**А. Л. Городенцев***

# А Л Г Е Б Р А

**2-й курс**

Независимый Московский Университет
2021/22 уч. год

* ВШЭ, ИТЭФ, НМУ, e-mail:gorod@itep.ru , http://gorod.bogomolov-lab.ru/

## Оглавление

## §1. Тензорные произведения

**1.1. Полилинейные отображения.** Над произвольным коммутативным кольцом $K$ рассмотрим набор $K$-модулей $V_1, \dots, V_n$ и ещё один модуль $W$. Отображение множеств

$$\varphi : V_1 \times \dots \times V_n \to W \tag{1-1}$$

называется *полилинейным*[1], если оно линейно отдельно по каждому из своих аргументов при произвольным образом зафиксированных остальных:

$$\varphi( \dots , \lambda v' + \mu v'' , \dots ) = \lambda \, \varphi( \dots , v' , \dots ) + \mu \, \varphi( \dots , v'' , \dots ) .$$

Например, 1-линейные отображения $V \to W$ суть просто линейные отображения, а 2-линейные отображения $V \times V \to K$ — это билинейные формы на модуле $V$. Полилинейные отображения (1-1) можно складывать и умножать на элементы из кольца $K$, так что они тоже образуют $K$-модуль. Он называется *модулем полилинейных отображений* и обозначается через $\mathrm{Hom}(V_1, \dots , V_n; W)$ или $\mathrm{Hom}_K(V_1, \dots , V_n; W)$, если важно явно указать кольцо.

Пример 1.1 (полилинейные отображения свободных модулей)
Если все модули $V_i$ и $W$ свободны с базисами $E_i \subset V_i$ и $E \subset W$, то модуль $\mathrm{Hom}(V_1, \dots , V_n; W)$ тоже свободен, и его базис равномощен $E \times E_1 \times \dots \times E_n$. В частности, если все модули имеют конечный ранг, то

$$\mathrm{rk}\,\mathrm{Hom}(V_1, \dots , V_n; W) = \mathrm{rk}\, W \cdot \prod_i \mathrm{rk}\, V_i \,.$$

В самом деле, полилинейное отображение (1-1) однозначно определяется своими значениями $\varphi(e_1, \dots , e_n) \in W$ на всевозможных сочетаниях базисных векторов $(e_1, \dots , e_n) \in E_1 \times \dots \times E_n$, ибо для произвольных $v_i = \sum_{e_i \in E_i} x_{e_i} e_i \in V_i$

$$\varphi(v_1, \dots , v_n) = \sum\nolimits_{(e_1,\dots,e_n) \in E_1 \times \dots \times E_n} x_{e_1} x_{e_2} \dots x_{e_n} \varphi(e_1, \dots , e_n) \,.$$

Запишем разложения векторов $\varphi(e_1, \dots , e_n)$ по базису $E \subset W$ как

$$\varphi(e_1, \dots , e_n) = \sum_{e \in E} a^e_{e_1,\dots,e_n} e$$

и сопоставим полилинейному отображению $\varphi$ набор чисел $a^e_{e_1,\dots,e_n} \in K$, организованный в $(n+1)$-мерную матрицу, ячейки которой нумеруются элементами множества[2] $E \times E_1 \times \dots \times E_n$. В терминах этой матрицы

$$\varphi(v_1, \dots , v_n) = \sum\nolimits_{(e, e_1,\dots,e_n) \in E \times E_1 \times \dots \times E_n} x_{e_1} x_{e_2} \dots x_{e_n} a^e_{e_1,\dots,e_n} e \,.$$

При сложении полилинейных отображений и умножении их на числа из $K$ соответствующие этим отображениям матрицы поэлементно складываются и умножаются на числа. Таким образом, мы получаем $K$-линейный изоморфизм между модулем полилинейных отображений и

[1] Или *$n$-линейным*, когда желательно точно указать количество аргументов.

[2] При $n = 1$ получается обычная двумерная матрица линейного отображения $V \to W$, строки которой биективно соответствуют базисным векторам пространства $W$, а столбцы — базисным векторам пространства $V$.

свободным модулем многомерных матриц. При этом изоморфизме стандартная базисная матрица, имеющая единицу в позиции $(\varepsilon,\ \varepsilon_1, \dots, \varepsilon_n)$ и нули в остальных местах, переходит в полилинейное отображение $\delta_\varepsilon^{\varepsilon_1 \dots \varepsilon_n} : (v_1, \dots, v_n) \mapsto x_{\varepsilon_1} x_{\varepsilon_2} \dots x_{\varepsilon_n} \cdot \varepsilon$, значения которого на базисных векторах суть

$$\delta_\varepsilon^{\varepsilon_1 \dots \varepsilon_n}(e_1, \dots, e_n) = \begin{cases} \varepsilon, & \text{если } (e_1, \dots, e_n) = (\varepsilon_1, \dots, \varepsilon_n), \\ 0 & \text{в остальных случаях.} \end{cases} \tag{1-2}$$

**1.1.1. Универсальное полилинейное отображение.** Вновь рассмотрим произвольные модули $U$, $W$ и $V_1, \dots, V_n$ над произвольным коммутативным кольцом $K$. Взятие композиции $K$-линейных отображений $F : U \to W$ с фиксированным полилинейным отображением

$$\tau : V_1 \times \dots \times V_n \to U \tag{1-3}$$

задаёт $K$-линейное по $F$ отображение модулей

$$\mathrm{Hom}(U, W) \to \mathrm{Hom}(V_1, \dots, V_n; W), \quad F \mapsto F \circ \tau. \tag{1-4}$$

Определение 1.1

Полилинейное отображение (1-3) называется *универсальным*, если для каждого $K$-модуля $W$ линейный оператор (1-4) является изоморфизмом. Иначе говоря, полилинейное отображение $\tau : V_1 \times \dots \times V_n \to U$ универсально, если для любого модуля $W$ и любого полилинейного отображения $\varphi : V_1 \times \dots \times V_n \to W$ существует единственный такой линейный оператор $F : U \to W$, что $\varphi = F \circ \tau$, т. е. пара полилинейных сплошных стрелок в диаграмме

$$\begin{tikzcd} & U \arrow[dd, dashed, "F"] \\ V_1 \times \dots \times V_n \arrow[ur, "\tau"] \arrow[dr, "\varphi"'] & \\ & W \end{tikzcd}$$

всегда замыкается в коммутативный треугольник единственным пунктирным линейным отображением.

Лемма 1.1

Для любых двух универсальных полилинейных отображений

$$\tau_1 : V_1 \times \dots \times V_n \to U_1 \qquad \text{и} \qquad \tau_2 : V_1 \times \dots \times V_n \to U_2$$

имеется единственный линейный изоморфизм $\iota : U_1 \xrightarrow{\sim} U_2$, такой что $\tau_2 = \iota \tau_1$.

Доказательство. В силу универсальности $\tau_1$ и $\tau_2$ существуют единственные такие линейные отображения $F_{21} : U_1 \to U_2$ и $F_{12} : U_2 \to U_1$, что $\tau_2 = F_{21}\tau_1$ и $\tau_1 = F_{12}\tau_2$, т. е. коммутативна диаграмма

$$\begin{tikzcd} U_1 \arrow[dr, dashed, "F_{21}"] \arrow[dd, equal, "\mathrm{Id}_{U_1}"'] & & & & U_2 \arrow[dl, dashed, "F_{12}"'] \arrow[dd, equal, "\mathrm{Id}_{U_2}"] \\ & U_2 \arrow[dl, dashed, "F_{12}"] & V_1 \times \dots \times V_n \arrow[l, "\tau_2"'] \arrow[r, "\tau_1"] \arrow[ull, "\tau_1"'] \arrow[dll, "\tau_1"] \arrow[urr, "\tau_2"] \arrow[drr, "\tau_2"'] & U_1 \arrow[dr, dashed, "F_{21}"'] & \\ U_1 & & & & U_2 . \end{tikzcd}$$

Равенства $F_{21}F_{12} = \mathrm{Id}_{U_2}$ и $F_{12}F_{21} = \mathrm{Id}_{U_1}$ выполняются в силу того, что разложения $\tau_1 = \varphi \circ \tau_1$ и $\tau_2 = \psi \circ \tau_2$ единственны и имеют место для $\varphi = \mathrm{Id}_{U_1}$, $\psi = \mathrm{Id}_{U_2}$. □

**1.2. Тензорное произведение модулей.** Универсальное полилинейное отображение называется *тензорным произведением векторов* и обозначается

$$\tau : V_1 \times \dots \times V_n \to V_1 \otimes \dots \otimes V_n \,. \tag{1-5}$$

Единственный с точностью до единственного изоморфизма, перестановочного с тензорным произведением векторов, модуль $V_1 \otimes \dots \otimes V_n$ называется *тензорным произведением* модулей $V_1, \dots, V_n$, а его элементы — *тензорами*. Тензорные произведения векторов обычно записывают в виде

$$v_1 \otimes \dots \otimes v_n \overset{\text{def}}{=} \tau(v_1, \dots, v_n) \,. \tag{1-6}$$

Они составляют образ универсального отображения (1-5) и называются *разложимыми* тензорами. Так как отображение (1-5) не линейно, а полилинейно, его образ, вообще говоря, не является $K$ подмодулем, и наугад взятая линейная комбинация мономов (1-6) скорее всего не разложится в тензорное произведение $n$ векторов.

**1.2.1. Существование тензорного произведения.** Предыдущее определение обеспечивает единственность универсального полилинейного отображения, но не даёт никаких гарантий его существования. Сейчас мы построим модуль $V_1 \otimes \dots \otimes V_n$ в терминах образующих и соотношений. Ниже, в теор. 1.1 на стр. 8 и теор. 1.2 на стр. 14 мы укажем, как упростить эту конструкцию для свободных модулей и для модулей, заданных образующими и соотношениями.

Рассмотрим свободный $K$-модуль $\mathcal{V}$, базисом в котором по определению являются всевозможные $n$-буквенные слова $[v_1 \dots v_n]$, в которых в качестве $i$-той буквы может выступать любой вектор $v_i \in V_i$. В этом огромном модуле рассмотрим подмодуль $\mathcal{R} \subset \mathcal{V}$, порождённый всевозможными трёхчленными линейными комбинациями вида

$$[\,\cdots\, (\lambda u + \mu w) \,\cdots\,] - \lambda\,[\,\cdots\, u \,\cdots\,] - \mu\,[\,\cdots\, w \,\cdots\,]\,, \tag{1-7}$$

где обозначенные многоточиями соответственные фрагменты во всех трёх словах одинаковы. Положим по определению

$$V_1 \otimes \dots \otimes V_n \overset{\text{def}}{=} \mathcal{V}/\mathcal{R}\,, \quad v_1 \otimes \dots \otimes v_n \overset{\text{def}}{=} [v_1 \dots v_n] \,(\mathrm{mod}\ \mathcal{R})\,. \tag{1-8}$$

Иными словами, модуль $V_1 \otimes \dots \otimes V_n$ состоит из конечных $K$-линейных комбинаций формальных тензорных мономов $v_1 \otimes \dots \otimes v_n$, в которых $v_i \in V_i$ и которые подчиняются стандартным соотношениям дистрибутивности: если любой из сомножителей (при фиксированных остальных) записать в виде линейной комбинации векторов, то такое произведение можно преобразовать по обычному правилу для раскрытия скобок:

$$\cdots \otimes (\lambda u + \mu w) \otimes \cdots = \lambda \cdot (\,\cdots \otimes u \otimes \cdots\,) + \mu \cdot (\,\cdots \otimes w \otimes \cdots\,)\,. \tag{1-9}$$

Лемма 1.2

Отображение $\tau : V_1 \times \dots \times V_n \to \mathcal{V}/\mathcal{R}$, $(v_1, \dots, v_n) \mapsto [v_1 \dots v_n] \,(\mathrm{mod}\ \mathcal{R})$, является универсальным полилинейным отображением.

Доказательство. Полилинейность тавтологически следует из наложенных соотношений и выражается в точности формулой (1-9). Докажем универсальность. Для любого отображения множеств $\varphi : V_1 \times \dots \times V_n \to W$ существует единственное линейное отображение $F : \mathcal{V} \to W$, переводящее базисный вектор $[v_1 \dots v_n] \in \mathcal{V}$ в $\varphi(v_1, \dots , v_n)$. Для того, чтобы это отображение было корректно определено на фактор модуле $\mathcal{V}/\mathcal{R}$, достаточно проверить, что $\mathcal{R} \subset \ker F$. Для каждого соотношения (1-7) из полилинейности $\varphi$ и линейности $F$ получаем

$$\begin{aligned} F\big([\dots(\lambda u + \mu w)\dots] - \lambda\,[\dots u \dots] - \mu\,[\dots w \dots]\big) = \\ = F\big([\dots(\lambda u + \mu w)\dots]\big) - \lambda\,F\big([\dots u \dots]\big) - \mu\,F\big([\dots w \dots]\big) = \\ = \varphi(\dots , (\lambda u + \mu w), \dots ) - \lambda\,\varphi(\dots , u, \dots ) - \mu\,\varphi(\dots , w, \dots ) = 0\,, \end{aligned}$$

что и требовалось. □

Следствие 1.1

Разложимые тензоры $v_1 \otimes \dots \otimes v_n$ линейно порождают модуль $V_1 \otimes \dots \otimes V_n$ над $K$.

Доказательство. Поскольку слова $[v_1 \dots v_n]$ линейно порождают $\mathcal{V}$, их образы $v_1 \otimes \dots \otimes v_n$ при факторизации $\mathcal{V} \twoheadrightarrow \mathcal{V}/\mathcal{R}$ линейно порождают фактор модуль $V_1 \otimes \dots \otimes V_n = \mathcal{V}/\mathcal{R}$. □

Теорема 1.1

Если каждый из модулей $V_i$ свободен с базисом $E_i \subset V_i$, то их тензорное произведение $V_1 \otimes \dots \otimes V_n$ также свободно с базисом

$$e_1 \otimes \dots \otimes e_n\,, \quad e_i \in E_i\,. \tag{1-10}$$

В частности, если $\operatorname{rk} V_i = |E_i| < \infty$ для всех $i$, то $\operatorname{rk} V_1 \otimes \dots \otimes V_n = \prod \operatorname{rk} V_i$.

Доказательство. Обозначим через $\mathcal{W}$ свободный модуль с базисом из выражений (1-10), которые мы временно будем воспринимать как формальные символы. Полилинейное отображение $\tau : V_1 \times \dots \times V_n \to \mathcal{W}$, переводящее каждый набор базисных векторов $(e_1, \dots , e_n) \in E_1 \times \dots \times E_n$ в соответствующий базисный вектор (1-10) модуля $\mathcal{W}$, универсально, поскольку для полилинейного $\varphi : V_1 \times \dots \times V_n \to W$ и линейного $F : \mathcal{W} \to W$ равенство $\varphi = F \circ \tau$ равносильно выполнению для всех $(e_1, \dots , e_n) \in E_1 \times \dots \times E_n$ равенств $F(e_1 \otimes \dots \otimes e_n) = \varphi(e_1, \dots , e_n)$, которые однозначно определяют $F$, если дано $\varphi$, и наоборот. По лем. 1.1 имеется единственный линейный изоморфизм $\mathcal{W} \xrightarrow{\sim} V_1 \otimes \dots \otimes V_n$, переводящий базисные векторы (1-10) модуля $\mathcal{W}$ в соответствующие тензорные произведения базисных векторов, вычисленные в $V_1 \otimes \dots \otimes V_n$. Тем самым, последние тоже образуют базис. □

Пример 1.2 (многочлены)

Обратите внимание, что теор. 1.1 верна и для свободных модулей *бесконечного* ранга. Например, тензорное произведение $n$ экземпляров модуля многочленов $K[x] \otimes \dots \otimes K[x]$ изоморфно модулю многочленов от $n$ переменных $K[x_1, \dots , x_n]$. Изоморфизм сопоставляет базисному разложимому тензору $x^{m_1} \otimes x^{m_2} \otimes \dots \otimes x^{m_n}$ базисный моном $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$.

Пример 1.3 (многообразия Сегре)

Тензорное произведение $\tau : V_1 \times \dots \times V_n \to V_1 \otimes \dots \otimes V_n$ конечномерных векторных пространств $V_i$ над полем $\Bbbk$ задаёт отображение $s : \mathbb{P}_{m_1} \times \dots \times \mathbb{P}_{m_n} \to \mathbb{P}_m$ из произведения проективных пространств $\mathbb{P}_{m_i} = \mathbb{P}(V_i)$ в проективное пространство $\mathbb{P}_m = \mathbb{P}\left(V_1 \otimes \dots \otimes V_n\right)$. Это отображение называется *вложением Сегре*. Оно переводит набор одномерных подпространств, натянутых на ненулевые векторы $v_i \in V_i$, в одномерное подпространство, порождённое тензором $v_1 \otimes \cdots \otimes v_n$.

Упражнение 1.1. Проверьте, что это определение корректно[1] и задаёт инъективное отображение.

Образ вложения Сегре состоит из классов пропорциональности разложимых тензоров и называется *многообразием Сегре*. По построению, многообразие Сегре заметается $n$ семействами проективных подпространств размерностей $m_1, \dots, m_n$. Его размерность $\sum m_i$ обычно гораздо меньше размерности $m = \prod(m_i + 1) - 1$ объемлющего пространства. При этом многообразие Сегре не содержится ни в какой гиперплоскости, поскольку линейная оболочка множества разложимых тензоров совпадает со всем пространством $V_1 \otimes \cdots \otimes V_n$.

**1.2.2. Линейные операторы как тензоры.** Для произвольных векторных пространств $U, W$ имеется билинейное отображение $W \times U^* \to \mathrm{Hom}(U, W)$, переводящее пару $(w, \xi) \in W \times U^*$ в линейный оператор

$$U \to W, \quad u \mapsto \xi(u) \cdot w, \tag{1-11}$$

с ядром $\mathrm{Ann}(\xi) \subset U$ и образом, порождённым вектором $w$. При ненулевых $\xi, w$ оператор (1-11) имеет ранг 1. Поскольку образ любого оператора $F : U \to W$ ранга 1 порождается некоторым ненулевым вектором $w \in W$, который определяется по $F$ однозначно с точностью до пропорциональности, значение такого оператора на произвольном векторе $u \in U$ равно $F(u) = \xi(u) \cdot w$ для некоторого $\xi \in \mathrm{Ann}\ker F \subset U^*$, однозначно определяемого по $F$ и $w$. Поэтому, переходя к проективизациям, мы получаем корректно определённое *вложение Сегре*

$$s : \mathbb{P}(W) \times \mathbb{P}(U^*) \hookrightarrow \mathbb{P}\big(\mathrm{Hom}(U, W)\big),$$

образ которого состоит из рассматриваемых с точностью до пропорциональности линейных операторов $U \to W$ ранга 1. В силу универсального свойства тензорного произведения, существует единственное линейное отображение

$$W \otimes U^* \to \mathrm{Hom}(U, V) \tag{1-12}$$

переводящее каждый разложимый тензор $w \otimes \xi$ в оператор (1-11). Если пространства $U$ и $W$ конечномерны с базисами $u_1, \dots, u_n$ и $w_1, \dots, w_m$, то $mn$ разложимых тензоров $w_j \otimes u_i^*$, где $u_1^*, \dots, u_n^* \in U^*$ это двойственный к $u_1, \dots, u_n$ базис пространства $U^*$, образуют базис пространства $W \otimes U^*$. Отображение (1-12) переводит тензор $w_j \otimes u_i^*$ в линейный оператор

$$U \to W, \quad u_k \mapsto \begin{cases} w_j & \text{при } k = i \\ 0 & \text{в остальных случаях}, \end{cases}$$

матрица которого в выбранных базисах имеет единицу в клетке $i, j$ и нули в остальных местах. Таким образом, стандартный базис тензорного произведения $W \otimes U^*$ переводится в стандартный базис пространства операторов, т. е. отображение (1-12) является линейным изоморфизмом. В дальнейшем мы часто будем отождествлять пространства $W \otimes U^*$ и $\mathrm{Hom}(U, W)$ при помощи изоморфизма (1-12) и обозначать оператор (1-11) через $w \otimes \xi$.

[1] Т. е. тензор $v_1 \otimes \cdots \otimes v_n$ отличен от нуля и заменяется на пропорциональный при замене векторов $v_i$ на пропорциональные.

Если записывать операторы $U \to W$ их матрицами $A = (a_{ij})$ в выбранных выше базисах, то точки $w = (x_0 : x_1 : \dots : x_n) \in \mathbb{P}_m = \mathbb{P}(W)$ и $\xi = (y_0 : y_1 : \dots : y_m) \in \mathbb{P}_n = \mathbb{P}(U^*)$ перейдут при вложении Сегре в $m \times n$ матрицу $A = w^t \cdot \xi$ с элементами $a_{ij} = x_i y_j$, а его образ, состоящий из матриц ранга 1, задастся однородными квадратичными уравнениями

$$\det \begin{pmatrix} a_{ij} & a_{ik} \\ a_{\ell j} & a_{\ell k} \end{pmatrix} = a_{ij}a_{\ell k} - a_{ik}a_{\ell j} = 0\,.$$

Два семейства координатных пространств $\xi \times \mathbb{P}_m$ и $\mathbb{P}_n \times w$ при этом перейдут в два семейства лежащих на многообразии Сегре проективных пространств, образованных матрицами ранга 1 с фиксированными отношениями между строками и столбцами соответственно.

Пример 1.4 (квадрика Сегре в $\mathbb{P}_3$)
При $U = W = \Bbbk^2$ вложение Сегре задаёт биекцию между $\mathbb{P}_1 \times \mathbb{P}_1$ и обсуждавшейся в курсе геометрии[1] квадрикой Сегре в $\mathbb{P}_3 = \mathbb{P}\left(\mathrm{Mat}_2(\Bbbk)\right)$, точками которой являются ненулевые матрицы $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ с $ad - bc = 0$, рассматриваемые с точностью до пропорциональности. Эта биекция переводит пару точек $(x_0 : x_1)$ и $(y_0 : y_1)$ в матрицу

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \cdot \begin{pmatrix} y_0 & y_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 & x_1 y_0 \\ x_0 y_1 & x_1 y_1 \end{pmatrix} \tag{1-13}$$

и отображает два семейства координатных прямых $\mathbb{P}_1 \times \{y\}$, $\{x\} \times \mathbb{P}_1 \subset \mathbb{P}_1 \times \mathbb{P}_1$ в два семейства проективных прямых на квадрике Сегре, образованных матрицами ранга 1 с фиксированными отношениями [строка 1] : [строка 2] $= (x_0 : x_1)$ и [столбец 1] : [столбец 2] $= (y_0 : y_1)$. В каждом из семейств все прямые попарно скрещиваются, а любые две прямые из разных семейств пересекаются, при этом каждая точка квадрики Сегре является точкой пересечения ровно одной пары прямых из разных семейств, и никаких других прямых на квадрике Сегре нет.

Упражнение 1.2. Докажите все эти геометрические утверждения.

**1.2.3. Тензорные произведения абелевых групп.** Для произвольных модулей над коммутативным кольцом строение модуля $V_1 \otimes \dots \otimes V_n$ отнюдь не очевидно из описанных в n° 1.2 образующих и соотношений. В этом разделе мы вычислим, исходя из определения, тензорные произведения некоторых конечно порождённых $\mathbb{Z}$-модулей. В общем виде ответ будет получен в прим. 1.6 на стр. 15 при помощи более совершенной техники.

Покажем сначала, что $\mathbb{Z}/(m) \otimes \mathbb{Z}/(n) = 0$ при взаимно простых $m$ и $n$. Так как класс $[n] = n \pmod{m}$ обратим в кольце $\mathbb{Z}/(m)$, каждый элемент $a \in \mathbb{Z}/(m)$ представляется в виде $a = na'$, где $a' = [n]^{-1}a$. С другой стороны, для всех $b \in \mathbb{Z}/(n)$ произведение $nb = 0$ в $\mathbb{Z}/(n)$. Поэтому

$$a \otimes b = (n \cdot a') \otimes b = n \cdot (a' \otimes b) = a' \otimes (n \cdot b) = \alpha' \otimes 0 = \alpha' \otimes (0 \cdot 0) = 0 \cdot (\alpha' \otimes 0) = 0$$

для любого разложимого тензора $a \otimes b \in \mathbb{Z}/(m) \otimes \mathbb{Z}/(n)$. Поскольку такие тензоры линейно порождают $\mathbb{Z}/(m) \otimes \mathbb{Z}/(n)$ над $\mathbb{Z}$, этот модуль нулевой.

Теперь покажем, что $\mathbb{Z}/(p^n) \otimes \mathbb{Z}/(p^m) \simeq \mathbb{Z}/(p^n)$ при $n \leqslant m$. Отображение

$$\mu : \mathbb{Z}/(p^n) \times \mathbb{Z}/(p^m) \to \mathbb{Z}/(p^n)\,, \quad \left([a]_{p^n}, [b]_{p^m}\right) \mapsto [ab]_{p^n} = ab \cdot [1]_{p^n}\,,$$

[1] См. раздел 19.4.1 на стр. 246 в http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2021/lec_19.pdf.

корректно определено и $\mathbb{Z}$-билинейно. Достаточно проверить, что оно универсально. Для любого билинейного отображения $\varphi : \mathbb{Z}/(p^n) \times \mathbb{Z}/(p^m) \to W$ выполняется соотношение

$$\varphi\left([a]_{p^n}, [b]_{p^m}\right) = ab \cdot \varphi\left([1]_{p^n}, [1]_{p^m}\right) .$$

Поэтому $\mathbb{Z}$-линейное отображение $F : \mathbb{Z}/(p^n) \to W$ удовлетворяет равенству $F \circ \mu = \varphi$ если и только если оно переводит образующую $e = [1]_{p^n}$ модуля $\mathbb{Z}/(p^n)$ в элемент $\varphi\left([1]_{p^n}, [1]_{p^m}\right) \in W$. Это правило однозначно задаёт $F$ при условии, что оно корректно, т. е. $\lambda e = 0$ в $\mathbb{Z}/(p^n)$ влечёт $\lambda\varphi\left([1]_{p^n}, [1]_{p^m}\right) = 0$ в $W$. Все линейные соотношения $\lambda e = 0$ на образующую $e$ вытекают из соотношения $p^n e = 0$, которому элемент $\varphi\left([1]_{p^n}, [1]_{p^m}\right)$ тоже удовлетворяет:

$$p^n \cdot \varphi\left([1]_{p^n}, [1]_{p^m}\right) = \varphi\left(p^n \cdot [1]_{p^n}, [1]_{p^m}\right) = \varphi\left(0, [1]_{p^m}\right) = 0 .$$

Поэтому $\mathbb{Z}$-линейное отображение $F : \mathbb{Z}/(p^n) \to W$, $e \mapsto \varphi\left([1]_{p^n}, [1]_{p^m}\right)$, существует.

Упражнение 1.3. Убедитесь, что отображение $\tau : \mathbb{Z} \times A \to A$, $(n, a) \mapsto na$, билинейно и универсально для любого $\mathbb{Z}$-модуля $A$, откуда $\mathbb{Z} \otimes A = A$.

Вычисление тензорных произведений произвольных конечно порождённых абелевых групп сводится к рассмотренным трём случаям при помощи канонических изоморфизмов коммутативности, ассоциативности и дистрибутивности, обсуждаемых в следующем разделе.

**1.3. Канонические изоморфизмы.** Всюду далее речь идёт о произвольных модулях над любым коммутативным кольцом $K$. Линейные отображения $f : V_1 \otimes \cdots \otimes V_n \to W$ удобно задавать указанием значений $f(v_1 \otimes \cdots \otimes v_n)$ на разложимых тензорах, а затем по линейности продолжать $f$ на произвольные тензоры. Поскольку разложимые тензоры линейно порождают $V_1 \otimes \cdots \otimes V_n$, такое продолжение единственно при условии, что оно существует. Последнее равносильно тому, что все линейные соотношения, которые имеются между разложимыми тензорами, выполняются и между их образами в модуле $W$. Поскольку все эти соотношения линейно порождаются соотношениями полилинейности из форм. (1-9) на стр. 7, мы получаем следующий полезный критерий.

Лемма 1.3
Линейное отображение $f : V_1 \otimes \cdots \otimes V_n \to W$, $v_1 \otimes \cdots \otimes v_n \mapsto f(v_1, \ldots, v_n)$, существует если и только если векторы $f(v_1, \ldots, v_n) \in W$ полилинейно зависят[1] от векторов $v_i \in V_i$. □

Предложение 1.1
Имеется канонический изоморфизм $U \otimes W \simeq W \otimes U$, $u \otimes w \mapsto w \otimes u$.

Доказательство. Так как правило $u \otimes w \mapsto w \otimes u$ билинейно по $u, w$, оно по лем. 1.3 корректно определяет линейное отображение $U \otimes W \to W \otimes U$. Аналогично, существует линейное отображение $W \otimes U \to U \otimes W$, $w \otimes u \mapsto u \otimes w$. Оно обратно предыдущему, поскольку обе их композиции тождественно действуют на разложимых тензорах. □

Предложение 1.2
Имеются канонические изоморфизмы $V \otimes (U \otimes W) \simeq V \otimes U \otimes W \simeq (V \otimes U) \otimes W$, переводящие тензоры $v \otimes (u \otimes w)$, $v \otimes u \otimes w$ и $(v \otimes u) \otimes w$ друг в друга.

[1] Т. е. линейны по каждому $v_i$ при фиксированных остальных.

Доказательство. Поскольку тензор $v \otimes (u \otimes w) \in V \otimes (U \otimes W)$ трилинейно зависит от $(v, u, w)$, существует линейное отображение $V \otimes U \otimes W \to V \otimes (U \otimes W)$, $v \otimes u \otimes w \mapsto v \otimes (u \otimes w)$. Обратное отображение строится в два шага. При каждом $v \in V$ тензор $v \otimes u \otimes w$ билинейно зависит от $u$ и $w$. Поэтому имеется линейное отображение

$$\tau_v : U \otimes W \to V \otimes U \otimes W, \quad u \otimes w \mapsto v \otimes u \otimes w,$$

которое само по себе линейно зависит от $v$. Так как тензор $\tau_v(t) = v \otimes t$ билинеен по $v \in V$ и $t \in U \otimes W$, мы получаем искомое линейное отображение

$$V \otimes (U \otimes W) \to V \otimes U \otimes W, \quad v \otimes (u \otimes w) \mapsto v \otimes u \otimes w.$$

Изоморфизм $V \otimes U \otimes W \simeq (V \otimes U) \otimes W$ устанавливается аналогично. □

Предложение 1.3

Имеются канонические изоморфизмы

$$V \otimes (U \oplus W) \simeq (V \otimes U) \oplus (V \otimes W) \quad \text{и} \quad (U \oplus W) \otimes V \simeq (U \otimes V) \oplus (W \otimes V),$$

действующие на разложимые тензоры по правилам:

$$v \otimes (u \dotplus w) \leftrightarrows (v \otimes u) \dotplus (v \otimes w) \quad \text{и} \quad (u \dotplus w) \otimes v \leftrightarrows (u \otimes v) \dotplus (w \otimes v)$$

где через $a \dotplus b$ для $a \in A$ и $b \in B$ обозначено сложение элементов $(a, 0)$ и $(0, b)$ в прямой сумме модулей $A \oplus B$.

Доказательство. Достаточно построить первый изоморфизм, второй получится из него применением предл. 1.1. Отображение

$$V \otimes (U \oplus W) \to (V \otimes U) \oplus (V \otimes W), \quad v \otimes (u \dotplus w) \mapsto (v \otimes u) \dotplus (v \otimes w), \tag{1-14}$$

существует, поскольку $(v \otimes u) \dotplus (v \otimes w)$ билинеен по $v$ и $u \dotplus w$. Обратное отображение снова строится в два шага: сначала строим линейные отображения

$$f_1 : V \otimes U \to V \otimes (U \oplus W), \quad v \otimes u \mapsto v \otimes (u \dotplus 0),$$
$$f_2 : V \otimes W \to V \otimes (U \oplus W), \quad v \otimes w \mapsto v \otimes (0 \dotplus w),$$

затем складываем их в отображение

$$f : (V \otimes U) \oplus (V \otimes W) \to V \otimes (U \oplus W), \quad a \dotplus b \mapsto f_1(a) + f_2(b),$$

очевидно, линейное и обратное к (1-14). □

**1.4. Тензорное произведение линейных отображений.** Для любого набора $K$-линейных отображений $f_i : U_i \to W_i$ между произвольными модулями над коммутативным кольцом $K$, тензор

$$f_1(u_1) \otimes f_2(u_2) \otimes \cdots \otimes f_n(u_n) \in W_1 \otimes \cdots \otimes W_n$$

полилинейно зависит от векторов $(u_1, \ldots, u_n) \in U_1 \times \cdots \times U_n$. Поэтому существует единственное линейное отображение

$$f_1 \otimes \cdots \otimes f_n : U_1 \otimes \cdots \otimes U_n \to W_1 \otimes \cdots \otimes W_n,$$
$$u_1 \otimes \cdots \otimes u_n \mapsto f_1(u_1) \otimes f_2(u_2) \otimes \cdots \otimes f_n(u_n).$$

Оно называется *тензорным произведением* отображений $f_i : U_i \to W_i$.

Пример 1.5 (кронекерово произведение матриц)
Рассмотрим векторные пространства $U$ и $W$ с базисами $u_1, \dots, u_n \in U$ и $w_1, \dots, w_m \in W$. Если линейные операторы $f : U \to U$ и $g : W \to W$ имеют в этих базисах матрицы $F = (\varphi_{ij})$ и $G = (\gamma_{k\ell})$, то матрица оператора $f \otimes g : U \otimes W \to U \otimes W$ в базисе из тензоров $u_j \otimes w_\ell$ имеет размеры $(mn) \times (mn)$, а её элементы естественно нумеруются упорядоченными парами $(\alpha, \beta)$, $1 \leqslant \alpha \leqslant n$, $1 \leqslant \beta \leqslant m$. Эта матрица называется *кронекеровым произведением* матриц $F$, $G$ и обозначается $F \otimes G$. Поскольку

$$f \otimes g\,(u_j \otimes w_\ell) = \Big(\sum_i u_i \varphi_{ij}\Big) \otimes \Big(\sum_k w_k \gamma_{k\ell}\Big) = \sum_{i,k} \varphi_{ij}\gamma_{k\ell} \cdot u_i \otimes w_k\,,$$

в пересечении $(i,k)$-ой строки и $(j,\ell)$-го столбца матрицы $F \otimes G$ стоит произведение $\varphi_{ij}\gamma_{k\ell}$. В лексикографически упорядоченном базисе

$$u_1 \otimes w_1,\ \dots\ ,\ u_1 \otimes w_m,\ u_2 \otimes w_1,\ \dots\ ,\ u_2 \otimes w_m,\ \dots\ , u_n \otimes w_1,\ \dots\ ,\ u_n \otimes w_m$$

матрица $F \otimes G$ имеет блочный вид и состоит из $n^2$ блоков размера $m \times m$, каждый из которых пропорционален матрице $G$:

$$F \otimes G = (\varphi_{ij}) \otimes (\gamma_{k\ell}) = \begin{pmatrix} \varphi_{11}G & \varphi_{12}G & \cdots & \varphi_{1n}G \\ \varphi_{21}G & \varphi_{22}G & \cdots & \varphi_{2n}G \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{n1}G & \varphi_{n2}G & \cdots & \varphi_{nn}G \end{pmatrix}.$$

Лемма 1.4
Если гомоморфизм $K$-модулей $f : U \twoheadrightarrow W$ сюрьективен, то для любого $K$-модуля $V$, гомоморфизм $\mathrm{Id}_V \otimes f : V \otimes U \to V \otimes W$ тоже сюрьективен.

Доказательство. Образ отображения $f \otimes \mathrm{Id}_V$ содержит все разложимые тензоры $v \otimes w \in V \otimes W$. □

Упражнение 1.4. Убедитесь, что для любого $K$-модуля $V$ имеется канонический изоморфизм $K \otimes V \xrightarrow{\sim} V$, $\lambda \otimes u \mapsto \lambda u$.

Лемма 1.5
Если ненулевой $K$-модуль $F$ свободен, то для любого инъективного гомоморфизма $K$-модулей $f : U \hookrightarrow W$ гомоморфизм $\mathrm{Id}_F \otimes f : F \otimes U \to F \otimes W$ тоже инъективен.

Доказательство. Если $F \simeq K$ имеет ранг 1, изоморфизмы из упр. 1.4

$$K \otimes U \xrightarrow{\sim} U\,, \quad \lambda \otimes u \mapsto \lambda u\,,$$
$$K \otimes W \xrightarrow{\sim} W\,, \quad \mu \otimes w \mapsto \mu w\,,$$

отождествляют отображение $\mathrm{Id}_F \otimes f : K \otimes U \to K \otimes W$ с исходным отображением $f : U \to W$, инъективным по условию. Произвольный свободный модуль с базисом $E$ является прямой суммой $F \simeq \bigoplus_{e \in E} Ke$ свободных модулей ранга 1, занумерованных базисными векторами $e \in E$. По предл. 1.3 и упр. 1.4 модули

$$\begin{aligned} F \otimes U &\simeq \bigoplus\nolimits_{e \in E} (Ke \otimes U) \simeq \bigoplus\nolimits_{e \in E} U_e \\ F \otimes W &\simeq \bigoplus\nolimits_{e \in E} (Ke \otimes W) \simeq \bigoplus\nolimits_{e \in E} W_e \end{aligned} \tag{1-15}$$

являются прямыми суммами занумерованных базисными векторами $e \in E$ одинаковых копий $U_e \overset{\text{def}}{=} Ke \otimes U \simeq U$ и $W_e \overset{\text{def}}{=} Ke \otimes W \simeq W$ модулей $U, W$, причём изоморфизмы (1-15) отождествляют линейное отображение $\mathrm{Id}_F \otimes f$ с диагональным отображением $\bigoplus_{e \in E} U_e \to \bigoplus_{e \in E} U_e$, переводящим последовательность векторов $\left(u_e\right)_{e \in E}$ в последовательность векторов $\left(f(u_e)\right)_{e \in E}$. При инъективном $f$ такое отображение тоже инъективно. □

Предостережение 1.1. Если модуль $V$ не свободен, тензорное произведение

$$\mathrm{Id}_V \otimes f : V \otimes U \to V \otimes W$$

может оказаться не инъективным даже для вложения $f : U \hookrightarrow W$ свободных модулей. Например, вложение $\mathbb{Z}$-модулей $f : \mathbb{Z} \hookrightarrow \mathbb{Z}$, $z \mapsto 2z$, при тензорном умножении на тождественный эндоморфизм модуля $\mathbb{Z}/(2)$ превращается в нулевой гомоморфизм $\mathbb{Z}/(2) \to \mathbb{Z}/(2)$, $[1]_2 \mapsto [0]_2$.

