K-линейным отображением****), если оно перестанофочно со сложением векторов и умножением векторов на числа:*

$$\varphi(v + w) = \varphi(v) + \varphi(w) \quad \text{и} \quad \varphi(\lambda v) = \lambda\varphi(v) \quad , \qquad \forall \lambda \in K \ , \forall v, w \in V \quad .$$

Гомоморфизм модулей $V \xrightarrow{\varphi} W$ называется ***мзоморфизмом****, если он обратим, т. е. существует гомоморфизм модулей $W \xrightarrow{\psi} V$, такой, что $\psi\varphi$ и $\varphi\psi$ – тождественные отображения. Эпиморфизмы и мономорфизмы — это гомоморфизмы, которые на уровне множеств являются отображениями "на" и "в" соответственно.*

Задача 5.10. Докажите, что для любой гомоморфизма K-модулей $V \xrightarrow{\varphi} W$ обладает следующими свойствами:

а) $\varphi(0) = 0$ б) $\varphi(-w) = -\varphi(w)$ в) $\varphi(v - w) = \varphi(v) - \varphi(w)$.

Как и для гомоморфизма колец, подмножества

$$\ker(\varphi) = \{\, v \in V \mid \varphi(v) = 0 \,\} \qquad \text{и} \qquad \mathrm{im}\,(\varphi) = \{\, w \in W \mid \exists v \in V\colon\ \varphi(v) = w \,\}$$

называются, соответственно, ***ядром*** и ***образом*** гомоморфизма $V \xrightarrow{\varphi} W$. В этих терминах эпиморфность φ означает равенство $\mathrm{im}\,\varphi = W$, а критерием мономорфности является

2.2.1. Предложение. $\ker(\varphi) = \{0\}$ *тогда и только тогда, когда $V \xrightarrow{\varphi} W$ — мономорфизм.*

Доказательство. Равенство $\varphi(v_1) = f(v_2)$ равносильно тому, что $v_1 - v_2 \in \ker\varphi$, ибо $\varphi(v_1 - v_2) = \varphi(v_1) - f(v_2)$.
□

2.2.2. Предложение. *Если $V \xrightarrow{\varphi} W$ – гомоморфизм модулей, то $\ker(\varphi)$ является подмодулем в V, а $\mathrm{im}\,(\varphi)$ – подмодулем в W.*

Доказательство. Чтобы проверить, что подмножество M является подмодулем в модуле V, достаточно проверить, что $\forall \lambda, \mu \in K$ и $\forall u, v \in K$ комбинация $\lambda u + \mu v$ также лежит в M. Если $\varphi(u) = \varphi(v) = 0$, то $\varphi(\lambda u + \mu v) = \lambda\varphi(u) + \mu\varphi(v) = 0$. Если $w_1 = \varphi(v_1)$ и $w_2 = \varphi(v_2)$, то $\lambda w_1 + \mu w_2 = \lambda\varphi(v_1) + \mu\varphi(v_2) = \varphi(\lambda v_1 + \mu v_2)$.
□

2.3. Примеры векторных пространств и модулей. Как мы уже видели в зад.5.6, примером векторного пространства является координатное векторное пространство из предыдущего параграфа. Рассмотрим некоторые другие примеры.

2.3.1. Многочлены. Ясно, что $K[x]$ является K-модуль. Все многочлены, степень которых не превосходит некоторого фиксированного числа, также образуют K-модуль[3], который уже не является кольцом. Мы далее будем обозначать этот модуль через $P_n = P_n(K)$.

Задача 5.11. Постройте изоморфизм пространства многочленов степенеи не выше n с коэффициентами из поля k с координатным пространством $k^{(n+1)}$.

Отображение $k[x] \xrightarrow{d/dx} k[x]$ (k – поле), сопоставляющее каждому многочлену его производную, является K-линейным эндоморфизмом пространства многочленов[4]. Если $\mathit{char}\,(k) = 0$, то его образ совпадает со всем пространством (почему?), а ядро есть пространство многочленов степени нуль (почему?).

Задача 5.12. Опишите $\ker(d/dx)$ и $\mathrm{im}\,(d/dx)$, если $\mathit{char}\,(k) = p \neq 0$.

Пусть $f(x) \in k[x]$ — некий многочлен степени n. Отображение res_f, сопоставляющее каждому многочлену $g(x) \in k[x]$ его остаток от деления на f, является гомоморфизмом k-модулей, отображающим $k[x]$ на пространство P_{n-1} многочленов степени не выше, чем $(n-1)$. Этот гомоморфизм сюръективен, а его ядро совпадает с идеалом $(f) \in k[x]$.

Задача 5.13. Убедитесь, что отображение $\varphi\colon\ k[x]/(f) \longrightarrow P_{n-1}$, переводящее класс $g(\bmod f)$ в $\mathit{res}_f(g)$ корректно определено и является изоморфизмом векторных пространств.