**1.5. Тензорное произведение модулей, заданных образующими и соотношениями.** Напомню[1], что если $K$-модуль $V$ линейно порождается над $K$ векторами $v_1, \dots, v_n$, то он изоморфен фактору $K^n / R_v$ свободного модуля $K^n$ по подмодулю $R_v \subset K^n$ линейных соотношений между образующими $v_i$, который состоит из всех таких строк $(x_1, \dots, x_n) \in K^n$, что $\sum x_i e_i = 0$ в $V$. Следующая далее теор. 1.2 описывает тензорное произведение $V_1 \otimes V_2$ двух представленных таким способом $K$-модулей $V_1 \simeq F_1 / R_1$ и $V_2 \simeq F_2 / R_2$ как фактор свободного модуля $F_1 \otimes F_2$ по подмодулю соотношений, устроенному следующим образом. По лем. 1.5 вложения $\iota_1 : R_1 \hookrightarrow F_1$ и $\iota_2 : R_2 \hookrightarrow F_2$ задают вложения $\iota_1 \otimes \mathrm{Id}_{F_2} : R_1 \otimes F_2 \hookrightarrow F_1 \otimes F_2$ и $\mathrm{Id}_{F_1} \otimes \iota_2 : F_1 \otimes R_2 \hookrightarrow F_1 \otimes F_2$, позволяющие рассматривать тензорные произведения $R_1 \otimes F_2$ и $F_1 \otimes R_2$ как подмодули свободного модуля $F \otimes G$. Искомый модуль соотношений является линейной оболочкой этих двух подмодулей и обозначается $R_1 \otimes F_2 + F_1 \otimes R_2 \subset F_1 \otimes F_2$.

Теорема 1.2
$\left(F_1/R_1\right) \otimes \left(F_1/R_1\right) \simeq \left(F_1 \otimes F_2\right) / \left(R_1 \otimes F_2 + F_1 \otimes R_2\right)$ для любых свободных модулей $F_1, F_2$ над произвольным коммутативным кольцом $K$ и любых их подмодулей $R_1 \subset F_1$, $R_2 \subset F_2$.

Доказательство. Положим $V_1 = F_1/R_1$, $V_2 = F_2/R_2$, $S = R_1 \otimes F_2 + F_1 \otimes R_2 \subset F_1 \otimes F_2$. Для любых $f_1 \in F_1$, $f_2 \in F_2$ класс $[f_1 \otimes f_2]_S = f_1 \otimes f_2 \pmod{S} \in \left(F_1 \otimes F_2\right)/S$ зависит только от классов $[f_1]_{R_1} = f_1 \pmod{R_1} \in V_1$ и $[f_2]_{R_2} = f_2 \pmod{R_2} \in V_2$, так как для всех $r_1 \in R_1$, $r_2 \in R_2$

$$(f_1 + r_1) \otimes (f_2 + r_2) = f_1 \otimes f_2 + \left(r_1 \otimes f_2 + f_1 \otimes r_2 + r_1 \otimes r_2\right) \equiv f_1 \otimes f_2 \pmod{S} .$$

Поэтому корректно определено билинейное отображение

$$\overline{\tau} : V_1 \times V_2 \to \left(F_1 \otimes F_2\right)/S , \quad ([f_1]_{R_1}, [f_2]_{R_2}) \mapsto [f_1 \otimes f_2]_S , \tag{1-16}$$

включающееся в коммутативную диаграмму

$$\begin{tikzcd} F_1 \times F_2 \arrow[r, "\tau"] \arrow[d, "\pi_1 \times \pi_2"'] & F_1 \otimes F_2 \arrow[d, "\pi"] \\ V_1 \times V_2 \arrow[r, "\overline{\tau}"] & \left(F_1 \otimes F_2\right)/S \end{tikzcd}$$

[1] См. пример 6.12 на стр. 87 в http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_06.pdf.

где через $\tau : F_1 \times F_2 \to F_1 \otimes F_2$ обозначено универсальное билинейное отображение, а

$$\pi_1 : F_1 \twoheadrightarrow V_1 , \quad \pi_2 : F_2 \twoheadrightarrow V_2 , \quad \pi : F_1 \otimes F_2 \twoheadrightarrow (F_1 \otimes F_2)/S$$

суть линейные проекции на факторы. Покажем, что отображение (1-16) универсально. Для любого билинейного отображения $\varphi : V_1 \times V_2 \to W$ композиция

$$\varphi \circ (\pi_1 \times \pi_2) : F_1 \times F_2 \to W , \quad (f_1, f_2) \mapsto \varphi\left([f_1]_{R_1}, [f_2]_{R_2}\right) ,$$

тоже билинейна. Поэтому существует единственное такое линейное отображение

$$\psi : F_1 \otimes F_2 \to W ,$$

что $\psi \circ \tau = \varphi \circ (\pi_1 \times \pi_2)$, т. е. мы имеем коммутативную диаграмму

$$\begin{tikzcd}
F_1 \times F_2 \arrow[r, "\tau"] \arrow[d, "\pi_1\times\pi_2"'] & F_1 \otimes F_2 \arrow[d, "\pi"] \arrow[ddr, "\psi"] & \\
V_1 \times V_2 \arrow[r, "\overline{\tau}"] \arrow[drr, "\varphi"'] & \left(F_1 \otimes F_2\right)/S \arrow[dr, "\overline{\psi}"] & \\
& & W .
\end{tikzcd} \tag{1-17}$$

Поскольку для всех $f_1 \in F_1$, $f_2 \in F_2$ выполняется равенство $\psi(f_1 \otimes f_2) = \varphi\left([f_1]_{R_1}, [f_2]_{R_2}\right)$, отображение $\psi$ аннулирует оба линейно порождающих $S$ подмодуля $R_1 \otimes F_2, F_1 \otimes R_2 \subset F_1 \otimes F_2$ и факторизуется до линейного отображения $\overline{\psi} : \left(F_1 \otimes F_2\right)/S \to W$, удовлетворяющего соотношению $\overline{\psi} \circ \pi \circ \tau = \varphi \circ (\pi_1 \times \pi_2)$. Поэтому $\overline{\psi} \circ \overline{\tau} \circ (\pi_1 \times \pi_2) = \overline{\psi} \circ \pi \circ \tau = \varphi \circ (\pi_1 \times \pi_2)$. Так как проекция $\pi_1 \times \pi_2$ сюрьективна, $\varphi = \overline{\psi} \circ \overline{\tau}$. Остаётся проверить, что любое линейное отображение $\eta : \left(F_1 \otimes F_2\right)/S \to W$, удовлетворяющее соотношению $\varphi = \eta \circ \overline{\tau}$, совпадает с $\overline{\psi}$. Поскольку

$$\eta \circ \pi \circ \tau = \eta \circ \overline{\tau} \circ (\pi_1 \times \pi_2) = \varphi \circ (\pi_1 \times \pi_2) = \overline{\psi} \circ \pi \circ \tau ,$$

универсальное свойство отображения $\tau$ влечёт равенство $\eta \circ \pi = \overline{\psi} \circ \pi$. Равенство $\eta = \overline{\psi}$ вытекает из него силу сюрьективности проекции $\pi$. □

Пример 1.6 (тензорные произведения $\mathbb{Z}$-модулей)
Все проделанные в n° 1.2.3 на стр. 10 вычисления сворачиваются при помощи теор. 1.2 в одну строчку: для любых $m, n \in \mathbb{Z}$

$$\frac{\mathbb{Z}}{(m)} \otimes \frac{\mathbb{Z}}{(n)} \simeq \frac{\mathbb{Z} \otimes \mathbb{Z}}{(m) \otimes \mathbb{Z} + \mathbb{Z} \otimes (n)} \simeq \frac{\mathbb{Z}}{(m, n)} = \frac{\mathbb{Z}}{(\text{нод}(m, n))} ,$$

где предпоследнее равенство задаётся изоморфизмом из упр. 1.4 на стр. 13.

## §2. Тензорная алгебра

**2.1. Тензорные степени.** Рассмотрим произвольный модуль $V$ над коммутативным кольцом $K$ с единицей. Тензорное произведение $n$ экземпляров этого модуля $V^{\otimes n} \overset{\text{def}}{=} V \otimes \cdots \otimes V$ называется $n$-той *тензорной степенью* модуля $V$. Мы полагаем $V^{\otimes 0} \overset{\text{def}}{=} K$ и $V^{\otimes 1} \overset{\text{def}}{=} V$. Тензорное умножение векторов задаёт на бесконечной прямой сумме $TV \overset{\text{def}}{=} \bigoplus_{n \geqslant 0} V^{\otimes n}$ структуру ассоциативной (некоммутативной) градуированной алгебры над $K$. Если модуль $V$ свободен с базисом $E \subset V$, то моном $1 \in V^0$ и всевозможные тензорные мономы от базисных векторов

$$e_1 \otimes \cdots \otimes e_m\,, \quad e_i \in E\,,\ m \in \mathbb{N}\,, \tag{2-1}$$

составляют базис модуля $TV$ над $K$ по теор. 1.1 на стр. 8. Умножение мономов (2-1) заключается в приписывании их друг к другу через знак $\otimes$, моном 1 служит единицей. Таким образом, фиксация базиса $E$ в $V$ позволяет отождествить алгебру $TV$ с алгеброй многочленов от *некоммутирующих* друг с другом переменных $e \in E$. При этом компонента $V^{\otimes n} \subset TV$ отождествляется с модулем однородных многочленов степени $n$.

Алгебра $TV$ называется *тензорной алгеброй* модуля $V$ или *свободной ассоциативной $K$-алгеброй*, порожденной $V$. Вложение $\iota : V \hookrightarrow TV$ в качестве подмодуля $V^{\otimes 1}$ обладает универсальным свойством, аналогичным универсальному свойству базиса в свободном модуле.

Предложение 2.1 (универсальное свойство тензорной алгебры)
Для любого $K$-линейного отображения $f : V \to A$ в произвольную ассоциативную $K$-алгебру $A$ существует единственный такой гомоморфизм $K$-алгебр $\alpha : TV \to A$, что $f = \alpha \circ \iota$. Другими словами, гомоморфизмы $K$-алгебр $TV \to A$ находятся в канонической биекции с $K$-линейными отображениям $V \to A$.

Доказательство. Искомый гомоморфизм $\alpha$ должен переводить каждый разложимый тензор

$$v_1 \otimes \cdots \otimes v_n \in TV$$

в произведение $f(v_1) \cdots f(v_n) \in A$. Поскольку разложимые тензоры линейно порождают алгебру $TV$, гомоморфизм $\alpha$ единствен, если существует. Так как для любого $K$-линейного отображения $f : V \to A$ произведение $f(v_1) \cdots f(v_n) \in A$ полилинейно по $v_i$, по лем. 1.3 на стр. 11 для каждого $n \in \mathbb{N}$ существует линейное отображение

$$\alpha_n : V^{\otimes n} \to A\,, \quad v_1 \otimes \cdots \otimes v_n \mapsto f(v_1) f(v_2) \cdots f(v_n)\,.$$

Нужный нам гомоморфизм $\alpha : TV \to A$ переводит конечную сумму $\sum_k t_k$ однородных тензоров $t_k \in V^{\otimes k}$ в сумму $\sum_k \alpha_k(t_k) \in A$, где $\alpha_0 : V^0 \to A$ переводит единицу в единицу. □

Упражнение 2.1. Убедитесь, что $K$-алгебра $TV$ вместе с вложением $\iota : V \hookrightarrow TV$ определяются своим универсальным свойством однозначно с точностью до единственного изоморфизма $K$-алгебр, перестановочного с вложением $\iota$.

**2.2. Свёртки.** Для двойственных векторных пространств $V, V^*$ над полем $\Bbbk$ и пары разложимых тензоров одинаковой степени $t = v_1 \otimes \cdots \otimes v_n \in V^{\otimes n}$ и $\vartheta = \xi_1 \otimes \cdots \otimes \xi_n \in V^{*\otimes n}$ число

$$\langle\, t\,, \vartheta\,\rangle \overset{\text{def}}{=} \prod_{i=1}^{n} \xi_i(v_i) = \prod_{i=1}^{n} \langle\, v_i\,, \xi_i\,\rangle \in \Bbbk \tag{2-2}$$

называется *полной свёрткой* тензоров $t$ и $\vartheta$. Поскольку при каждом $\vartheta \in V^{*\otimes n}$ число (2-2) полилинейно по векторам $v_i$, существует единственный ковектор $c_\vartheta \in V^{\otimes n*}$

$$c_\vartheta : V^{\otimes n} \to \Bbbk, \quad v_1 \otimes \cdots \otimes v_n \mapsto \langle\, v_1 \otimes \cdots \otimes v_n \,,\, \vartheta \,\rangle,$$

и этот ковектор полилинеен по сомножителям $\xi_1, \dots, \xi_n$ разложимого тензора $\vartheta$. Поэтому существует единственное линейное отображение

$$V^{*\otimes n} \to V^{\otimes n*}, \quad \vartheta \mapsto c_\vartheta\,. \tag{2-3}$$

Иначе говоря, полная свёртка (2-2) корректно задаёт билинейное спаривание[1]

$$V^{\otimes n} \times V^{*\otimes n} \to \Bbbk, \quad (t, \vartheta) \mapsto \langle\, t \,,\, \vartheta \,\rangle\,. \tag{2-4}$$

Предложение 2.2

Для конечномерного пространства $V$ спаривание (2-4) совершенно, т. е. линейное отображение (2-3) является изоморфизмом.

Доказательство. Тензорные мономы $e_{i_1} \otimes \cdots \otimes e_{i_n}$ и $e^*_{i_1} \otimes \cdots \otimes e^*_{i_n}$, составленные из векторов двойственных друг другу базисов в пространствах $V$ и $V^*$ образуют двойственные базисы в $V^{\otimes n}$ и $V^{*\otimes n}$. □

Следствие 2.1

Сопоставление разложимому тензору $\xi = \xi_1 \otimes \cdots \otimes \xi_n \in V^{*\otimes n}$ полилинейной формы

$$\xi : V \times \cdots \times V \to \Bbbk, \quad \xi(v_1, \dots, v_n) = \prod_{i=1}^{n} \xi_i(v_i)\,,$$

задаёт для любого конечномерного пространства $V$ изоморфизм

$$V^{*\otimes n} \simeq \mathrm{Hom}(V, \dots, V;\, \Bbbk)\,. \tag{2-5}$$

Доказательство. В силу универсального свойства тензорного произведения пространство $V^{\otimes n*}$ линейных отображений $V^{\otimes n} \to \Bbbk$ изоморфно пространству $n$-линейных форм $V \times \cdots \times V \to \Bbbk$. Изоморфизм (2-5) является композицией этого изоморфизма с изоморфизмом (2-3). □

**2.2.1. Частичные свертки.** Любая пара инъективных, но не обязательно монотонных отображений

$$\{1, 2, \dots\, p\} \xleftarrow{\;I\;} \{1, 2, \dots\, m\} \xhookrightarrow{\;J\;} \{1, 2, \dots\, q\}$$

задаёт два слова $I = (i_1, \dots, i_m)$, $J = (j_1, \dots, j_m)$ одинаковой длины $m$, состоящие из неповторяющихся в пределах каждого слова индексов $i_\nu = I(\nu)$ и $j_\nu = J(\nu)$. Линейный оператор

$$\begin{gathered} c^I_J : V^{*\otimes p} \otimes V^{\otimes q} \;\to\; V^{*\otimes(p-m)} \otimes V^{\otimes(q-m)}\,, \\ \xi_1 \otimes \cdots \otimes \xi_p \otimes v_1 \otimes \cdots \otimes v_q \mapsto \prod_{\nu=1}^{m} \xi_{i_\nu}(v_{j_\nu}) \cdot \bigotimes_{i \notin I} \xi_i \otimes \bigotimes_{j \notin J} v_j\,, \end{gathered} \tag{2-6}$$

[1] См. раздел 7.2 части I

который для каждого $\nu = 1, \dots, m$ сворачивает $i_\nu$-й сомножитель произведения $V^{*\otimes p}$ с $j_\nu$-м сомножителем произведения $V^{\otimes q}$, оставляя все остальные тензорные сомножители в их первоначальном порядке, называется *частичной сверткой* по индексам $I$ и $J$. Отметим, что разные пары отображений $I$, $J$ могут приводить к *разным* отображениям свёртки даже в тех случаях, когда они имеют одинаковые пары образов и отличаются лишь упорядочением индексов внутри этих образов.

Пример 2.1 (свертка вектора с полилинейной формой)
Интерпретируем $n$-линейную форму $\varphi(v_1, \dots, v_n)$ как тензор из $\varphi \in V^{*\otimes n}$ посредством изоморфизма из сл. 2.1. Свёртка формы $\varphi$ с произвольно выбранным вектором $v \in V$ по первому тензорному сомножителю лежит в $V^{*\otimes(n-1)}$ и может интерпретироваться как $(n-1)$-линейная форма на $V$. Эта форма называется *внутренним произведением* $v$ и $\varphi$ и обозначается $v \lrcorner \varphi$ или $i_v\varphi$. Поскольку для разложимой формы $\varphi = \varphi_1 \otimes \dots \otimes \varphi_n$ имеет место линейное по $\varphi$ равенство

$$i_v\varphi(w_1, \dots, w_{n-1}) = \varphi(v, w_1, \dots, w_{n-1}), \tag{2-7}$$

это равенство выполнено для всех полилинейных форм $\varphi$, т. е. внутреннее умножение формы на вектор означает фиксацию этого вектора в качестве первого аргумента формы.

**2.2.2. Линейный носитель тензора.** Для заданного тензора $t \in V^{\otimes n}$ пересечение всех таких векторных подпространств $U \subset V$, что $t \in U^{\otimes n}$, называется *линейным носителем* тензора $t$ и обозначается $\operatorname{supp}(t) \subset V$. Иначе носитель можно охарактеризовать как такое наименьшее по включению или же по размерности подпространство $U \subset V$, что $t \in U^{\otimes n}$. Эквивалентность всех приведённых описаний вытекает из равенства $U^{\otimes n} \cap W^{\otimes n} = (U \cap W)^{\otimes n}$.

Упражнение 2.2. Докажите это равенство.

Размерность носителя называется *рангом* тензора и обозначается $\operatorname{rk} t \overset{\text{def}}{=} \dim \operatorname{supp}(t)$. Тензор $t$ называется *вырожденным*, если его носитель $\operatorname{supp}(t) \subsetneq V$ имеет положительную коразмерность. Это означает, что некоммутативный многочлен $t$ «эффективно зависит» от меньшего, чем $\dim V$, числа переменных, и при помощи линейной замены базиса можно убрать часть переменных из $t$. Например, если $\dim \operatorname{supp}(t) = 1$, то $t = c \cdot v^{\otimes n}$ для некоторых $c \in \Bbbk$ и $v \in V$.

Явно указать векторы, линейно порождающие $\operatorname{supp}(t)$ над $\Bbbk$ можно при помощи свёрток. Для любой последовательности $J = j_1, \dots, j_{n-1}$ из $n-1$ неповторяющихся индексов[1] $1 \leqslant j_\nu \leqslant n$ обозначим через

$$t_J : V^{*\otimes(n-1)} \to V, \quad \xi \mapsto c^{1,\dots,(n-1)}_{j_1,\dots,j_{n-1}}(\xi \otimes t), \tag{2-8}$$

полную свёртку с тензором $t$, которая спаривает $\nu$-й сомножитель произведения $V^{*\otimes(n-1)}$ с $j_\nu$-м сомножителем тензора $t$ для всех $1 \leqslant \nu \leqslant (n-1)$. Если записать $t$ в виде суммы разложимых тензоров вида $v_1 \otimes \dots \otimes v_n$, то результатом такой свёртки будет линейная комбинация векторов $v_i$ с $i \notin J$. Очевидно, что она лежит в $\operatorname{supp}(t)$.

Теорема 2.1
Пространство $\operatorname{supp}(t)$ линейно порождается образами всех свёрток (2-8).

Доказательство. Обозначим $\operatorname{supp}(t)$ через $W \subset V$. Достаточно доказать, каждая линейная форма $\xi \in V^*$, аннулирующая образы всех свёрток (2-8), аннулирует подпространство $W$. Предположим противное: пусть ковектор $\xi \in V^*$ имеет ненулевое ограничение на $W$, но аннулирует

[1] Подчеркнём, что индексы в последовательности не обязаны возрастать или убывать.

$t_J\left(V^{*\otimes(n-1)}\right)$ для всех $J$. Выберем в $V^*$ базис $\xi_1, \dots, \xi_d$, в котором $\xi_1 = \xi$ и ограничения ковекторов $\xi_1, \dots, \xi_k$ на $W$ образуют базис в $W^*$. Обозначим через $w_1, \dots, w_k$ двойственный базис пространства $W$ и разложим $t$ по этому базису. Значение $\xi\left(t_J(\xi_{i_1} \otimes \dots \otimes \xi_{i_{n-1}})\right)$ равно полной свёртке тензора $t$ с базисным тензорным мономом $\xi_{i_1} \otimes \dots \otimes \xi_{i_{n-1}} \otimes \xi_1$ по всем $n$ тензорным сомножителям в том порядке, который предписан последовательностью[1] $J$. Получающееся в результате этой свёртки число равно коэффициенту, с которым соответствующий двойственный тензорный моном[2] от базисных векторов $w_i$ входит в разложение $t$. Подбирая надлежащие $J$, можно получить коэффициент при любом содержащем $w_1$ мономе, входящем в разложение $t$. Тем самым, все они нулевые, т. е. $w_1 \notin \operatorname{supp}(t)$ вопреки нашему выбору. □

**2.3. Коммутативные и грассмановы многочлены.** В некоммутативном кольце $R$ бывают идеалы трёх типов. Подкольцо $I \subset R$ называется *левым идеалом*, если $xa \in I$ для всех $a \in I$, $x \in R$. Симметричным образом, $I \subset R$ называется *правым идеалом*, если $ax \in I$ для всех $a \in I$, $x \in R$. Идеал $I \subset R$ называется *двусторонним*, если он одновременно и левый, и правый.

Иначе двусторонние идеалы можно охарактеризовать как ядра гомоморфизмов колец. Действительно, если элемент $a \in R$ аннулируется гомоморфизмом $\varphi : R \to S$, то для любых $x, y \in R$ выполняется равенство $\varphi(xay) = \varphi(x)\varphi(a)\varphi(y) = 0$. Наоборот, если аддитивная подгруппа $I \subset R$ является двусторонним идеалом, то на фактор группе $R/I$ можно корректно задать умножение правилом $[a][b] \stackrel{\text{def}}{=} [ab]$.

Упражнение 2.3. Убедитесь в этом.

При этом аддитивный гомоморфизм фактризации $R \twoheadrightarrow R/I$ становится гомоморфизмом колец с ядром $I$. Из теоремы о строении гомоморфизма абелевых групп[3] вытекает, что каждый гомоморфизм колец $\varphi : R \to S$ является композицией сюрьективного гомоморфизма факторизации $R \twoheadrightarrow R/\ker\varphi \simeq \operatorname{im}\varphi$ и вложения $R/\ker\varphi \simeq \operatorname{im}\varphi \hookrightarrow S$.

Алгебры многочленов и грассмановых многочленов являются факторами тензорной алгебры по двусторонним идеалам, порождённым соотношениями *коммутирования* и *антикоммутирования*.

**2.3.1. Симметрическая алгебра модуля.** Рассмотрим в тензорной алгебре $TV$ произвольного модуля $V$ над коммутативным кольцом $K$ двусторонний идеал $\mathcal{I}_{\text{sym}} \subset TV$, порождённый всевозможными разностями

$$u \otimes w - w \otimes u \in V \otimes V\,. \tag{2-9}$$

Он состоит из конечных линейных комбинаций тензоров, которые можно получить умножая разности (2-9) с обеих сторон на любые элементы тензорной алгебры. Таким образом, пересечение $\mathcal{I}_{\text{sym}} \cap V^{\otimes n}$ линейно порождается разностями вида

$$(\cdots \otimes v \otimes w \otimes \cdots) - (\cdots \otimes w \otimes v \otimes \cdots)\,,$$

где оба заключённых в скобки тензора разложимы и обозначенные многоточиями фрагменты у них одинаковы. Весь идеал $\mathcal{I}_{\text{sym}}$ является прямой сумой таких однородных компонент:

$$\mathcal{I}_{\text{sym}} = \bigoplus_{n \geqslant 2} \left(\mathcal{I}_{\text{sym}} \cap V^{\otimes n}\right)\,.$$

[1] Т. е. $j_\nu$-й сомножитель тензора $t$ сворачивается с $\xi_{i_\nu}$ при $1 \leqslant \nu \leqslant n-1$, а оставшийся в $t$ сомножитель с номером $\{1, \dots, n\} \smallsetminus J$ сворачивается с $\xi_1$.

[2] $j_\nu$-й множитель этого монома равен $w_{i_\nu}$ при $1 \leqslant \nu \leqslant n-1$, а оставшийся сомножитель с номером $\{1, \dots, n\} \smallsetminus J$ равен $w_1$.

[3] См. http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_02.pdf, предложение 2.1 на стр. 28.

Фактор алгебра $SV \stackrel{\text{def}}{=} TV/\mathcal{I}_{\text{sym}}$ называется *симметрической алгеброй* модуля $V$. Умножение, индуцированное в ней тензорным произведением векторов, называется *коммутативным умножением* и обозначается точкой, которую обычно опускают. Как $K$-модуль, симметрическая алгебра является прямой суммой своих однородных компонент:

$$SV = \bigoplus_{n\geqslant 0} S^n V\,, \quad \text{где} \quad S^n V \stackrel{\text{def}}{=} V^{\otimes n}/(\mathcal{I}_{\text{sym}} \cap V^{\otimes n})\,.$$

Модуль $S^nV$ называется *$n$-й симметрической степенью* пространства $V$. Обратите внимание, что $S^0V = K$ и $S^1V = V$. Включение $\iota : V \hookrightarrow SV$ в качестве прямого слагаемого $S^1V$ обладает следующим универсальным свойством.

Упражнение 2.4. Убедитесь, что для любого $K$-линейного отображения $f : V \to A$ из модуля $V$ в произвольную коммутативную $K$-алгебру $A$ имеется единственный такой гомоморфизм $K$-алгебр $\tilde{f} : SV \to A$, что $f = \tilde{f} \circ \iota$, причём $SV$ и $\iota$ определяются этим свойством однозначно с точностью до единственного перестановочного с $\iota$ изоморфизма $K$-алгебр.

По этой причине симметрическую алгебру $SV$ иначе называют *свободной* коммутативной $K$-алгеброй с единицей, порождённой $K$-модулем $V$.

**2.3.2. Симметричные полилинейные отображения.** Полилинейное отображение

$$\varphi : V \times \cdots \times V \to U \tag{2-10}$$

называется *симметричным*, если $\varphi(v_{g_1}, \dots , v_{g_n}) = \varphi(v_1, \dots , v_n)$ для всех перестановок $g \in S_n$. Симметричные полилинейные отображения образуют $K$-подмодуль

$$\mathrm{Sym}^n(V, U) \subset \mathrm{Hom}(V, \dots , V; U)$$

в модуле всех $n$-линейных отображений (2-10). Композиция фиксированного симметричного $n$-линейного отображения (2-10) с линейными отображениями $F : U \to W$ доставляет линейное по $F$ отображение

$$\mathrm{Hom}(U, W) \to \mathrm{Sym}^n(V, W)\,, \quad F \mapsto F \circ \varphi\,.$$

Если это отображение является изоморфизмом для всех модулей $W$, отображение $\varphi$ называется *универсальным* симметричным $n$-линейным отображением или *коммутативным произведением* векторов.

Упражнение 2.5. Покажите, что модуль, в котором принимает значение коммутативное произведение, единствен с точностью до единственного перестановочного с этим произведением изоморфизма.

Предложение 2.3

Композиция $\sigma_n = \pi_{S^n} \circ \tau$ тензорного произведения $\tau : V \times \cdots \times V \to V^{\otimes n}$ с последующей проекцией $\pi_{S^n} : V^{\otimes n} \twoheadrightarrow S^nV$ является универсальным симметричным $n$-линейным отображением.

Доказательство. В силу универсального свойства тензорного произведения любое $n$-линейное отображение $\varphi : V \times \cdots \times V \to W$ однозначно представляется в виде композиции $\varphi = \widetilde{F} \circ \tau$ с линейным отображением $\widetilde{F} : V^{\otimes n} \to W$. Если $\varphi$ симметрично, $\widetilde{F}$ аннулирует соотношения коммутативности (2-9): $\widetilde{F}\big((\cdots \otimes v \otimes w \otimes \cdots) - (\cdots \otimes w \otimes v \otimes \cdots)\big) = \widetilde{F}(\cdots \otimes v \otimes w \otimes \cdots) - - \widetilde{F}(\cdots \otimes w \otimes v \otimes \cdots) = \varphi(\dots , v, w, \dots) - \varphi(\dots , w, v, \dots) = 0$, и значит, корректно факторизуется до линейного отображения $F: S^nV \to W$, $v_1 \dots v_n \mapsto \varphi(v_1, \dots, v_n)$. Таким образом, $\varphi = \widetilde{F} \circ \tau = F \circ \pi_{S^n} \circ \tau = F \circ \sigma_n$. Из-за универсальности $\tau$ любое линейное отображение $F' : S^nV \to W$, для которого $\varphi = F' \circ \sigma_n = F' \circ \pi_{S^n} \circ \tau$, удовлетворяет равенству $F' \circ \pi_{S^n} = F \circ \pi_{S^n}$, влекущему равенство $F' = F$ в силу сюрьективности проекции $\pi_{S^n}$. □

Следствие 2.2
Для любого[1] векторного пространства $V$ над произвольным полем $\Bbbk$ пространство $\mathrm{Sym}^n(V, \Bbbk)$ симметричных $n$-линейных форм $V \times \dots \times V \to \Bbbk$ канонически двойственно $n$-той симметрической степени $S^nV$.

Доказательство. Отправляя линейную форму $\xi : S^nV \to \Bbbk$ в её композицию с коммутативным умножением $\sigma_n : V \times \dots \times V \to S^nV$, мы получаем линейное отображение $(S^nV)^* \to \mathrm{Sym}^n(V, \Bbbk)$, являющееся изоморфизмом в силу универсального свойства $\sigma_n$. □

Следствие 2.3
Если модуль $V$ свободен с базисом $E \subset V$, то модуль $S^nV$ тоже свободен, и коммутативные мономы $e^{\boldsymbol{m}} = \prod_{e \in E} e^{m(e)}$, занумерованные всевозможными функциями $\boldsymbol{m} : E \to \mathbb{Z}_{\geqslant 0}$, $e \mapsto m(e)$, с конечным носителем и суммой значений $\sum_{e \in E} m(e) = n$, составляют базис в $S^nV$. Иначе говоря, выбор базиса в $V$ задаёт изоморфизм симметрической алгебры $SV$ с алгеброй многочленов от базисных векторов, причём подмодуль $S^nV$ переводится этим изоморфизмом в модуль однородных многочленов степени $n$.

Доказательство. Обозначим через $U$ свободный $K$-модуль с базисом из мономов $e^{\boldsymbol{m}}$, которые мы будем воспринимать как формальные символы, и рассмотрим симметричное полилинейное отображение $\mu : V \times \dots \times V \to U$, значение которого на каждом наборе базисных векторов равно моному, в котором каждый базисный вектор представлен в степени, равной числу его вхождений в набор. Это отображение универсально, поскольку для симметричного полилинейного отображения $\varphi : V \times \dots \times V \to W$ и линейного ображения $F : U \to W$ равенство $\varphi = F \circ \mu$ равносильно выполнению равенств

$$\varphi(\underbrace{e_1, \dots, e_1}_{m_1}, \dots, \underbrace{e_k, \dots, e_k}_{m_k}) = F(e_1^{m_1} e_2^{m_2} \dots e_k^{m_k}) \tag{2-11}$$

для всех конечных подмножеств $\{e_1, \dots, e_k\} \subset E$ и всех функций

$$m : \{e_1, \dots, e_k\} \to \mathbb{N}, \quad e_i \mapsto m_i,$$

с суммой значений $\sum_i m_i = n$, и равенства (2-11) однозначно определяют $F$, если задано $\varphi$, и наоборот. По упр. 2.5 существует изоморфизм $U \simeq S^nV$, переводящий каждый базисный вектор $e_1^{m_1} e_2^{m_2} \dots e_k^{m_k} \in U$ в коммутативное произведение $e_1^{m_1} e_2^{m_2} \dots e_k^{m_k} \in S^nV$. Стало быть, такие произведения образуют базис в $S^nV$. □

Упражнение 2.6. Найдите $\mathrm{rk}\, S^nV$ если $\mathrm{rk}\, V = d$.

[1] В том числе бесконечномерного.

**2.3.3. Внешняя алгебра модуля.** Обозначим через $\mathcal{I}_{\text{skew}} \subset TV$ двусторонний идеал, порождённый тензорами квадратами

$$v \otimes v \in V \otimes V \tag{2-12}$$

всевозможных векторов $v \in V$. Линейная оболочка тензоров (2-12) содержит также все суммы $u \otimes w + w \otimes u = (u+w) \otimes (u+w) - u \otimes u - w \otimes w$ и линейно порождается ими, если $1+1 \neq 0$ в $K$. Как модуль над $K$, идеал

$$\mathcal{I}_{\text{skew}} = \bigoplus_{n \geqslant 2} \mathcal{I}_{\text{skew}} \cap V^{\otimes n}$$

является прямой суммой однородных компонент $\mathcal{I}_{\text{skew}} \cap V^{\otimes n}$, каждая из которых является линейной оболочкой разложимых тензоров вида $\cdots \otimes v \otimes v \otimes \cdots$ и содержит все суммы

$$(\cdots \otimes v \otimes w \otimes \cdots) + (\cdots \otimes w \otimes v \otimes \cdots),$$

где оба слагаемых разложимы и обозначенные многоточиями фрагменты одинаковы.

Фактор алгебра $\Lambda V \overset{\text{def}}{=} TV/\mathcal{I}_{\text{skew}}$ называется *внешней* или *грассмановой* алгеброй $K$-модуля $V$. Умножение в $\Lambda V$, индуцированное тензорным произведением в $TV$, называется *внешним* или *грассмановым* умножением и обозначается знаком $\wedge$. Как модуль над $K$, внешняя алгебра является прямой суммой $\Lambda V = \bigoplus_{n \geqslant 0} \Lambda^n V$ своих однородных компонент $\Lambda^n V \overset{\text{def}}{=} V^{\otimes n}/(\mathcal{I}_{\text{skew}} \cap V^{\otimes n})$, которые называются *внешними степенями* модуля $V$. При этом $\Lambda^0 V = K$, $\Lambda^1 V = V$ и $\Lambda^k V \wedge \Lambda^m V \subset \Lambda^{k+m} V$ для всех $k, m$. Из описания идеала $\mathcal{I}_{\text{skew}}$ вытекает, что $u \wedge w = -w \wedge u$ для всех $u, w \in V$, и $v \wedge v = 0$ для всех $v \in V$. Перестановка сомножителей в составленном из векторов грассмановом мономе равносильна умножению этого монома на знак перестановки:

$$\forall\, g \in S_k \quad v_{g_1} \wedge \ldots \wedge v_{g_k} = \operatorname{sgn}(g) \cdot v_1 \wedge \ldots \wedge v_k\,.$$

Поэтому для однородных элементов $\omega \in \Lambda^k V$, $\eta \in \Lambda^m V$ выполняется равенство

$$\omega \wedge \eta = (-1)^{km} \eta \wedge \omega\,.$$

Градуированные алгебры[1] с таким свойством называются *s-коммутативными*[2]. Отождествление $V$ с $\Lambda^1 V$ задаёт вложение $\iota : V \hookrightarrow \Lambda V$, которое обладает следующим универсальным свойством.

Упражнение 2.7. Покажите, что для любого линейного отображения $f : V \to L$ в произвольную s-коммутативную $K$-алгебру $L$ существует единственный такой гомоморфизм $K$-алгебр $\tilde{f} : \Lambda V \to L$, что $f = \tilde{f} \circ \iota$, причём алгебра $\Lambda V$ и вложение $\iota$ определяются этим свойством однозначно с точностью до единственного перестановочного с $\iota$ изоморфизма $K$-алгебр.

По этой причине алгебра $\Lambda V$ иначе называется *свободной* s-коммутативной $K$-алгеброй, порождённой модулем $V$.

---

[1] $K$-алгебра $A$ называется *градуированной*, если как модуль над $K$ она распадается в прямую сумму $A = \bigoplus_{k \geqslant 0} A_k$, и $A_k A_m \subset A_{k+m}$ для всех $k, m$.

[2] Префикс «s» можно по желанию воспринимать как аббревиатуру для *super* или для *skew*.

**2.3.4. Кососимметричные полилинейные отображения.** Полилинейное отображение

$$\alpha : V \times \dots \times V \to U \tag{2-13}$$

называется *кососимметричным*, если оно принимает нулевое значение всякий раз, когда какие-либо два аргумента совпадают. Всякое кососимметричное полилинейное отображение *знакопеременно*, т. е. $\alpha(v_{g(1)}, v_{g(2)}, \dots, v_{g(m)}) = \operatorname{sgn} g \cdot \alpha(v_1, \dots, v_n)$ для всех $g \in S_n$.

Упражнение 2.8. Убедитесь в этом и покажите, что когда $1 + 1 \neq 0$ в $K$, знакопеременность равносильна кососимметричности.

Кососимметричные $n$-линейные отображения образуют подмодуль

$$\mathrm{Alt}^n(V, U) \subset \mathrm{Hom}(V, \dots, V; U)$$

в $K$-модуле всех $n$-линейных отображений. Сопоставляя всевозможным линейным отображениям $F : U \to W$ их композицию $F \circ \alpha$ с фиксированным кососимметричным $n$-линейным отображением (2-13), мы получаем $K$-линейное отображение $\mathrm{Hom}(U, W) \to \mathrm{Alt}^n(V, W)$, $F \mapsto F \circ \alpha$. Если оно является изоморфизмом для всех $K$-модулей $W$, отображение $\alpha$ называется *универсальным* кососимметричным $n$-линейным отображением, а также *антикоммутативным* или *грассмановым* произведением векторов.

Упражнение 2.9. Покажите, что пространство, в котором принимает значение грассманово произведение, единственно с точностью до единственного изоморфизма, перестановочного с этим произведением.

Предложение 2.4
Композиция $\alpha_n = \pi_{S^n} \circ \tau$ тензорного произведения $\tau : V \times \dots \times V \to V^{\otimes n}$ с последующей проекцией $\pi_{\Lambda^n} : V^{\otimes n} \twoheadrightarrow \Lambda^n V$ является универсальным кососимметричным $n$-линейным отображением.

Доказательство. В силу универсальности $\tau$ любое $n$-линейное отображение $\varphi : V \times \dots \times V \to W$ однозначно представляется в виде композиции $\varphi = \widetilde{F} \circ \tau$, где $\widetilde{F} : V^{\otimes n} \to W$ линейно. Если $\varphi$ кососимметрично, $\widetilde{F}$ аннулирует линейные порождающие подпространства $\mathcal{I}_{\text{skew}} \cap V^{\otimes n} = \ker \pi_{\Lambda^n}$:

$$\widetilde{F}(\,\cdots \otimes w \otimes w \otimes \,\cdots) = \varphi(\dots, w, w, \dots) = 0\,,$$

и значит, корректно факторизуется до линейного отображения

$$F : \Lambda^n V \to W\,, \quad v_1 \wedge \ldots \wedge v_n \mapsto \varphi(v_1, \dots, v_n)\,.$$

Таким образом, $\varphi = \widetilde{F} \circ \tau = F \circ \pi_{\Lambda^n} \circ \tau = F \circ \alpha_n$. Из-за универсальности $\tau$ любое линейное отображение $F' : \Lambda^n V \to W$, для которого $\varphi = F' \circ \alpha_n = F' \circ \pi_{\Lambda^n} \circ \tau$, удовлетворяет равенству $F' \circ \pi_{\Lambda^n} = F \circ \pi_{\Lambda^n}$, откуда $F' = F$ в силу сюрьективности проекции $\pi_{\Lambda^n}$. □

Упражнение 2.10. Убедитесь, что для любого (в том числе бесконечномерного) векторного пространства $V$ над произвольным полем $\Bbbk$ пространство $\mathrm{Alt}^n(V, \Bbbk)$ кососимметричных $n$-линейных форм $V \times \dots \times V \to \Bbbk$ канонически двойственно $n$-той внешней степени $\Lambda^n V$.

Следствие 2.4
Если $K$-модуль $V$ свободен с базисом $E \subset V$, то при каждом $m$ модуль $\Lambda^m V$ тоже свободен, и мономы $e_M = e_1 \wedge \ldots \wedge e_m$, занумерованные всевозможными $m$-элементными подмножествами $M = \{e_1, \dots, e_m\} \subset E$, образуют базис в $\Lambda^m V$. При перестановке элементов множества $M$, моном $e_M$ умножается на знак перестановки.

Доказательство. Рассмотрим свободный модуль $U$ с базисом из символов $e_M$, где $M$ пробегает $m$-элементные подмножества в $E$. В каждом таком подмножестве $M$ мы произвольным образом занумеруем элементы, так что $M$ запишется как $\{e_1, \dots, e_m\}$, и рассмотрим кососимметричное полилинейное отображение $\alpha : V \times \dots \times V \to U$, переводящее каждый упорядоченный набор из $m$ различных базисных векторов, образующих перестановку $e_{g_1}, \dots, e_{g_m}$ элементов некоторого множества $M = \{e_1, \dots, e_m\} = \{e_{g_1}, \dots, e_{g_m}\} \subset E$, в вектор $\mathrm{sgn}(g) \cdot e_M$. Отображение $\alpha$ универсально, поскольку для любого кососимметричного полилинейного отображения $\varphi : V \times \dots \times V \to W$ и линейного отображения $F : U \to W$ равенство $\varphi = F \circ \alpha$ равносильно тому, что $F(e_{\{e_1,\dots,e_m\}}) = \mathrm{sgn}(g) \cdot \varphi(e_{g(1)}, \dots, e_{g(m)})$ для каждого $m$-элементного подмножества $\{e_1, \dots, e_m\} \subset E$ и всех перестановок $g \in S_m$, причём эти условия корректно и однозначно определяют $F$, если задано $\varphi$, и наоборот. Тем самым, имеется единственный изоморфизм $U \xrightarrow{\sim} \Lambda^n V$, переводящий базисный вектор $e_{\{e_1,\dots,e_m\}} \in U$ в грассманово произведение $e_1 \wedge \ldots \wedge e_m \in \Lambda^n V$. □

Следствие 2.5
Если модуль $V$ имеет конечный базис $e_1, \dots, e_d$, то $\mathrm{rk}\, \Lambda^m V = \binom{d}{m}$ для всех $m$, и мономы

$$e_I = e_{i_1} \wedge \ldots \wedge e_{i_m}, \quad \text{где} \quad 1 \leqslant i_1 < i_2 < \dots < i_m \leqslant d\,. \tag{2-14}$$

составляют базис модуля $\Lambda^m V$ над $K$. В частности, $\Lambda^m V = 0$ при $m > d$, и $\mathrm{rk}\, \Lambda V = 2^d$.

Упражнение 2.11. В условиях сл. 2.5 покажите, что $\omega \in \Lambda U$ однороден степени $\mathrm{rk}\, U$ если и только если $u \wedge \omega = 0$ для всех $u \in U$.

**2.4. Симметрические и кососимметрические тензоры.** Начиная с этого места и до конца §2 речь будет идти про векторные пространства над полем $\Bbbk$ характеристики нуль. Симметрическая группа $S_n$ действует на тензорной степени $V^{\otimes n}$ такого векторного пространства $V$ перестановками сомножителей в разложимых тензорах. А именно, для каждого $g \in S_n$ положим

$$g(v_1 \otimes \dots \otimes v_n) = v_{g(1)} \otimes v_{g(2)} \otimes \dots \otimes v_{g(n)}\,. \tag{2-15}$$

Поскольку правая часть полилинейно зависит от $v_1, \dots, v_n$, формула (2-15) корректно определяет линейный оператор $g : V^{\otimes n} \to V^{\otimes n}$. Подпространства

$$\mathrm{Sym}^n V \overset{\text{def}}{=} \{\, t \in V^{\otimes n} \mid \forall\, g \in S_n\ g(t) = t \}$$
$$\mathrm{Alt}^n V \overset{\text{def}}{=} \{\, t \in V^{\otimes n} \mid \forall\, g \in S_n\ g(t) = \mathrm{sgn}(g) \cdot t \}$$

называются пространствами *симметричных* и *знакопеременных* тензоров в $V^{\otimes n}$.

**2.4.1. Стандартный базис пространства симметричных тензоров.** Зафиксируем в пространстве $V$ некоторый базис $E$, а $V^{\otimes n}$ — базис из тензорных мономов $e_1 \otimes \dots \otimes e_n$ с $e_i \in E$. В разложении произвольного симметричного тензора $t \in \mathrm{Sym}^n V$ по последнему базису все мономы, составляющие одну орбиту группы $S_n$, входят с одним и тем же коэффициентом, зависящим только от орбиты. Орбиты действия $S_n$ на базисных мономах нумеруются функциями $\boldsymbol{m} : E \to \mathbb{Z}_{\geqslant 0}$, $e \mapsto m(e)$ с конечным носителем и суммой значений $\sum_{e \in E} m(e) = n$. Орбита $E_{\boldsymbol{m}}$, отвечающая такой функции, состоит из всех тензорных мономов, в которые каждый вектор

$e \in E$ входит ровно $m(e)$ раз. Сумма всех мономов из орбиты $E_{\boldsymbol{m}}$ обозначается $e_{\boldsymbol{m}}$ и называется *полным симметрическим тензором*. Таким образом, полные симметрические тензоры веса $|\boldsymbol{m}| \overset{\text{def}}{=} \sum_{e \in E} m(e) = n$ образуют базис пространства $\mathrm{Sym}^n(V)$.

Упражнение 2.12. Пусть функция $\boldsymbol{m} : E \to \mathbb{Z}_{\geqslant 0}$ принимает ненулевые значения $m(e_i) = m_i$ только на базисных векторах $e_1, \dots, e_d$. Покажите, что орбита $E_{\boldsymbol{m}}$ состоит из

$$|E_{\boldsymbol{m}}| = \frac{n!}{m_1!\, m_2! \,\cdots\, m_d!}$$

различных тензорных мономов.

**2.4.2. Стандартный базис пространства знакопеременных тензоров.** В разложении знакопеременного тензора $t \in \mathrm{Alt}^n V$ по базисным мономам тензорной алгебры присутствуют лишь мономы, в которых каждый базисный вектор $e \in E$ встречается не более одного раза, причём вместе с каждым таким мономом $e_1 \otimes \cdots \otimes e_n$ в разложение $t$ входят все $n!$ мономов

$$g(e_1 \otimes \cdots \otimes e_n) = e_{g_1} \otimes \cdots \otimes e_{g_n} ,$$

которые получаются из него перестановками $g \in S_n$, причём коэффициенты при $e_1 \otimes \cdots \otimes e_n$ и $g(e_1 \otimes \cdots \otimes e_n)$ отличаются друг от друга множителем $\mathrm{sgn}(g)$. Таким образом, базис в пространстве $\mathrm{Alt}^n V$ составляют *полные знакопеременные тензоры*

$$e_I = \sum_{g \in S_n} \mathrm{sgn}(g) \cdot e_{g_1} \otimes \cdots \otimes e_{g_n} \tag{2-16}$$

находящиеся в биекции с $n$-элементным подмножествам $I = \{e_1, \dots, e_n\} \subset E$. При этом мы считаем, что на множестве $E$ базисных векторов зафиксирован некоторый порядок, вводим индуцированный порядок на каждом конечном подмножестве $I \subset E$ и располагаем сомножители тензора $e_1 \otimes \cdots \otimes e_n$, отвечающего тождественной перестановке в формуле (2-16), в порядке возрастания.

Предложение 2.5

Над полем характеристики нуль ограничение проекции $\pi_{S^n} : V^{\otimes n} \twoheadrightarrow S^n V$ на подпространство $\mathrm{Sym}^n \subset V^{\otimes n}$ и ограничение проекции $\pi_{\Lambda^n} : V^{\otimes n} \twoheadrightarrow \Lambda^n V$ на подпространство $\mathrm{Alt}^n \subset V^{\otimes n}$ являются изоморфизмами векторных пространств.

Доказательство. Для каждой функции $\boldsymbol{m} : E \to \mathbb{Z}_{\geqslant 0}$ с конечным носителем

$$\mathrm{supp}(\boldsymbol{m}) = \{e_1, \dots, e_k\}$$

и значениями $\boldsymbol{m}(e_i) = m_i$, все $\frac{n!}{m_1! m_2! \cdots m_k!}$ тензоров из орбиты $E_{\boldsymbol{m}}$ отобразятся проекцией

$$\pi_{S^n} : V^{\otimes n} \twoheadrightarrow S^n V$$

в один и тот же коммутативный моном $e_1^{m_1} e_2^{m_2} \dots e_k^{m_k}$. Точно так же, для любого конечного подмножества $I = \{e_1, \dots, e_n\} \subset E$ каждое из $n!$ слагаемых суммы (2-16), перейдёт при проекции $\pi_{\Lambda^n} : V^{\otimes n} \twoheadrightarrow \Lambda^n V$ в грассманов моном $e_1 \wedge \dots \wedge e_n$. Тем самым, образы стандартных базисных симметричных и знакопеременных тензоров пропорциональны базисным коммутативным и грассмановым мономам:

$$\pi_{S^n}(e_{\boldsymbol{m}}) = \frac{n!}{m_1! m_2! \cdots m_d!} \cdot e_1^{m_1} e_2^{m_2} \dots e_k^{m_k} , \tag{2-17}$$

$$\pi_{\Lambda^n}(e_I) = n! \cdot e_1 \wedge e_2 \wedge \dots \wedge e_n . \tag{2-18}$$

□

Предостережение 2.1. Не смотря на предл. 2.5, подпространства $\mathrm{Sym}^n V$ и $\mathrm{Alt}^n V$, которые лежат внутри $V^{\otimes n}$, не следует путать с фактор пространствами $S^n V$ и $\Lambda^n V$, которые получаются из $V^{\otimes n}$ отождествлением некоторых тензоров между собою. Над полем характеристики $p > 0$ многие симметричные тензоры и все кососимметричные тензоры, степень которых больше $p$, аннулируются проекциями $\pi_{S^n}$ и $\pi_{\Lambda^n}$. Даже в характеристике нуль изоморфизмы из предл. 2.5 не отождествляют друг с другом стандартные базисные векторы тензорных и полиномиальных пространств буквально, но выражают их друг через друга с поправочными комбинаторными множителями, которые приходится учитывать как при подъёме на пространства симметричных и знакопеременных тензоров тех умножений, что имеются в алгебрах многочленов $SV$ и $\Lambda V$, так и при спуске на пространства многочленов тех операций свёртки, что имеются на тензорных алгебрах двойственных друг другу векторных пространств.

**2.5. Поляризация коммутативных многочленов.** Обратное к изоморфизму из предл. 2.5 отображение $\pi_{S^n}^{-1} : S^n V^* \xrightarrow{\sim} V^{*\otimes n}$ называется *полной поляризацией* многочленов. Оно сопоставляет однородному многочлену $f \in S^n V^*$ тот единственный симметричный тензор $\tilde{f} \in \mathrm{Sym}^n V^*$, который проектируется в $f$ при факторизации по соотношениям коммутирования. Тензор $\tilde{f}$ можно интерпретировать как симметричную $n$-линейную форму

$$\tilde{f} : V \times \dots \times V \to \Bbbk , \quad \tilde{f}(v_1, \dots , v_n) \overset{\text{def}}{=} \langle\, v_1 \otimes \dots \otimes v_n \, , \, \tilde{f} \,\rangle .$$

Полной поляризацией базисного монома $x_1^{m_1} x_2^{m_2} \dots x_k^{m_k}$ степени $\sum_i m_i = n$ является симметрический тензор

$$\frac{m_1!\, m_2! \, \cdots \, m_k!}{n!} \cdot x_{\boldsymbol{m}} , \tag{2-19}$$

пропорциональный сумме всех тензорных мономов, состоящих из $m_1$ ковекторов $x_1$, $m_2$ ковекторов $x_2$, … , $m_k$ ковекторов $x_k$. Полная поляризация произвольного многочлена может быть вычислена отсюда по линейности. Ниже, в n° 2.5.2 и в форм. (2-25) на стр. 29 мы приведём более явные рецепты для вычисления значения $\tilde{f}(v_1, \dots , v_n)$ в терминах многочлена $f$.

Упражнение 2.13. Убедитесь, что полная поляризация квадратичной формы $q \in S^2 V^*$ это в точности билинейная симметричная форма $\tilde{f} : V \times V \to \Bbbk$, определяемая соотношением $2\tilde{f}(u, w) = f(u + w) - f(u) - f(w)$, которая обсуждалась в первом семестре[1].

**2.5.1. Вычисление значения многочлена на векторе.** Сопоставим каждому многочлену $f \in S^n V^*$ *полиномиальную функцию*

$$f : V \to \Bbbk , \quad f(v) = \tilde{f}(v, \dots , v) , \tag{2-20}$$

где $\tilde{f} = \pi_{S^n}^{-1}(f) \in \mathrm{Sym}^n V^*$ это полная поляризация $f$. Обратите внимание, что это определение не зависит от выбора базиса и имеет смысл также и для бесконечномерных пространств $V$.

Для конечномерного пространства $V$ с базисом $e_1, \dots , e_d$ и двойственным базисом $x_1, \dots , x_d$ в $V^*$ алгебра $SV^*$ изоморфна алгебре многочленов $\Bbbk[x_1, \dots , x_d]$, и для однородного полинома $f(x_1, \dots , x_d)$ степени $n$ и вектора $v = \sum \alpha_i e_i \in V$ значение (2-20) равно результату подстановки в $f$ значений $x_i = \alpha_i$, т. е. $f(v) = f(\alpha_1, \dots , \alpha_d)$. Действительно, в силу линейности полной поляризации по $f$, достаточно проверить это равенство для $f = x_1^{m_1} x_2^{m_2} \dots x_d^{m_d}$, и в этом случае полная свёртка

$$\langle\, \tilde{f} \, , \, v^{\otimes n} \,\rangle = \frac{m_1! \cdot m_2! \, \cdots \, m_d!}{n!} \langle\, x_{\boldsymbol{m}} \, , \, v^{\otimes n} \,\rangle$$

[1] См. http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_14.pdf, раздел 14.3 на стр. 205.

является суммой $\frac{n!}{m_1!m_2!\cdots m_k!}$ одинаковых слагаемых, равных

$$\frac{m_1!m_2!\,\cdots\,m_d!}{n!}\langle\, x_1\,,\, v\,\rangle^{m_1}\langle\, x_2\,,\, v\,\rangle^{m_2}\cdots\langle\, x_k\,,\, v\,\rangle^{m_k}=\frac{m_1!m_2!\,\cdots\,m_d!}{n!}\alpha_1^{m_1}\alpha_2^{m_2}\ldots\alpha_d^{m_d}\,,$$

и совпадает с результатом подстановки $x_i = \alpha_i$ в этот моном. В качестве следствия мы заключаем, что результат подстановки в многочлен $f(x_1, \ldots, x_d)$ координат вектора $v$ зависит только от $f \in SV$ и $v \in V$, но не от выбора пары двойственных друг другу базисов $V$ и $V^*$, используемых для записи $f$ в виде многочлена от координат и вычисления значений координат вектора $v$.

**2.5.2. Комбинаторная формула для полной поляризации.** Поскольку значение симметричной $n$-линейной формы не меняется при перестановках её аргументов, мы будем обозначать через $\tilde f\left(v_1^{m_1}, \ldots, v_n^{m_k}\right)$ значение полной поляризации $\tilde f$ многочлена $f$ на наборе векторов, содержащем $m_i \geqslant 0$ копий вектора $v_i$ для каждого $i = 1, \ldots, k$, так что $\sum_{i=1}^k m_i = \deg f = n$. В этих обозначениях, для всех $f \in S^nV^*$ и любых $v_1, \ldots, v_k \in V$ выполняется ровно та же мультиномиальная формула, что и при раскрытия скобок в выражении $(v_1 + \cdots + v_k)^n$, а именно,

$$f(v_1+\cdots+v_k)=\tilde f\big((v_1+\cdots+v_k)^n\big)=\sum_{m_1,\ldots,m_k}\frac{n!}{m_1!\cdots m_k!}\cdot\tilde f\left(v_1^{m_1},\ldots,v_k^{m_k}\right)\,, \tag{2-21}$$

где суммирование идёт по всем таким наборам целых чисел $m_1, \ldots, m_k$, что $0 \leqslant m_i \leqslant n$ при каждом $i$ и $m_1 + \cdots + m_k = n$.

Упражнение 2.14. Убедитесь в этом.

Предложение 2.6
Значение полной поляризации любого однородного многочлена $f \in S^nV^*$ на (необязательно конечномерном) векторном пространстве $V$ над полем характеристики нуль можно вычислять по формуле

$$n!\cdot\,\tilde f(v_1,\ldots,v_n)=\sum_{I\subsetneq\{1,\ldots,n\}}(-1)^{\ell(I)}f\Big(\sum_{i\notin I}v_i\Big)\,, \tag{2-22}$$

где суммирование идёт по всем собственным подмножествам $I \subsetneq \{1, \ldots, n\}$, включая пустое подмножество $I = \varnothing$, а $\ell(I)$ означает число элементов в $I$. Например, для $f \in S^3V^*$ получаем

$$6\,\tilde f(u,v,w)=f(u+v+w)-f(u+v)-f(u+w)-f(v+w)+f(u)+f(v)+f(w)\,.$$

Доказательство. Воспользуемся разложением (2-21) для $k = n$. Сумма в правой части формулы содержит ровно один член, зависящий от всех $n$ векторов $v_i$, а именно, $n!\cdot\tilde f(v_1, \ldots, v_n)$. Для каждого собственного подмножества $I \subsetneq \{1, \ldots, n\}$ не зависящие от векторов $v_i$ с $i \in I$ слагаемые из правой части формулы (2-21) входят в неё ровно с тем же самым коэффициентом, что и в разложение (2-21) для $f\left(\sum_{i\notin I} v_i\right)$, поскольку последнее получается из разложения для $f(v_1+\cdots+v_n)$ подстановкой $v_i = 0$ для всех $i \in I$. Таким образом, все слагаемые, не содержащие хотя бы один из векторов $v_i$, могут быть удалены из (2-21) при помощи стандартной процедуры включения-исключения, что и даёт искомую формулу

$$n!\cdot\tilde f(v_1,\ldots,v_n)=f\big(\sum_{\nu}v_\nu\big)-\sum_{\{i\}}f\big(\sum_{\nu\neq i}v_\nu\big)+\sum_{\{i,j\}}f\big(\sum_{\nu\neq i,j}v_\nu\big)-\sum_{\{i,j,k\}}f\big(\sum_{\nu\neq i,j,k}v_\nu\big)+\,\cdots\,.$$

□

**2.5.3. Двойственность.** Для конечномерного пространства $V$ над полем характеристики нуль полная свёртка между $V^{\otimes m}$ и $V^{*\otimes m}$ индуцирует невырожденное спаривание между пространствами $S^m V$ и $S^m V^*$, сопоставляющее многочленам $f \in S^n V$ и $g \in S^n V^*$ полную свёртку их полных поляризаций $\tilde{f} \in V^{\otimes m}$ и $\widetilde{g} \in V^{*\otimes m}$.

Упражнение 2.15. Проверьте, что ненулевые спаривания между мономами, составленными из элементов двойственных базисов пространств $V$ и $V^*$, исчерпываются значениями

$$\langle\, e_1^{m_1} e_2^{m_2} \dots e_d^{m_d}\,,\, x_1^{m_1} x_2^{m_2} \dots x_d^{m_d}\,\rangle = \frac{m_1! \cdot m_2! \cdot \,\cdots\, \cdot m_d!}{n!}\,. \tag{2-23}$$

**2.5.4. Производная многочлена в направлении вектора.** Внутреннее умножение[1] на фиксированный вектор $v \in V$ задаёт линейное отображение $i_v : V^{*\otimes n} \to V^{*\otimes(n-1)}$. Применяя его к полной поляризации $\tilde{f}$ многочлена $f \in S^n V^*$ и затем проектируя результат из $V^{*\otimes(n-1)}$ в $S^{n-1}V^*$, мы получаем линейное отображение $\mathrm{pl}_v : S^n V^* \to S^{n-1}V^*$, которое называется *поляризацией* вдоль $v$ и включается в коммутативную диаграмму

$$\begin{tikzcd} V^{*\otimes n} \supset \mathrm{Sym}^n V^* \arrow[r, "i_v"] \arrow[d, "\pi_{S^n}"', "\wr"] & V^{*\otimes(n-1)} \arrow[d, "\pi_{S^{n-1}}"] \\ S^n V^* \arrow[r, "\mathrm{pl}_v"] & S^{n-1}V^*\,. \end{tikzcd}$$

Поляризация переводит многочлен $f(x) = \tilde{f}(x^n) \in S^n V^*$ в билинейно зависящий от $f$ и $v$ многочлен $\mathrm{pl}_v f(x) = \tilde{f}(v, x^{n-1}) \in S^{n-1}V^*$, который называется *полярой* вектора $v$ относительно $f$. При $n = 2$ мы получаем в точности полярное преобразование относительно проективной квадрики $V(f) \subset \mathbb{P}(V)$, которое сопоставляет точке $v$ её полярную гиперплоскость.

Рассмотрим двойственные базисы $e_1, \dots, e_d \in V$, $x_1, \dots, x_d \in V^*$ и базисный симметричный тензор[2] $x_{(m_1,\dots,m_d)} \in \mathrm{Sym}^n V^*$, равный сумме всех тензорных мономов, в которые каждый базисный ковектор $x_\nu$ входит ровно $m_\nu$ раз. Свёртка $x_{(m_1,\dots,m_d)}$ с базисным вектором $e_i \in V$ по первому тензорному сомножителю зануляется при $m_i = 0$, а во всех остальных случаях равна базисному симметричному тензору $x_{(m'_1,\dots,m'_d)} \in \mathrm{Sym}^{n-1} V^*$, имеющему $m'_i = m_i - 1$ и $m'_\nu = m_\nu$ при $\nu \neq i$. Поэтому

$$\begin{aligned} \mathrm{pl}_{e_i} x_1^{m_1} x_2^{m_2} \dots x_d^{m_d} &= \frac{m_1! \cdots m_d!}{n!}\, \pi_{S^{n-1}}\left(x_{(m'_1,\dots,m'_d)}\right) = \\ &= \frac{m_i}{n}\, x_1^{m_1} \dots x_{i-1}^{m_{i-1}} x_i^{m_i - 1} x_{i+1}^{m_{i+1}} \dots x_d^{m_d} = \frac{1}{n}\frac{\partial}{\partial x_i}\, x_1^{m_1} x_2^{m_2} \dots x_d^{m_d}\,. \end{aligned}$$

Так как многочлен $\mathrm{pl}_v f$ билинейно зависит от $v$ и $f$, поляра произвольного вектора $v = \sum \alpha_i e_i$ относительно любого однородного многочлена $f$ равна разделённой на степень $\deg f$ *частной производной* от многочлена $f$ в направлении вектора $v$:

$$\mathrm{pl}_v f = \frac{1}{\deg(f)}\,\partial_v f = \frac{1}{\deg(f)} \sum \alpha_i \frac{\partial f}{\partial x_i}\,.$$

Обратите внимание, что поскольку левая часть этой формулы определена инвариантно, правая часть тоже не зависит от выбора двойственных координат в $V$ и $V^*$. Из равенств

$$\mathrm{pl}_u \mathrm{pl}_w f(v) = \tilde{f}\left(u, w, v^{n-1}\right) = \mathrm{pl}_w \mathrm{pl}_u f(v)$$

[1] См. прим. 2.1 на стр. 18.
[2] См. n° 2.4.1 на стр. 24.

вытекает, что частные производные коммутируют: $\partial_u\partial_w = \partial_w\partial_u$ для всех $u, w \in V$. Кроме того, для любых векторов $u, w \in V$, целых неотрицательных чисел $k$, $m$ и многочлена $f \in S^{k+m}V^*$ выполняется равенство

$$k!\,\partial_u^k f(w) = (k+m)!\,\tilde{f}\left(u^k, w^m\right) = m!\,\partial_w^m f(u)\,. \tag{2-24}$$

Наконец, мы получаем ещё одну формулу для полной поляризации:

$$\tilde{f}(v_1, \dots, v_n) = \frac{1}{n!}\,\partial_{v_1} \dots \partial_{v_n} f \tag{2-25}$$

для любого многочлена $f \in S^nV^*$ и любых $n$ векторов $v_1, \dots, v_n \in V$.

Упражнение 2.16. Докажите *правило Лейбница*: $\partial_v(fg) = g\partial_v(f) + f\partial_v(g)$.

Пример 2.2 (разложение Тейлора)
Для любых двух векторов $u, w \in V$ и многочлена $f \in S^nV^*$ по формуле бинома[1] получаем

$$f(u+w) = \tilde{f}\left((u+w)^n\right) = \sum_{m=0}^{n} \binom{n}{m} \cdot \tilde{f}(u^m, w^{n-m})\,.$$

Формула (2-24) позволяет переписать это равенство в виде *разложения Тейлора*

$$f(u+w) = \sum_{m=0}^{\deg f} \frac{1}{m!}\,\partial_w^m f(u)\,. \tag{2-26}$$

Обратите внимание, что это *точное равенство* в $S^nV^*$, причём его правая часть *явно* симметрична по $u$ и $w$ в силу соотношений (2-24).

**2.5.5. Поляры и касательные к проективной гиперповерхности.** Рассмотрим проективную гиперповерхность $S = V(f) \subset \mathbb{P}(V)$, заданную однородным полиномиальным уравнением $f(x) = 0$ степени $n$. Пересечение гиперповерхности $S$ с произвольной прямой $\ell = (pq)$ состоит из таких точек $\lambda p + \mu q \in \ell$, что отношение $(\lambda : \mu) \in \mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ удовлетворяет уравнению $f_{pq}(\lambda, \mu) = 0$, где $f_{pg}(\lambda, \mu) = f(\lambda p + \mu q) \in \Bbbk[\lambda, \mu]$. Над алгебраически замкнутым полем $\Bbbk$ однородный многочлен $f_{pq}(\lambda, \mu)$ либо тождественно нулевой, либо является произведением $n$ линейных форм:

$$f(\lambda, \mu) = \prod_i (\alpha_i''\lambda - \alpha_i'\mu)^{s_i} = \prod_i \det{}^{s_i} \begin{pmatrix} \lambda & \alpha_i' \\ \mu & \alpha_i'' \end{pmatrix}\,, \tag{2-27}$$

где $a_i = (\alpha_i' : \alpha_i'') \in \mathbb{P}_1$ суть различные нули многочлена $f_{pq}$ на $\mathbb{P}_1$, и $\sum_i s_i = n$. Если $f_{pq} = 0$, то $(pq) \subset S$. Если $f_{pq} \neq 0$, пересечение $\ell \cap S$ состоит из точек $a_i = \alpha_i' p + \alpha_i'' q$. Показатель $s_i$, с которым линейная форма $\alpha_i''\mu - \alpha_i'\lambda$ входит в разложение (2-27), называется локальной *кратностью пересечения* поверхности $S$ с прямой $\ell$ в точке $a_i$ и обозначается $(S, \ell)_{a_i}$. Суммарное количество точек пересечения, учтённых каждая со своей кратностью, равно степени гиперповерхности. Если $(S, \ell)_{a_i} = 1$, пересечение $S$ с $\ell$ в точке $a_i$ называется *простым* или *трансверсальным*. Если $(S, \ell)_a \geqslant 2$ или $\ell \subset S$, то прямая $\ell$ называется *касательной* к гиперповерхности $S$ в точке $a$.

Таким образом, прямая $(pq)$ касается гиперповерхности $S$ в точке $p \in S$ если и только если полином $f(p+tq) \in \Bbbk[t]$ имеет кратный корень в нуле или тождественно нулевой. По формуле

[1] См. формулу (2-21) на стр. 27.

Тейлора[1] $f(p+tq) = t\binom{d}{1}\tilde f(p^{n-1},q) + t^2\binom{d}{2}\tilde f(p^{n-2},q^2)+\cdots$. Стало быть, прямая $\ell = (pq)$ касается $S$ в точке $p\in S$ если и только если $\tilde f(p^{n-1},q) = 0$. Это обобщает обсуждавшееся в курсе геометрии[2] описание касательных прямых к проективной квадрике.

Если $f(p^{n-1},x)$ не является тождественно нулевой линейной формой от $x$, то точки $q$, удовлетворяющие уравнению $f(p^{n-1},q)=0$, образуют в проективном пространстве $\mathbb{P}(V)$ гиперплоскость, которая называется *касательным пространством* к $S$ в точке $p\in S$ и обозначается $T_pS$. В этом случае точка $p$ называется *гладкой* точкой гиперповерхности $S$. Сама гиперповерхность $S$ называется *гладкой*, если гладки все её точки.

Если линейная по $x$ форма $f(p^{n-1},x)$ нулевая, гиперповерхность $S$ называется *особой* в точке $p$, а $p$ называется *особой точкой* гиперповерхности $S$. Коэффициентами линейной формы $\tilde f\left(p^{n-1},x\right) = \partial_x f(p)$ являются частные производные многочлена $f$, вычисленные в точке $p$. Таким образом, точка $p$ особа если и только если $\frac{\partial f}{\partial x_i}(p) = 0$ при всех $i$. В этом случае любая проходящая через $p$ прямая касается $S$ в $p$, и касательное пространство $T_pS$, понимаемое как объединение всех касающихся $S$ в точке $p$ прямых, совпадает со всем пространством $\mathbb{P}(V)$.

Для лежащей на гиперповерхности $S$ гладкой точки $q$ или произвольной точки $q$ вне $S$ полярный к $q$ относительно $f$ многочлен $\mathrm{pl}_q f(x) = \tilde f(q,x^{n-1})$ имеет по $x$ степень $n-1$ и отличен от нуля, поскольку иначе нулевой будет и его производная $\partial_q^{n-2}\mathrm{pl}_q f(x) = \tilde f(q^{n-1},x)$, а это значит, что $q\in S$ и является особой точкой $S$. Множество нулей полинома $\mathrm{pl}_q f$ в $\mathbb{P}(V)$ обозначается

$$\mathrm{pl}_q S \overset{\text{def}}{=} V(\mathrm{pl}_q f) = \{x\in\mathbb{P}(V)\mid \tilde f(q,x^{n-1}) = 0\} \tag{2-28}$$

и называется *полярной гиперповерхностью* точки $q$ относительно $S$. Пересечение $S\cap\mathrm{pl}_q S$ состоит из точек касания с гиперповерхностью $S$ всевозможных касательных, опущенных на неё из $q$, и называется *видимым контуром* гиперповерхности $S$ из точки $q$. Для квадрик эта конструкция подробно обсуждалась в курсе геометрии[3].

Более общим образом, *полярой степени* $r$ точки $q$ относительно $S$ называется гиперповерхность

$$\mathrm{pl}_q^{n-r} S \overset{\text{def}}{=} \{x\in\mathbb{P}(V)\mid \tilde f(q^{n-r},x^r) = 0\}\,.$$

Если $q$ является гладкой точкой на $S$, то поляра степени 1 это касательная гиперплоскость $T_qS$. При $r\geqslant 2$ поляра степени $r$ представляет собою такую проходящую через $q$ гиперповерхность степени $r$, относительно которой $q$ имеет точно такие же поляры степени меньше $r$, что и относительно исходной гиперповерхности $S$. Например, квадратичная поляра это квадрика, имеющая в точке $q$ ту же касательную гиперплоскость, что и $S$. Кубическая поляра это кубика, имеющая в $q$ те же квадратичную поляру и касательную гиперплоскость, что $S$, и т. д.

**2.5.6. Линейный носитель многочлена.** Линейный носитель[4] $\mathrm{supp}(\tilde f)\subset V^*$ полной поляризации $\tilde f$ многочлена $f\in S^nV^*$ называется *линейным носителем многочлена* $f$. Обратите внимание, что линейный носитель является векторным подпространством в $V^*$, а не в $V$.

Упражнение 2.17. Убедитесь, что каждый многочлен $f$ корректно задаёт полиномиальную функцию на $V/\mathrm{Ann}\big(\mathrm{supp}(f)\big)$ по правилу $f([v]) = f(v)$.

---

[1] См. прим. 2.2 на стр. 29.

[2] См. http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2021/lec_17.pdf, раздел 17.3.1 на стр. 212.

[3] См. ссылку выше и http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2021/lec_19.pdf, раздел 19.1 на стр. 237.

[4] См. n° 2.2.2 на стр. 18.

Согласно теор. 2.1 на стр. 18, подпространство $\mathrm{supp}(f) \subset V^*$ является образом полной свёртки $c_f : V^{\otimes(n-1)} \to V^*$ с тензором $\tilde{f}$, причём из-за симметричности тензора $\tilde{f}$ эта свёртка не зависит от выбора индексов, по которым она производится. Иначе говоря, $\mathrm{supp}(f)$ линейно порождается всеми частными производными порядка $n-1$ от $f$:

$$\frac{\partial^{m_1}}{\partial x_1^{m_1}} \frac{\partial^{m_2}}{\partial x_2^{m_2}} \cdots \frac{\partial^{m_d}}{\partial x_d^{m_d}} f(x) , \quad \text{где} \quad \sum m_\nu = n - 1 . \tag{2-29}$$

Вклад в коэффициент при $x_i$ у линейной формы (2-29) вносит лишь тот коэффициент многочлена $f$, что стоит при $x_1^{m_1} \dots x_{i-1}^{m_{i-1}} x_i^{m_i+1} x_{i+1}^{m_{i+1}} \dots x_d^{m_d}$. Записывая многочлен $f$ в виде

$$f = \sum_{\nu_1 \dots \nu_d} \frac{n!}{\nu_1! \cdots \nu_d!} a_{\nu_1 \dots \nu_d} x_1^{\nu_1} \cdots x_d^{\nu_d} , \tag{2-30}$$

мы получаем для линейной формы (2-29) следующее выражение:

$$n! \cdot \sum_{i=1}^{d} a_{m_1 \dots m_{i-1} (m_i+1) m_{i+1} \dots m_d} x_i , \tag{2-31}$$

и всего таких линейных форм имеется[1] $\binom{n+d-2}{d-1}$.

Предложение 2.7

Однородный многочлен $f$ вида (2-30) над алгебраически замкнутым полем $\Bbbk$ характеристики нуль тогда и только тогда является $n$-той степенью линейной формы, когда $d \times \binom{n+d-2}{d-1}$-матрица из коэффициентов линейных форм (2-31) имеет ранг 1. В этом случае есть ровно $n$ линейных форм $\varphi$, удовлетворяющих уравнению $\varphi^n = f$, все они пропорциональны формам (2-31) и получаются друг из друга умножением на корни $n$-той степени из единицы в поле $\Bbbk$.

Доказательство. Равенство $f = \varphi^n$ означает, что $\mathrm{supp}(f)$ одномерен и порождён формой $\varphi$. В этом случае все формы (2-31) пропорциональны форме $\varphi$, и уравнение $t^n = f$ имеет в целостном кольце $\Bbbk[x_1, \dots , x_d]$ ровно $n$ корней вида $\zeta \cdot \varphi$, где $\zeta$ пробегает множество корней из единицы в поле $\Bbbk$. Наоборот, если все формы (2-31) пропорциональны, и $\psi \neq 0$ — одна из них, то $\mathrm{supp}(f) = \Bbbk \cdot \psi$ и $f = \lambda \psi^n$ для некоторого $\lambda \in \Bbbk$, а $\varphi = \sqrt[n]{\lambda} \cdot \psi$. □

Пример 2.3 (бинарные формы ранга 1)

Однородный многочлен степени $n$ от двух переменных $f(x_0, x_1) = \sum_k a_k \cdot \binom{n}{k} \cdot x_0^{n-k} x_1^k$ представляется в виде $(\alpha_0 x_0 + \alpha_1 x_1)^n$ если и только если $a_i : a_{i+1} = \alpha_0 : \alpha_1$ не зависит от $i$, что равносильно условию

$$\mathrm{rk} \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = 1 , \tag{2-32}$$

и выражается квадратичными соотношениями $a_i a_{j+1} = a_{i+1} a_j$ на коэффициенты $f$.

Упражнение 2.18. Убедитесь, что столбцы матрицы (2-32) суть делённые на $n!$ коэффициенты $n$ линейных форм $\frac{\partial^k}{\partial x_0^k} \frac{\partial^m}{\partial x_1^m} f$, где $k + m = n - 1$.

[1] Это количество разложений числа $n-1$ в сумму $d$ занумерованных целых неотрицательных слагаемых $m_1, \dots , m_d$.