2.3.2. Расширения полей. Если $k \subset K$ — расширение полей, то поле K часто бывает удобно рассматривать как векторное пространство над k. Если $K = k[\vartheta]$ – алгебраическое расширение при помощи элемента ϑ, удовлетворяющего минимальному уравнению

$$Q(\vartheta) = \vartheta^n + q_1\vartheta^{n-1} + \cdots + q_{n-1}\vartheta + q_n = 0$$

степени n с коэффициентами из k, то K как векторное пространство над k, изоморфно координатному пространству k^n. В самом деле, во лекции 3 мы видели, что элементы поля K однозначно записываются многочленами от ϑ степени $\leq (n-1)$, причём такое представление согласовано со сложением и умножением на числа из k. Сопоставляя многочлену столбец его коэффициентов, мы и получим изоморфизм между K и k^n. В частности, если поле k — конечное поле из q элементов, то поле K будет полем из q^n элементов.

Задача 5.14. Докажите, что число элементов в любом конечном поле является степенью простого числа.

Указание: представьте конечное поле как расширение простого подполя при помощи одного алгебраического элемента, или дождитесь Пр.3.7.1

Если K является конечным алгебратческим расширениям поля $\mathbb{Q}$, то его можно воспринимать как полноценное геометрическое пространство, в котором можно заниматься "настоящей" наглядной геометрией, что позволяет элегантно доказывать трудные арифметические теоремы и вылилось в настоящее время в целую науку, именуемую *геометрией чисел.*

2.3.3. Модули и идеалы. Если отвлечься от геометрии, то с алгебраической точки зрения модуль есть обобщение идеала. Действительно, сопоставление определений показывает, что подмножество $I \subset K$ тогда и только тогда является K-подмодулем, когда I — это идеал в K. В лекциях 2,3 мы задавали идеалы *образующими*, т. е. представляли их в виде

$$I = (a_1, a_2, \ldots, a_m) = a_1K + a_2K + \cdots a_mK\ .$$

Модули тоже удобно задавать образующими (или *порождающими*) элементами (ср. с n° 1.6).

[3]отметим, что множество всех многочленов строго фиксированной степени не является K-модулем

[4]аналогично, интегрирование, переход к пределу и т. д. также являются линейными отображениями в соответствующих пространствах функций

§3. Образующие, базисы и линейная зависимость.

3.1. Образующие. Про (возможно бесконечный) набор векторов $\{v_i\}$ K-модуля V говорят, что он *порождает* V, если каждый вектор $v \in V$ можно представить в виде *конечной линейной комбинации* векторов v_i с коэффициентами из K, т. е. записать в виде:

$$v = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n \qquad \text{с} \quad x_i \in K\ . \tag{5-1}$$

Векторы v_i в этом случае называются *образующими* модуля V над K.

Модуль называется *конечно порожденным*, если он допускает конечное множество образующих.

3.2. Базисы и координаты. Набор векторов $\{e_i\} \subset V$ (возможно бесконечный) называется *базисом*, если он порождает V и для любого $v \in V$ существует *ровно одно* разложение (5-1): $v = \sum x_i e_i$, т. е. из равенства

$$\sum x_i e_i = \sum y_i e_i$$

вытекает, что $x_i = y_i\ \forall i$. При этом коэффициенты x_i разложения $v = \sum x_i e_i$ называются *координатами* вектора v в базисе e_i. Модули, обладающие базисом, называются *свободными.*

3.3. Линейная зависимость. Набор векторов $\{v_i\}$ в K-модуле V называется *линейно-независимым*, если из того, что конечная линейная комбинация $\sum \lambda_i v_i$ векторов из этого набора равна нулевому вектору, вытекает, что все коэффициенты λ_i — нулевые.

Напротив, если для некоторых x_i, среди которых есть ненулевые, выполнено равенство $\sum x_i v_i = 0$, то набор $\{v_i\}$ называется *линейно-зависимым*, а само это соотношение называется *линейной зависимостью.*

3.3.1. Предложение. *Порождающий набор векторов тогда и только тогда является базисом, когда он линейно независим.*

Доказательство. Если $\sum \lambda_i e_i = 0$ и не все λ_i нулевые, то всякий вектор $v = \sum x_i e_i$ можно *иначе* разложить в виде $v = \sum (x_i + \lambda_i) e_i$.

Наоборот, если $v = \sum x_i e_i = \sum y_i e_i$ — два различных представления одного вектора, то перенося праую часть в середину, получаем линейную зависимость $\sum (x_i - y_i) v_i = 0$.
□

3.4. Кручение. Разумеется, неверно, что любой модуль свободен. Простейшим[5] препятствием к свободе является кручение. Элемент v K-модуля V называется *элементом кручения*, если $v \neq 0$ и набор $\{v\}$, состоящий из одного этого вектора, линейно зависим, т. е. $\lambda v = 0$ для некоторого ненулевого $\lambda \in K$.

Если $I \subset K$ - идеал в K, то элементы кручения в K-модуле I — это в точности делители нуля в I. Но даже если K — это целостное кольцо, K-модули, не являющиеся идеалами, вполне могут иметь кручение.

Например, множество вычетов $\mathbb{Z}/n\mathbb{Z}$ с операцией сложения является абелевой группой, а стало быть, $\mathbb{Z}$-модулем. Более того, он может быть порождён над $\mathbb{Z}$ одним элементом.

> Задача 5.15. Докажите, что если m взаимно просто с n, то класс $v(\bmod n)$ порождает $\mathbb{Z}$-модуль $\mathbb{Z}/n\mathbb{Z}$.

Вместе с тем, все элементы в $\mathbb{Z}/n\mathbb{Z}$ являются элементами кручения, ибо $\forall\, a \in \mathbb{Z}\ /n\mathbb{Z}$, класс $na(\bmod n)$ равен нулю в $\mathbb{Z}/n\mathbb{Z}$, хотя $n \neq 0$ в $\mathbb{Z}$. Поэтому любой набор векторов из $\mathbb{Z}/n\mathbb{Z}$ линейно зависим, и значит, в этом модуле нет базиса.

[5] но, конечно, не единственным

Задача 5.16. Докажите, что все элементы кручения вместе с нулевым вектором составляют подмодуль в любом K-модуле V над произвольным коммутативным кольцом K (он обозначается $Tors(V)$ и называется *подмодулем кручения*)

3.5. Конечно порождённые свободные модули. Координатный модуль K^n определяется для произвольного коммутативного кольца K дословно также, как и координатное пространство k^n. Отметим, что как множество он совпадает с n-кратной прямой суммой кольца K самого с собой, но мы забываем часть мультипликативной структуры, принимая во внимание лишь умножение на диагональные элементы $(\lambda, \lambda, \dots, \lambda) \subset K^{\oplus n}$.

Если V — конечно порождённый свободный K-модуль с базисом $(e_1, e_2, \dots, e_n)$, то сопоставляя произвольному вектору $v \in V$ столбец из его координат в этом базисе, мы получим изоморфизм V с K^n.

Задача 5.17. Убедитесь в этом.

Наоборот, фиксация некоторого изоморфизма $\kappa\colon V \longrightarrow K^n$ равносильна выбору базиса в V — в качестве базисных можно взять прообразы стандартных базисных векторов из K^n.

Задача 5.18. Убедитесь, что эти прообразы действительно образуют базис.

Таким образом, изоморфизмы $V \xrightarrow{\sim} K^n$ биективно соответствуют базисам из n векторов в V. В следующей лекции мы докажем[6], что модули K^n и K^m неизоморфны при $n \neq m$. Поэтому число векторов во всех базисах произвольного свободного модуля V одно и то же. Оно называется *рангом* свободного модуля и обозначается $\operatorname{rk} V$.

Задача 5.19. Докажите, что многочлены степени $\le n$ с коэффициентами из произвольного коммутативного кольца K составляют свободный K-модуль ранга $(n+1)$.

3.6. Гомоморфизмы и соотношения. Пусть $\varphi\colon V \longrightarrow W$ — гомоморфизм модулей, и модуль V порождается (возможно бесконечным) набором образующих $\{e_i\}$. Тогда φ однозначно восстанавливается по их образам $\varphi(e_i) \in W$. Действительно, разложив произвольный вектор $v \in V$ по e_i: $v = \sum x_i e_i$, мы получаем

$$f(v) = \sum x_i \varphi(e_i)\ .$$

Наоборот, произвольным образом выбрав векторы $w_i \in W$, можно попытаться задать гомомрфизм $V \xrightarrow{\varphi} W$, полагая $\varphi(e_i) = w_i$ и распространяя его на произвольные $v \in V$ при помощи предыдущей формулы (это называется *продолжением по линейности* теоретико-множественного отображения $e_i \longmapsto w_i$). Однако, такое задание гомомрфизма может оказаться некорректным, поскольку вектор v может иметь несколько разных выражений через образующие.

Рассмотрим, например, $\mathbb{Z}$-модули $V = \mathbb{Z}/n\mathbb{Z}$ и $W = \mathbb{Z}$. Тогда V порождается одним элементом $[1] = 1(\bmod n)$, и поланая $f([1]) = k \in \mathbb{Z}$, мы получим гомоморфизм лишь в единственном случае: при $k = 0$. Действительно, в $\mathbb{Z}/n\mathbb{Z}$ выполнено соотношение $n[1] = [0]$, и если φ – гомоморфизм, то в $\mathbb{Z}$ должно выполняться соотношение:

$$n\varphi([1]) = \varphi(n[1]) = \varphi(0) = 0\ ,$$

откуда $f([1]) = 0$, ибо $\mathbb{Z}$ – целостное кольцо.