**2.6. Поляризация грассмановых многочленов.** Согласно предл. 2.5, над полем нулевой характеристики факторизация антисимметричных по соотношениям антикоммутирования

$$\pi_{\Lambda^n}:\ \mathrm{Alt}^n V \to \Lambda^n V$$

является изоморфизмом. Обратный изоморфизм $\pi_{\Lambda^n}^{-1}:\ \Lambda^n V \xrightarrow{\sim} \mathrm{Alt}^n V$, как и в коммутативном случае, называется *полной поляризацией* грассмановых многочленов[1]. Он сопоставляет полиному $\omega \in \Lambda^n V$ единственный знакопеременный тензор $\widetilde{\omega} \in \mathrm{Alt}^n V \subset V^{\otimes n}$, лежащий в классе $\omega$ по модулю подпространства[2] $\mathcal{I}_{\text{skew}} \cap V^{\otimes n}$. Тензор $\widetilde{\omega}$ можно воспринимать как кососимметричную $n$-линейную форму $\widetilde{\omega}:\ V^* \times \dots \times V^* \to \Bbbk$, $(\xi_1, \dots, \xi_n) \mapsto \langle\, \xi_1 \otimes \dots \otimes \xi_n\,,\, \widetilde{\omega}\,\rangle$. Полная поляризация базисного грассманова монома $e_1 \wedge \ldots \wedge e_n$ по форм. (2-18) на стр. 25 равна

$$\frac{1}{n!} \sum_{g \in S_n} \mathrm{sgn}(g) \cdot e_{g_1} \wedge \ldots \wedge e_{g_n}\,.$$

Поляризация произвольного грассманова многочлена может быть получена отсюда по линейности.

**2.6.1. Двойственность.** Для двойственных конечномерных векторных пространств $V$, $V^*$ над полем характеристики нуль полная свёртка $\langle\, \widetilde{\omega}\,,\, \tilde{\xi}\,\rangle \in \Bbbk$ полных поляризаций $\widetilde{\omega} \in \mathrm{Alt}^n V$, $\tilde{\xi} \in \mathrm{Alt}^n V^*$ однородных грассмановых многочленов $\omega \in \Lambda^n V$, $\xi \in \Lambda^n V^*$ задаёт невырожденное спаривание между пространствами $\Lambda^n V^*$ и $\Lambda^n V$. Грассмановы мономы, составленные из векторов $e_i$ и $e_i^*$ двойственных друг другу базисов в $V$ и $V^*$ спариваются при этом по правилу

$$\langle\, e_{i_1} \wedge \ldots e_{i_n}\,,\, e^*_{j_1} \wedge \ldots e^*_{j_n}\,\rangle = \begin{cases} \mathrm{sgn}(g)/n! & \text{если } \exists\, g \in S_n:\ \forall\, \nu\ i_\nu = j_{g(\nu)} \\ 0 & \text{в остальных случаях}\,. \end{cases}$$

Упражнение 2.19. Убедитесь в этом.

**2.6.2. Грассмановы производные.** Как и для обычных многочленов, определим отображение *поляризации* грассмановых многочленов вдоль ковектора $\xi \in V^*$

$$\mathrm{pl}_\xi \overset{\text{def}}{=} \pi_{\Lambda^{n-1}} \circ i_\xi \circ \pi_{\Lambda^n}^{-1}:\ \Lambda^n V \to \Lambda^{n-1} V\,, \tag{2-33}$$

которое переводит грассманов многочлен $\omega \in \Lambda^n V$ в проекцию на $\Lambda^{n-1} V$ внутреннего произведения[3] $i_\xi \widetilde{\omega}$ ковектора $\xi$ и полной поляризации $\widetilde{\omega}$ многочлена $\omega$. Отображение (2-33) вписывается в коммутативную диаграмму

$$\begin{tikzcd} V^{*\otimes n} \supset \mathrm{Alt}^n V^* \arrow[r, "i_\xi"] \arrow[d, "\pi_{\Lambda^n}"', "\wr"] & V^{*\otimes(n-1)} \arrow[d, "\pi_{\Lambda^{n-1}}"] \\ \Lambda^n V^* \arrow[r, "\mathrm{pl}_\xi"] & \Lambda^{n-1} V^*\,. \end{tikzcd}$$

[1] Для удобства дальнейшего использования мы рассматриваем здесь грассмановы многочлены от базисных векторов самого пространства $V$, а не двойственного пространства $V^*$, как это было в предыдущем разделе.

[2] См. n° 2.3.3 на стр. 22.

[3] Т. е. свёртки $\xi$ с $\omega$ по первому тензорному сомножителю, см. прим. 2.1 на стр. 18.

Назовём *грассмановой производной* однородного грассманова многочлена $\omega$ в направлении ковектора $\xi \in V^*$ грассманов многочлен $\partial_\xi \omega \overset{\text{def}}{=} \deg \omega \cdot \mathrm{pl}_\xi \omega$. Так как тензор $\widetilde{\omega}$ кососимметричен, для любых $\xi$, $\eta$, $\psi_1, \dots, \psi_{n-2} \in V^*$ выполняется равенство

$$i_\xi i_\eta \widetilde{\omega}\left(\psi_1, \dots \psi_{n-2}\right) = \omega\left(\xi, \eta, \psi_1, \dots \psi_{n-2}\right) = -\omega\left(\eta, \xi, \psi_1, \dots \psi_{n-2}\right) = -i_\eta i_\xi \widetilde{\omega}\left(\psi_1, \dots \psi_{n-2}\right) .$$

Поэтому и грассмановы поляризации, и грассмановы производные антикоммутируют:

$$\mathrm{pl}_\xi \mathrm{pl}_\eta = -\mathrm{pl}_\eta \mathrm{pl}_\xi \quad \text{и} \quad \partial_\xi \partial_\eta = -\partial_\eta \partial_\xi ,$$

в частности $\partial_\xi^2 = 0$ для любого $\xi \in V^*$, что согласуется с тем, что грассмановы многочлены линейны по каждой переменной. Как и в коммутативном случае[1], выполняется равенство

$$\widetilde{\omega}(\xi_1, \dots, \xi_n) = \frac{1}{n!}\, \partial_{\xi_1} \dots \partial_{\xi_n} \omega . \tag{2-34}$$

Если ковекторы $x_i \in V^*$ и векторы $e_i \in V$ образуют двойственные друг другу базисы пространств $V$ и $V^*$, то в силу билинейной зависимости $\mathrm{pl}_\xi \omega$ от $\xi$ и $\omega$, грассманова производная в направлении ковектора $\xi = \sum_i \alpha_i x_i$ может быть записана как $\partial_\xi = \sum_i \alpha_i\, \partial_{x_i}$. При этом ненулевой вклад в $\partial_{x_i} \omega$ будет лишь от входящих в $\omega$ мономов $e_J$ с $J \ni i$.

Упражнение 2.20. Убедитесь, что $\partial_{x_{i_1}} e_{i_1} \wedge \ldots \wedge e_{i_n} = e_{i_2} \wedge \ldots \wedge e_{i_n}$ для любой[2] последовательности попарно разных индексов $i_1, \dots, i_n$.

Таким образом, дифференцирование грассманова монома в направлении базисного ковектора, двойственного к первой слева переменной в мономе, ведёт себя как обычная частная производная $\partial / \partial_{e_{i_1}}$ по этой переменной. В силу анткоммутативности грассмановых переменных, дифференцирование по $k$-той слева переменной монома ведёт себя как $(-1)^{k-1} \partial / \partial_{e_{i_k}}$:

$$\begin{aligned} \partial_{x_{i_k}} e_{i_1} \wedge \ldots \wedge e_{i_n} &= \partial_{x_{i_k}} (-1)^{k-1} e_{i_k} \wedge e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_{i_{k+1}} \ldots e_{i_n} = \\ &= (-1)^{k-1} e_{i_1} \wedge \ldots \wedge e_{i_{k-1}} \wedge e_{i_{k+1}} \ldots e_{i_n} . \end{aligned}$$

Иначе говоря, грассмановы производные удовлетворяют *грассманову правилу Лейбница*: для любых однородных грассмановых многочленов $\omega, \tau \in \Lambda V$ и любого ковектора $\xi \in V^*$

$$\partial_\xi(\omega \wedge \eta) = \partial_\xi(\omega) \wedge \eta + (-1)^{\deg \omega} \omega \wedge \partial_\xi(\eta) . \tag{2-35}$$

Упражнение 2.21. Докажите формулу (2-35).

**2.6.3. Линейный носитель грассманова многочлена.** Как и в коммутативном случае, *линейный носитель* $\mathrm{supp}(\omega) \subset V$ однородного грассманова многочлена $\omega \in \Lambda^n V$ определяется как линейный носитель[3] $\mathrm{supp}(\widetilde{\omega})$ его полной поляризации $\widetilde{\omega} \in \mathrm{Alt}^n V \subset V^{\otimes n}$.

Упражнение 2.22. Убедитесь, что $\mathrm{supp}(\omega) \subset V$ является пересечением всех таких подпространств $U \subset V$, что $\omega \in \Lambda^n U$, и стало быть, является наименьшим из этих подпространств, как по включению, так и по размерности.

[1] Ср. с 2-25 на стр. 29

[2] Не обязательно возрастающей.

[3] См. n° 2.2.2 на стр. 18.

Согласно теор. 2.1 на стр. 18, подпространство $\mathrm{supp}(\omega) = \mathrm{supp}(\widetilde{\omega}) \subset V$ является образом полной свёртки $c_\omega : V^{*\otimes(n-1)} \to V$ с тензором $\widetilde{\omega} \in V^{\otimes n}$ по любым[1] его $n-1$ тензорным сомножителям, т. е. линейно порождается векторами $\partial_J\omega \overset{\text{def}}{=} \partial_{x_{j_1}} \dots \partial_{x_{j_{n-1}}} \omega$, где $J = j_1 \dots j_{n-1}$ пробегает всевозможные последовательности из $n-1$ не повторяющихся[2] натуральных чисел $1 \leqslant j_\nu \leqslant d$. Запишем $\omega$ в виде суммы

$$\omega = \sum_I a_I e_I = \sum_{i_1 \dots i_n} \alpha_{i_1 \dots i_n} e_{i_1} \wedge \dots \wedge e_{i_n} \tag{2-36}$$

где $I = i_1 \dots i_n$ пробегает все последовательности из $n$ неповторяющихся индексов, а коэффициенты $\alpha_{i_1 \dots i_n}$ кососимметричны по $i_1, \dots, i_n$. Вклад в $\partial_J\omega$ дают лишь те слагаемые $a_I e_I$, у которых $I \supset J$. С точностью до общего знака,

$$\partial_J\omega = \pm \sum_{i \notin J} \alpha_{j_1 \dots j_{n-1} i}\, e_i\,. \tag{2-37}$$

Предложение 2.8

Следующие три условия на грассманов многочлен (2-36) эквивалентны:

1) $\omega = u_1 \wedge \dots \wedge u_n$ для некоторых $u_1, \dots, u_n \in V$

2) $u \wedge \omega = 0$ для всех $u \in \mathrm{supp}(\omega)$

3) для всех наборов $i_1 \dots i_{m+1}$ и $j_1 \dots j_{m-1}$, состоящих, соответственно, из $n+1$ и $n-1$ неповторяющихся в каждом из наборов индексов, выполнены *соотношения Плюккера*

$$\sum_{\nu=1}^{m+1} (-1)^{\nu-1} a_{j_1 \dots j_{m-1} i_\nu} a_{i_1 \dots \hat{i}_\nu \dots i_{m+1}} = 0\,, \tag{2-38}$$

где «крышка» в $a_{i_1 \dots \hat{i}_\nu \dots i_{m+1}}$ означает, что индекс $i_\nu$ следует пропустить.

Доказательство. Условие (1) означает, что $\omega$ лежит в старшей внешней степени $\Lambda^{\dim \mathrm{supp}(\omega)}$ своей линейной оболочки $\mathrm{supp}(\omega)$. По упр. 2.11 на стр. 24 это равносильно условию (2). Соотношение (2-38) представляет собою координатную запись условия (2) для $u = \partial_{j_1 \dots j_{m-1}}\omega$ и констатирует обнуление коэффициента при $e_{i_1} \wedge \dots \wedge e_{i_{m+1}}$ в произведении $(\partial_{j_1 \dots j_{m-1}}\omega) \wedge \omega$. Поскольку такие векторы $u$ линейно порождают пространство $\mathrm{supp}(\omega)$, соотношения Плюккера равносильны условию (2). □

Пример 2.4 (квадрика Плюккера в $\mathbb{P}_5$)

Для четырёхмерного пространства $V$ с базисом $e_1$, $e_2$, $e_3$, $e_4$ запись квадратичного многочлена $\omega \in \Lambda^2 V$ в виде (2-36) выглядит как $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j$, где коэффициенты $a_{ij}$ образуют кососимметричную матрицу размера $4\times4$. Соотношение Плюккера для наборов $(i_1, i_2, i_3) = (2, 3, 4)$ и $j_1 = 1$ имеет вид

$$a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23} = 0\,. \tag{2-39}$$

[1] В силу знакопеременности тензора $\widetilde{\omega}$ изменение последовательности сворачиваемых сомножителей может привести лишь к смене знака у результата.

[2] В силу кососимметричности грассмановых частных производных можно было бы ограничиться только строго возрастающими последовательностями, но мы умышленно этого не делаем, чтобы упростить предстоящие далее вычисления.

Любой другой выбор непересекающихся наборов $(i_1, i_2, i_3)$ и $j_1 \notin \{i_1, i_2, i_3\}$ приводит к тому же самому квадратичному соотношению (2-39).

Упражнение 2.23. Проверьте это.

Если же взять $j_1 \in \{i_1, i_2, i_3\}$, то получится тривиальное соотношение $0 = 0$, поскольку в каждом из произведений $a_{ij}a_{km}$ будет сомножитель вида $a_{nn} = 0$. Таким образом, множество разложимых в произведение двух линейных множителей грассмановых квадратичных форм от четырёх переменных описывается уравнением (2-39), которое задаёт гладкую квадрику в $\mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$.

Упражнение 2.24. Убедитесь, что соотношение (2-39) на грассманову квадратичную форму $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j \in \Lambda^2 \Bbbk^4$ равносильно условию $\omega \wedge \omega = 0$.

Пример 2.5 (разложимые квадратичые формы)
Пусть $\dim V = n$. Всякая грассманова квадратичная форма $\omega \in \Lambda^2 V$ раскладывается по базисным мономам как $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j$, где числа $a_{ij} \in \Bbbk$ образуют кососимметричную $n \times n$ матрицу $A$, являющуюся матрицей Грама билинейной формы $\widetilde{\omega} : V^* \times V^* \to \Bbbk$ в двойственном базисе пространства $V^*$.

Упражнение 2.25. Убедитесь в этом.

В базисе $e_1, \dots, e_d$, который двойствен к такому базису пространства $V^*$, где матрица Грама кососимметричной билинейной формы $\widetilde{\omega}$ имеет блочный диагональный вид из $2 \times 2$ блоков[1] $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, форма $\omega$ приобретает вид $\omega = e_1 \wedge e_2 + e_3 \wedge e_4 + \dots$. Если в этой сумме ровно одно слагаемое, то форма $\omega = e_1 \wedge e_2$ разложима, и $\omega \wedge \omega = 0$. Если слагаемых больше одного, то $\omega \wedge \omega = 2e_1 \wedge e_2 \wedge e_3 \wedge e_4 + \dots \neq 0$, и стало быть, форма $\omega$ не представляется в виде $u \wedge w$ ни для каких $u, w \in V$. Таким образом, грассманова квадратичная форма $\omega \in \Lambda^2 V$ разложима в произведение двух линейных форм если и только если $\omega \wedge \omega = 0$. При $\dim V = 4$ и $\dim \Lambda^4 V = 1$ условие $\omega \wedge \omega = 0$ на форму $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j$ записывается одним квадратичным соотношением (2-39), констатирующим обнуление коэффициента при $e_1 \wedge e_2 \wedge e_3 \wedge e_4$ в $\omega \wedge \omega$.

**2.6.4. Грассманианы.** Множество $m$-мерных векторных подпространств в векторном пространстве $V$ обозначается $\mathrm{Gr}(m, V)$ и называется *грассманианом* $m$-мерных подпространств в $V$. Если $V = \Bbbk^d$ или природа пространства $V$ несущественна, мы пишем $\mathrm{Gr}(m, d)$ вместо $\mathrm{Gr}(m, V)$, где $d = \dim V$. Грассманиан $\mathrm{Gr}(m, V)$ вкладывается в проективное пространство $\mathbb{P}(\Lambda^m V)$ *отображением Плюккера*

$$p_m : \mathrm{Gr}(m, V) \to \mathbb{P}(\Lambda^m V), \quad U \mapsto \Lambda^m U \subset \Lambda^m V, \tag{2-40}$$

которое сопоставляет каждому $m$-мерному подпространству $U \subset V$ одномерное подпространство $\Lambda^m U \subset \Lambda^m V$. Если векторы $u_1, \dots, u_m$ составляют базис в $U$, то с точностью до ненулевого постоянного множителя $p_m(U) = u_1 \wedge \dots \wedge u_m$.

Упражнение 2.26. Убедитесь, что отображение (2-40) инъективно.

Образ плюккерова вложения (2-40) состоит из ненулевых грассмановых полиномов $\omega \in \Lambda^m V$, полностью разложимых в произведение $m$ линейных множителей, т. е. имеющих линейный носитель минимально возможной размерности $\dim \operatorname{supp} \omega = \deg \omega = m$. Такие полиномы называются *разложимыми*. По предл. 2.8, классы пропорциональности таких полиномов составляют в $\mathbb{P}(\Lambda^m V)$ алгебраическое многообразие, задаваемое плюккеровыми квадратичными соотношениями (2-38).

[1] См. раздел n° 16.5.2 части I.

**2.6.5. Однородные и плюккеровы координаты.** Грассманиан $\mathrm{Gr}(m,d)$ является прямым обобщением проективного пространства $\mathbb{P}_n = \mathrm{Gr}(1, n+1)$. Векторное подпространство $U \subset V$ размерности $m$ в координатном пространстве $V = \Bbbk^d$ можно задавать $m \times d$ матрицей $X_{\boldsymbol{u}}$, в $m$ строках которой стоят координаты векторов некоторого базиса $\boldsymbol{u} = (u_1, \dots, u_m)$ пространства $U$ в стандартном базисе $e_1, \dots, e_d$ пространства $\Bbbk^d$. При выборе в подпространстве $U$ другого базиса $(w_1, \dots, w_m) = (u_1, \dots, u_m) \cdot C_{\boldsymbol{uw}}$, где $C_{\boldsymbol{uw}} \in \mathrm{GL}_m(\Bbbk)$ обозначает (обратимую) матрицу перехода от базиса $\boldsymbol{w}$ к базису $\boldsymbol{u}$, матрица $X_{\boldsymbol{u}}$ заменится матрицей $X_{\boldsymbol{w}} = C^t_{\boldsymbol{uw}} X_{\boldsymbol{u}}$.

Упражнение 2.27. Убедитесь в этом.

Таким образом, подпространству $U \subset V$ взаимно однозначно соответствует всех множество $m \times d$ матриц ранга $m$, образующих одну орбиту действия группы $\mathrm{GL}_m(\Bbbk)$ на пространстве $\mathrm{Mat}_{m\times d}(\Bbbk)$ левыми умножениями, т. е. грассманиан $\mathrm{Gr}(m,d)$ представлет сбою множество $m\times d$ матриц ранга $m$, рассматриваемых с точностью до умножения слева на произвольные обратимые $m \times m$ матрицы. При $m = 1$ мы получаем строки $(x_1, \dots, x_d) \in \mathrm{Mat}_{1\times d} = \Bbbk^d$, рассматриваемые с точностью до умножения на ненулевые константы $\lambda \in \mathrm{GL}_1(\Bbbk) = \Bbbk^*$, т. е. в точности однородные координаты на $\mathbb{P}_{d-1} = \mathrm{Gr}(1,d)$. Поэтому по аналогии с проективным пространством мы будем называть матрицу $X_{\boldsymbol{u}}$, отвечающую базису $\boldsymbol{u}$ подпространства $U$, *матрицей однородных координат* точки $U \in \mathrm{Gr}(m,d)$. Подчеркнём ещё раз, что матрица однородных координат определена лишь с точностью до умножения слева на произвольные матрицы из $\mathrm{GL}_m(\Bbbk)$.

Упражнение 2.28. Убедитесь, что каждый коэффициент $x_{i_1\dots i_n}$ в разложении

$$u_1 \wedge \ldots \wedge u_m = \sum_{i_1<\dots<i_m} x_{i_1\dots i_n} e_{i_1} \wedge \ldots \wedge e_{i_n}$$

равен $m \times m$ минору матрицы $X_{\boldsymbol{u}}$, расположенному в столбцах $i_1, \dots, i_m$.

Набор рассматриваемых с точностью до пропорциональности $m \times m$ миноров $x_{i_1\dots i_n}$ матрицы $X_{\boldsymbol{u}}$, т. е. набор однородных координат плюккерова образа $p_m(U) \in \mathbb{P}(\Lambda^m V)$ подпространства $U \subset V$, называется *плюккеровыми координатами* точки $U \in \mathrm{Gr}(m,d)$.

**2.6.6. Многообразие Сегре как сечение грассманиана.** Рассмотрим прямую сумму

$$W = V_1 \oplus \dots \oplus V_n$$

конечномерных векторных пространств $V_i$. Для каждого $k \in \mathbb{N}$ и произвольной последовательности целых чисел $m_1, \dots, m_n$, в которой $0 \leqslant m_i \leqslant \dim V_i$ при всех $i$ и $\sum_\nu m_\nu = k$, обозначим через $W_{m_1\dots m_n} \subset \Lambda^k W$ линейную оболочку всех тех грассмановых мономов $w_1 \wedge \ldots \wedge w_k$, у которых для каждого $i$ ровно $m_i$ из сомножителей $w_\nu$ лежит в $V_i$.

Упражнение 2.29. Покажите, что правило $\omega_1 \otimes \dots \otimes \omega_n \mapsto \omega_1 \wedge \dots \wedge \omega_n$ корректно задаёт линейный изоморфизм $\Lambda^{m_1} V_1 \otimes \dots \otimes \Lambda^{m_n} V_n \xrightarrow{\sim} W_{m_1\dots m_n}$ и что

$$\Lambda^k W = \bigoplus_{m_1,\dots,m_n} W_{m_1\dots m_n} \simeq \bigoplus_{m_1,\dots,m_n} \Lambda^{m_1} V_1 \otimes \dots \otimes \Lambda^{m_n} V_n \,. \tag{2-41}$$

В частности, тензорное произведение $V_1 \otimes \dots \otimes V_n$ канонически изоморфно прямому слагаемому $W_{1\dots 1} \subset \Lambda^n W$ разложения (2-41). Этот изоморфизм переводит разложимые тензоры $v_1 \otimes \dots \otimes v_n$ в грассмановы мономы $v_1 \wedge \ldots \wedge v_n$. Таким образом, многообразие Сегре прим. 1.3 на стр. 8 представляет собою сечение грассманиана $\mathrm{Gr}(n, W) \subset \mathbb{P}(\Lambda^n W)$ проективным подпространством $\mathbb{P}\left(W_{1\dots 1}\right) \subset \mathbb{P}(\Lambda^n W)$ и является проективным алгебраическим многообразием, задаваемым ограничениями квадратичных соотношений из предл. 2.8 на стр. 34 на линейное подпространство $W_{1\dots 1} \subset \Lambda^n W$.

## §3. Симметрические функции

**3.1. Симметрические и кососимметрические многочлены.** Симметрическая группа $S_n$ действует на кольце многочленов $\mathbb{Z}[x_1, \dots, x_n]$ переставляя переменные:

$$\forall\, g \in S_n \quad gf(x_1, \dots, x_n) \overset{\text{def}}{=} f(x_{g(1)}, x_{g(2)}, \dots, x_{g(n)})\,. \tag{3-1}$$

Многочлен $f \in \mathbb{Z}[x_1, \dots, x_n]$ называется *симметрическим*, если $gf = f$ для всех $g \in S^n$, и *кососимметрическим* — если $gf = \operatorname{sgn}(g)\cdot f$ для всех $g \in S^n$. Симметрические многочлены образуют в $\mathbb{Z}[x_1, \dots, x_n]$ подкольцо, а кососимметрические — модуль над этим кольцом[1]. При отождествлении кольца многочленов от $n$ переменных с $n$-й тензорной степенью кольца многочленов от одной переменной при помощи канонического изоморфизма из прим. 1.2 на стр. 8:

$$\varkappa : \mathbb{Z}[x_1, \dots, x_n] \xrightarrow{\sim} \mathbb{Z}[t]^{\otimes n}\,, \quad x_1^{m_1} x_2^{m_2} \dots x_n^{m_n} \mapsto t^{m_1} \otimes t^{m_2} \otimes \dots \otimes t^{m_n}\,, \tag{3-2}$$

(косо)симметрические многочлены превращаются в точности в (косо)симметричные тензоры, а умножение многочленов — в покомпонентное умножение

$$\big(f_1 \otimes \dots \otimes f_n\big) \cdot \big(g_1 \otimes \dots \otimes g_n\big) \overset{\text{def}}{=} (f_1 g_1) \otimes (f_2 g_2) \otimes \dots \otimes (f_n g_n)\,.$$

Упражнение 3.1. Проверьте, что такое умножение наделяет $\mathbb{Z}$-модуль $\mathbb{Z}[t]^{\otimes n}$ структурой коммутативного кольца с единицей $1 \otimes \dots \otimes 1$.

Описанные в n° 2.4.1 на стр. 24 и n° 2.4.2 на стр. 25 стандартные базисы в $\mathbb{Z}$-модулях симметричных тензоров $\operatorname{Sym}^n(\mathbb{Z}[t])$ и знакопеременных тензоров $\operatorname{Alt}^n(\mathbb{Z}[t])$ переносятся изоморфизмом (3-2) в базисы $\mathbb{Z}$-модулей симметрических и кососимметрических многочленов, которые принято называть соответственно *мономиальным* и *детерминантным* базисами.

**3.1.1. Мономиальный базис модуля симметрических многочленов.** Поскольку симметрический многочлен вместе с каждым своим мономом содержит с тем же самым коэффициентом и все мономы из его $S_n$-орбиты, а $S_n$-орбита любого монома однозначно определяется лексикографически старшим мономом в орбите, показатели которого не убывают слева направо, всякий симметрический многочлен единственным способом представляется в виде целочисленной линейной комбинации многочленов

$$m_\lambda = (\text{сумма всех мономов из } S_n\text{-орбиты монома } x_1^{\lambda_1} x_2^{\lambda_2} \dots x_n^{\lambda_n})\,, \tag{3-3}$$

где $\lambda = (\lambda_1, \dots, \lambda_n)$ пробегает диаграммы Юнга из $n$ строк (часть из которых может быть нулевой длины). Многочлен (3-3) называется *мономиальным симметрическим многочленом*. При изоморфизме (3-2) он переходит в стандартный базисный симметрический тензор[2], равный сумме всех различных тензорных произведений, содержащих $m_0(\lambda)$ сомножителей $1 = t^0$, $m_1(\lambda)$ сомножителей $t^1$, $m_2(\lambda)$ сомножителей $t^2$ и т. д., где через $m_i(\lambda)$ здесь и далее всегда обозначается количество строк длины $i$ в диаграмме Юнга $\lambda$.

[1] Ибо при умножении кососимметрического многочлена на симметрический получается кососимметрический многочлен.

[2] См. n° 2.4.1 на стр. 24.

**3.1.2. Детерминантные базисы.** Так как при транспозиции любых двух переменных кососимметрический многочлен меняет свой знак, в каждом мономе такого многочлена степени всех переменных попарно различны. Поэтому базис $\mathbb{Z}$-модуля кососимметрических многочленов образуют альтернированные $S_n$-орбиты вида

$$\Delta_\nu = \sum_{g \in S_n} \operatorname{sgn}(g)\, x_{g(1)}^{\nu_1} x_{g(2)}^{\nu_2} \cdots x_{g(n)}^{\nu_n}\,, \tag{3-4}$$

занумерованные диаграммами Юнга $\nu$ из $n$ строк строго убывающей длины

$$\nu_1 > \nu_2 > \ldots > \nu_n \geqslant 0\,.$$

Все такие диаграммы $\nu$ содержат в себе минимальную треугольную диаграмму

$$\delta = \big((n-1),\, (n-2),\, \ldots\,,\, 1,\, 0\big)$$

из $n$ строк разной длины, и разности

$$\lambda = \nu - \delta \overset{\text{def}}{=} \big((\nu_1 - n + 1),\, (\nu_2 - n + 2),\, \ldots\,,\, (\nu_{n-1} - 1),\, \nu_n\big)$$

имеют $\lambda_i = \nu_i - n + i$ и пробегают множество всех диаграмм Юнга из $n$ строк безо всяких ограничений на их длины (которые могут быть и нулевыми). Часто бывает удобно нумеровать базис (3-4) именно такими диаграммами $\lambda$, и тогда мы будем писать $\Delta_{\lambda+\delta}$ вместо $\Delta_\nu$.

Легко усмотреть, что многочлен (3-4) представляет собою определитель[1]

$$\Delta_\nu = \det(x_j^{\nu_i}) = \det \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix} \tag{3-5}$$

Упражнение 3.2. Убедитесь в этом прямым раскрытием правой части (3-5).

В частности, при $\nu = \delta$ получаем *определитель Вандермонда*

$$\Delta_\delta = \det(x_j^{n-i}) = \det \begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ \vdots & \vdots & \cdots & \vdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{pmatrix} = \prod_{i<j} (x_i - x_j)\,. \tag{3-6}$$

Упражнение 3.3. Убедитесь в справедливости равенства $\Delta_\delta = \prod_{i<j}(x_i - x_j)$.

[1] Здесь и далее запись $(f(i,j))$, где $f(i,j)$ — какая-либо функция от $i$, $j$, означает матрицу, в $i$-й строке и $j$-м столбце которой стоит результат применения функции $f$ к данным $i$ и $j$.

**3.1.3. Базис Шура.** Поскольку любой кососимметрический многочлен $f$ обращается в нуль при подстановке $x_i = x_j$, он делится в кольце $\mathbb{Z}[x_1, \dots, x_n]$ на $(x_i - x_j)$, а так как каждая из разностей $(x_i - x_j)$ неприводима, $f$ делится на их произведение $\Delta_\delta = \prod_{i<j}(x_i - x_j)$, и частное от деления $f/\Delta_\delta \in \mathbb{Z}[x_1, \dots, x_n]$ является симметрическим многочленом. Мы получаем

Предложение 3.1
Умножение на определитель Вандермонда $\Delta_\delta$ задаёт биекцию между симметричными и кососимметричными многочленами. Эта биекция является изоморфизмом модулей над кольцом симметрических многочленов (и в частности — $\mathbb{Z}$-модулей). □

Следствие 3.1
Многочлены[1] $s_\lambda = \Delta_{\delta+\lambda}/\Delta_\delta$, где $\lambda$ пробегает все диаграммы Юнга из не более $n$ строк, образуют базис $\mathbb{Z}$-модуля симметрических многочленов.

**3.2. Элементарные симметрические многочлены.** Коэффициенты многочлена от $t$

$$E(t) = \prod_i (1 + x_i t) = \sum_{k=0}^{n} e_k(x) \cdot t^k \in \mathbb{Z}[x_1, \dots, x_n][t] \tag{3-7}$$

называются *элементарными симметрическими многочленами*. Раскрыв скобки в (3-7), заключаем, что $e_0 = 1$ и

$$e_k(x) = \sum_{i_1 < i_2 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k} \tag{3-8}$$

(сумма всех произведений из $k$ различных переменных, где $k \geqslant 1$). Эти же многочлены $e_k$ возникают и в *формулах Виета*: если $\alpha_1, \dots, \alpha_n$ являются корнями приведённого многочлена

$$t^n + a_1 t^{n-1} + \dots + a_{n-1} t + a_n = \prod_{i=1}^{n} (x - \alpha_i)\,, \tag{3-9}$$

то $a_i = (-1)^i e_i(\alpha_1, \dots, \alpha_n)$.

**3.2.1. Разложение по мономиальному базису.** Для диаграммы Юнга $\lambda = (\lambda_1, \dots, \lambda_k)$ положим $e_\lambda \overset{\text{def}}{=} e_{\lambda_1} \dots e_{\lambda_k} = \prod_{i=1}^{k} e_{\lambda_i}$. Это всего лишь другое обозначение для монома $e_1^{m_1} \dots e_n^{m_n}$, показатель $m_i$ которого равен количеству строк длины $i$ в диаграмме $\lambda$, причём диаграмма Юнга $\lambda$ и набор неотрицательных показателей $m = (m_1, \dots, m_n)$ взаимно однозначно определяются друг другом из равенства $e_{\lambda_1} \dots e_{\lambda_k} = e_1^{m_1} \dots e_n^{m_n}$. Запись мономов от букв $e_i$ в виде $e_\lambda$ часто упрощает многие вычисления. Например, лексикографически старший по переменным $x_1, \dots, x_n$ мономом в симметрическом многочлене $e_\lambda$ получается при перемножении монома $x_1 \dots x_{\lambda_1}$ из $e_{\lambda_1}$, монома $x_1 \dots x_{\lambda_2}$ из $e_{\lambda_2}$ и т. д. вплоть до $x_1 \dots x_{\lambda_k}$ из $e_{\lambda_k}$. Его удобно представлять себе как результат перемножения переменных $x_i$, вписанных в клетки диаграммы Юнга $\lambda$ так, что номер переменной совпадает с номером столбца, в котором она стоит. Моном от $x$, который получится в результате перемножения всех переменных из диаграммы $\lambda$, имеет вид $x_1^{\lambda_1^t} x_2^{\lambda_2^t} \dots x_n^{\lambda_n^t}$, где $\lambda^t = (\lambda_1^t, \dots, \lambda_n^t)$ — это диаграмма Юнга, транспонированная[2] к $\lambda$. Мы заключаем, что разложение многочлена $e_\lambda$ по базису из мономиальных симметрических многочленов[3] $m_\lambda$ имеет вид:

$$e_\lambda = m_{\lambda^t} + (\text{лексикографически младшие члены}) \tag{3-10}$$

[1] Многочлены $s_\lambda = \Delta_{\delta+\lambda}/\Delta_\delta$ называются (*детерминантными*) *многочленами Шура*.
[2] строками которой служат столбцы диаграммы $\lambda$, как при транспонировании матрицы.
[3] См. формулу (3-3) на стр. 37.

Предложение 3.2
Многочлены $e_\lambda = e_{\lambda_1} \dots e_{\lambda_m}$, где $\lambda$ пробегает диаграммы Юнга из $n$ столбцов (длины столбцов могут быть и нулевыми), образуют базис $\mathbb{Z}$-модуля симметрических функций.

Доказательство. Мономиальные многочлены $m_\mu$ из форм. (3-3) на стр. 37 нумеруются диаграммами Юнга из $n$ строк (длины которых могут быть нулевыми). Выпишем их в строку в порядке лексикографического возрастания диаграмм $\mu$. Многочлены $e_\lambda$, занумерованные диаграммами $\lambda$ из $n$ столбцов (длины которых также могут быть нулевыми), тоже выпишем в строку, но в порядке лексикографического возрастания транспонированных диаграмм $\lambda^t$. Формула (3-10) утверждает, что вторая строка получается из первой умножением справа на квадратную целочисленную верхнегортанную матрицу с единицами по главной диагонали. Поскольку такая матрица обратима над $\mathbb{Z}$, многочлены $e_\lambda$ также образуют базис. □

Следствие 3.2
Многочлены $e_1, \dots, e_n$ алгебраически независимы в $\mathbb{Z}[x_1, \dots, x_n]$ и любой симметрический многочлен однозначно записывается в виде многочлена от $e_1, \dots, e_n$.

Доказательство. Вспоминаем, что каждое произведение $e_\lambda = e_{\lambda_1} \dots e_{\lambda_k}$ представляет собою моном $e^m \overset{\text{def}}{=} e_1^{m_1} \dots e_n^{m_n}$, у которого показатель $m_i$ равен количеству строк длины $i$ в диаграмме $\lambda$, и что множество многочленов $e_\lambda$ — это в точности множество всех различных мономов от $e_1, \dots, e_n$. □

Следствие 3.3
Всякий симметрический многочлен от корней приведённого многочлена $f(t)$ можно переписать как многочлен от коэффициентов $f$. □

**3.3. Полные симметрические многочлены.** Сумма всех мономов степени $k$ в $\mathbb{Z}[x_1, \dots, x_n]$ обозначается $h_k$ и называется *полным симметрическим многочленом* степени $k$. Он равен коэффициенту при $t^k$ у формального степенного ряда $H(t) \in \mathbb{Z}[x_1, \dots, x_n]\,[[t]]$, возникающего при перемножении $n$ бесконечных геометрических прогрессий[1]

$$H(t) = \prod_i \frac{1}{1 - x_i t} = \prod_i \left(1 + x_i t + x_i^2 t^2 + x_i^3 t^3 + \cdots \right) = \sum_{k \geqslant 0} h_k(x) \cdot t^k . \tag{3-11}$$

Поэтому $H(t)E(-t) = 1$. Вычисляя в этом равенстве коэффициент при $t^k$ получаем рекурсивные формулы, выражающие $e_i$ и $h_i$ друг через друга:

$$(-1)^{k+1} h_k = e_k - e_{k-1} h_1 + e_{k-2} h_2 - \cdots + (-1)^{k-1} e_1 h_{k-1} \tag{3-12}$$
$$(-1)^{k+1} e_k = h_k - h_{k-1} e_1 + h_{k-2} e_2 - \cdots + (-1)^{k-1} h_1 e_{k-1} . \tag{3-13}$$

Предложение 3.3
Отображение $\omega$, переводящее многочлен $e_k$ в многочлен $h_k$ (при $k = 1, \dots, n$) является инволютивным автоморфизмом кольца симметрических многочленов.

[1] Выбирая в $i$-й скобке $m_i$-е слагаемое, получаем после их перемножения моном $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$.

Доказательство. Так как кольцо симметрических функций изоморфно кольцу многочленов от $e_1, \dots, e_n$, отображение $e_k \mapsto h_k$ однозначно продолжается до гомоморфизма $\omega$ из кольца симметрических функций в себя. Из рекурсивных формул (3-12) и (3-13) вытекает, что этот гомоморфизм переводит $h_k$ обратно в $e_k$, т. е. является инволютивной[1] биекцией. □

Следствие 3.4
Многочлены $h_1, \dots, h_n$ алгебраически независимы в $\mathbb{Z}[x_1, \dots, x_n]$ и любой симметрический многочлен (в том числе $h_m$ с $m > n$) однозначно записывается в виде многочлена от $h_1, \dots, h_n$.