3.6.1. Предложение. *Для того чтобы отображение $e_i \longmapsto w_i$, $w_i \in W$, можно было продолжить по линейности до гомоморфизма модуля, порождённого векторами e_i, в модуль*

[6] для векторных пространств мы сделаем это уже в Сл.3.7.5

W, необходимо и достаточно, чтобы всякая конечная линейная зависимость

$$\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_n e_n = 0$$

между векторами e_i в V влекла бы точно такую же зависимость

$$\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_n w_n = 0$$

между векторами w_i в W.

Доказательство. В одну сторону утверждение следует непосредственно из определения гомомрфизма: если φ – гомоморфизм, то

$$\sum \lambda_i w_i = \sum \lambda_i \varphi(e_i) = \varphi(\sum \lambda_i e_i) = \varphi(0) = 0\ ,$$

как только $\sum \lambda_i e_i = 0$.

Наоборот, проверим, что продолжение по линейности корректно, если только все соотношения между e_i выполнены и между w_i. Пусть

$$v = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n = y_1 e_1 + y_2 e_2 + \cdots + y_n e_n$$

два разных разложения. Тогда $\sum(x_i - y_i)e_i = 0$, и по предположению, $\sum(x_i - y_i)w_i = 0$. Но тогда и

$$x_1 w_1 + x_2 w_2 + \cdots + x_n w_n = y_1 w_1 + y_2 w_2 + \cdots + y_n w_n$$

в W, и стало быть $\varphi(v)$ не зависит от того, каким из разложений пользоваться.
□

Задача 5.20. Если модуль W не имеет кручения, то всякий гомоморфизм $V \xrightarrow{\varphi} W$ переводит все элементы кручения из V в нуль.

3.6.2. Следствие. *Модуль V тогда и только тогда является свободным с (возможно, бесконечным) базисом $E = \{e_i\}$, когда всякое теоретико-множественное отображение $E \longrightarrow W$ из множества базисных векторов в произвольный модуль W может быть единственным способом продолжено до гомомрфизма $V \longrightarrow W$.*

Доказательство. То, что любое теоретико-множественное отображение базиса свободного модуля в произвольный модуль можно единственным способом продолжить до гомомрфизма модулей, вытекает непосредственно из предыдущего предложения.

Наоборот, пусть некий набор векторов $\{e_1, e_2, \ldots, e_n\}$ некого модуля V обладает указанным в следствии свойством. Возьмём в качестве W свободный модуль с n образующими $(w_1, w_2, \ldots, w_n)$ и отобразим биективно e_i на w_i. Тогда это отображение продолжается до гомоморфизма модулей $V \xrightarrow{\varphi} W$. Этот гомоморфизм является изоморфизмом, ибо у него есть обратный — гомоморфизм $W \xrightarrow{\psi} V$, который продолжает по линейности отображение $w_i \longmapsto e_i$ (он существует по предыдущему абзацу). В самом деле, композиция $V \xrightarrow{\psi\varphi} V$ есть гомоморфизм, который продолжает тождественное отображение из e_i в себя, а стало быть, совпадает с тождественным отображением (вследствие единственности продолжения). Аналогично, композиция $W \xrightarrow{\varphi\psi} W$ будет тождественным отображением из W в W.
□

3.7. Конечномерные векторные пространства. Всюду в этом пункте мы будем считать, что k — произвольное поле. Конечно порождённые векторные пространства над k

называются *конечномерными*. Теория конечномерных векторных пространств много проще, чем теория произвольных модулей, поскольку в ней не возникает никаких неприятностей, связанных с несвободой и неоднозначностью разложения в линейные комбинации.

Задача 5.21. Пусть k – поле. Докажите, что любой набор многочленов $f_i(x) \in k[x]$, $i = 0, 1, 2, \ldots, n$, таких что $\deg(f_i)$ равна в точности i, составляет базис в пространстве всех многочленов степени $\le n$ над k.

3.7.1. Предложение. *Всякое конечномерное векторное пространство обладает базисом, причём этот базис можно получить из любой наперёд заданной системы образующих удаляя из из неё (если надо) некоторые векторы*[7].