**3.4. Степенные суммы Ньютона.** Сумма $k$-тых степеней всех переменных

$$p_k(x) = \sum_i x_i^k \tag{3-14}$$

называется $k$-тым *симметрическим многочленом Ньютона*. Многочлены $p_k(x)$ с $k \geqslant 1$ удобно воспринимать как коэффициенты ряда

$$\begin{aligned} P(t) = \sum_{k\geqslant 1} p_k(x)\, t^{k-1} = \sum_i \sum_{k\geqslant 1} x_i^k\, t^{k-1} = \sum_i \frac{d}{dt} \sum_{k\geqslant 1} x_i^k\, \frac{t^k}{k} = \\ = -\frac{d}{dt} \sum_i \ln(1 - x_i\, t) = \frac{d}{dt}\, \ln \prod_i \frac{1}{1 - x_i\, t} = \frac{d}{dt}\, \ln H(t) \end{aligned} \tag{3-15}$$

который является логарифмической производной от ряда $H(t) = 1/E(-t)$. Таким образом,

$$P(t) = H'(t)/H(t) = E'(-t)/E(-t)\,.$$

Сравнивая коэффициенты при $t^{k-1}$ в равенствах $H(t)P(t) = H'(t)$ и $E(-t)P(t) = E'(-t)$, получаем *формулы Ньютона*, рекурсивно выражающие $p_k$ через $h_k$ или через $e_k$:

$$p_k = kh_k - h_{k-1}p_1 - h_{k-2}p_2 - \cdots - h_1 p_{k-1} \tag{3-16}$$

$$(-1)^{k-1}p_k = ke_k - e_{k-1}p_1 + e_{k-2}p_2 - \cdots + (-1)^{k-1}e_1 p_{k-1}\,. \tag{3-17}$$

Индукция по $k$ показывает, что многочлен $p_k$ является собственным вектором инволюции $\omega$ из предл. 3.3 с собственным значением $(-1)^{k-1}$ :

$$\omega(p_k) = (-1)^{k-1} p_k\,. \tag{3-18}$$

Следствие 3.5
Многочлены $p_1, \dots, p_n$ алгебраически независимы в $\mathbb{Q}[x_1, \dots, x_n]$ и любой симметрический многочлен с рациональными коэффициентами (в том числе $p_m$ с $m > n$) однозначно записывается в виде многочлена с рациональными коэффициентами от $p_1, \dots, p_n$.

Доказательство. Из формулы (3-17) вытекает, что при любом $N \in \mathbb{N}$ в пространстве многочленов степени $\leqslant N$ от $x_1, \dots, x_n$ с рациональными коэффициентами $\mathbb{Q}$-линейная оболочка всевозможных мономов от $p_1, \dots, p_n$ совпадает с $\mathbb{Q}$-линейной оболочкой всевозможных мономов от $e_1, \dots, e_n$. Поскольку при фиксированном $N$ количества этих мономов одинаковы и мономы от $e_1, \dots, e_n$ образуют базис, то и мономы от $p_1, \dots, p_n$ тоже образуют базис. В частности, они линейно независимы над $\mathbb{Q}$. □

[1] Т. е. обратной самой себе.

**3.4.1. Явное выражение $e_k$ и $h_k$ через $p_k$.** Как и в n° 3.2.1 выше, для каждой диаграммы Юнга $\lambda = (\lambda_1, \lambda_2, \dots)$, состоящей из $m_1$ единиц, $m_2$ двоек, $m_3$ троек[1] и т. д., положим

$$\begin{aligned} e_\lambda &\overset{\text{def}}{=} e_{\lambda_1} e_{\lambda_2} e_{\lambda_3} \dots = e_1^{m_1} e_2^{m_2} e_3^{m_3} \dots \\ h_\lambda &\overset{\text{def}}{=} h_{\lambda_1} h_{\lambda_2} h_{\lambda_3} \dots = h_1^{m_1} h_2^{m_2} h_3^{m_3} \dots \\ p_\lambda &\overset{\text{def}}{=} p_{\lambda_1} p_{\lambda_2} p_{\lambda_3} \dots = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots \end{aligned} \tag{3-19}$$

и условимся более не различать между собою диаграммы $\lambda$, получающиеся друг из друга добавлением или удалением строк нулевой длины, т. е. приписыванием к $\lambda_1, \lambda_2, \dots$ или удалением оттуда любого количества нулей справа. Таким образом, множество многочленов вида $p_\lambda$ — это в точности множество всевозможных мономов[2] от формальных переменных $p_i$, и то же самое справедливо для многочленов $e_\lambda$ и $h_\lambda$.

Многочлены $p_\lambda$ являются собственными векторами инволюции $\omega$ из предл. 3.3 на стр. 40:

$$\omega(p_\lambda) = \varepsilon_\lambda \cdot p_\lambda\,, \quad \text{где} \quad \varepsilon_\lambda = (-1)^{\sum (k-1)m_k} = (-1)^{|\lambda|}(-1)^{\sum m_k} = (-1)^{\sum(\lambda_i - 1)}\,. \tag{3-20}$$

Далее, для каждой диаграммы Юнга $\lambda$ обозначим через

$$z_\lambda \overset{\text{def}}{=} \prod_k \left(m_k! \cdot k^{m_k}\right) \tag{3-21}$$

порядок централизатора перестановки циклового типа[3] $\lambda$ в симметрической группе $S_{|\lambda|}$.

Упражнение 3.4. Убедитесь, что количество перестановок, коммутирующих с данной перестановкой циклового типа $\lambda$, действительно равно (3-21), и покажите, что в $S_{|\lambda|}$ имеется всего $|\lambda|!/z_\lambda$ перестановок циклового типа $\lambda$.

Предложение 3.4
Многочлены $e_k$ и $h_k$ выражаются через $\mathbb{Q}$-базис $p_\lambda$ по формулам:

$$h_k = \sum_{|\lambda|=k} z_\lambda^{-1} p_\lambda\,, \quad e_k = \sum_{|\lambda|=k} \varepsilon_\lambda z_\lambda^{-1} p_\lambda\,, \tag{3-22}$$

где суммирование ведётся по всем $k$-клеточным диаграммам Юнга.

Доказательство. Докажем левую формулу, правая получается из неё применением инволюции $\omega$ из предл. 3.3. Согласно форм. (3-15) на стр. 41,

$$H(t) = e^{\int P(t)\,dt} = e^{\sum p_i t^i/i} = \prod e^{p_i t^i/i} = \prod_{i \geqslant 1} \sum_{m \geqslant 0} \frac{p_i^m}{i^m m!} t^{im}\,.$$

Если выбрать в $i$-м сомножителе $m_i$-е слагаемое, то их произведение даст вклад в коэффициент при $t^k$ если и только если $\sum_i i \cdot m_i = k$. Такие выборы биективно соответствуют $k$-клеточным диаграммам Юнга $\lambda$ с $m_1$ строками длины 1, $m_2$ строками длины 2 и т. д., а вклад произведения, отвечающего такой диаграмме, равен $p_\lambda / z_\lambda$. □

---

[1] Отметим, что $\sum_k k \cdot m_k = |\lambda|$.

[2] Напомню, что переход от нумерации мономов диаграммами Юнга к их обычной нумерации показателями степеней — это переход от неубывающей последовательности $\lambda = (\lambda_1, \lambda_2, \dots)$ неотрицательных целых чисел к вектору $m(\lambda) = (m_1, \cdots, m_n)$ с неотрицательными целочисленными координатами, у которого $i$-тая координата $m_i$ равна количеству строк длины $i$ в диаграмме $\lambda$.

[3] См. http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_11.pdf, раздел 9.1.2 на стр. 150.

**3.5. Формула Джамбелли** выражает детерминантные многочленами Шура $s_\lambda$ через полные симметрические многочлены $h_k$ в кольце $\mathbb{Z}[x_1, \dots , x_n]$. Для её получения обозначим через

$$e_k^{(p)} = e_k^{(p)}(x_1, \dots , \hat{x}_p, \dots , x_n)\,,$$

симметрическую функцию от $(n-1)$ переменных[1], которая получается из элементарного симметрического многочлена $e_k = e_k(x_1, \dots , x_n)$ подстановкой $x_p = 0$. При фиксированном $p$ производящая функция для многочленов $e_k^{(p)}$ имеет вид $E^{(p)}(t) = \sum_k e_k^{(p)}(x) \cdot t^k = \prod_{i\neq p}(1 + x_i t)$. Поэтому $H(t)E^{(p)}(-t) = (1 - x_p t)^{-1}$. Сравнивая коэффициенты при $t^k$ в обеих частях, получаем для каждого целого неотрицательного $k$ соотношение

$$\begin{aligned} x_p^k = h_{k-n+1} \cdot (-1)^{n-1} e_{n-1}^{(p)} + h_{k-n+2} \cdot (-1)^{n-2} e_{n-2}^{(p)} + \dots + h_k \cdot e_0^{(p)} = \\ = \sum_{j=1}^{n} h_{k-n+j} \cdot (-1)^{n-j} e_j^{(p)}\,, \end{aligned} \tag{3-23}$$

в правой части которого стоит произведение $n$-мерных строки $(h_{k-n+1}, \dots , h_k)$ и столбца

$$\begin{pmatrix} (-1)^{n-1} e_{n-1}^{(p)} \\ \vdots \\ e_2^{(p)} \\ -e_1^{(p)} \\ 1 \end{pmatrix}$$

Для данных $\nu_1 > \nu_2 > \ldots > \nu_n$ организуем $h$-строки, отвечающие $k = \nu_1, \dots , \nu_n$, в матрицу[2]

$$H_\nu = \left(h_{\nu_i - n + j}\right) = \begin{pmatrix} h_{\nu_1-n+1} & h_{\nu_1-n+2} & \cdots & h_{\nu_1} \\ h_{\nu_2-n+1} & h_{\nu_2-n+2} & \cdots & h_{\nu_2} \\ \vdots & \vdots & \ddots & \vdots \\ h_{\nu_n-n+1} & h_{\nu_n-n+2} & \cdots & h_{\nu_n} \end{pmatrix}\,,$$

а $e^{(p)}$-столбцы, отвечающие $p = 1,\ 2,\ \dots\ ,\ n,$ — в матрицу

$$M = \left((-1)^{n-i} e_{n-i}^{(j)}\right) = \begin{pmatrix} (-1)^{n-1} e_{n-1}^{(1)} & (-1)^{n-1} e_{n-i}^{(2)} & \cdots & (-1)^{n-1} e_{n-1}^{(n)} \\ (-1)^{n-2} e_{n-2}^{(1)} & (-1)^{n-2} e_{n-i}^{(2)} & \cdots & (-1)^{n-2} e_{n-2}^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}\,.$$

Тогда формула (3-23) превратится в матричное равенство $D_\nu = H_\nu \cdot M$, где

$$D_\nu = (x_j^{\nu_i}) = \begin{pmatrix} x_1^{\nu_1} & x_2^{\nu_1} & \cdots & x_n^{\nu_1} \\ x_1^{\nu_2} & x_2^{\nu_2} & \cdots & x_n^{\nu_2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\nu_n} & x_2^{\nu_n} & \cdots & x_n^{\nu_n} \end{pmatrix}\,.$$

[1] Как обычно, крышка над $x_p$ означает пропуск этой переменной.
[2] В которой мы для унификации записи полагаем $h_j = 0$ при $j < 0$.

Таким образом, для любой диаграммы Юнга $\nu$ со строго убывающими длинами строк

$$\Delta_\nu = \det D_\nu = \det H_\nu \cdot \det M\,.$$

Так как при $\nu = \delta$ матрица $H_\delta$ верхняя унитреугольная, $\det H_\delta = 1$ и $\Delta_\delta = \det M$. Мы получаем искомое выражение полиномов Шура через полные симметрические функции:

$$s_\lambda = \Delta_{\delta+\lambda}/\Delta_\delta = (\det H_{\delta+\lambda}\cdot \det M)/\det M = \det H_{\delta+\lambda} = \det\left(h_{\lambda_i+j-i}\right)\,. \tag{3-24}$$

Предложение 3.5 (формула Джамбелли)

$$s_\lambda = \det\begin{pmatrix} h_{\lambda_1} & h_{\lambda_1+1} & \cdots & h_{\lambda_1+n-1} \\ h_{\lambda_2-1} & h_{\lambda_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & h_{\lambda_{n-1}+1} \\ h_{\lambda_n-n+1} & \cdots & h_{\lambda_n-1} & h_{\lambda_n} \end{pmatrix} \tag{3-25}$$

где по главной диагонали стоят $h_{\lambda_1}, \dots , h_{\lambda_n}$, и в каждой строке индексы у $h$ увеличиваются слева направо на единицу от клетки к клетке. □

**3.5.1. Примеры.** При $n = 2$ в $\mathbb{Z}[x_1, x_2]$ получаем соотношение

$$s_{(2,1)} = \det\begin{pmatrix} h_2 & h_3 \\ 1 & h_1 \end{pmatrix} = h_1h_2 - h_3 = e_1e_2 - e_3\,.$$

При $n = 3$ в $\mathbb{Z}[x_1, x_2, x_3]$ получаем соотношение

$$s_{(2,1)} = s_{(2,1,0)} = \det\begin{pmatrix} h_2 & h_3 & h_4 \\ 1 & h_1 & h_2 \\ 0 & 0 & 1 \end{pmatrix} = \det\begin{pmatrix} h_2 & h_3 \\ 1 & h_1 \end{pmatrix}\,,$$

дающее то же самое выражение $s_{(2,1)}$ через $h_i$, что и при $n = 2$.

Упражнение 3.5. Убедитесь, что выражение $s_\lambda$ через $h_k$, полученное при числе переменных $n$, равном высоте диаграммы $\lambda$, сохраняется и при любом большем числе переменных.

Беря $\lambda = (k)$, т. е. одну строку длины $k$, получаем равенство $s_{(k)} = h_k$, очевидное при $n = 1$ и по упр. 3.5 справедливое для всех $n$. Отметим, что при непосредственном вычислении определителей $\Delta_{\delta+(k)}$ и $\Delta_\delta$ произвольного размера $n \times n$ равенство $\Delta_{\delta+(k)} = h_k \cdot \Delta_\delta$ не вполне очевидно.

**3.6. Формула Пьери** выражает произведение $s_\lambda \cdot h_k = s_\lambda \cdot s_{(k)}$ через многочлены $s_\mu$. Для её вывода нам придётся слегка обобщить сказанное в n° 3.1. Рассмотрим кольцо формальных степенных рядов $\mathbb{Z}[\![x_1, \dots , x_n]\!]$, а в нём — симметрические и кососимметрические ряды (первые образуют подкольцо, вторые — модуль над этим подкольцом). То же рассуждение, что и в n° 3.1.2 показывает, что всякий кососимметричный ряд $A$ однозначно записывается в виде бесконечной целочисленной линейной комбинации альтернированных $S_n$-орбит мономов:

$$A = \sum_{\nu_1>\nu_2>\cdots>\nu_n} c_\nu \cdot \Delta_\nu\,, \quad \text{где} \quad \Delta_\nu = \sum_{g\in S_n} \operatorname{sgn}(g)\, x_{g(1)}^{\nu_1} x_{g(2)}^{\nu_2} \cdots x_{g(n)}^{\nu_n}\,, \tag{3-26}$$

суммирование происходит по всем диаграммам Юнга $\nu = (\nu_1, \dots , \nu_n)$ из $n$ строк строго убывающей длины, и коэффициенты $c_\nu \in \mathbb{Z}$.

Лемма 3.1
Разложение (3-26) для произведения базисного кососимметрического многочлена $\Delta_\nu$ на симметрический ряд $H(x) = \prod_{i=1}^n (1-x_i)^{-1} = \prod_{i=1}^n (1 + x_i + x_i^2 + x_i^3 + \cdots) = \sum_{k\geqslant 0} h_k(x)$ имеет вид $\Delta_\nu \cdot H = \sum\limits_\eta \Delta_\eta$, где суммирование идёт по всем таким $\eta = (\eta_1, \dots, \eta_n)$, что

$$\eta_1 \geqslant \nu_1 > \eta_2 \geqslant \nu_2 > \cdots \eta_n \geqslant \nu_n .$$

Доказательство. Для любых $n$ рядов $f_1(t), \dots, f_n(t) \in \mathbb{Z}[\![t]\!]$ положим

$$f_1 \wedge \ldots \wedge f_n = \sum_{g\in S_n} \operatorname{sgn}(g) f_1(x_{g(1)}) \cdots f_n(x_{g(n)}) .$$

Ряд $f_1 \wedge \ldots \wedge f_n \in \mathbb{Z}[\![x_1, \dots, x_n]\!]$ кососимметричен и полилинейно и кососимметрично зависит от $f_1, \dots, f_n$. В частности, $f_1 \wedge \ldots \wedge f_n$ не изменяется при добавлении к любому из рядов любой линейной комбинации остальных.

Упражнение 3.6. Убедитесь, что $t^{\nu_1} \wedge \ldots \wedge t^{\nu_n} = \Delta_\nu$.

В этих обозначениях

$$\Delta_\nu \cdot H = \sum_{g\in S_n} \operatorname{sgn}(g) \prod_{i=1}^n x_{g(i)}^{\nu_i} \left(1 - x_{g(i)}\right)^{-1} = f_1 \wedge \ldots \wedge f_n$$

для $f_i(t) = t^{\nu_i} / (1-t) = t^{\nu_i} + t^{\nu_i+1} + t^{\nu_i+2} + \cdots$. Вычитая $f_1$ из всех остальных рядов, мы обрезаем их до многочленов степени $< \nu_1$. Вычитая второй из полученных многочленов из всех последующих, мы обрезаем последние до многочленов степени $< \nu_2$. Действуя в таком духе, приходим к равенству $f_1 \wedge \ldots \wedge f_n = \overline{f}_1 \wedge \ldots \wedge \overline{f}_n$, в котором $\overline{f}_1 = f_1 = \sum_{j\geqslant\nu_1} t^j$, а

$$\overline{f}_i = t^{\nu_i} + t^{\nu_i+1} + \cdots + t^{\nu_{i-1}-1} \text{ при } 2 \leqslant i \leqslant n .$$

В силу полилинейности $\overline{f}_1 \wedge \ldots \wedge \overline{f}_n = \sum_\eta t^{\eta_1} \wedge t^{\eta_2} \wedge \ldots \wedge t^{\eta_n} = \sum_\eta \Delta_\eta$, где суммирование идёт по всем $\eta_1 \geqslant \nu_1 > \eta_2 \geqslant \nu_2 > \eta_3 \geqslant \nu_3 > \cdots \eta_n \geqslant \nu_n$. □

Следствие 3.6 (формула Пьери)
$s_\lambda \cdot h_k = \sum_\mu s_\mu$, где суммирование происходит по всем диаграммам $\mu$ из $\leqslant n$ строк, которые можно получить, добавляя к диаграмме $\lambda$ ровно $k$ клеток так, чтобы никакие две из них не попали в один столбец.

Доказательство. По лем. 3.1 имеем равенство $\Delta_{\delta+\lambda} \sum_{k\geqslant 0} h_k = \sum_\tau \Delta_{\delta+\mu}$, где суммирование происходит по всем таким диаграммам $\mu$, что[1] $\mu_1 \geqslant \lambda_1 \geqslant \mu_2 \geqslant \lambda_2 \geqslant \ldots$. Деля обе части на $\Delta_\delta$ и беря в полученном равенстве однородную компоненту степени $|\lambda| + k$ по $x$, получаем требуемую формулу. □

Замечание 3.1. Если диаграмма $\lambda$ состоит из $k < n$ строк, т. е. $\lambda_i = 0$ при $i > k$, диаграммы $\mu$ в формуле Пьери могут содержать на одну ненулевую строку больше, чем $\lambda$. Например, при $n = 2$ получаем $s_{(2)} \cdot h_1 = s_{(2,1)} + s_{(3)}$, что вновь приводит к выражению $s_{(2,1)} = h_2 h_1 - h_3$ из n° 3.5.1 на стр. 44.

[1] Напомним (см. n° 3.1.2), что $\lambda_i = \nu_i - n + i$, $\mu_i = \eta_i - n + i$, поэтому неравенства $\eta_i \geqslant \nu_i > \eta_{i+1}$ равносильны неравенствам $\mu_i \geqslant \lambda_i \geqslant \mu_{i+1}$.

**3.7. Кольцо симметрических функций.** Удобно думать про симметрические многочлены не привязываясь к конкретному числу переменных, но считая, что их достаточно много для того, чтобы все нужные функции были определены. Формализуется это так. Условимся не различать между собою две диаграммы $\lambda'$, $\lambda''$, а также два набора показателей $m'$, $m''$, если они получаются друг из друга дописыванием справа любого числа нулей. Для каждого набора занумерованных натуральными числами $i \in \mathbb{N}$ букв $q_i$ положим

$$q_\lambda = q_{\lambda_1} q_{\lambda_2} q_{\lambda_3} \dots \quad \text{и} \quad q^m = q_1^{m_1} q_2^{m_2} q_3^{m_3} \dots \,.$$

Мы пишем $\lambda = (\lambda_1, \lambda_2, \lambda_3, \dots) = (1^{m_1}, 2^{m_2}, 3^{m_3}, \dots)$ если диаграмма Юнга $\lambda$ содержит $m_i$ строк длины $i$ при каждом $i \in \mathbb{N}$, что равносильно равенству $q_\lambda = q^m$. Для симметрических многочленов $m_\lambda$ и $s_\lambda$ мы полагаем $m_\lambda = s_\lambda = 0$ всякий раз, когда число переменных меньше количества строк в диаграмме $\lambda$, а для элементарных симметрических многочленов $e_\lambda$ мы полагаем $e_\lambda = 0$, когда число переменных меньше количества столбцов в диаграмме $\lambda$. При таких соглашениях каждый из симметрических многочленов $m_\lambda(x)$, $s_\lambda(x)$, $e_\lambda(x)$, $h_\lambda(x)$ и $p_\lambda(x)$ становится определён для переменной $x = (x_1, \dots, x_r)$ любой размерности $r$, причём при $r > s$ подстановка

$$x_{s+1} = x_{s+2} = \dots = x_r = 0 \tag{3-27}$$

превращает каждый из этих многочленов в одноимённый многочлен от меньшего набора переменных $x = (x_1, \dots, x_s)$. Подстановка (3-27) задаёт сюрьективный гомоморфизм колец

$$\zeta_{sr} : \mathbb{Z}[x_1, \dots, x_r] \twoheadrightarrow \mathbb{Z}[x_1, \dots, x_s]\,. \tag{3-28}$$

Будем называть последовательность симметрических многочленов $f^{(n)} \in \mathbb{Z}[x_1, \dots, x_n]$ *симметрической функцией степени* $d$, если выполняются следующие два условия:

$$\text{1) } \forall\, n \text{ многочлен } f^{(n)} \text{ однороден степени } d \qquad \text{2) } \zeta_{rs}\left(f^{(r)}\right) = f^{(s)} \text{ при } r > s.$$

Поскольку в выражении $f^{(n)}(x_1, \dots, x_n)$ верхний индекс у $f$ равен числу подставляемых переменных, писать его не имеет смысла, и мы всегда будем сокращать предыдущую запись до

$$f(x_1, \dots, x_n) \stackrel{\text{def}}{=} f^{(n)}(x_1, \dots, x_n)\,.$$

Так, для фиксированной диаграммы $\lambda$ веса $|\lambda| = d$ последовательность мономиальных многочленов $m_\lambda(x_1, \dots, x_n)$ образует симметрическую функцию степени $d$, которая обозначается $m_\lambda$. Например, кубическая симметрическая функция $m_{(2,1)}$ на наборах из одной, двух и трёх переменных имеет вид

$$\begin{aligned} m_{(2,1)}(x_1) &= 0 \\ m_{(2,1)}(x_1, x_2) &= x_1^2 x_2 + x_1 x_2^2 \\ m_{(2,1)}(x_1, x_2, x_3) &= x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2\,. \end{aligned}$$

Аналогичным образом определяются и симметрические функции $s_\lambda$, $e_\lambda$, $h_\lambda$ и $p_\lambda$ степени $|\lambda|$.

Симметрические функции степени $d$ образуют $\mathbb{Z}$-модуль. Его принято обозначать $\Lambda_d$. Из сказанного в предыдущих разделах вытекает, что симметрические функции $m_\lambda$, $s_\lambda$, $e_\lambda$ и $h_\lambda$, занумерованные всевозможными диаграммами Юнга веса $|\lambda| = d$, являются базисами в $\Lambda_d$, а симметрические функции $p_\lambda$ составляют базис векторного пространства $\mathbb{Q} \otimes \Lambda_d$ симметрических функций с рациональными коэффициентами. Таким образом, $\Lambda_d$ является свободным модулем *конечного* ранга, равного количеству диаграмм Юнга веса $d$. Это количество принято обозначать $p(d)$ и называть *числом разбиений* натурального числа $d$. Произведение симметрических функций степеней $d_1$ и $d_2$ является симметрической функцией степени $d_1 d_2$, так что прямая сумма $\Lambda = \bigoplus_{d \geqslant 0} \Lambda_d$ является градуированным кольцом. Оно называется *кольцом симметрических функций*. Все доказанные выше соотношения между функциями $m_\lambda$, $s_\lambda$, $e_\lambda$, $h_\lambda$ и рекурсивные выражения $p_i$ через $e_j$ и $h_j$ являются тождествами в кольце $\Lambda$, а выражения $h_i$ и $e_i$ через $p_\lambda$ — тождествами в кольце $\mathbb{Q} \otimes \Lambda$ симметрических функций с рациональными коэффициентами.

## §4. Исчисление массивов, таблиц и диаграмм

**4.1. Массивы и элементарные операции над ними.** Зафиксируем два конечных упорядоченных множества $I = \{1, \dots, n\}$ и $J = \{1, \dots, m\}$ из $n$ и $m$ элементов и будем рассматривать прямоугольные таблицы из $n$ столбцов и $m$ строк, занумерованных элементами $I$ и $J$ соответственно. Такую таблицу $a$ мы будем называть *массивом* и размещать в *первом* квадранте декартовой системы координат так, чтобы элементы из $I$ росли слева направо по горизонтальной оси, а элементы из $J$ росли снизу вверх по вертикальной оси. Содержимое $a(i,j)$ клетки с координатами $(i,j)$ у нас всегда будет целым неотрицательным числом, которое стоит воспринимать как «количество» или «массу». Весь массив удобно представлять себе как набор шариков одинаковой массы, наделённых двумя группами признаков и в соответствии с этим разложенных по ячейкам массива. Мы никогда не будем проделывать с величинами $a(i,j)$ вычисления, но будем перекладывать шарики из ячейки в ячейку, меняя тем самым их принадлежность к тому или иному признаку каждой из двух групп и соответственно меняя значения $a(i,j)$.

С массивом $a$ связан *столбцовый вес* (или *$I$-вес*)

$$w^I = \Big( \sum_j a(1,j)\,,\ \sum_j a(2,j)\,,\ \dots\,,\ \sum_j a(n,j) \Big) \in \mathbb{Z}^n_{\geqslant 0}\,. \tag{4-1}$$

Это $n$-мерный целочисленный вектор, $i$-тая координата которого равна общему количеству шариков в $i$-том столбце. Аналогично определяется *строчный вес* (или *$J$-вес*)

$$w^J = \Big( \sum_i a(i,1)\,,\ \sum_i a(i,2)\,,\ \dots\,,\ \sum_i a(i,m) \Big) \in \mathbb{Z}^m_{\geqslant 0}\,. \tag{4-2}$$

Массивы можно транспонировать относительно диагонали $i = j$:

$$a \mapsto a^t \ :\ a^t(i,j) = a(j,i)\,. \tag{4-3}$$

На множестве $\mathcal{M}$ всех массивов действуют четыре набора *уплотняющих операций*

$$D_j\,,\quad U_j\,,\quad L_i\,,\quad R_i\,,\quad \text{где } 1 \leqslant i \leqslant n-1,\ 1 \leqslant j \leqslant m-1.$$

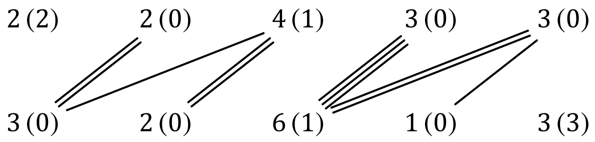
При применении любой из этих операций к данному массиву $a \in \mathcal{M}$ массив $a$ либо никак не меняется, либо ровно один его шарик перемещается ровно на одну клетку вниз (Down), вверх (Up), влево (Left) или вправо (Right) в соответствии с обозначением для операции.

**4.1.1. Вертикальные операции $\boldsymbol{D_j}$ и $\boldsymbol{U_j}$** перемещают один шар по вертикали в пределах соседних $j$-й и $(j+1)$-й строк или ничего не делают. Чтобы узнать, какой именно шар следует передвинуть или убедиться в том, что такого шара нет, следует вначале установить между этими строками *устойчивое паросочетание*[1]. Делается это следующим образом.

Будем последовательно перебирать шары в $(j+1)$-й строке двигаясь слева направо и либо назначать им партнёров в $j$-й строке, либо объявлять *свободными*. Пусть очередной шар $\boldsymbol{ш}$ лежит в клетке $(i, j+1)$. Его партнёром называем *самый правый* шар из тех, что лежат в $j$-й строке *строго левее* $i$-го столбца и ещё не назначены никому партнёрами. Если таких шаров нет, шар $\boldsymbol{ш}$ объявляется свободным. После того, как все шары $(j+1)$-й строки будут разделены на свободные

[1] По-английски: *stable matching*.

и имеющие партнёров, все шары $j$-й строки, не являющиеся ничьими партнёрами, также объявляются свободными. Вот пример такого паросочетания (в скобках указано число свободных шаров):




(4-4)

Операция $D_j$ опускает на одну клетку вниз самый правый свободный шар $(j+1)$-й строки или ничего не делает, если свободных шаров в $(j+1)$-й строчке нет. Операция $U_j$ поднимает на одну клетку вверх самый левый свободный шар $j$-й строки или ничего не делает, если в $j$-й строке нет свободных шаров. Так, в примере (4-4) операция $D_j$ (соотв. $U_j$) опускает вниз (соотв. поднимает вверх) верхний (соотв. нижний) свободный шар в третьей колонке.

Если операция изменяет массив, мы будем говорить, что она действует на этот массив *эффективно*. Из конструкции устойчивого паросочетания видно, что все свободные шары $j$-й строки лежат нестрого правее свободных шаров $(j+1)$-й строки, и когда операция $D_j$ действует на массив $a$ эффективно, опущенный ею шар становится самым левым свободным шаром $j$-й строки в устойчивом паросочетании между преобразованными строками. Поэтому операция $U_j$, применённая к массиву $D_j a$ поднимет этот опущенный шар назад, т. е. $U_j D_j a = a$ всякий раз, когда $D_j$ действует на $a$ эффективно. Аналогично, если $U_j$ действует эффективно, то $D_j U_j a = a$. Говоря неформально, набор вертикальных операций $D$, $U$ образует структуру, близкую к групповой — исходный массив $a$ однозначно восстанавливается из результата применения к нему слова $D = D_{j_1} \cdots D_{j_k}$ по формуле $a = U_{j_k} \cdots U_{j_1} D_{j_1} \cdots D_{j_k} a$ при условии, что каждая буква $D_j$ действует эффективно. Мы будем называть такие $D$-слова *$a$-эффективными* или просто *эффективными*, если понятно, о каком $a$ идёт речь.

**4.1.2. Горизонтальные операции $L_i$ и $R_i$** определяются симметричным образом: они действуют в $i$-м и $(i+1)$-м столбцах и превращаются в операции $D$ и $U$ при транспонировании массива, т. е. $L_i(a) = \left(D_i(a^t)\right)^t$ и $R_i(a) = \left(U_i(a^t)\right)^t$.

Упражнение 4.1. Проговорите это определение явно: объясните, как установить устойчивое паросочетание между $i$-м и $(i+1)$-м столбцом, и укажите какой именно шар перемещают горизонтальные операции $R_i$ и $L_i$.

Отметим, что операции $D$, $L$ сохраняют столбцовый вес, а операции $R$, $L$ — строчный.

Лемма 4.1 (лемма о коммутировании)
Каждая из горизонтальных операций $L_i$, $R_i$ перестановочна с каждой из вертикальных операций $D_j$, $U_j$.

Доказательство. Мы покажем, что $D_j$ и $U_j$ перестановочны с $L_i$ — остальные случаи разбираются аналогично. Пусть действие операции $L_i$ заключается в перемещении шара $\boldsymbol{ш}$ на одну клетку влево. Достаточно убедиться, что устойчивое паросочетание между $(j+1)$-й и $j$-й строками можно организовать так, что после перемещения шара $\boldsymbol{ш}$ связанными в пары будут ровно те же самые шары, что и до его перемещения. Это очевидно, когда $\boldsymbol{ш}$ лежит вне $(j+1)$-й и $j$-й строк. Рассмотрим оставшиеся два случая.

Пусть $\boldsymbol{ш}$ лежит в $(j+1)$-й строчке, т. е. в клетке $(i+1, j+1)$, как на левом из рис. 4◇1. Тогда все шары из клетки $(i, j)$ имеют партнёров в клетке $(i+1, j+1)$, иначе шар $\boldsymbol{ш}$ получил бы себе партнёра в клетке $(i, j)$ в паросочетании между $i$-м и $(i+1)$-м столбцом. Поэтому, если в строчном паросочетании у шара ***ш*** был партнёр, то он был строго левее клетки $(i, j)$, а значит, останется партнёром после перемещения ***ш*** на клетку влево. А если партнёра у ***ш*** не было, то он и не появится. Таким образом, при перемещении ***ш*** строчное паросочетание не изменяется.

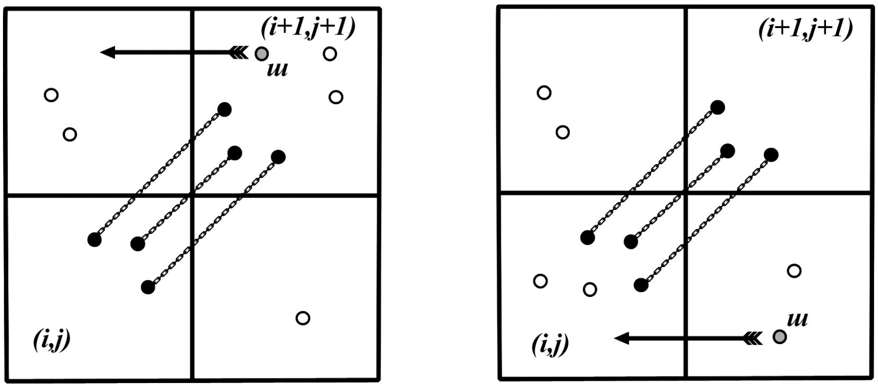



**Рис. 4⋄1.** Действие $L_i$ не меняет устойчивого вертикального паросочетания.

Пусть теперь ***ш*** лежит в $j$-й строчке, как на правом из рис. 4⋄1. Поскольку он является самым верхним свободным шаром в столбцовом паросочетании, все шары из клетки $(i+1, j+1)$ имеют партнёров в клетке $(i, j)$. Но тогда и в строчном паросочетании все шары из $(i+1, j+1)$-й клетки имеют партнёров в клетке $(i, j)$. Поэтому если после перемещения на клетку влево у шара ***ш*** имеется партнёр в строчном паросочетании, то он находится строго правее клетки $(i+1, j+1)$, а значит, является партнёром шара ***ш*** и до его перемещения. А если у перемещённого шара ***ш*** нет партнёра в строчном паросочетании, то его не было и до перемещения. □

Следствие 4.1
Слово $H$, составленное из горизонтальных операций, тогда и только тогда эффективно действует на массив $a$, когда оно эффективно действует на любой массив, получающийся из $a$ вертикальными операциями. Симметричным образом, слово $V$, составленное из вертикальных операций, эффективно действует на $a$ если и только если оно эффективно действует на любой массив, получающийся из $a$ горизонтальными операциями.

Доказательство. Мы докажем первое утверждение, второе получается из него транспонированием. Достаточно проверить, что для любых $i$, $j$ операция $L_i$ эффективно действует на $a$ тогда и только тогда, когда она эффективно действует на $D_j a$, и только тогда, когда она эффективно действует на $U_j a$. Если $L_i a = a$, то $L_i D_j a = D_j L_i a = D_j a$, и $L_i U_j a = U_j L_i a = U_j a$. Наоборот, если $L_i a \neq a$, то $i$-тая компонента столбцового веса $w^I(L_i a)$ будет строго больше $i$-й компоненты $w^I(a)$, а так как $D_j$ и $U_j$ не меняют столбцовый вес, то $L_i D_j a = D_j L_i a \neq D_j a$, и $L_i U_j a = U_j L_i a \neq U_j a$. □

**4.2. Уплотнение массивов.** Будем называть массив D-, L-, R- или U-*плотным* (т. е. плотным вниз, влево, вправо или вверх), если все элементарные операции соответствующего типа действуют на него тождественно. Применение к произвольному массиву достаточно большого числа операций одного из типов приводит к плотному в соответствующую сторону массиву. Такое уплотнение, как правило, можно производить многими разными способами. На рис. 4⋄2 на стр. 51 показаны два пути уплотнения достаточно произвольного массива $3 \times 2$. Обратите внимание, что результат уплотнения оказался не зависящим от способа уплотнения. Мы докажем это фундаментальное свойство уплотнений в предл. 4.1, но прежде сделаем одно важное замечание о связи массивов с диаграммами Юнга.

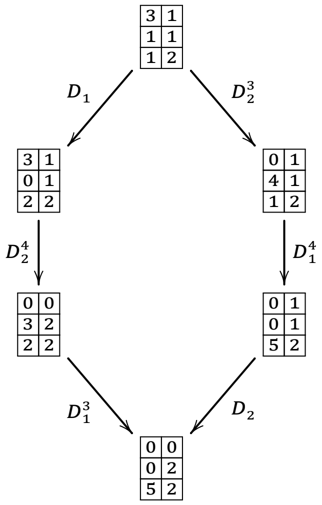



**Рис. 4◇2.** Два пути уплотнения вниз.

**4.2.1. Биплотные массивы и диаграммы Юнга.** Из сл. 4.1 вытекает, что при действии вертикальных операций на плотный влево или вправо массив этот массив будет оставаться плотным в ту же сторону. То же самое справедливо для действия горизонтальных операций на массив, который плотен вниз или вверх. Поэтому любой массив можно сделать плотным одновременно в каком-нибудь вертикальном и в каком-нибудь горизонтальном направлении. Мы будем называть такие массивы DL-плотными, DR-плотными, и т. п. Поскольку далее мы будем заниматься в основном DL-уплотнениями, условимся называть просто *биплотными* массивы, плотные одновременно *вниз* и *влево*. Все шары в биплотном массиве лежат лишь в клетках главной диагонали $i = j$, причём их количества нестрого убывают с ростом $i$. Поэтому столбцовый вес биплотного массива равен строчному и представляет собой диаграмму Юнга $\lambda = w^I(b) = w^J(b)$, т. е. биплотные массивы $b$ взаимно однозначно соответствуют диаграммам Юнга[1]. Диаграмма Юнга, отвечающая биплотному массиву, который получается DU-уплотнением данного массива $a$, называется *формой* массива $a$ и обозначается $\Phi(a)$. Докажем теперь, что это понятие корректно.