Доказательство. Пусть V – векторное пространство над полем k, порождённое конечным набором векторов $(e_1, e_2, \ldots, e_n)$. Из всех таких наборов мы выберем набор, состоящий из наименьшего возможного количества векторов. Покажем, что он линейно-независим. Действительно, пусть $\sum \lambda_i e_i = 0$, и скажем, $\lambda_n \neq 0$. Тогда

$$e_n = -\sum_{i=1}^{n-1} \frac{\lambda_i}{\lambda_n} e_i$$

линейно выражается через первые $(n-1)$ векторов, и подставляя это выражение в разложение произвольного вектора $v \in V$ через e_i, мы видим, что V в действительности порождается первыми $(n-1)$ векторами нашей системы вопреки предположению.
□

3.7.2. Следствие. *Всякое конечномерное векторное пространство над полем k изоморфно некоторому координатному векторному пространству k^n.*

□

3.7.3. Предложение. *Всякий набор $(v_1, v_2, \ldots, v_m)$ из $m > n$ векторов в k^n линейно-зависим.*

Доказательство. Пусть A — это матрица, составленная из вектор-столбцов v_i. Подобрать ненулевой набор констант x_i, дающих линейную зависимость

$$x_1 v_1 + x_2 v_2 + \cdots + x_m v_m = 0$$

это то же самое, что найти ненулевое решение системы однородных линейных уравнений

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} .$$

Как мы видели в прошлой лекции, в нашем случае, когда уравнений меньше, чем неизвестных, ненулевое решение всегда существует.
□

3.7.4. Следствие. *Векторные пространства k^m и k^n изоморфны тогда и только тогда, когда $m = n$.*

---

[7] машинерия “трансфинитной” теории множеств (теорема Цермело или лемма Цорна) позволяет распространить приводимое ниже доказательство и на случай пространств, порождённых бесконечными семействами образующих, так что предложение сохраняет силу для любых векторных пространств

□

3.7.5. Следствие. *Все базисы конечномерного векторного пространства V состоят из одного и того же числа векторов (это число называется размерностью V и обозначается $\dim V$).*

□

3.7.6. Следствие. *Всякий линейно независимый набор векторов может быть дополнен до базиса.*

Доказательство. Точно также, как и в доказательстве Пр.3.7.1, легко увидеть, что если вектор v не выражается через линейно-независимый набор векторов $(v_1, v_2, \dots, v_m)$, то набор $(v, v_1, v_2, \dots, v_m)$ также будет линейно-независим. Добавляя таким образом к набору новые векторы мы в конце концов получим базис, ибо число векторов в линейно-независимом наборе не может превысить $\dim V$.

□

3.7.7. Предложение. *Пусть $V \xrightarrow{\varphi} W$ — гомоморфизм конечномерных векторных пространств. Тогда в V и W можно так выбрать базисы $(v_1, v_2, \dots, v_n)$ и $(w_1, w_2, \dots, w_m)$, что*

$$f(e_i) = \begin{cases} w_i\,, \text{ при } & 1 \le i \le r \\ 0\,, \text{ при } & r < i \le m \end{cases} \quad ,$$

причём число $r = \dim(\operatorname{im}\varphi) = \dim(V) - \dim(\ker\varphi)$ не зависит от выбора базисов.

Доказательство. Выберем базис в $\ker\varphi \subset V$, обозначим его через $(v_{r+1}, \dots, v_n)$ (это определение числа r), и дополним его до базиса $(v_1, v_2, \dots, v_n)$ в V. Векторы

$$\varphi(v_1), \varphi(v_2), \dots, \varphi(v_r)$$

порождают $\operatorname{im}\varphi$ (ибо остальные базисные векторы V переходят в нуль) и линейно независимы, поскольку из равенства

$$0 = \sum_{i=1}^{r} \lambda_i \varphi(v_i) = \varphi\left(\sum_{i=1}^{r} \lambda_i v_i\right)$$

вытекает равенство $\sum\limits_{i=1}^{r} \lambda_i v_i \in \ker\varphi$, означающее, что эта сумма линейно выражается через векторы $v_{r+1}, \dots, v_n$, что из-за единственности разложения по базису возможно лишь при $\sum\limits_{i=1}^{r} \lambda_i v_i = 0$, т. е. только если все $\lambda_i - 0$. Тем самым, векторы $w_i \overset{\text{def}}{=} \varphi(v_i)$ с $1 \le i \le r$ составляют базис в $\operatorname{im}\varphi$. Дополняя этот базис до базиса$(w_1, w_2, \dots, w_m)$ в W получаем утверждение предложения.

□

§4. Матричный формализм

4.1. Векторы как матрицы. Условимся записывать наборы векторов матрицами-строками, элементами которых служат эти векторы, а наборы чисел[8] — матрицами-столбцами, составленными из этих чисел. Договоримся также, что векторы можно умножать на числа и справа и слева, полагая по определению $v \cdot \lambda \overset{\text{def}}{=} \lambda v$.