Предложение 4.1

Результат D- , L- , R- или U- уплотнения не зависит от выбора последовательности уплотняющих операций.

Доказательство. Мы рассмотрим только случай D-уплотнения. Если массив $a$ плотен влево, то результат его D-уплотнения — это биплотный массив, отвечающий диаграмме Юнга $w^I(a)$. Поскольку $w^I(a)$ не меняется при вертикальных уплотняющих операциях, результат D-уплотнения

[1] Здесь и далее в этом параграфе мы отождествляем между собою две конечных последовательности неотрицательных целых чисел, получающиеся одна из другой приписыванием справа любого числа нулей. Например, мы считаем равными диаграммы $(2, 1, 1)$ и $(2, 1, 1, 0, 0, 0)$.

L-плотного массива не зависит от способа уплотнения. Пусть теперь $a$ произволен. Зафиксируем какое-нибудь слово $L = L_{i_k} \dots L_{i_1}$, эффективно уплотняющее $a$ влево до L-плотного массива $a' = La$. Тогда для любого такого слова $D = D_{j_m} \dots D_{j_1}$, что $Da$ плотен вниз, действие $L$ на $Da$ тоже будет эффективным, а массив $LDa = DLa$ будет биплотен[1]. Таким образом, мы можем записать $Da$ как $L^{-1}DLa$. Поскольку массив $DLa$ является D-уплотнением L-плотного массива $La$, он по уже доказанному не зависит от выбора уплотняющего слова $D$, а значит и массив $Da = L^{-1}DLa$ тоже не зависит от выбора $D$. $\square$

**4.2.2. Плотные массивы и таблицы Юнга.** Из любого массива высоты $m$ и ширины $n$ можно изготовить $m$ слов (по одному слову из каждой строки массива), записанных алфавитом $\{1, \dots, n\}$. Делается это при помощи процедуры, которая называется *строчной развёрткой* массива и состоит в следующем. Интерпретируем все шарики массива как буквы, равные номеру того столбца, где стоит шарик. После этого пройдём по каждой строке слева направо, выписывая подряд все встречающиеся буквы. В результате $j$-тая строка массива развернётся в слово

$$\underbrace{1 \dots 1}_{a(1,j)} \underbrace{2 \dots 2}_{a(2,j)} \dots \dots \dots \underbrace{n \dots n}_{a(n,j)} .$$

Получающиеся $m$ слов запишем друг под другом в столбик, *сверху вниз*[2], выровняв их по левому краю. Например:

$$\begin{array}{|c|c|c|c|c|}\hline 0&0&0&0&1\\\hline 0&0&1&1&0\\\hline 0&4&0&0&0\\\hline 3&1&0&0&1\\\hline\end{array} \;\rightsquigarrow\; \begin{array}{lllll} 1&1&1&2&5\\ 2&2&2&2&\\ 3&4&&&\\ 5&&&& \end{array}, \qquad \begin{array}{|c|c|c|c|c|}\hline 2&0&3&0&1\\\hline 0&2&1&1&0\\\hline 0&1&0&2&3\\\hline 1&1&2&0&1\\\hline\end{array} \;\rightsquigarrow\; \begin{array}{llllll} 1&1&3&3&3&5\\ 2&2&3&4&&\\ 2&4&4&5&5&5\\ 1&2&3&3&5& \end{array}.$$

Очевидно, что буквы в каждом слове строчной развёртки нестрого возрастают. Условие плотности массива вниз (как в левом примере выше) означает, что под каждой буквой «$i$» в $j$-том слове, т. е. под шариком, пришедшим из клетки $a(i, j)$, стоит строго большая, чем «$i$», буква из $(j+1)$-го слова — партнёр этого шарика при устойчивом паросочетании между $j$-й и $(j + 1)$-й строками. Следовательно, длины слов строчной развёртки плотного вниз массива нестрого убывают сверху вниз, т. е. образуют диаграмму Юнга, а буквы $\{1, \dots, n\}$ заполняют эту диаграмму нестрого возрастая по строкам и *строго* возрастая по столбцам. Такие заполнения данной диаграммы $\lambda$ называются *таблицами Юнга* формы $\lambda$ на алфавите $I = \{1, \dots, n\}$. Мы доказали следующий комбинаторный факт:

Лемма 4.2

Строчная развёртка задаёт биекцию между плотными вниз массивами размера $m \times n$ и таблицами Юнга из не более $m$ строк на алфавите $\{1, \dots, n\}$. $\square$

**4.2.3. Плотные массивы и тексты Яманучи.** L-плотность массива $a$ можно воспринимать как D-плотность транспонированного массива $a^t$ и формулировать в терминах столбцовой развёртки: плотные влево массивы размера $m \times n$ биективно соответствуют таблицам Юнга из не более $n$ строк в алфавите $J$. Полезно, однако, охарактеризовать L-плотность в терминах *строчной* развёртки. Для этого будем читать слова строчной развёртки L-плотного массива $a$ *справа налево* одно за другим, сверху вниз. Условие плотности влево означает тогда, что в любом начальном куске получающейся последовательности букв единиц будет не меньше, чем двоек,

[1]Ибо применение $L$ сохраняет свойство массива $Da$ быть плотным вниз, а применение $D$ сохраняет свойство массива $La$ быть плотным влево.

[2]Таким образом, из нижней строки массива получается верхнее слово и т. д.

двоек — не меньше, чем троек, и т. д. для всех пар последовательных букв «$i$» и «$(i+1)$» из $I$. В комбинаторике такой текст называют *текстом Яманучи*. Например, левая из двух строчных развёрток

$$\begin{array}{lll} 1 & & \\ 1 & 2 & \\ 1 & 1 & 2 \\ 3 & 3 & \end{array} \quad , \quad \begin{array}{llll} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & \\ 2 & 3 & 3 & \\ 1 & 2 & & \end{array}$$

является текстом Яманучи, а правая — нет. Итак, нами установлена

Лемма 4.3
Строчная развёртка задаёт биекцию между плотными влево массивами размера $m \times n$ и текстами Яманучи из не более $m$ слов в алфавите $\{1, \dots, n\}$. □

**4.2.4. Послойное произведение.** Если заданы два отображения множеств $\varphi : X \to Z$ и $\psi : Y \to Z$, то дизъюнктное объединение прямых произведений их слоёв над всеми точками $z \in Z$ обозначается

$$X \underset{Z}{\times} Y \overset{\text{def}}{=} \bigsqcup_{z \in Z} \varphi^{-1}(z) \times \psi^{-1}(z)$$

и называется *послойным* (или *расслоенным*) произведением множеств $X$ и $Y$ над $Z$ по отображениям $\varphi$ и $\psi$. Послойные проекции $\pi_X : (x, y) \mapsto x$ и $\pi_Y : (x, y) \mapsto y$ включаются в коммутативную диаграмму

$$\begin{tikzcd} & X \underset{Z}{\times} Y \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] & \\ X \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\ & Z & \end{tikzcd} \tag{4-5}$$

которая называется *декартовым квадратом*. Она универсальна в том смысле, что для любого другого коммутативного квадрата

$$\begin{tikzcd} & M \arrow[dl, "\xi"'] \arrow[dr, "\eta"] & \\ X \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\ & Z & \end{tikzcd}$$

имеется единственное такое отображение $\alpha : M \to X \underset{Z}{\times} Y$, что $\xi = \pi_X \circ \alpha$ и $\eta = \pi_Y \circ \alpha$.

Упражнение 4.2. Убедитесь в этом и покажите, что универсальное свойство определяет верхний угол квадрата (4-5) однозначно с точностью до единственного изоморфизма, перестановочного со всеми стрелками квадрата.

Теорема 4.1
Множество всех массивов $\mathcal{M}$ является послойным произведением множеств плотных влево массивов $\mathcal{L}$ и плотных вниз массивов $\mathcal{D}$ над множеством биплотных массивов $\mathcal{B}$ по отображениям

уплотнения влево и уплотнения вниз, т. е. коммутативный квадрат

$$\begin{tikzcd} & \mathcal{M} \arrow[dl, "L"'] \arrow[dr, "D"] & \\ \mathcal{L} \arrow[dr, "D"'] & & \mathcal{D} \arrow[dl, "L"] \\ & \mathcal{B} & \end{tikzcd}$$

в котором стрелки $L$ и $D$ переводят массив в его уплотнения влево и вниз, является декартовым.

Доказательство. По предл. 4.1 стрелки $L$ и $D$ корректно определены и перестановочны друг с другом. Надо показать, что отображение $\mathcal{M} \to \mathcal{L} \times_{\mathcal{B}} \mathcal{D}$, сопоставляющее массиву $a$ пару $(La, Da)$ со свойством $DLa = LDa \in \mathcal{B}$, взаимно однозначно. Докажем его инъективность. Пусть массивы $a$ и $a'$ таковы, что $La = La'$ и $Da = Da'$, а слово $\Lambda$ эффективно уплотняет массив $Da = Da'$ влево. Тогда $\Lambda$ эффективно действует на $a$ и $a'$ так, что $\Lambda a = La = La' = \Lambda a'$, откуда $a = \Lambda^{-1}La = \Lambda^{-1}La' = a'$. Теперь докажем сюрьективность. Для любой пары массивов $(a_\ell, a_d)$, в которой $a_\ell$ плотен влево, $a_d$ плотен вниз, и $Da_\ell = La_d$, рассмотрим слово $\Lambda$, эффективно уплотняющее $a_d$ влево до $La_d$. Обратное слово $\Lambda^{-1}$ эффективно действует на $La_d = Da_\ell$, а значит, и на $a_\ell$. Массив $a = \Lambda^{-1}a_\ell$ таков, что $La = a_\ell$ и $Da = D\Lambda^{-1}a_\ell = \Lambda^{-1}Da_\ell = \Lambda^{-1}La_d = a_d$. □

Пример 4.1 (графики отображений и стандартные таблицы)
График отображения множеств $a : I \to J$ — это массив, в каждом столбце которого имеется ровно один шарик. По теор. 4.1 такие массивы взаимно однозначно параметризуются парами $(a_\ell, a_d)$ в которой $a_\ell$ плотен влево, $a_d$ плотен вниз, причём оба этих массива имеют одинаковую форму $Da_\ell = La_d$, и $w^I(a_d) = (1, \dots, 1)$. Согласно n° 4.2.2, каждая такая пара однозначно описывается следующим набором данных:

- форма $\Phi(a)$ массива $a$, т. е. диаграмма Юнга $\lambda = DLa$ веса $|\lambda| = n$
- строчная развёртка D-уплотнения $a_d$ массива $a$, т. е. таблица Юнга формы $\lambda$ на алфавите $I$, в которой каждая буква встречается ровно один раз
- столбцовая развёртка L-уплотнения[1] $a_\ell$ массива $a$, т. е. таблица Юнга формы $\lambda$ на алфавите $J$.

Число всех таблиц Юнга формы $\lambda$ на $m$-буквенном алфавите принято обозначать через $d_\lambda(m)$. Таблицы формы $\lambda$ заполненные без повторений числами от 1 до $|\lambda|$ называются *стандартными таблицами* формы $\lambda$, и их число обозначается просто через $d_\lambda$. Так как всего имеется $m^n$ отображений $I \to J$, мы получаем соотношение

$$\sum_\lambda d_\lambda \cdot d_\lambda(m) = m^n\,, \tag{4-6}$$

где суммирование идёт по всем $n$-клеточным диаграммам Юнга и числа $d_\lambda(m)$ отличны от нуля только для диаграмм из $\leqslant m$ строк. В ситуации, когда $\#J = \#I = n$ и рассматриваются только взаимно однозначные отображения $I \xrightarrow{\sim} J$, предыдущая конструкция устанавливает биекцию

[1] Т. е. строчная развёртка транспонированного массива $a_\ell^t$.

между $n!$ элементами симметрической группы $S_n$ и парами стандартных таблиц одинаковой формы веса $n$, откуда

$$\sum_\lambda d_\lambda^2 = n!\,, \tag{4-7}$$

где сумма идёт о всем $n$-клеточным диаграммам. Эта биекция индуцирует взаимно однозначное соответствие между инволютивными перестановки[1] $\sigma \in S_n$ и самосопряжёнными массивами $a = a^t$, которым в по теор. 4.1 отвечают пары одинаковых стандартных таблиц. Поэтому

$$\sum_\lambda d_\lambda = \#\{\sigma \in S_n \mid \sigma^2 = 1\}\,. \tag{4-8}$$

**4.3. Действие симметрической группы на DU-множествах.** Всякое множество массивов, которое переводится в себя вертикальными операциями $D$ и $U$, называется *DU-множеством*. Гомоморфизмы DU-множеств — это отображения, перестановочные с действием операций $D$ и $U$ на этих множествах. DU-множество, на котором операции $D$ и $U$ действуют транзитивно, называется *DU-орбитой*. DU-орбиты взаимно однозначно соответствуют плотным вниз массивам. Орбита $O$ такого массива $a_d$ состоит из всевозможных массивов, которые можно получить из $a_d$ эффективными $U$-словами. Мы будем называть $a_d$ *нижним концом* орбиты $O$.

Лемма 4.4
Объединения, пересечения и разности DU-множеств также являются DU-множествами. Всякое DU-множество является дизъюнктным объединением DU-орбит.

Доказательство. Не вполне очевидно, разве что, утверждение про разности. Пусть $A'$ и $A''$ DU-инвариантны и $a' \in A' \smallsetminus A''$. Если $D_j a' \in A''$, то $D_j$ действует эффективно, и тогда $a' = U_j D_j a'$ тоже лежит в $A''$. □

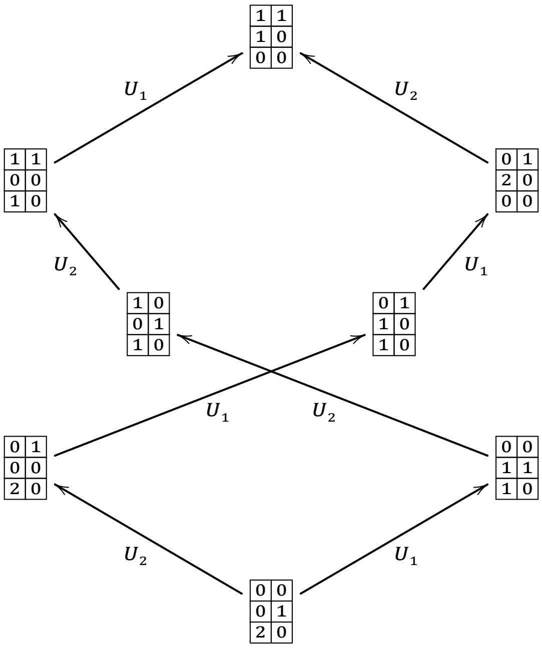



**Рис. 4◇3.** Стандартная DU-орбита $O_{(2,1)}$.

[1] Т. е. такие, что $\sigma^2 = 1$.

**4.3.1. Стандартные орбиты.** DU-орбиты $O_\lambda$ биплотных массивов $\lambda$ называются *стандартными*. Например, при $m = 3$ стандартная орбита $O_{(2,1)}$, отвечающая диаграмме – таблице – массиву

$$\begin{array}{|c|c|}\hline \phantom{0} & \phantom{0} \\ \hline \phantom{0} & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad - \quad \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 & \multicolumn{1}{c}{} \\ \cline{1-1} \end{array} \quad - \quad \begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & 1 \\ \hline 2 & 0 \\ \hline \end{array}$$

состоит из восьми массивов, представленных на рис. 4◇3.

Из теоремы о биекции вытекает, что уплотнение влево задаёт изоморфизм любой DU-орбиты $O$ со стандартной орбитой $O_\lambda$, нижний конец которой является биуплотнением нижнего конца орбиты $O$. Мы будем называть диаграмму $\lambda$ *типом* орбиты $O$. Количество орбит типа $\lambda$ в данном DU-множестве $M$ равно количеству плотных вниз массивов строчного веса $\lambda$, имеющихся в $M$.

**4.3.2. Действие симметрической группы $\boldsymbol{S_m = \mathrm{Aut}(J)}$.** На каждом DU-множестве массивов $M$ имеется действие элементарных транспозиций $\sigma_j = (j, j+1)$, порождающих симметрическую группу $S_m$ перестановок вертикального множества индексов $J$. Оно определяется следующим образом. Пусть после установления устойчивого паросочетания между $j$-й и $(j+1)$-й строками в них оказалось $s_j$ и $s_{j+1}$ свободных шаров соответственно. Положим

$$\sigma_j = D_j^{s_{j+1}-s_j} = U_j^{s_j-s_{j+1}}\,. \tag{4-9}$$

Подробнее эту процедуру можно описать так. Свернём массив в вертикальный цилиндр, приклеив правую границу $n$-го столбца к левой границе первого, и продолжим устойчивое паросочетание по кругу, т. е. назначим в пару самому правому нижнему свободному шару самый левый свободный верхний и т. д. В результате останется ровно $|s_{j+1} - s_j|$ свободных шаров и все они будут располагаться или только в верхней или только в нижней строке — там где их вначале было больше. Операция $\sigma_j$ просто передвигает их по вертикали в другую строку или ничего не делает, если $s_j = s_{j+1}$. В частности, действие $\sigma_j$ на строчный вес $w^J$ состоит в перестановке $j$-й и $(j+1)$-й координаты.

Из предыдущего описания видно, что $\sigma_j^2 = \mathrm{Id}$, а также, что $\sigma_j$ *коммутирует с циклическими перестановками столбцов*. Очевидно также, что $\sigma_j$ перестановочна с горизонтальными операциями $R$, $L$ и со всеми $\sigma_k$ с $|k-j| \geqslant 2$. Чтобы действие $\sigma_j$ непротиворечиво продолжалось на всю симметрическую группу $S_m$ достаточно проверить *соотношения треугольника* $\sigma_j\sigma_{j+1}\sigma_j = \sigma_{j+1}\sigma_j\sigma_{j+1}$. При этом можно считать массив трёхстрочным. Левое уплотнение $L$ и циклическая перестановка столбцов $C$ превращает любой трёхстрочный массив в одностолбцовый:

$$\begin{array}{|c|c|c|c|c|c|}\hline * & * & * & * & * & * \\ \hline * & * & * & * & * & * \\ \hline * & * & * & * & * & * \\ \hline \end{array} \xrightarrow{L} \begin{array}{|c|c|c|}\hline * & * & * \\ \hline * & * & 0 \\ \hline * & 0 & 0 \\ \hline \end{array} \xrightarrow{C} \begin{array}{|c|c|c|}\hline * & * & * \\ \hline * & 0 & * \\ \hline 0 & 0 & * \\ \hline \end{array} \xrightarrow{L} \begin{array}{|c|c|c|}\hline * & * & 0 \\ \hline * & 0 & 0 \\ \hline * & 0 & 0 \\ \hline \end{array} \xrightarrow{C} \begin{array}{|c|c|}\hline * & * \\ \hline 0 & * \\ \hline 0 & * \\ \hline \end{array} \xrightarrow{L} \begin{array}{|c|c|}\hline * & 0 \\ \hline * & 0 \\ \hline * & 0 \\ \hline \end{array}$$

на который $\sigma_j$ и $\sigma_{j+1}$ действуют перестановками строк, и соотношение треугольника, таким образом, выполняется.

**4.4. Полиномы Шура.** Интерпретируем все шары в $j$-й строке как переменные $x_j$ и сопоставим каждому массиву $a$ моном $x^a \stackrel{\text{def}}{=} x_1^{w_1^J(a)} x_2^{w_2^J(a)} \cdots x_m^{w_m^J(a)}$, равный произведению всех его шаров. Сумма этих мономов по всем массивам данного DU-множества $M$ обозначается

$$s_M(x) \stackrel{\text{def}}{=} \sum_{a \in M} x^a \in \Bbbk[x_1, \dots, x_m]$$

и называется (*комбинаторным*) *многочленом Шура* DU-множества $M$. Симметрическая группа $S_m$ переставляет координаты весового вектора и действует на мономы $x^a$ перестановками переменных. Таким образом, все многочлены Шура являются симметрическими.

Поскольку каждое DU-множество $M$ является объединением непересекающихся орбит, а всякая орбита изоморфна стандартной орбите $O_\lambda$, произвольный полином Шура является линейной комбинацией с неотрицательными целыми коэффициентами *стандартных* многочленов Шура $s_\lambda(x)$, отвечающих биплотным массивам (диаграммам Юнга) $\lambda$:

$$s_M(x) = \sum_{\lambda \in \Phi(M)} c_M^\lambda \cdot s_\lambda(x)\,, \tag{4-10}$$

где суммирование происходит по всем формам $\lambda$ массивов из $M$, и коэффициент $c_M^\lambda$ равен числу DU-орбит, изоморфных $O_\lambda$, т. е. количеству всех плотных вниз массивов $J$-веса $\lambda$ в $M$. Согласно n° 4.2.2, элементы стандартной орбиты $O_\lambda$ суть всевозможные L-плотные массивы формы $\lambda$, и столбцовая развёртка устанавливает биекцию между такими массивами и таблицами Юнга формы $\lambda$ в алфавите $\{x_1, \dots, x_m\}$. Таким образом, стандартный полином Шура имеет вид

$$s_\lambda(x) = \sum_\eta K_{\lambda,\eta} \cdot x^\eta = \sum_\eta K_{\lambda,\eta} \cdot x_1^{\eta_1} x_2^{\eta_2} \cdots x_m^{\eta_m}\,, \tag{4-11}$$

где $\eta \in \mathbb{Z}_{\geqslant 0}^m$ пробегает $m$-мерные целочисленные векторы с неотрицательными координатами, а коэффициент $K_{\lambda,\eta}$ равен числу таблиц формы $\lambda$, заполненных $\eta_1$ единицами, $\eta_2$ двойками и т. д. Мы будем говорить, что такая таблица имеет *состав* $\eta$.

Например, при $m = 3$ из представленной на рис. 4◇3 на стр. 55 схемы получаем

$$s_{(2,1)}(x_1, x_2, x_3) = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + 2\, x_1 x_2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2\,.$$

Число $K_{\lambda,\eta}$ таблиц формы $\lambda$ и состава $\eta$ называется *числом Костки*. Отметим, что $K_{\lambda,(1^{|\lambda|})} = d_\lambda$ равно числу стандартных таблиц формы $\lambda$, все $K_{\lambda,\lambda} = 1$, и $K_{\lambda,\eta} \neq 0$ только когда при каждом $j = 1, 2, 3, \dots$ выполняется неравенство $\lambda_1 + \dots + \lambda_j \geqslant \eta_1 + \dots + \eta_j$. В этой ситуации говорят, что диаграмма $\lambda$ *доминирует* вектор $\eta$ и пишут $\lambda \trianglerighteq \eta$.

Упражнение 4.3. Покажите, что отношение доминирования задаёт на множестве диаграмм Юнга заданного веса $n$ частичный порядок, полный при $n \leqslant 5$, и приведите пример двух несравнимых между собою диаграмм Юнга веса 6.

Из (4-11) видно, что стандартные полиномы Шура $s_\lambda(x_1, \dots, x_m)$, где $\lambda$ пробегает все диаграммы Юнга из не более $m$ строк, выражаются через базисные мономиальные симметрические многочлены $m_\mu$ при помощи унитреугольной матрицы

$$s_\lambda = \sum_{\mu \trianglelefteq \lambda} K_{\lambda,\mu} \cdot m_\mu\,. \tag{4-12}$$

Поскольку такая матрица обратима над $\mathbb{Z}$, многочлены $s_\lambda$ тоже образуют базис $\mathbb{Z}$-модуля симметрических функций.

Пример 4.2 (полные и элементарные симметрические многочлены)
Многочлен $s_{(k)}(x)$, отвечающий DU-орбите одностолбцового массива формы

$$\lambda = (k) = (k, 0, \dots, 0) = \underbrace{\square\square \cdots \square\square}_{k}\,,$$

представляет собой *полный симметрический многочлен* $h_k(x)$ — сумму всех мономов общей степени $k$ от $x_1, \dots, x_n$. В самом деле, столбцовая развёртка плотного влево массива из орбиты $O_{(k)}$ — это однострочная таблица Юнга, и для любого содержания $\eta$ веса $|\eta| = k$ имеется ровно одна такая таблица[1]. Эквивалентно: DU-орбита одностолбцового массива веса $k$ образована всеми возможными расположениями $k$ шариков по $m$ ящикам столбца.

Симметричным образом, многочлен $s_{(1^k)}$ DU-орбиты $k$-столбцового массива формы

$$\lambda = 1^k = (\underbrace{1, \dots, 1}_{k}) = \left.\begin{array}{|c|}\hline \phantom{0} \\ \hline \end{array}\atop{\vdots \atop \begin{array}{|c|}\hline \phantom{0} \\ \hline \end{array}}\right\} k$$

это *элементарный симметрический многочлен* $e_k(x)$, т. е. сумма всех линейных по каждой переменной мономов общей степени $k$ от $x_1, \dots, x_n$. Причина та же, только теперь столбцовая развёртка каждого плотного влево массива из орбиты $O_{1^k}$ представляет собою одностолбцовую таблицу Юнга, в которой все номера переменных строго возрастают сверху вниз.

Пример 4.3 (тождества Коши и Шура.)
Интерпретируем каждый шарик в клетке $(i, j)$ массива $a$ как билинейный моном $x_i y_j$ от двух наборов переменных $x = x^I = (x_1, \dots, x_n)$ и $y = y^J = (y_1, \dots, y_m)$. Перемножая вместе все шарики массива $a$, мы получим (в обозначениях n° 4.4) моном $x^{a^t} y^a$. По теореме о биекции из теор. 4.1 сумма таких мономов по всем массивам $a$ фиксированной формы $\lambda = \Phi(a)$ равна произведению многочленов Шура $s_\lambda(x) \cdot s_\lambda(y)$, и значит сумма мономов $x^{a^t} y^a$ по вообще всем массивам $a$ формата $I \times J$ равна сумме таких произведений по всем диаграммам Юнга $\lambda$. С другой стороны, сумма всех мономов $x^{a^t} y^a$ по всем массивам $a$ получается при раскрытии скобок в произведении геометрических прогрессий $\prod_{I \times J} \left(1 + x_i y_j + (x_i y_j)^2 + (x_i y_j)^3 + \cdots\right)$, поскольку выбирая из $(i, j)$-го сомножителя слагаемое $(x_i y_j)^{a(i,j)}$, мы получаем моном $x^{a^t} y^a$, отвечающий массиву $a$. Мы получили *тождество Коши*:

$$\sum_\lambda s_\lambda(x) \cdot s_\lambda(y) = \prod_{i,j} \frac{1}{1 - x_i y_j} \,. \tag{4-13}$$

Если взять $I = J$, ограничиться только симметричными массивами $a = a^t$, положить $x = y = \xi$, извлечь из каждого полученного $a$-монома корень $\xi^a = \sqrt{\xi^{a^t} \xi^a}$ и просуммировать по всем симметричным массивам $a$ заданной формы $\lambda$, мы получим многочлен $s_\lambda(\xi)$, а суммируя по вообще всем симметричным массивам $a$ — сумму $\sum_\lambda s_\lambda(\xi)$. Тот же ответ даст раскрытие скобок в произведении $\prod_k (1 + \xi_k + (\xi_k)^2 + (\xi_k)^3 + \cdots) \cdot \prod_{i<j} (1 + \xi_i \xi_j + (\xi_i \xi_j)^2 + (\xi_i \xi_j)^3 + \cdots)$. Записывая геометрические прогрессии рациональными дробями, получаем *тождество Шура*:

$$\sum_\lambda s_\lambda(\xi) = \prod_i \frac{1}{1 - \xi_i} \cdot \prod_{i<j} \frac{1}{1 - \xi_i \xi_j} \,. \tag{4-14}$$

**4.5. Правило Литтлвуда – Ричардсона.** Произведение $s_M(x) \cdot s_N(x)$ полиномов Шура DU-множеств $M$ и $N$ является полиномом Шура для DU-множества, состоящего из всевозможных массивов вида $ab$ размера $(2n) \times m$, получающихся приписыванием какого-нибудь массива $b \in N$

[1] В которой все переменные упорядочены по нестрогому возрастанию номеров.

справа к какому-нибудь массиву[1] $a \in M$. Множество таких массивов естественно обозначить через $M \otimes N$ и называть *тензорным произведением* DU-множеств $M$ и $N$. Итак,

$$s_M(x) \cdot s_N(x) = \Big(\sum_{a\in M} x^a\Big) \cdot \Big(\sum_{b\in N} x^b\Big) = \sum_{\substack{a\in M\\ b\in N}} x^{ab} = \sum_{c\in M\otimes N} x^c\,.$$

Поскольку стандартные полиномы $s_\lambda$ образуют базис модуля симметрических функций, произведение $s_\lambda s_\mu$ можно записать как

$$s_\lambda \cdot s_\mu = \sum_\nu c^\nu_{\lambda\mu} \cdot s_\nu\,. \tag{4-15}$$

Теорема 4.2 (правило Литтлвуда – Ричардсона)
Суммирование в формуле (4-15) происходит по всем диаграммам $\nu$, получающимся добавлением $|\mu|$ клеток к диаграмме $\lambda$, а коэффициент $c^\nu_{\lambda\mu}$ равен количеству таких заполнений этих дописанных клеток $\mu_1$ единицами, $\mu_2$ двойками, $\mu_3$ тройками и т. д., что вдоль строк «косой диаграммы» $\nu \smallsetminus \lambda$ числа возрастают нестрого, а вдоль столбцов — строго (как в таблице Юнга), и одновременно текст, получающееся при прочтении этой «косой диаграммы» строку за строкой справа налево сверху вниз, содержит в каждом своём начальном куске единиц не меньше, чем двоек, двоек не меньше, чем троек и т. д. (т. е. является текстом Яманеучи[2]).

Упражнение 4.4. Пользуясь правилом Литтлвуда – Ричардсона, вычислите[3] $s_{(1)} \cdot s_{(1,1)}$ и $s^2_{2,1}$.

Доказательство. Мы должны подсчитать в DU-множестве $O_\lambda \otimes O_\mu$ количество DU-орбит, которые уплотняются влево до стандартной орбиты $O_\nu$. Пусть массив $ab$ лежит в такой орбите. Поскольку массивы $a$, $b$ получены из биплотных массивов $\lambda$, $\mu$ вертикальными операторами, оба они плотны влево и имеют $I$-веса $\lambda$ и $\mu$ соответственно. Заметим, что действие вертикальной уплотняющей операции $D_j$ на «толстый» массив $ab$ состоит либо в её действии отдельно на[4] $b$ , либо в её действии отдельно на[5] $a$. Поэтому при уплотнении вниз «толстого» массива $ab$ мы получим массив вида $a'b'$, в котором $a'$ плотен вниз, и оба массива $a'$, $b'$ по прежнему плотны влево и имеют $I$-веса $\lambda$, $\mu$. Таким образом, $a'$ биплотен формы $\lambda$. Если форма массива $a'b' = \lambda b'$ равна $\nu$, то строки горизонтальной развёртки массива $b'$ — это выровненные по левому краю строки «косой таблицы» $\nu \smallsetminus \lambda$, заполненные именно так, как требует правило Литтлвуда – Ричардсона: первое, «табличное», ограничение выражает плотность вниз «толстого» массива $ab$, а второе, «текстовое», ограничение выражает, согласно n° 4.2.3, плотность влево массива $b'$. □

[1]При этом вертикальный $J$-алфавит не меняется, а горизонтальный $I$-алфавит заменяется дизъюнктным объединением $I$-алфавитов массивов $a$ и $b$.

[2]См. n° 4.2.3 на стр. 52.

[3]При этом поучительно убедиться в том, что применение теор. 4.2 к $s_{(1)} \cdot s_{(1,1)}$ и к $s_{(1,1)} \cdot s_{(1)}$ (что не всё равно) приводит к одному и тому же результату.

[4]Если самый правый свободный шар при паросочетании внутри «толстого» массива $ab$ лежит в $b$, то он подавно будет самым правым свободным шаром и для паросочетания, установленного отдельно внутри $b$.

[5]Если в $b$ нет свободных шаров при паросочетании внутри «толстого» массива $ab$.

Упражнение 4.5 (формулы Пьери). Выведите из теор. 4.2 *формулы Пьери*:

$$s_\lambda \cdot e_k = s_\lambda \cdot s_{(1^k)} = \sum_\mu s_\mu \tag{4-16}$$

$$s_\lambda \cdot h_k = s_\lambda \cdot s_{(k)} = \sum_\nu s_\nu \tag{4-17}$$

где $\mu$ и $\nu$ пробегают все диаграммы, которые можно получить приписыванием $k$ новых клеток к диаграмме $\lambda$ так, чтобы никакие две новые клетки не попали в одну строку $\mu$ и в один столбец $\nu$.

**4.5.1. Тождество Якоби – Труди.** Из формулы Пьери (4-17) и формулы Пьери из сл. 3.6 на стр. 45 вытекает, что детерминантные полиномы Шура $\Delta_{\delta+\lambda} / \Delta_\delta$ из предыдущего параграфа и комбинаторные полиномы Шура $s_\lambda$ стандартных DU-орбит — это одни и те же полиномы. В самом деле, формулы Пьери позволяют однозначно выразить все многочлены Шура через многочлены $h_k$. Например, согласно (4-17)

$$\begin{aligned}
s_{(2,2,1)} &= s_{(2,2)}h_1 - s_{(3,2)}\\
s_{(3,2)} &= s_{(3)}h_2 - s_{(5)} - s_{(4,1)} = h_3h_2 - h_5 - s_{(4,1)}\\
s_{(2,2)} &= s_{(2)}h_2 - s_{(3,1)} - s_{(4)} = h_2^2 - h_4 - s_{(3,1)}\\
s_{(4,1)} &= s_{(4)}h_1 - s_{(5)} = h_4h_1 - h_5\\
s_{(3,1)} &= s_{(3)}h_1 - s_{(4)} = h_3h_1 - h_4
\end{aligned}$$

откуда[1] $s_{(2,2,1)} = -h_3h_2+h_4h_1+h_1(h_2^2-h_1h_3)$. В общем случае, оставляя в правой части формулы (4-17) диаграмму с самой длинной нижней строкой среди всех диаграмм с наибольшим количеством строк, мы выражаем её через $h_k$ (где $k$ равно длине этой нижней строки) и диаграммы, имеющие то же число строк, но более короткую нижнюю строчку, или строго меньшее число строк. Далее используем убывающую индукцию по количеству строк диаграммы Юнга и длине её нижней строки. Совпадение детерминантного и комбинаторного полиномов Шура известно как *тождество Якоби – Труди*.

**4.5.2. Выражение $e_\lambda$ и $h_\lambda$ через $s_\lambda$.** Напомним, что для диаграммы Юнга $\mu$ мы обозначаем через $m_i$ количество строк длины $i$ в этой диаграмме и полагаем

$$\begin{aligned}
e_\mu &= e_{\mu_1}e_{\mu_2} \cdots e_{\mu_r} = e_1^{m_1}e_2^{m_2} \cdots e_n^{m_n}\\
h_\mu &= h_{\mu_1}h_{\mu_2} \cdots h_{\mu_r} = h_1^{m_1}h_2^{m_2} \cdots h_n^{m_n}\,,
\end{aligned}$$

где для $k \in \mathbb{N}$ многочлены $e_k(x) = s_{(1^k)}(x_1,\dots,x_m)$ и $h_k(x) = s_{(k)}(x_1,\dots,x_m)$ суть элементарный[2] и полный[3] симметрические многочлены. Для произвольной диаграммы $\eta$ многочлен $h_\eta = s_{(\eta_1)}\dots s_{(\eta_r)}$ является полиномом Шура DU-множества $\mathcal{O}_{(\eta_1)} \otimes \cdots \otimes \mathcal{O}_{(\eta_r)}$. Орбиты формы $\nu$ в этом множестве биективно соответствуют своим нижним концам, которые в свою очередь, взаимно однозначно описываются таблицами формы $\nu$ и содержания $\eta$. Тем самым,

$$h_\eta = \sum_\nu K_{\nu,\eta} \cdot s_\nu\,. \tag{4-18}$$

[1] Читателю рекомендуется проверить этот результат по формуле Джамбелли (3-25).

[2] См. n° 3.2 на стр. 39.

[3] См. n° 3.3 на стр. 40.

Многочлен $e_\eta = s_{(1^{\eta_1})} \dots s_{(1^{\eta_r})}$ — это многочлен Шура DU-множества $O_{(1^{\eta_1})} \otimes \cdots \otimes O_{(1^{\eta_r})}$, каждый массив в котором имеет $|\eta|$ столбцов, разбитых на вертикальные подмассивы $a_1, \dots, a_r$ ширины $\eta_1, \dots, \eta_r$, причём в каждом столбце находится ровно один шар, и $j$-номера этих шаров строго возрастают внутри каждого вертикального подмассива $a_i$. При уплотнении вниз последнее свойство сохранится, и в результате такого уплотнения мы получим массив $a'_1 \dots a'_r$, в котором шары каждого подмассива $a'_i$ располагаются в разных строках, номера которых строго возрастают слева направо. Тем самым, каждый подмассив $a'_i$ внесёт не более одного шара в каждую компоненту $J$-веса. Если суммарный $J$-вес при этом получится $\nu$, то записывая в каждую строку диаграммы $\nu$ последовательно номера $i$ тех подмассивов $a'_i$, которые дают вклад в эту компоненту $J$-веса, мы получим таблицу содержания $\eta$ и формы $\nu^t$, *сопряжённой*[1] к форме $\nu$: в силу вышесказанного номера будут строго возрастать по строкам диаграммы $\nu$, а поскольку массив плотен вниз, они также должны не строго возрастать по столбцам; кроме того, по построению, каждый номер $i$ будет представлен ровно в $\eta_i$ различных строчках. Итак,

$$e_\eta = \sum_\nu K_{\nu^t,\eta} \cdot s_\nu \,. \tag{4-19}$$

Следствие 4.2
Инволюция $\omega$ из предл. 3.3, переводящая $e_k$ и $h_k$ друг в друга, действует на полиномы Шура по правилу $\omega(s_\lambda) = s_{\lambda^t}$, т. е. переводит друг в друга многочлены, отвечающие транспонированным диаграмм Юнга.

Доказательство. Так как многочлены $s_\lambda$ образуют базис $\mathbb{Z}$-модуля симметрических функций, отображение $s_\lambda \mapsto s_{\lambda^t}$ однозначно задаёт на модуле симметрических функций $\mathbb{Z}$-линейную инволюцию. Из формул (4-18) и (4-19) следует, что эта инволюция переводит $e_k$ в $h_k$ и наоборот, т. е. совпадает с $\omega$. □

Следствие 4.3 (вторая формула Джамбелли)

$$s_{\lambda^t} = \det \begin{pmatrix} e_{\lambda_1} & e_{\lambda_1+1} & \ddots & e_{\lambda_1+n-1} \\ e_{\lambda_2-1} & e_{\lambda_2} & \ddots & \ddots \\ \ddots & \ddots & \ddots & e_{\lambda_{n-1}+1} \\ e_{\lambda_n-n+1} & \ddots & e_{\lambda_n-1} & e_{\lambda_n} \end{pmatrix}, \tag{4-20}$$

где по главной диагонали стоят $e_{\lambda_1}, \dots, e_{\lambda_n}$, и при движении вдоль строк слева направо индексы у $e$ с каждым шагом увеличиваются на единицу. □

Доказательство. Применяем инволюцию $\omega$ к форм. (3-25) на стр. 44. □

**4.6. Скалярное произведение на модуле симметрических функций.** Введём на $\mathbb{Z}$-модуле симметрических функций[2] $\Lambda$ евклидово скалярное произведение $\langle \ast\,,\, \ast \rangle$, для которого базис из полиномов Шура $s_\lambda$ является ортонормальным. Из формул (4-18) и (4-12)

$$h_\lambda = \sum_{\mu \trianglerighteq \lambda} K_{\mu,\lambda} \cdot s_\mu \,, \quad s_\mu = \sum_{\lambda \trianglerighteq \mu} K_{\mu,\lambda} \cdot m_\lambda$$

[1] Или *транспонированной*, т. е. симметрично отражённой относительно главной диагонали.
[2] См. n° 3.7 на стр. 46.

вытекает, что $\langle\, h_\lambda\,,\, s_\mu\,\rangle = K_{\mu,\lambda} = \langle\, m^*_\lambda\,,\, s_\mu\,\rangle$, где $m^*_\lambda$ — базис, евклидово двойственный к $m_\lambda$. Таким образом, $m^*_\lambda = h_\lambda$, т. е. базисы $h_\lambda$ и $m_\lambda$ двойственны друг другу:

$$\langle\, h_\lambda\,,\, m_\mu\,\rangle = \delta_{\lambda\mu}\,. \tag{4-21}$$

Из сл. 4.2 вытекает, что инволюция $\omega$ является ортогональным оператором.

Предложение 4.2

Многочлены Ньютона $p_\lambda$ составляют ортогональный базис пространства $\mathbb{Q}\otimes\Lambda$ симметрических функций с рациональными коэффициентами и имеют скалярные квадраты $\langle\, p_\lambda\,,\, p_\lambda\,\rangle = z_\lambda$, где[1] $z_\lambda = \prod_k \left(m_k!\cdot k^{m_k}\right)$.

Доказательство. Выразим произведение геометрических прогрессий в правой части тождества Коши (4-13) через функции Ньютона от наборов переменных $x$ и $y$:

$$\begin{aligned}\sum_\lambda s_\lambda(x)s_\lambda(y) &= \prod_{i,j}\frac{1}{1-x_iy_j} = \prod_j H(y_j) = \prod_j \exp\left(\int_0^{y_j} P(t)\,dt\right) = \\ &= \exp\left(\sum_j\sum_k \frac{1}{k}\,p_k(x)y_j^k\right) = \exp\left(\sum_k \frac{p_k(x)p_k(y)}{k}\right) = \prod_k \exp\left(\frac{p_k(x)p_k(y)}{k}\right) = \\ &= \prod_k \sum_{\ell\geqslant 0}\frac{1}{\ell!\cdot k^\ell}\,\left(p_k(x)p_k(y)\right)^\ell = \sum_\lambda \frac{1}{z_\lambda}\,p_\lambda(x)p_\lambda(y)\end{aligned}$$

(последнее равенство объясняется точно также, как в доказательстве предл. 3.4 на стр. 42). Если обозначить через $C_{\lambda\mu} = \langle\, s_\lambda\,,\, p_\mu\,\rangle$ коэффициенты разложений Ньютоновских полиномов по базису из полиномов Шура, так что $p_\mu = \sum_\lambda C_{\lambda\mu}s_\lambda$, то подставляя эти разложения в правую часть полученного выше равенства и приравнивая коэффициенты при $s_\lambda(x)s_\eta(y)$ в левой и правой части, получаем соотношения

$$\sum_\nu C_{\nu\lambda}C_{\nu\eta} = \begin{cases} z_\lambda & \text{при } \eta = \lambda \\ 0 & \text{при } \eta \neq \lambda, \end{cases}$$

т. е. матрица Грама $\left(\langle\, p_\lambda\,,\, p_\mu\,\rangle\right) = C^t\cdot C$ диагональна с диагональными элементами $z_\lambda$. □

[1] Ср. с форм. (3-21) на стр. 42.

## §5. Основные понятия теории представлений.

**5.1. Представления множества операторов.** Для произвольного множества $R$ условимся обозначать через $R \otimes \Bbbk$ векторное пространство с базисом $R$ над полем $\Bbbk$, состоящее из всевозможных конечных формальных линейных комбинаций элементов из $R$ с коэффициентами в $\Bbbk$, а через $A_R \stackrel{\text{def}}{=} T(R \otimes \Bbbk)$ — тензорную алгебру этого векторного пространства, т. е. свободную ассоциативную $\Bbbk$-алгебру, порождённую множеством $R$.

Например, если множество $R = \{t\}$ состоит из одного элемента $t$, то векторное пространство $t \otimes \Bbbk = \Bbbk\, t$ одномерно с базисом $t$, а ассоциативная алгебра $A_t = T(\Bbbk\, t)$, т. е. тензорная алгебра одномерного векторного пространства, изоморфна алгебре $\Bbbk[t]$ многочленов от одной переменной: изоморфизм сопоставляет базисному тензору $t \otimes \cdots \otimes t \in (\Bbbk\, t)^{\otimes n}$ моном $t^n$.

Отображение $\varrho : R \to \mathrm{End}(W)$ множества $R$ в алгебру линейных эндоморфизмов какого-нибудь векторного пространства $W$ над полем $\Bbbk$ называется *линейным представлением* множества $R$ эндоморфизмами пространства $W$. По универсальному свойству свободной алгебры $A_R$, линейные представления $\varrho : R \to \mathrm{End}(W)$ биективно соответствуют гомоморфизмам ассоциативных алгебр $\tilde{\varrho} : A_R \to \mathrm{End}(W)$. Последние называются *линейными представлениями* алгебры $A_R$ в пространстве $W$. Пространство $W$ с фиксированным на нём представлением множества $R$ или алгебры $A_R$ называется, соответственно, $R$-модулем или $A_R$-модулем. И то, и другое равносильно сопоставлению каждому элементу $f \in R$ линейного оператора $\varrho(f) : W \to W$. Произвольные тензоры $f = \sum_{f_1,\dots f_m \in R} x_{f_1 \dots f_m} f_1 \otimes \cdots \otimes f_m \in A_R$ с $f_\nu \in R$, $x_{f_1 \dots f_m} \in \Bbbk$ при этом представляются линейными операторами $\tilde{\varrho}(f) = \sum x_{f_1 \dots f_m} \varrho(f_1) \circ \varrho(f_2) \circ \cdots \circ \varrho(f_m) : W \to W$, а образ гомоморфизма алгебр $\tilde{\varrho} : A_R \to \mathrm{End}(W)$ состоит из всех операторов $W \to W$, которые можно получить из представляющих элементы множества $R$ операторов $\varrho(f)$ при помощи композиций, сложения и умножения на числа. Он называется *ассоциативной оболочкой* множества операторов $\varrho(R) \subset \mathrm{End}(W)$ и обозначается $\mathrm{Ass}\big(\varrho(R)\big) \stackrel{\text{def}}{=} \mathrm{im}\, \tilde{\varrho}$.

Когда понятно, о каком представлении $\varrho$ идёт речь, мы обозначаем результат применения оператора $\tilde{\varrho}(f)$, где $f \in A_R$, к вектору $w \in W$ просто через $fw$. Для подпространства $U \subset W$ и набора операторов $F \subset A_R$ мы полагаем $FU \stackrel{\text{def}}{=} \{fu \mid f \in F,\ u \in U\}$.

**5.1.1. Разложимость, приводимость и полупростота.** Векторное подпространство $U$ в $R$-модуле $W$ называется *$R$-подмодулем* или *$R$-инвариантным подпространством*, если $RU \subset U$. Как обычно, мы называем $R$-подмодуль $U$ *нетривиальным*, если он отличен от нуля и всего пространства $W$.

Упражнение 5.1 (фактор модули). Убедитесь, что для всякого $R$-подмодуля $U \subset W$ на фактор пространстве $V = W/U$ имеется структура $R$-модуля, на котором элементы $f \in R$ действуют по правилу $f[w] \stackrel{\text{def}}{=} [fw]$, где $[w] = w + U$ означает класс вектора $w \in W$ по модулю $U$.

$R$-модуль $W$ называется *простым*, если у него нет нетривиальных подмодулей. Представление $\varrho : R \to \mathrm{End}(W)$, задающее простой модуль, называется *неприводимым*. $R$-модуль $W$ и соответствующее ему представление называются *разложимыми*, если $W$ является прямой суммой своих нетривиальных $R$-подмодулей. Всякий конечномерный $R$-модуль является прямой суммой неразложимых, однако неразложимые модули, вообще говоря, могут быть приводимыми.

Если $R$-модуль $W$ является прямой суммой *неприводимых* $R$-подмодулей, то он называется *полупростым*, а соответствующее представление $\varrho : R \to \mathrm{End}(W)$ — *вполне приводимым*. Обратите внимание, что каждый неприводимый $R$-модуль по определению полупрост и неразложим, и что прямая сумма любого множества полупростых модулей полупроста.

Упражнение 5.2. Убедитесь, что для заданных подпространств $U_1, U_2 \subset W$ условия $RU_1 \subset U_2$ и

$A_R U_1 \subset U_2$ равносильны, и выведите отсюда, что простота, полупростота и разложимость пространства $W$ относительно произвольного множества операторов $S \subset \mathrm{End}(W)$ и относительно ассоциативной оболочки $\mathrm{Ass}(S)$ этих операторов означают одно и то же.

Пример 5.1 (пространство с одним оператором)
Если множество $R$ состоит из одного элемента $t$, то $A_R \simeq \Bbbk[t]$ является кольцом многочленов от этого элемента. Представление $\varrho : R \to \mathrm{End}\, W$ заключается в выборе на пространстве $W$ линейного оператора $f = \varrho(t) : W \to W$ и наделяет пространство $W$ структурой модуля над кольцом многочленов, которая задаётся гомоморфизмом

$$\tilde{\varrho} = \mathrm{ev}_f : \Bbbk[t] \to \mathrm{End}(W)\,,\ t \mapsto f\,, \tag{5-1}$$

переводящим многочлен $F \in \Bbbk[t]$ в результат подстановки в него оператора $f$ вместо переменной $t$. Если пространство $W$ конечномерно, гомоморфизм (5-1) имеет ненулевое ядро — главный идеал $(\mu_f)$, порождённый приведённым многочленом наименьшей степени, аннулирующим оператор[1] $f$. Ассоциативная оболочка оператора $f$, т. е. образ гомоморфизма (5-1), представляет собою множество всех многочленов от оператора $f$ и изоморфна фактор алгебре $\Bbbk[t]/(\mu_f)$. По теореме о строении конечно порождённых модулей над кольцом главных идеалов конечномерный $\Bbbk[t]$-модуль $W$, будучи модулем кручения, изоморфен прямой сумме фактор модулей

$$\frac{\Bbbk[t]}{(p_1^{m_1})} \oplus \dots \oplus \frac{\Bbbk[t]}{(p_s^{m_s})}\,, \tag{5-2}$$

где все многочлены $p_i \in \Bbbk[t]$ неприводимы и приведены, а действие оператора состоит в умножении на $t$, и два таких модуля изоморфны если и только если они отличаются друг от друга перестановкой прямых слагаемых. В частности, всякое неразложимое пространство с оператором изоморфно пространству $\Bbbk[t]/(p^m)$ с оператором умножения на $t$, и два таких пространства с разными $p$ или $m$ не изоморфны друг другу.

Упражнение 5.3. Убедитесь, что $\Bbbk[t]$-модуль $\Bbbk[t]/(p^m)$ неприводим если и только если $m = 1$.

Тем самым, всякое неприводимое пространство с оператором изоморфно $\Bbbk[t]/(p)$, где $p \in \Bbbk[t]$ приведён и неприводим, а оператор действует умножением на $t$, а всякое полупростое — прямой сумме нескольких таких пространств.

Упражнение 5.4. Докажите, что оператор $f$ над произвольным полем $\Bbbk$ диагонализуем если и только если он аннулируется многочленом, полностью разлагающимся в $\Bbbk[t]$ в произведение попарно различных линейных множителей[2].

Пример 5.2 (коммутирующие операторы)
В прошлом году мы видели[3], что если основное поле $\Bbbk$ алгебраически замкнуто, а векторное пространство $W$ конечномерно, то любое множество коммутирующих операторов $R \subset \mathrm{End}(W)$ имеет общий для всех операторов собственный вектор. Таким образом, над алгебраически замкнутым полем конечномерные неприводимые представления любого множества коммутирующих операторов исчерпываются одномерными представлениями[4].

[1] Напомню, что он называется *минимальным многочленом* оператора $f$.

[2] В частности, если оператор диагонализуем на всём пространстве, то он диагонализуем и на любом своём инвариантном подпространстве

[3] См. раздел 10.2.7 на стр. 142 лекции
http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_10.pdf.

[4] Обратите внимание, что любое одномерное представление по очевидным причинам неприводимо.

Тогда же и там же мы видели, что если все операторы из $R$ диагонализуемы, то их можно одновременно диагонализовать в некотором общем для всех операторов базисе. Это означает, что каждое конечномерное представление любого множества диагонализуемых коммутирующих операторов вполне приводимо и является прямой суммой одномерных представлений.

Лемма 5.1
Пусть $R$-модуль[1] $W$ линейно порождается над $\Bbbk$ некоторым множеством $\mathcal{S}$ своих неприводимых $R$-подмодулей. Тогда у любого $R$-подмодуля $U \subsetneq W$ имеется дополнительный $R$-подмодуль $V \subset W$, такой что $W = U \oplus V$, причём этот подмодуль $V$ является прямой суммой подходящих подмодулей из множества $\mathcal{S}$. Для нулевого подмодуля $U = 0$ это утверждение означает, что весь модуль $W$ является прамой суммой подходящих подмодулей из множества $\mathcal{S}$. В частности, такой модуль $W$ автоматически полупрост.

Доказательство. Так как $U \neq W$ и $W$ линейно порождается подмодулями $S \in \mathcal{S}$, в множестве $\mathcal{S}$ найдётся подмодуль $S \not\subset U$. Сумма $U + S$ является прямой, поскольку пересечение $S \cap U \subsetneq S$, будучи собственным подмодулем неприводимого модуля $S$, равно нулю. Обозначим через $\mathcal{S}'$ множество всех полупростых подмодулей $M \subset W$, разложимых в прямую сумму модулей из $\mathcal{S}$ и таких, что сумма $U + M$ прямая. По предыдущему, множество $\mathcal{S}'$ непусто. Введём на нём частичный порядок, полагая $M_1 < M_2$, когда $M_2 = M_1 \oplus M$ для некоторого $M \in \mathcal{S}'$.

Упражнение 5.5. Убедитесь, что $\mathcal{S}'$ является полным чумом[2].

По лемме Цорна[3] в множестве $\mathcal{S}'$ имеется максимальный элемент $V$. Покажем, что $U \oplus V = W$. Если $U \oplus V \neq W$, то повторяя проведённое в начале доказательства рассуждение для подмодуля $U \oplus V$ в роли подмодуля $U$, мы найдём в $\mathcal{S}$ такой подмодуль $S \subset W$, что сумма $(U \oplus V) + S$ прямая. Это означает, что $V \oplus S \in \mathcal{S}'$ строго больше, чем $V$. Всё сказанное работает и для $U = 0$. □

Теорема 5.1
Модуль $W$ полупрост если и только если каждый ненулевой подмодуль в $W$ содержит простой ненулевой подмодуль и для каждого нетривиального $R$-подмодуля $U \subset W$ найдётся такой $R$-подмодуль $V \subset W$, что $W = U \oplus V$.

Доказательство. Если модуль $W$ полупрост, т. е. является прямой суммой простых подмодулей, подмодуль $V \subset W$, дополнительный к произвольно заданному подмодулю $U \subset W$, существует по лем. 5.1, применённой к множеству $\mathcal{S}$ всех простых подмодулей в $W$.

Упражнение 5.6. Убедитесь, что проекция $\pi : W = U \oplus V \twoheadrightarrow U$, $u + v \mapsto u$, перестановочна с действием операторов из $R$, т. е. $\pi(fw) = f\pi(w)$ для всех $f \in R$ и $w \in W$.

Так как $W$ линейно порождается простыми подмодулями, проекция $\pi$ переводит хотя бы один из них в ненулевое векторное подпространство в $U$.

Упражнение 5.7. Убедитесь, что это подпространство является простым $R$-подмодулем в $U$.

Это доказывает прямую импликацию «только если». Чтобы доказать обратную импликацию, обозначим через $\mathcal{S}$ множество всех полупростых ненулевых подмодулей $S \subseteq W$. Это множе-

---

[1] Не обязательно конечномерный как векторное пространство над $\Bbbk$.

[2] Т. е. каждое линейно упорядоченное подмножество в $\mathcal{S}'$ имеет верхнюю грань, см. раздел 1.7 на стр. 15 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_01.pdf.

[3] См. раздел 1.9 на стр. 17 той же лекции.

ство непусто, поскольку содержит ненулевой простой подмодуль, имеющийся в $W$ по условию. Зададим на $\mathcal{S}$ частичный порядок, полагая $S_1 < S_2$ когда $S_2 = S_1 \oplus S$ для некоторого $S \in \mathcal{S}$.

Упражнение 5.8. Убедитесь, что чум $\mathcal{S}$ полон.

По лемме Цорна, в $\mathcal{S}$ есть максимальный элемент $M$. Если он не совпадает с $W$, то найдётся такой нетривиальный подмодуль $V \subset W$, что $W = M \oplus V$. Поскольку в $V$ есть нетривиальный простой подмодуль $S \subset V$, сумма $M \oplus S \in \mathcal{S}$ будет строго больше, чем $M$. Тем самым, $M = W$. □

Следствие 5.1 (критерии полупростоты)
Пусть каждый ненулевой $R$-подмодуль в $R$-модуле[1] $W$ содержит в себе конечномерный ненулевой $R$-подмодуль. Тогда следующие свойства модуля $W$ эквивалентны:

1) $W$ полупрост

2) $W$ линейно порождается над $\Bbbk$ простыми $R$-подмодулями

3) для любого нетривиального $R$-подмодуля $U \subset W$ существует такой $R$-подмодуль $V \subset W$, что $W = U \oplus V$.

Доказательство. Если $R$-подмодуль конечномерен как векторное пространство над $\Bbbk$, то каждый его $R$-подмодуль минимальной положительной размерности автоматически прост. Поэтому каждый ненулевой подмодуль в $W$ обладает простым ненулевым подмодулем, и условия (1) и (3) эквивалентны по теор. 5.1. Импликация (1) ⇒ (2) очевидна. Импликация (2) ⇒ (3) была установлена в лем. 5.1. □

**5.1.2. Гомоморфизмы представлений.** Линейное отображение $\varphi : W_1 \to W_2$ между $R$-модулями, отвечающими линейным представлениям $\varrho_1 : R \to \mathrm{End}(W_1)$ и $\varrho_2 : R \to \mathrm{End}(W_2)$, называется гомоморфизмом $R$-модулей[2], если оно перестановочно с действием всех операторов из $R$, т. е. для всех $f \in R$ коммутативна диаграмма

$$\begin{tikzcd} W_1 \arrow[r, "\varphi"] & W_2 \\ W_1 \arrow[u, "\varrho_1(f)"] \arrow[r, "\varphi"] & W_2 \arrow[u, "\varrho_2(f)"'] \end{tikzcd}.$$

Примером $R$-линейного отображения является проекция разложимого $R$-модуля $U \oplus V$ на подмодуль $U$ вдоль подмодуля $V$ из упр. 5.6 на стр. 65. Множество всех $R$-линейных гомоморфизмов обозначается через $\mathrm{Hom}_R(W_1, W_2) \stackrel{\text{def}}{=} \{\varphi : W_1 \to W_2 \mid \forall\, w \in W_1,\ \forall\, f \in R\ \varphi(fw) = f\varphi(w)\}$.

Упражнение 5.9. Убедитесь, что а) $\mathrm{Hom}_R(W_1, W_2) = \mathrm{Hom}_{A_R}(W_1, W_2)$ является векторным подпространством в $\mathrm{Hom}(W_1, W_2)$ б) композиция $R$-линейных отображений $R$-линейна в) ядро и образ гомоморфизма $R$-модулей являются $R$-подмодулями г) образ и полный прообраз любого $R$-модуля относительно гомоморфизма $R$-модулей являются $R$-модулями.

Лемма 5.2 (лемма Шура)
Всякий ненулевой гомоморфизм неприводимых $R$-модулей является изоморфизмом. Если основное поле $\Bbbk$ алгебраически замкнуто, то все $R$-линейные эндоморфизмы неприводимого $R$-модуля скалярны, т. е. имеют вид $\lambda\,\mathrm{Id}$, где $\lambda \in \Bbbk$.

[1] Который не предполагается конечномерным.

[2] А также *сплетающим оператором*, *гомоморфизмом представлений* или *$R$-линейным отображением*.

Доказательство. Пусть представления $\varrho_1 : R \to \mathrm{End}(W_1)$, $\varrho_2 : R \to \mathrm{End}(W_2)$ неприводимы, а линейное отображение $\varphi : W_1 \to W_2$ перестановочно со всеми операторами из $R$. Поскольку $\ker\varphi \subset W_1$ и $\operatorname{im}\varphi \subset W_2$ являются $R$-подмодулями простых модулей, либо $\ker\varphi = W_1$ и $\varphi = 0$, либо $\ker\varphi = 0$ и тогда при $\varphi \neq 0$ ненулевой подмодуль $\operatorname{im}\varphi \subset W_2$ совпадает с $W_2$, т. е. $\varphi$ одновременно инъективно и сюрьективно.

Рассмотрим теперь $R$-линейный эндоморфизм $\varphi : W \to W$. Для каждого $\lambda \in \Bbbk$ эндоморфизм $\lambda\,\mathrm{Id} - \varphi$ тоже $R$-линеен. Если поле $\Bbbk$ алгебраически замкнуто, существует такое $\lambda \in \Bbbk$, что $R$-подмодуль $\ker(\lambda\,\mathrm{Id} - \varphi) \neq 0$. Если $W$ неприводим, это ядро совпадает со всем модулем $W$, т. е. $\varphi = \lambda\,\mathrm{Id}$. □

Следствие 5.2
Если основное поле алгебраически замкнуто, а $R$-модули $U$ и $W$ неприводимы, то

$$\dim \mathrm{Hom}_R(U, W) = \begin{cases} 0 & \text{если } U \text{ и } W \text{ не изоморфны} \\ 1 & \text{если } U \text{ и } W \text{ изоморфны.} \end{cases}$$

Доказательство. Любые два ненулевых изоморфизма $\varphi, \psi : U \xrightarrow{\sim} W$ пропорциональны, поскольку $\psi^{-1}\varphi = \lambda \cdot \mathrm{Id}_U$ для некоторого $\lambda \in \Bbbk^*$. □

Упражнение 5.10. Пусть линейный оператор $\pi : V \to V$ имеет $\pi^2 = \pi$. Убедитесь, что $V = \ker\pi \oplus \operatorname{im}\pi$ и $\pi$ проектирует $V$ на $\operatorname{im}\pi$ вдоль $\ker\pi$, причём если оператор $\pi$ является $R$-линейным, то $\ker\pi$ и $\operatorname{im}\pi$ являются $R$-подмодулями, а оператор $1 - \pi$ является $R$-линейным проектором на $\ker\pi$ вдоль $\operatorname{im}\pi$.

Следствие 5.3
Фактор модуль любого полупростого $R$-модуля $W$ тоже полупрост.

Доказательство. По лемме Шура образ любого простого $R$-подмодуля $S \subset W$ при любой $R$-линейной сюрьекции $\pi : W \twoheadrightarrow U$ либо нулевой, либо изоморфен $S$ и, стало быть, прост. Поскольку $W$ линейно порождается простыми подмодулями $S \subset W$, модуль $U$ линейно порождается ненулевыми подмодулями $\pi(S)$. □

Предложение 5.1
В условиях сл. 5.1 на стр. 66 полупростота $R$-модуля $W$ равносильна тому, что для любого подмодуля $U \subset W$ существует такой $R$-линейный эндоморфизм $\pi_U \in \mathrm{End}_R(W)$, что $\pi_U^2 = \pi_U$ и $\operatorname{im}\pi_U = U$.

Доказательство. В прошлом году мы видели[1], что каждый $\Bbbk$-линейный оператор $\pi : W \to W$, удовлетворяющий соотношению $\pi^2 = \pi$, проектирует пространство $W$ на подпространство $\operatorname{im}\pi$ вдоль подпространства $\ker\pi$, т. е. $V = \ker\pi \oplus \operatorname{im}\pi$ и $\pi(u) = u$ для всех $u \in \operatorname{im}\pi$. Если оператор $\pi_U : W \to W$ удовлетворяет условиям предложения и $R$-линеен, его ядро и образ являются $R$-подмодулями в $W$, и наличие такого оператора равносильно наличию прямого разложения $W = U \oplus \ker\pi_U$. □

[1] См. пример 10.4 на стр. 143 лекции
http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_11.pdf.

Следствие 5.4
Каждый подмодуль полупростого $R$-модуля тоже полупрост.

Доказательство. Пусть $R$-модуль $L$ является нетривиальным подмодулем полупростого $R$-модуля $W$. Каждый $R$-подмодуль $U \subset L$, будучи подмодулем и в $W$, является образом $R$-линейного проектора $W \twoheadrightarrow U$. Ограничение этого проектора на подмодуль $L$ является $R$-линейным проектором $L \twoheadrightarrow U$. □

**5.2. Представления ассоциативной алгебры.** Пусть $A$ — ассоциативная алгебра над произвольным полем $\Bbbk$, а $V$ — любое векторное пространство над $\Bbbk$. Гомоморфизм $\Bbbk$-алгебр

$$\varrho : A \to \operatorname{End} V$$

называется *линейным представлением* алгебры $A$ в векторном пространстве $V$. Пространство $V$ называется в этой ситуации $A$-модулем. Представления ассоциативных алгебр являются специальными примерами представлений множеств операторов, и к ним в полной мере приложима вся терминология из n° 5.1.1 на стр. 63. Для двух $A$-модулей $U$, $W$ мы полагаем

$$\operatorname{Hom}_A(U,V) \stackrel{\text{def}}{=} \{\varphi : U \to W \mid \forall f \in A,\ \forall u \in U\ \varphi(fu) = f\varphi(u)\}$$

и называем такие отображения $\varphi : U \to W$ *$A$-линейными*. Когда $U = W$ все $A$-линейные эндоморфизмы $A$-модуля $W$ образуют ассоциативную $\Bbbk$-подалгебру $\operatorname{End}_A(W) \subset \operatorname{End}_{\Bbbk}(W)$ в $\Bbbk$-алгебре всех $\Bbbk$-линейных эндоморфизмов векторного пространства $W$. Подалгебру $\operatorname{End}_A(W)$ обычно называют *централизатором $A$* в $\operatorname{End}_{\Bbbk}(W)$.

Пусть $W = V_1 \oplus \dots \oplus V_n$ является прямой суммой своих $A$-подмодулей $V_\nu$. Обозначим через $\iota_\nu : V_\nu \hookrightarrow W$ вложение каждого из них в $W$, а через $\pi_\mu : W \twoheadrightarrow V_\mu$ — проекцию прямой суммы $V_1 \oplus \dots \oplus V_n$ на $\mu$-е слагаемое.

Упражнение 5.11. Убедитесь, что $\sum_\nu \iota_\nu \pi_\nu = \operatorname{Id}_W$, $\pi_\nu \iota_\nu = \operatorname{Id}_{V_\nu}$ для всех $\nu$, $\pi_\nu \iota_\mu = 0$ и $\iota_\mu \pi_\nu = 0$ для всех $\mu \neq \nu$.

Для каждого $\varphi \in \operatorname{End}(W)$ положим $\varphi_{\mu\nu} \stackrel{\text{def}}{=} \pi_\mu \circ \varphi \circ \iota_\nu$ и организуем эндоморфизмы $\varphi_{\mu\nu} : V_\nu \to V_\mu$ в квадратную матрицу $\left(\varphi_{\mu\nu}\right)$. Исходный эндоморфизм $\varphi$ восстанавливается из этой матрицы как

$$\varphi = \operatorname{Id}_W \circ \varphi \circ \operatorname{Id}_W = \left(\sum_\mu \iota_\mu \pi_\mu\right) \circ \varphi \circ \left(\sum_\nu \iota_\nu \pi_\nu\right) = \sum_{\mu,\nu} \iota_\mu \varphi_{\mu\nu} \pi_\nu \,.$$

При этом $\varphi \in \operatorname{End}_A(W)$ если и только если все $\varphi_{\mu\nu} \in \operatorname{Hom}_A(V_\nu, V_\mu)$. Таким образом, имеет место изоморфизм векторных пространств

$$\operatorname{End}_A(W) \xrightarrow{\sim} \bigoplus_{\mu,\nu} \operatorname{Hom}_A(V_\nu, V_\mu)\,, \quad \varphi \mapsto \left(\varphi_{\mu\nu}\right)\,. \tag{5-3}$$

Упражнение 5.12. Убедитесь, что изоморфизм (5-3) переводит композицию эндоморфизмов в произведение матриц.

В ситуации, когда все слагаемые $V_\nu = V$ являются копиями одного и того же $A$-модуля $V$, изоморфизм (5-3) превращается в изоморфизм $\Bbbk$-алгебр

$$\operatorname{End}_A\left(V^{\oplus n}\right) \simeq \operatorname{Mat}_n\left(\operatorname{End}_A(V)\right)\,. \tag{5-4}$$

Теорема 5.2 (теорема о двойном централизаторе)
Пусть конечномерное векторное пространство $V$ полупросто над ассоциативной подалгеброй $A \subset \mathrm{End}(V)$, и $B = \mathrm{End}_A(V)$. Тогда $\mathrm{End}_B(V) = A$.

Доказательство. Включение $A \subset \mathrm{End}_B(V)$ очевидно из определений. Чтобы установить обратное включение, зафиксируем в $V$ базис $e_1, \dots, e_n$ и покажем, что для каждого $B$-линейного оператора $\varphi \in \mathrm{End}_B(V)$ найдётся такой оператор $a \in A$, что $\varphi e_i = a e_i$ при всех $i$ — это обеспечит равенство $\varphi = a$. Рассмотрим $n$-кратную прямую сумму $W = V^{\oplus n}$ и введём на ней структуру модуля над алгебрами $A$, $B$ и $\mathrm{End}_B(V)$, полагая $f(v_1, \dots, v_n) = (fv_1, \dots, fv_n)$ для каждого оператора $f$ из $A$, из $B$ или из $\mathrm{End}_B(V)$. Обозначим вектор $(e_1, \dots, e_n) \in W$ через $e$. Достаточно убедиться, что $\varphi e \in Ae$. Поскольку $W$ полупрост как $A$-модуль, его $A$-подмодуль $Ae \subset W$ является образом некоторого $A$-линейного проектора $\pi : W \twoheadrightarrow Ae$, тождественно действующего на $Ae$. Если $\pi$ коммутирует с $\varphi$, то $\varphi(e) = \varphi(\pi e) = \pi(\varphi e) \in Ae$, что и требуется. Покажем, что $\pi$ действительно коммутирует с $\varphi$. Для этого запишем эндоморфизм $\pi : V^{\oplus n} \to V^{\oplus n}$ матрицей $(\pi_{ij})$ с элементами $\pi_{ij} \in \mathrm{End}(V)$, как это объяснялось выше. Так как $\pi$ перестановочен с действием $A$ на $W$, каждая компонента $\pi_{ij}$ перестановочна с действием $A$ на $V$, т. е. лежит в $\mathrm{End}_A(V) = B$. Поэтому диагональная матрица, по диагонали которой стоят одинаковые элементы $\varphi \in \mathrm{End}_B(V)$, коммутирует с $\pi$. □

Следствие 5.5 (теорема Бернсайда)
Если основное поле $\Bbbk$ алгебраически замкнуто, а конечномерное векторное пространство $V$ неприводимо как модуль над множеством операторов $R \subset \mathrm{End}(V)$, то ассоциативная оболочка $\mathrm{Ass}(R) \subset \mathrm{End}_\Bbbk(V)$ этих операторов совпадает со всей алгеброй эндоморфизмов $\mathrm{End}_\Bbbk(V)$. В частности, все конечномерные неприводимые представления $A \to \mathrm{End}(V)$ любой ассоциативной алгебры $A$ эпиморфны.

Доказательство. По лемме Шура[1] $\mathrm{End}_{\mathrm{Ass}(R)}(V) = \Bbbk$, откуда $\mathrm{End}_\Bbbk(V) = \mathrm{Ass}(R)$. □

Упражнение 5.13. Докажите, что обратная импликация: если $\mathrm{Ass}(R) = \mathrm{End}(V)$, то $R$-модуль $V$ неприводим, имеет место над любым полем $\Bbbk$.

**5.3. Изотипные компоненты.** Зафиксируем ассоциативную алгебру $A$. Для произвольных $A$-модулей $U$, $W$ на тензорном произведении $\mathrm{Hom}_A(U, W) \otimes U$ имеется естественная структура $A$-модуля, на котором элементы $a \in A$ действуют по правилу $a(\varphi \otimes u) \stackrel{\text{def}}{=} \varphi \otimes (au)$. При этом каноническая свёртка

$$c_{WU} : \ \mathrm{Hom}_A(U, W) \otimes U \to W\,, \ \ \varphi \otimes u \mapsto \varphi(u)\,, \tag{5-5}$$

является $A$-линейным гомоморфизмом.

Упражнение 5.14. Убедитесь в этом.

Для простого $A$-модуля $U$ образ канонической свёртки (5-5) обозначается $W_U = \operatorname{im} c_{WU} \subset W$ и называется *$U$-изотипной компонентой* модуля $W$. Он равен сумме всех имеющихся в $W$ неприводимых подмодулей, изоморфных модулю $U$. Действительно, всякий ненулевой гомоморфизм $\psi : U \to W$ инъективен, и любой вектор вида $\sum \psi_i(u_i) \in W$ с $u_i \in U$ и $\psi_i \in \mathrm{Hom}_A(U, W)$ лежит в сумме подмодулей $\psi_i(U) \subset W$, каждый из которых изоморфен $U$, и наоборот, если векторы $v_i = \psi_i(u_i)$ лежат в образах $A$-линейных вложений $\psi_i : U \hookrightarrow W$, то $\sum v_i = c(\sum \psi_i \otimes u_i)$.

[1] См. лем. 5.2 на стр. 66.

Предложение 5.2
Всякий гомоморфизм $A$-модулей $\varphi : V \to W$ переводит $U$-изотипную компоненту $V_U \subset V$ в $U$-изотипную компоненту $W_U \subset W$. В частности, для любого подмодуля $V \subset W$ выполнено равенство $V_U = V \cap W_U$.

Доказательство. Гомоморфизм $\varphi$ переводит любой лежащий в $\operatorname{im} c_{VU}$ вектор $\sum \psi_i(u_i)$, у которого $\psi_i \in \operatorname{Hom}_A(U,V)$, а $u_i \in U$, в вектор $\sum \varphi\psi_i(u_i) \in \operatorname{im} c_{WU}$, ибо $\varphi\psi_i \in \operatorname{Hom}_A(U,W)$. □

Предложение 5.3
Над алгебраически замкнутым полем $\Bbbk$ для любого неприводимого $A$-модуля $U$ и произвольного $A$-модуля $W$ каноническая свёртка (5-5) инъективна и, тем самым, задаёт изоморфизм

$$c_{WU} : \operatorname{Hom}_A(U,W) \otimes U \xrightarrow{\sim} W_U .$$

Доказательство. Будучи линейно порождённым простыми подмодулями, изоморфными $U$, модуль $W_U$ полупрост и раскладывается в прямую сумму $W_U = \bigoplus_i V_i$ простых подмодулей $V_i$, каждый из которых изоморфен $U$. Зафиксируем для каждого $i$ вложение $\psi_i : U \hookrightarrow W$, изоморфно отображающее $U$ на подмодуль $V_i \subset W$. По сл. 5.2 пространство $\operatorname{Hom}_A(U,W) = \operatorname{Hom}_A(U,W_U) = \bigoplus_i \operatorname{Hom}_A(U,V_i)$ является прямой суммой одномерных пространств, порождённых вложениями $\psi_i$. Поэтому каждый элемент модуля $\operatorname{Hom}_A(U,W) \otimes U$ однозначно записывается в виде $\sum \psi_i \otimes u_i$ с $u_i \in U$. Если $c_{WU}(\sum \psi_i \otimes u_i) = \sum \psi_i(u_i) = 0$, то каждое слагаемое $\psi_i(u_i) \in V_i$ равно нулю в отдельности, ибо сумма $W_U = \bigoplus_i V_i$ прямая. Так как все $\psi_i$ инъективны, все $u_i = 0$. □

Предложение 5.4 (изотипное разложение)
Если $A$-модуль $W$ полупрост, то в любом его разложении в прямую сумму простых подмодулей сумма тех слагаемых, что изоморфны $U$, совпадает с $U$-изотипной компонентой $W_U \subset W$. В частности, она не зависит от выбора разложения $W$ в прямую сумму простых подмодулей, и если зафиксировать в каждом классе изоморфных простых модулей какой-нибудь представитель $U$, то всякий полупростой модуль будет иметь каноническое *изотипное разложение*

$$W = \bigoplus\nolimits_U W_U , \tag{5-6}$$

где суммирование происходит по всем неизоморфным друг другу неприводимым $A$-модулям $U$, для которых $\operatorname{Hom}_A(U,W) \neq 0$.