[8]обычно это будут координаты или коэффициенты разложения по образующим

В этих соглашениях равенство $v = \sum\limits_{i=1}^{n} x_i v_i$ можно интерпретировать как матричное равенство

$$(v) = (v_1, v_2, \ldots, v_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} ,$$

где (v) есть 1×1-матрица с единственным элементом v.

4.2. Матрицы перехода. Пусть $(v_1, v_2, \ldots, v_s)$ — какой-либо набор векторов K-модуля V, порождённого векторами $(e_1, e_2, \ldots, e_n)$. Матрицу размера $n \times s$, по столбцам которой стоят коэффициенты разложений векторов v_i по образующим e_i, мы будем называть *матрицей перехода от* v_i *к* e_i и обозначать C_{ev}. Отметим, что это обозначение не вполне корректно, ибо если e_i линейно-зависимы, то можно написать много разных матриц перехода. Тем не менее, любая из них, по определению, удовлетворяет матричному равенству

$$(v_1, v_2, \ldots, v_s) = (e_1, e_2, \ldots, e_n) C_{ev} .$$

Если набор $(v_1, v_2, \ldots, v_s)$ также порождает V, то наряду с матрицей C_{ev} можно рассматривать матрицу перехода C_{ve} от e_i к v_i, по столбцам которой стоят коэффициенты разложений векторов e_i через образующие v_i. Возникает равенство

$$(e_1, e_2, \ldots, e_n) = (v_1, v_2, \ldots, v_s) C_{ve} = (e_1, e_2, \ldots, e_n) C_{ev} C_{ve} ,$$

которое означет, что произведение $C_{ev} C_{ve}$ является матрицей перехода C_{ee} набора e_i к самому же набору e_i, т. е. имеет в качестве столбцов коэффициенты разложения векторов e_i по самим себе.

Допустим теперь, что набор векторов e_i составляет *базис* в V. Тогда разложение каждого e_i по этому базису единственно: $e_i = e_i$, и матрица C_{ee} — это единичная матрица E размера $n \times n$. Таким образом, для любого базиса $(e_1, e_2, \ldots, e_n)$ и любого набора векторов $(v_1, v_2, \ldots, v_s)$, порождающего V, мы имеем соотношение

$$C_{ev} C_{ve} = E .$$

4.2.1. Предложение. *Пусть набор векторов $(e_1, e_2, \ldots, e_n)$ является базисом свободного модуля V над коммутативным кольцом K. Другой набор из n векторов $(v_1, v_2, \ldots, v_n)$ тогда и только тогда является базисом V, когда матрица перехода C_{ev} обратима в $Mat_n(K)$. При этом противоположный переход будет задаваться обратной матрицей $C_{ve} = C_{ev}^{-1}$.*

Доказательство. В одну сторону мы всё уже доказали: если $(v_1, v_2, \ldots, v_n)$ — базис в V, то как мы видели выше, матрицы перехода обязяны удовлетворять соотношениям $C_{ev} C_{ve} = C_{ve} C_{ev} = E$, где E — единичная матрица размера $n \times n$.

Докажем противоположную имликацию. Пусть C_{ev} обратима в $Mat_n(K)$. Тогда из равенства $(v_1, v_2, \ldots, v_n) = (e_1, e_2, \ldots, e_n) C_{ev}$ вытекает, что $(e_1, e_2, \ldots, e_n) = (v_1, v_2, \ldots, v_n) C_{ev}^{-1}$. Покажем, что v_i порождают V. Всякий вектор $v \in V$ имеет разложение вида

$$v = \sum x_i e_i = (e_1, e_2, \ldots, e_n) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = (v_1, v_2, \ldots, v_n) C_{ev}^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} ,$$

которое показывает, что $v = \sum y_i v_i$, где $\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = C_{ev}^{-1} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Остаётся проверить, что набор $(v_1, v_2, \dots, v_n)$ линейно-независим. Пусть

$$\sum \lambda_i v_i = (v_1, v_2, \dots, v_n) \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = 0 .$$

Подставляя $(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n) C_{ev}$, получим $\sum \mu_i e_i = 0$, где $\begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{pmatrix} = C_{ev} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$.
Поскольку e_i линейно-независимы, левый столбец последнего равенства должен быть нулевым. Умножая обе части на C_{ev}^{-1} получаем, что и столбец из λ_i тоже нулевой. Итак, v_i – это тоже базис в V.
□

Отметим, что из доказательства леммы вытекает следующее правило для пересчёта координат:

4.2.2. Следствие. *Если $(e_1, e_2, \dots, e_n)$ и $(v_1, v_2, \dots, v_n)$ — два базиса в свободном модуле V и x_i^e и x_i^v — координаты одного и того же вектора $w \in V$ в этих базисах, то*

$$\begin{pmatrix} x_1^e \\ x_2^e \\ \vdots \\ x_n^e \end{pmatrix} = C_{ev} \begin{pmatrix} x_1^v \\ x_2^v \\ \vdots \\ x_n^v \end{pmatrix} .$$

□

4.3. Матрицы гомоморфизмов. Пусть $V = K^n$, $W = K^m$ — свободные модули, и A — некая матрица размера $m \times n$ с элементами из K. Гомоморфизм

$$\mu_A \colon K^n \longrightarrow K^m \quad : \qquad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \longmapsto A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^m$$

называется *гомоморфизмом умножения на матрицу A*

Задача 5.22. Проверьте, что μ_A есть гомоморфизмом K-модулей.

4.3.1. Предложение. *Всякий гомоморфизм модулей $K^n \xrightarrow{\varphi} K^m$ является гомоморфизмом умножения на матрицу, которая однозначно определяется по φ и называется матрицей гомоморфизма φ.*

Доказательство. Пусть $e_i \in K^n$ — стандартные базисные векторы. Обозначим через Φ матрицу размера $m \times n$, столбцы которой суть вектор-столбцы $\varphi(e_i) \in K^m$. Тогда φ и μ_Φ одинаково действуют на базис e_i свободного модуля K^n, и согласно Сл.3.6.2, $\varphi = \mu_\Phi$.
□

Для произвольных свободных модулей V и W выбор в V базиса $(v_1, v_2, \ldots, v_n)$, а в W – базиса $(w_1, w_2, \ldots, w_m)$ позволяет записать любой гомоморфизм $V \xrightarrow{\varphi} W$ в виде умножения на $m \times n$-матрицу $\Phi = \Phi_{wv}$, по столбцам которой стоят координаты векторов $\varphi(e_i)$ в базисе w_i. Эта матрица называется *матрицей*[9] φ *в базисах* v_i *и* w_i.

4.3.2. Следствие. *Пусть V и W — свободные модули с базисами v_i и w_i, и $V \xrightarrow{\varphi} W$ — гомоморфизм модулей с матрицей Φ_{wv}. Тогда вектор с координатами переходит в вектор с координатами x_i^w, вычисляемыми по формуле*

$$\begin{pmatrix} x_1^w \\ x_2^w \\ \vdots \\ x_m^w \end{pmatrix} = \Phi_{wv} \begin{pmatrix} x_1^v \\ x_2^v \\ \vdots \\ x_n^v \end{pmatrix} .$$

□

В случае, когда $W = V$, т. е. $V \xrightarrow{\varphi} V$ – эндоморфизм свободного модуля V, достаточно выбрать один базис $(e_1, e_2, \ldots, e_n)$ в V и рассматривать его и как базис в образе и как базис в прообразе. Соответствующая матрица Φ_{ee} обозначается просто Φ_e и называется матрицей φ в базисе e.

Задача 5.23. Пусть k – поле, и $q(x) \in k[x]$ — произвольный многочлен. Убедитесь, что фактор-кольцо $k[x]/(q)$ имеет естественную структуру конечномерного векторного пространства над k размерности $\sum \deg q_i$, постройте какой-либо базис в нём и напишите матрицу оператора умножения на класс $x \bmod q$ в этом базисе.

Задача 5.24. Пусть в условиях предыдущей задачи $k = \mathbb{C}$ и $q(x) = (x - \lambda)^n$, где $\lambda \in \mathbb{C}$. Постройте в $k[x]/(q)$ базис, в котором матрица оператора умножения на класс $x \bmod q$ имеет вид $\begin{pmatrix} \lambda & 1 & & & 0 \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda \end{pmatrix}$.

4.3.3. Изменение матрицы гомомрфизма при замене базисов. Разумеется, матрица Φ_{wv} гомомрфизма $V \xrightarrow{\varphi} W$ зависит от выбора базисов. Если выбрать другие базисы

$$(v_1', v_2', \ldots, v_n') = (e_1, e_2, \ldots, e_n) C_{ee'} \qquad \text{и} \qquad (w_1', w_2', \ldots, w_m') = (w_1, w_2, \ldots, w_m) C_{ww'} ,$$

то матрица $\Phi_{w'v'}$ гомоморфизма φ в этих новых базисах определяется соотношением

$$(f(v_1'), f(v_2'), \ldots, f(v_n')) = (w_1', w_2', \ldots, w_n') \Phi_{w'v'} .$$

С другой стороны, имеем:

$$\begin{aligned} (f(v_1'), f(v_2'), \ldots, f(v_n')) &= (f(v_1), f(v_2), \ldots, f(v_n)) C_{vv'} = \\ &= (w_1, w_2, \ldots, w_m) \Phi_{wv} C_{vv'} = \\ &= (w_1', w_2', \ldots, w_m') C_{w'w} \Phi_{wv} C_{vv'} , \end{aligned}$$

[9] здесь и всюду далее мы будем обозначать гомомрфизмы модулей маленькими греческими буквами, а их матрицы – соответствующими большими буквами

откуда $\Phi_{w'v'} = C_{w'w}\Phi_{wv}C_{vv'} = C_{ww'}^{-1}\Phi_{wv}C_{vv'}$.

4.3.4. Пример: элементарные преобразования. Если $m \times n$ матрица A рассматривается как матрица $A = \Phi_{wv}$ гомомрфизма $V \xrightarrow{\varphi} W$ между свободными модулями, то элементарные преобразования матрицы A, скоторыми мы имели дело в прошлой лекции, можно интерпретировать как элементарные замены базисов в V и W.

> Задача 5.25. Убедитесь, что элементарные преобразования строк 1-го, 2-го и 3-го типа индуцированы следующими заменами базиса $(w_1, w_2, \dots, w_m)$ модуля W: перестановкой пары векторов w_i, w_j, заменой w_j на $w_j - \lambda w_i$ и умножением w_i на обратимый элемент кольца K. Убедитесь также, что элементарным преобразованиям столбцов отвечают аналогичные замены базисных векторов в V.

В частности, Пр.3.7.7 можно получить как следствие теоремы о том, что всякую матрицу над полем можно одновременными элементарными преобразованиями строк и столбцов привести к диагональному виду

$$D = \left.\underbrace{\begin{pmatrix} 1 & & & & & \\ & 1 & & & 0 & \\ & & \ddots & & & \\ & & & 1 & & \\ & 0 & & & 0 & \\ & & & & & \ddots \end{pmatrix}}_{n}\right\}m \quad .$$

Действительно, пусть в некоторых базисах v_i и w_i гомоморфизм φ имеет матрицу Φ. В прошлой лекции мы построили обратимые матрицы B и C (возникавшие как произведения элементарных матриц), такие что $B\Phi C = D$. Тогда в базисах

$$(v_1, v_2, \dots, v_n) = (e_1, e_2, \dots, e_n)C \quad \text{и} \quad (w_1, w_2, \dots, w_m) = (e_1, e_2, \dots, e_m)B^{-1}$$

(где e_i — стандартные координатные базисные векторы) гомомрфизм φ будет задаваться матрицей D, что и требуется в Пр.3.7.7.

4.4. Ранг матрицы над полем. Размерность образа оператора $k^n \xrightarrow{\mu_A} k^m$ умножения на матрицу A называется *рангом* этой матрицы и обозначается $\operatorname{rk} A$.

4.5. Теорема. (Теорема о ранге матрицы.) *Пусть A — прямоугольная матрица размера из m строк и n столбцов с элементами из поля k. Тогда следующие числа совпадают:*

(i) $\operatorname{rk} A$*;*

(ii) размерность подпространства, порождённого в k^m столбцами A;

(iii) размерность подпространства, порождённого в k^n строками A;

(iv) число ненулевых строк после приведения матрицы A к строгому ступенчатому виду элементарными преобразованиями строк;

(v) число диагональных единиц после приведения матрицы A к диагональному виду элементарными преобразованиями строк и столбцов

(в частности, последние два числа не зависят от способа приведения).

Доказательство. Образ гомоморфизма умножения на матрицу A порождается её столбцами. Поэтому число в (ii) совпадает с $\dim(\operatorname{im} \mu_A)$.

Поскольку элементарные преобразования матрицы A суть матрицы того же самого гомоморфизма μ_A, но в других базисах, $\dim(\operatorname{im}\mu_A)$ не меняется при элементарных преобразованиях строк и столбцов. Когда матрица приобретает диагональный вид, эта размерность, очевидно, равна числу диагональных единиц.

Если рассмотреть транспонированную матрицу A^t, полученную из A симметрией относительно главной диагонали (т. е. $a^t_{ij} \stackrel{\text{def}}{=} a_{ji}$), то строки и столбцы A и A^t поменяются ролями, тогда как число единиц в диагональном виде A^t будет тем же самым. Поэтому числа (iii) и (v) также совпадают.

Наконец ясно, что ненулевые строки матрицы, полученной в результате приведения матрицы A к строго ступенчатому виду элементарными преобразованиями строк, составляют базис в подпространстве, порождённом в k^n строками A (эти строки линейно-независимы, и их число не меньше числа единиц в диагональном виде).

□

Задача 5.26. Проверьте, что транспонирование $A \longmapsto A^t$ является кольцевым *антигомоморфизмом* (т. е. $(A+B)^t = A^t + B^t$, но $(AB)^t = B^t A^t$), — сложение сохраняется, а в произведениях изменяется порядок сомножителей).