Доказательство. Пусть $W = \bigoplus_i W_i$, где все $W_i$ просты. Так как $\operatorname{Hom}_A(U,W) = \bigoplus_i \operatorname{Hom}_A(U,W_i)$ и $\operatorname{Hom}_A(U,W_j) = 0$ для всех $W_j \not\simeq U$, образ канонической свёртки (5-5) лежит в сумме тех подмодулей $W_i$, что изоморфны $U$. □

Определение 5.1
Для простого модуля $U$ и полупростого модуля $W$ количество изоморфных $U$ слагаемых в любом разложении модуля $W$ в прямую сумму неприводимых подмодулей, обозначается

$$m_U \overset{\text{def}}{=} \dim W_U / \dim U , \tag{5-7}$$

и называется *кратностью* простого модуля $U$ в полупростом модуле $W$.

Следствие 5.6
Для конечномерных полупростых $A$-модулей $V$, $W$ над алгебраически замкнутым полем выполняется равенство $\dim \mathrm{Hom}_A(V,W) = \sum_U m_U(U)\, m_U(W) = \dim \mathrm{Hom}_A(W,V)$, где суммирование происходит по всем представителям $U$ различных классов изоморфных простых модулей.

Доказательство. Пусть $V = \bigoplus_i V_i$ и $W = \bigoplus_j W_j$, где все $V_i$ и $W_j$ неприводимы. По лемме Шура пространства $\mathrm{Hom}_A(V_i, W_j)$ нулевые при $V_i \not\simeq W_j$ и одномерные при $V_i \simeq W_j$. Поэтому размерность пространства $\mathrm{Hom}_A(V,W) = \bigoplus_{ij} \mathrm{Hom}_A(V_i, W_j)$ равна $\sum_U m_U(U)\, m_U(W)$, и то же самое верно для $\mathrm{Hom}_A(W,V)$. □

**5.4. Линейные представления группы.** Действие группы $G$ на векторном пространстве $V$ линейными преобразованиями или, что то же самое, гомоморфизм групп $\varrho : G \to \mathrm{GL}(V)$, называется *линейным представлением* группы $G$ в векторном пространстве $V$. Пространство $V$ называется в этом случае $G$-модулем. Прямая сумма, тензорное произведение, а также внешние и симметрические степени $G$-модулей $U$, $W$ канонически наделяются такими структурами $G$-модулей, что операторы $g \in G$ действуют по правилам

$$g(u \dotplus w) \overset{\text{def}}{=} (gu) \dotplus (gw) \qquad g(u \otimes w) \overset{\text{def}}{=} (fu) \otimes (gw)$$
$$g(u_1 \wedge u_2) \overset{\text{def}}{=} (gu_1) \wedge (gu_2) \qquad g(u_1 \cdot u_2) \overset{\text{def}}{=} (gu_1) \cdot (gu_2)\,.$$

Для любого $G$-подмодуля $V \subset W$ фактор пространство $W/V$ также является $G$-модулем с действием $g[v] \overset{\text{def}}{=} [gv]$.

Упражнение 5.15. Убедитесь, что все эти формулы корректно задают гомоморфизмы группы $G$ в $\mathrm{GL}(U \oplus W)$, $\mathrm{GL}(U \otimes W)$, $\mathrm{GL}\big(\Lambda(U)\big)$, $\mathrm{GL}\big(S(U)\big)$ и $\mathrm{GL}(W/V)$ соответственно.

Для каждого представления $\varrho : G \to \mathrm{GL}(V)$ *двойственное представление* $\varrho^* : G \to \mathrm{GL}(V^*)$ определяется таким образом, чтобы свёртка векторов с ковекторами была $G$-инвариантна, т. е.

$$\forall\, g \in G,\ \forall\, \xi \in V^*,\ \forall\, w \in V \quad \langle\, \varrho^*(g)\,\xi\,,\, \varrho(g)\,w\,\rangle = \langle\, \xi\,,\, w\,\rangle\,. \tag{5-8}$$

Так как каждый оператор $\varrho(g)$ обратим, равенство (5-8) равносильно равенству

$$\langle\, \varrho^*(g)\xi\,,\, v\,\rangle = \langle\, \xi\,,\, \varrho(g^{-1})v\,\rangle\,,$$

которое означает, что оператор $\varrho^*(g) = \varrho(g^{-1})^*$ двойствен оператору $\varrho(g)^{-1}$ и переводит ковектор $\xi \in V^*$ в композицию $\xi \circ g^{-1} : v \mapsto \xi(g^{-1}v)$. В частности, матрица оператора $\varrho^*(g)$ в двойственном базисе получается из матрицы $\varrho(g)$ обращением и транспонированием.

Упражнение 5.16. Убедитесь, что $\varrho^* : G \to \mathrm{GL}(V^*)$ является гомоморфизмом групп.

Для любых двух представлений $\varrho : G \to \mathrm{GL}(U)$ и $\lambda : G \to \mathrm{GL}(W)$ представление $\varrho^* \otimes \lambda$ задаёт действие группы $G$ на пространстве $U^* \otimes V \simeq \mathrm{Hom}(U,V)$ всех линейных операторов $\varphi : U \to V$ по правилу

$$g : \varphi \mapsto g\varphi g^{-1}\,. \tag{5-9}$$

Упражнение 5.17. Убедитесь в этом.

Подпространство неподвижных векторов представления (5-9) обозначается

$$\mathrm{Hom}_G(U,V) \overset{\text{def}}{=} \{\varphi : U \to V \mid \forall\, g \in G\ \, g\varphi = \varphi g\}$$

и называется пространством $G$-*инвариантных* операторов[1].

[1] А также *сплетающих* операторов, $G$-*линейных* операторов или $G$-*гомоморфизмов*.

Лемма 5.3
Пусть $|G| = n$, а основное поле $\Bbbk$ содержит все $n$ корней $n$-той степени из единицы и $\operatorname{char} \Bbbk \nmid n$. Тогда в любом конечномерном представлении группы $G$ над полем $\Bbbk$ все её элементы действуют диагонализуемыми операторами.

Доказательство. Каждый оператор из группы $G$ аннулируются многочленом $t^n - 1$, который в силу сделанных предположений не имеет кратных корней и полностью раскладывается в $\Bbbk[t]$ на линейные множители. По упр. 5.4 такой оператор диагонализуем. □

**5.4.1. Представления конечных абелевых групп.** Пусть $G$ — конечная абелева группа, основное поле $\Bbbk$ алгебраически замкнуто, и $\operatorname{char}(\Bbbk) \nmid |G|$. Из лем. 5.3 и сказанного в прим. 5.2 на стр. 64 следует, что всякое конечномерное линейное представление группы $G$ является прямой суммой одномерных. Так как любой линейный оператор на одномерном пространстве $V$ скалярен, операторы $g \in G$ действуют на векторы $v \in V$ по правилу

$$gv = \chi(g)\, v\,, \text{ где } \chi : \ G \to \Bbbk^* \text{ — мультипликативный гомоморфизм,} \tag{5-10}$$

сопоставляющий элементу $g \in G$ тот скаляр, которым он действует на $V$. Гомоморфизмы абелевой группы $G$ в мультипликативную группу поля $\Bbbk$ называются *мультипликативными характерами* группы $G$. Одномерный $G$-модуль, на котором $G$ действует по формуле (5-10) обозначается через $V_\chi$.

Упражнение 5.18. Убедитесь, что $V_\chi \simeq V_\psi$ как $G$-модули если и только если $\chi = \psi$ как гомоморфизмы из $G$ в $\Bbbk^*$.

Поскольку $\chi(g)^{|G|} = \chi\left(g^{|G|}\right) = \chi(e) = 1$ для всех $g \in G$, множество значений любого характера лежит в мультипликативной подгруппе $\boldsymbol{\mu}_{|G|}(\Bbbk) \subset \Bbbk^*$ корней $|G|$-той степени из 1 в поле $\Bbbk$. Сами характеры образуют мультипликативную абелеву подгруппу в алгебре $\Bbbk^G$ всех функций на группе $G$ со значениями в поле $\Bbbk$. Эта группа обозначается $G^\wedge$ и называется *двойственной по Понтрягину* к группе $G$. Единицей в $G^\wedge$ служит *тривиальный характер* $\chi_{\mathbb{1}} \equiv 1$, отвечающий тривиальному представлению. Обратный к $\chi \in G^\wedge$ характер $\chi^{-1}$ действует по правилу $\chi^{-1}(g) \overset{\text{def}}{=} \chi(g)^{-1} = \chi(g^{-1})$.

Упражнение 5.19. Проверьте, что характер тензорного произведения одномерных представлений абелевой группы равен произведению их характеров, а характер двойственного представления обратен характеру исходного.

Пример 5.3 (представление в пространстве функций на группе)
Группа $G$ действует на пространстве $\Bbbk^G$ функций $G \to \Bbbk$ по правилу $g : \ f(x) \mapsto f(g^{-1}x)$.

Упражнение 5.20. Убедитесь, что для любой (в том числе неабелевой) группы $G$ это правило задаёт гомоморфизм группы $G$ в группу линейных автоморфизмов пространства $\Bbbk^G$.

Для каждого характера $\chi \in G^\wedge$ изотипная компонента $\Bbbk^G_\chi$ представления группы $G$ в пространстве $\Bbbk^G$ состоит из таких функций $f : \ G \to \Bbbk$, что $f(g^{-1}x) = \chi(g)f(x)$ для всех $x, g \in G$. Каждая такая функция пропорциональна характеру $\chi^{-1}$, обратному к $\chi$ в группе $G^\wedge$, поскольку полагая в предыдущем равенстве $x = e$, получаем $f(g^{-1}) = \chi(g)\, f(e)$ для всех $g \in G$, откуда, переобозначая $g^{-1}$ через $h$, получаем для всех $h \in G$ равенство $f(h) = f(e)\chi(h^{-1}) = f(e)\chi^{-1}(h)$. Таким образом, каждая изотипная компонента представления $\Bbbk^G$ одномерна, и изотипное разложение пространства функций на группе $G$ имеет вид $\Bbbk^G = \bigoplus_{\chi \in G^\wedge} \Bbbk\, \chi$, т. е. в представлении группы $G$ на пространстве функций $G \to \Bbbk$ содержится с кратностью один каждое из неприводимых представлений группы $G$. В частности, $|G^\wedge| = |G|$ и характеры образуют базис пространства функций на группе $G$ со значениями в поле $\Bbbk$.

Упражнение 5.21. Покажите, что всякое множество различных гомоморфизмов $G \to \Bbbk^*$ произвольной (не обязательно абелевой) группы $G$ в мультипликативную группу любого поля $\Bbbk$ линейно независимо в пространстве $\Bbbk^G$.

Теорема 5.3 (двойственность Понтрягина)
Для каждого $g \in G$ функция вычисления $\mathrm{ev}_g : G^\wedge \to \Bbbk$, $\chi \mapsto \chi(g)$, является характером группы $G^\wedge$, а отображение $G \to G^{\wedge\wedge}$, $g \mapsto \mathrm{ev}_g$ является изоморфизмом групп.

Доказательство. Первое утверждение проверяется выкладкой

$$\mathrm{ev}_g(\chi_1\chi_2) = \chi_1(g)\,\chi_2(g) = \mathrm{ev}_g(\chi_1) \cdot \mathrm{ev}_g(\chi_2)\,.$$

Равенства $\mathrm{ev}_{g_1g_2}(\chi) = \chi(g_1g_2) = \chi(g_1) \cdot \chi(g_2) = \mathrm{ev}_{g_1}(\chi)\ \mathrm{ev}_{g_2}(\chi)$ показывают, что отображение $g \mapsto \mathrm{ev}_g$ является гомоморфизмом групп. Если элемент $g \in G$ лежит в его ядре, то $\chi(g) = 1$ для всех $\chi \in G^\wedge$ и $g$ тривиально действует в любом конечномерном представлении группы $G$. Поэтому $f(g^{-1}x) = f(x)$ для любой функции $f : G \to \Bbbk$, что возможно только при $g = e$. Поскольку $|G^{\wedge\wedge}| = |G|$, инъективность гомоморфизма $g \mapsto \mathrm{ev}_g$ влечёт его биективность. □

Замечание 5.1. (преобразование Фурье) Двойственность Понтрягина имеет место в классе всех локально компактных топологических абелевых групп, и конечные абелевы группы являются лишь простейшими примерами таких групп. В качестве двойственной к произвольной локально компактной топологической абелевой группе $G$ берётся группа $G$ *непрерывных* гомоморфизмов $G \to \mathbb{C}^*$. Например, мультипликативная группа $\mathrm{U}(1)$ комплексных чисел единичной длины двойственна по Понтрягину аддитивной группе целых чисел $\mathbb{Z}$: каждому $n \in \mathbb{Z}$ отвечает характер $\mathrm{U}(1) \to \mathbb{C}^*$, $z \mapsto z^n$, а каждому $e^{2\pi i t} \in \mathrm{U}(1)$ — характер $\mathbb{Z} \to \mathbb{C}^*$, $m \mapsto e^{2\pi i m t}$. Аддитивная группа $\mathbb{R}$ вещественных чисел двойственна сама себе: каждому $\alpha \in \mathbb{R}$ отвечает характер $\mathbb{R} \to \mathbb{C}^*$, $x \mapsto e^{2\pi i \alpha x}$. Сказанное в прим. 5.3 выше также обобщается: каждая достаточно регулярная функция на группе единственным образом «линейно выражается» через характеры. Для группы $\mathrm{U}(1)$ это означает разложение функции $f : \mathrm{U}(1) \to \mathbb{C}$ в бесконечный ряд Фурье

$$f(z) = \sum_{m\in\mathbb{Z}} f^\wedge(m)\, z^m$$

с коэффициентами $f^\wedge(m) \in \mathbb{C}$, которые можно воспринимать как функцию $f^\wedge : \mathbb{Z} \to \mathbb{C}$ на двойственной по Понтрягину группе. Для аддитивной группы $\mathbb{R}$ «линейное выражение» через характеры означает представление функции $f : \mathbb{R} \to \mathbb{C}$ в виде интеграла Фурье

$$f(x) = \int_{-\infty}^{+\infty} f^\wedge(\alpha)\, e^{2\pi i \alpha x}\, d\alpha\,,$$

в котором «семейство коэффициентов» $f^\wedge(\alpha)$ представляет собою функцию $f^\wedge : \mathbb{R} \to \mathbb{C}$ на двойственной по Понтрягину группе. Функции $f : G \to \mathbb{C}$ и $f^\wedge : G^\wedge \to \mathbb{C}$ однозначно восстанавливаются друг по другу по простым явным формулам[1], и с учётом двойственности Понтрягина $f^{\wedge\wedge} = f$. Инволюция $f \leftrightarrow f^\wedge$ называется *преобразованием Фурье*.

[1] Для конечных (в том числе неабелевых) групп мы напишем эти формулы в n° 6.2.1 на стр. 86 ниже.

**5.4.2. Проектор на инварианты.** Рассмотрим теперь линейное представление $V$ произвольной, не обязательно абелевой, группы $G$. Векторы, неподвижные относительно всех преобразований из $G$, образуют в $V$ *подмодуль $G$-инвариантов*, обозначаемый

$$V^G \overset{\text{def}}{=} \{ v \in V \mid gv = v \ \ \forall g \in G \} .$$

Если группа $G$ конечна и её порядок не делится на характеристику поля $\Bbbk$, каждое линейное представление $V$ группы $G$ допускает $G$-инвариантную проекцию на подмодуль инвариантов. Она обозначается $v \mapsto v^\natural$ («$v$-бекар») и сопоставляет вектору $v \in V$ центр тяжести[1] его $G$-орбиты в аффинном пространстве $\mathbb{A}(V)$:

$$v^\natural \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} gv \,, \tag{5-11}$$

Упражнение 5.22. Убедитесь прямым вычислением, что при $\mathrm{char}(\Bbbk) \nmid |G|$ оператор $v \mapsto v^\natural$ перестановочен с действием $G$ и линейно проектирует $V$ на $V^G$, а также приведите пример конечной группы $G$ и неразложимого $G$-модуля $V$ над конечным полем $\Bbbk$, имеющего ненулевой подмодуль инвариантов $V^G$.

Теорема 5.4
Любое линейное представление $V$ конечной группы $G$ над полем, характеристика которого не делит $|G|$, вполне приводимо[2].

Доказательство. Покажем, что любой $G$-подмодуль $U \subset V$ является образом $G$-инвариантного проектора[3]. Группа $G$ действует на пространстве $\Bbbk$-линейных отображений $\mathrm{Hom}(V, U)$ по правилу $g : \varphi \mapsto g\varphi g^{-1}$. Достаточно убедиться в том, что проекция на инварианты этого действия

$$\varphi \mapsto \varphi^\natural = |G|^{-1} \sum_{g \in G} g \varphi g^{-1}$$

переводит любой проектор $\pi : V \twoheadrightarrow U$ тоже в проектор $V$ на $U$. Поскольку $g\pi g^{-1} U \subset U$ для всех $g \in G$, образ $\mathrm{im}\, \pi^\natural \subset U$. С другой стороны, любой вектор $u \in U$ неподвижен относительно $\pi^\natural$, так как $g^{-1} U \subset U$ и $\pi|_U = \mathrm{Id}_U$ влекут $g\pi g^{-1} u = g g^{-1} u = u$. □

**5.5. Групповая алгебра.** С каждой группой $G$ связана ассоциативная алгебра $\Bbbk[G]$, которая называется *групповой алгеброй* группы $G$ над полем $\Bbbk$ и представляет собою векторное пространство с базисом $G$, т. е. состоит из всевозможных формальных линейных комбинаций $\sum_{g \in G} c_g g$ элементов группы с произвольными коэффициентами $c_g \in \Bbbk$, из которых только конечное число отлично от нуля. Сложение и умножение таких выражений происходит по стандартным правилам раскрытия скобок. При этом константы $c_g$ по определению коммутируют с элементами группы и перемножаются так, как это происходит в поле $\Bbbk$, а элементы группы перемножаются согласно имеющемуся в группе закону композиции, т. е.

$$\begin{gathered} \Big(\sum_g a_g g\Big) \Big(\sum_h b_h h\Big) = \sum_{gh} a_g b_h gh = \sum_f c_f f \,, \\ \text{где} \quad c_f = \sum_{gh = f} a_g b_h = \sum_t a_{ft^{-1}} b_t = \sum_s a_s b_{s^{-1} f} \,. \end{gathered} \tag{5-12}$$

[1] Если $|G| \,\vdots\, \mathrm{char}(\Bbbk)$, то сумма весов элементов орбиты нулевая, и центр тяжести не определён.
[2] Т. е. является прямой суммой неприводимых представлений.
[3] См. предл. 5.1 на стр. 67.

Группа $G$ вложена в алгебру $\Bbbk[G]$ в качестве мультипликативной подгруппы. Всякое линейное представление $G \to \mathrm{GL}(V)$ однозначно продолжается по линейности до представления групповой алгебры $\Bbbk[G] \to \mathrm{End}(V)$, образ которого является одновременно и линейной, и ассоциативной оболочкой всех операторов из группы $G$.

Упражнение 5.23. Убедитесь, что правило $m \mapsto t^m$ задаёт изоморфизмы

$$\Bbbk[\mathbb{Z}] \xrightarrow{\sim} \Bbbk[t, t^{-1}] \qquad \text{и} \qquad \Bbbk[\mathbb{Z}/(n)] \xrightarrow{\sim} \Bbbk[t]/(t^n - 1)\,.$$

Если $\mathrm{char}(\Bbbk) \nmid |G|$, то в групповой алгебре $\Bbbk[G]$ имеется *оператор усреднения*

$$\pi_{\mathbb{1}} \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} g \in \Bbbk[G]\,. \tag{5-13}$$

Каждое линейное представление $\varrho : \Bbbk[G] \to \mathrm{End}(V)$ переводит элемент (5-13) в проектор (5-11) на подмодуль $V^G \subset V$ инвариантов представления $\varrho$.

Упражнение 5.24. Покажите, что элемент (5-13) лежит в центре[1] алгебры $\Bbbk[G]$.

**5.5.1. Центр групповой алгебры** конечной группы $G$

$$Z(\Bbbk[G]) \overset{\text{def}}{=} \{z \in \Bbbk[G] \mid \forall\, x \in \Bbbk[G]\ zx = xz\} = \{z \in \Bbbk[G] \mid \forall\, g \in G\ gzg^{-1} = z\}$$

состоит из всех таких линейных комбинаций $z = \sum_h z_h h \in \Bbbk[G]$, коэффициенты которых $z_h$ постоянны на классах сопряжённости. Поэтому элементы

$$z_C = \sum_{h \in C} h\,, \tag{5-14}$$

где $C$ пробегает множество $\mathrm{Cl}(G)$ классов сопряжённости группы $G$, образуют базис $Z(\Bbbk[G])$ как векторного пространства над $\Bbbk$. В частности, $\dim_{\Bbbk} Z(\Bbbk[G]) = |\mathrm{Cl}(G)|$. Мы будем называть это число *числом классов*. Каждое линейное представление $\Bbbk[G] \to \mathrm{End}(V)$ переводит все центральные элементы групповой алгебры в эндоморфизмы пространства $V$, перестановочные со всеми операторами из группы $G$. Из теоремы Бернсайда[2] вытекает, что в любом неприводимом представлении над алгебраически замкнутым полем все центральные элементы действуют умножениями на скаляры.

**5.5.2. Изотипные разложения.** Пусть $G$ — конечная группа. Зафиксируем в каждом классе изоморфных неприводимых представлений группы $G$ какого-нибудь представителя

$$\lambda : G \to \mathrm{GL}(U_\lambda)$$

и обозначим множество всех таких представителей через $\mathrm{Ir}(G)$. По теор. 5.4 на стр. 74 и предл. 5.4 на стр. 70 каждый конечномерный $G$-модуль $V$ обладает *изотипным разложением*

$$V = \bigoplus_{\lambda \in \mathrm{Ir}(G)} V_\lambda\,, \tag{5-15}$$

[1] Напомню, что *центром* кольца или группы $K$ называется множество всех элементов, мультипликативно коммутирующих со всеми элементами $K$.

[2] См. сл. 5.5 на стр. 69.

каждая компонента $V_\lambda$ которого является суммой всех простых подмодулей, изоморфных данному $U_\lambda \in \mathrm{Ir}(G)$. Подмодуль $V_\lambda \subset W$ является образом канонической свёртки

$$c: \ \mathrm{Hom}_G(U_\lambda, W) \otimes U_\lambda \to V\,, \ \ \varphi \otimes u \mapsto \varphi(u)\,. \tag{5-16}$$

В любом разложении $V$ в прямую сумму простых $G$-модулей сумма всех изоморфных $U_\lambda$ слагаемых совпадает[1] с $V_\lambda$, и их количество $m_\lambda(V) = \dim V_\lambda / \dim U_\lambda$ называется *кратностью* неприводимого представления $\lambda$ в представлении $V$. Если поле $\Bbbk$ алгебраически замкнуто, каноническая свёртка (5-16) является изоморфизмом на изотипную компоненту $V_\lambda$, и для любых двух представлений $V$ и $W$ группы $G$

$$\dim \mathrm{Hom}_G(V, W) = \sum_{\lambda \in \mathrm{Ir}(G)} m_\lambda(V)\, m_\lambda(W) = \dim \mathrm{Hom}_G(W, V)\,. \tag{5-17}$$

Пример 5.4 (левое регулярное представление)
Для каждого $\lambda \in \mathrm{Ir}(G)$ обозначим через $I_\lambda \subset \Bbbk[G]$ $\lambda$-изотипную компоненту *левого регулярного представления* $g : x \mapsto gx$ группы $G$ в $\Bbbk[G]$. Таким образом,

$$\Bbbk[G] = \bigoplus_{\lambda \in \mathrm{Ir}(G)} I_\lambda\,. \tag{5-18}$$

Будучи $G$-подмодулем левого регулярного представления, изотипная компонента $I_\lambda$ является левым идеалом алгебры $\Bbbk[G]$. Правое умножение на любой элемент $h: \ x \to xh$ является $G$-автоморфизмом левого регулярного представления[2] и, стало быть, переводит каждую изотипную компоненту $I_\lambda$ в себя. Поэтому каждая изотипная компонента $I_\lambda$ является двусторонним идеалом алгебры $\Bbbk[G]$. Так как $I_\lambda \cap I_\varrho = 0$ при $\lambda \neq \varrho$, и $I_\lambda I_\varrho \subset I_\lambda \cap I_\varrho$, мы заключаем, что

$$I_\lambda I_\varrho = 0 \quad \text{при} \quad \lambda \neq \varrho\,. \tag{5-19}$$

Упражнение 5.25. Докажите, что $I_\lambda$ являются минимальными по включению ненулевыми двусторонними идеалами алгебры $\Bbbk[G]$, и что все двусторонние идеалы $\Bbbk[G]$ в исчерпываются прямыми суммами идеалов $I_\lambda$.

Лемма 5.4
Любое представление $\varrho: \ \Bbbk[G] \to \mathrm{End}(V)$, не содержащее в своём разложении неприводимого представления $\lambda$, переводит изотипный идеал $I_\lambda \subset \Bbbk[G]$ в нуль.

Доказательство. Поскольку $I_\lambda$ является левым идеалом в $\Bbbk[G]$, для любого вектора $v \in V$ подпространство $I_\lambda v = \{fv \mid f \in I_\lambda\}$ является $G$-подмодулем в $V$, и правило $f \mapsto fv$ задаёт сюрьективный гомоморфизм $G$-модулей $I_\lambda \twoheadrightarrow I_\lambda v$. Поскольку такой гомоморфизм переводит $\lambda$-изотипный подмодуль в $\lambda$-изотипный, подмодуль $I_\lambda v$ содержится в изотипной компоненте $V_\lambda$ представления $V$. Если она нулевая, то $I_\lambda v = 0$ для всех $v \in V$. □

[1] См. предл. 5.4 на стр. 70.

[2] Ибо левое и правое умножение на любые два фиксированных элемента группы перестановочны друг с другом.

Теорема 5.5 (теорема Машке)
Над алгебраически замкнутым полем $\Bbbk$ гомоморфизм алгебр

$$\mathfrak{rep}: \Bbbk[G] \to \prod_{\lambda \in \mathrm{Ir}(G)} \mathrm{End}(U_\lambda), \tag{5-20}$$

переводящий элемент $f \in \Bbbk[G]$ в набор операторов, которыми этот элемент действует во всех неприводимых представлениях группы $G$, является изоморфизмом алгебр. Его ограничение на изотипный идеал $I_\lambda \subset \Bbbk[G]$ является изоморфизмом $I_\lambda$ на матричную алгебру $\mathrm{End}(U_\lambda)$.

Доказательство. Сначала установим инъективность гомоморфизма $\mathfrak{rep}$. Если элемент $h \in \Bbbk[G]$ действует нулевым оператором во всех неприводимых представлениях, то он действует нулевым оператором вообще на любом конечномерном $G$-модуле, в частности — в левом регулярном представлении. Но $f \cdot 1 = 0$ влечёт $f = 0$. Для доказательства последнего утверждения заметим, что по лем. 5.4 на стр. 76 каждое неприводимое представление $\lambda: \Bbbk[G] \to \mathrm{End}(U_\lambda)$ отображает в нуль все прямые слагаемые разложения (5-18) за исключением $I_\lambda$. Однако по теореме Бернсайда[1] оно эпиморфно. Поэтому ограничение $\mathfrak{rep}|_{I_\lambda}: I_\lambda \xrightarrow{\sim} \mathrm{End}(U_\lambda)$ является изоморфизмом. Отсюда сразу следует, что неприводимых представлений $U_\lambda$ имеется лишь конечное число и каждое из них присутствует в изотипном разложении (5-18) левого регулярного представления с кратностью $m_\lambda(\Bbbk[G]) = \dim(I_\lambda) / \dim(U_\lambda) = \dim \mathrm{End}(U_\lambda) / \dim U_\lambda = \dim U_\lambda$. Для доказательства сюрьективности гомоморфизма $\mathfrak{rep}$ остаётся заметить, что по уже доказанному для любого набора операторов $\varphi_\lambda \in \mathrm{End}(U_\lambda)$ найдутся такие элементы $f_\lambda \in I_\lambda$, что $\lambda(f_\lambda) = \varphi_\lambda$. Поскольку $\varrho(f_\lambda) = 0$ для всех неприводимых $\varrho \neq \lambda$, мы заключаем, что $\mathfrak{rep}(\sum_\lambda f_\lambda) = \prod_\lambda \varphi_\lambda$. □

Следствие 5.7
Число неприводимых представлений конечной группы $G$ над алгебраически замкнутым полем $\Bbbk$, характеристика которого не делит $|G|$, конечно и равно числу классов сопряжённости $|\mathrm{Cl}(G)|$ группы $G$, а сумма квадратов размерностей всех неприводимых равна порядку $|G|$. При этом $m_\lambda(\Bbbk[G]) = \dim U_\lambda$.

Доказательство. Первое утверждение вытекает из того, что размерность центра прямой суммы матричных алгебр равна количеству слагаемых, второе — из равенства размерностей правого и левого пространств в (5-20). □

Пример 5.5 (простенькие представления симметрических групп)
Сопоставление перестановке $g \in S_n$ её циклового типа устанавливает биекцию между классами сопряжённых элементов в $S_n$ и $n$-клеточными диаграммами Юнга[2]. Таким образом, неприводимые представления симметрической группы $S_n$ биективно соответствуют $n$-клеточным диаграммам Юнга. У каждой симметрической группы $S_n$ есть два одномерных представления: тривиальное и *знаковое*, в котором перестановка $\sigma$ действует умножением на знак $\mathrm{sgn}(\sigma)$. Если характеристика поля не делит $n$, операторы симметризации и альтернирования

$$\mathrm{sym}_n = \frac{1}{n!} \sum_{g \in S_n} g \quad \text{и} \quad \mathrm{alt}_n = \frac{1}{n!} \sum_{g \in S_n} \mathrm{sgn}(g)\, g$$

[1] См. сл. 5.5 на стр. 69.
[2] Длины строк диаграммы суть длины независимых циклов, на которые раскладывается перестановка.

являются $S_n$-инвариантными проекторами на тривиальную и знаковую изотипные компоненты любого $S_n$-модуля.

Упражнение 5.26. Убедитесь в этом.

Тавтологическое $n$-мерное представление группы $S_n$ перестановками стандартных базисных векторов $e_i$ пространства $\Bbbk^n$ имеет тривиальный одномерный подмодуль, порождённый суммой $e = e_1 + \cdots + e_n$ всех базисных векторов. Индуцированное $(n-1)$-мерное представление в фактор пространстве $\Bbbk^n/\Bbbk\, e$ называется *симплициальным*[1], поскольку над полем $\mathbb{R}$ его образ представляет собою полную группу правильного $(n-1)$-мерного симплекса в $\mathbb{R}^{n-1} = \mathbb{R}^n/\mathbb{R}\cdot e$ с центром в нуле и вершинами в классах векторов $e_i$ по модулю $e$.

Упражнение 5.27. Покажите, что симплициальное представление неприводимо.

Неприводимые представления группы $S_3$, имеющей ровно три класса сопряжённости, исчерпываются тривиальным и знаковым одномерными представлениями и двумерным представлением $U_\Delta$ группой треугольника, что согласуется с равенством $1^2+1^2+2^2=6$. Инвариантный проектор на $U_\Delta$-изотипную компоненту любого представления задаётся оператором

$$\pi_\Delta \overset{\text{def}}{=} 1 - \mathrm{sym}_3 - \mathrm{alt}_3 = 1 - \frac{1}{6}\sum_{g\in S_3}(1+\mathrm{sgn}(g))g = 1 - \frac{1}{3}\left(1+\tau+\tau^2\right)\,,$$

где $\tau = |123\rangle \in S_3$ это цикл длины 3.

Упражнение 5.28. Проверьте прямым вычислением в групповой алгебре, что $\pi_\Delta$ идемпотентен и лежит в центре, аннулирует тривиальный и знаковый модули, и тождественно действует в представлении группой треугольника.

У группы $S_4$, имеющей 5 классов сопряжённости, кроме одномерного тривиального, одномерного знакового и 3-мерного представления несобственной группой тетраэдра имеется ещё одно трёхмерное представление несобственной группой куба, а также двумерное представление группой треугольника, возникающее из факторизации $S_4 \twoheadrightarrow S_3$ по подгруппе Клейна $D_2 \subset S_4$. Равенство $2\cdot 1^2 + 2\cdot 3^2 + 2^2 = 24$ указывает на то, что это хорошие кандидаты на полный список неприводимых представлений.

Упражнение 5.29. Покажите, что два трёхмерных представления не изоморфны и получаются одно из другого тензорным умножением на знаковое представление.

**5.6. Представления Шура полной линейной группы.** Пусть $\Bbbk$ — произвольное поле характеристики нуль, а $V$ ненулевое конечномерное векторное пространство над $\Bbbk$. Симметрическая группа $S_n$ действует на $V^{\otimes n}$ перестановками сомножителей в разложимых тензорах. Изотипное разложение этого представления

$$V^{\otimes n} = \bigoplus_{\lambda\in\mathrm{Ir}(S_n)} V_\lambda^{\otimes n} \tag{5-21}$$

называется разложением по *типам симметрии* тензоров. Про тензоры, лежащие в изотипной компоненте $V_\lambda^{\otimes n}$, говорят, что они имеют тип симметрии $\lambda$.

Пример 5.6 (квадратичные и кубические тензоры)
Два неприводимых представления группы $S_2 \simeq \mathbb{Z}/(2)$ задают разложение тензорного квадрата

$$V^{\otimes 2} = \mathrm{Sym}^2(V) \oplus \mathrm{Skew}^2(V)\,.$$

[1] При $n=2$ оно совпадает со знаковым.

Группа $S_2$ действует на первом слагаемом тривиально, на втором — знакопеременно. Трём неприводимым представлениям группы $S_3$: тривиальному, знаковому и группой треугольника отвечает разложение

$$V^{\otimes 3} = \mathrm{Sym}^3(V) \oplus \mathrm{Skew}^3(V) \oplus V_\Delta^{\otimes 3}\,, \tag{5-22}$$

компоненты которого являются образами $S_3$-инвариантных проекторов $\mathrm{sym}_3$, $\mathrm{alt}_3$ и $\pi_\Delta$, описанных в прим. 5.5. Пространство неподвижных тензоров последнего

$$V_\Delta^{\otimes 3} = \{t \in V^{\otimes 3} \mid t + \tau t + \tau^2 t = 0\}$$

состоит из всех кубических тензоров, которые аннулируются усреднением по 3-циклу. Такие тензоры называются *лиевскими*[1], а соотношение $t + \tau t + \tau^2 t = 0$, которому они удовлетворяют, называется *тождеством Якоби*. $S_3$-орбита каждого лиевского тензора порождает в $V^{\otimes 3}$ двумерное векторное пространство, на котором $S_3$ действует как группа треугольника. Примером лиевского тензора служит $[u,[u,w]] = u\otimes u\otimes w - 2\,u\otimes w\otimes u + w\otimes u\otimes u$, где $u, w \in V$ — линейно независимые векторы, а $[a,b] \overset{\text{def}}{=} a\otimes b - b\otimes a$ обозначает коммутатор в тензорной алгебре $T(V)$.

Упражнение 5.30. Покажите, что подпространство $V_\Delta^{\otimes 3} \subset V^{\otimes 3}$ является линейной оболочкой всех кубических тензоров, которые можно получить из векторов пространства $V$ при помощи бинарной операции взятия коммутатора в $T(V)$.

**5.6.1. Действие $\mathrm{GL}(V)\times S_n$ на $V^{\otimes n}$.** Гомоморфизм групп

$$\mathrm{GL}(V) \to \mathrm{GL}(V^{\otimes n})\,, \quad f \mapsto f^{\otimes n}\,,$$

задаёт представление полной линейной группы $\mathrm{GL}(V)$ в пространстве $V^{\otimes n}$. В этом представлении оператор $f \in \mathrm{GL}(V)$ действует на разложимые тензоры по правилу

$$f : v_1 \otimes \dots \otimes v_n \mapsto f v_1 \otimes \dots \otimes f v_n\,.$$

Так как это действие перестановочно с действием симметрической группы, пространство $V^{\otimes n}$ является модулем над прямым произведением групп $\mathrm{GL}(V)\times S_n$: элемент $f\times g \in \mathrm{GL}(V)\times S_n$ действует на нём оператором

$$v_1\otimes\dots\otimes v_n \mapsto f(v_{g(1)})\otimes\dots\otimes f(v_{g(n)})\,.$$

Будучи перестановочными с операторами из $S_n$, операторы из $\mathrm{GL}(V)$ переводят в себя каждую изотипную компоненту разложения $V^{\otimes n} = \bigoplus_{\lambda\in\mathrm{Ir}(S_n)} V_\lambda^{\otimes n}$ по типам симметрии тензоров. Тем самым, все $S_n$-изотипные подпространства $V_\lambda^{\otimes n}$ тоже являются $\mathrm{GL}(V)\times S_n$-модулями.

Для каждого неприводимого $S_n$-модуля $U_\lambda$ тензорное произведение

$$\mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right)\otimes U_\lambda$$

является $\mathrm{GL}(V)\times S_n$-модулем с действием $f\times g : \varphi\otimes u \mapsto (f^{\otimes n}\circ\varphi)\otimes(gu)$. По предл. 5.3 свёртка $\varphi\otimes u\mapsto\varphi(u)$ задаёт изоморфизм[2]

$$c : \mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right)\otimes U_\lambda \xrightarrow{\sim} V_\lambda^{\otimes n}\,, \tag{5-23}$$

[1] В честь норвежского математика Софуса Ли.

[2] Строго говоря, предл. 5.3 утверждает это над алгебраически замкнутым полем, однако мы увидим ниже, что все комплексные неприводимые представления группы $S_n$ определены над $\mathbb{Q}$, так что для симметрических групп предл. 5.3 справедливо над $\mathbb{Q}$.

очевидно перестановочный с действием $\mathrm{GL}(V) \times S_n$. Пространство

$$\mathbb{S}^\lambda V \stackrel{\text{def}}{=} \mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right) \tag{5-24}$$

с действием $\mathrm{GL}(V)$ по правилу $f : \varphi \mapsto f^{\otimes n} \circ \varphi$ называется *модулем Шура* над полной линейной группой $\mathrm{GL}(V)$.

Лемма 5.5
Линейная оболочка операторов вида $f^{\otimes n}$ с $f \in \mathrm{GL}(V)$ совпадает с централизатором $\mathrm{End}_{S_n}\left(V^{\otimes n}\right)$ действия $S_n$ на $V^{\otimes n}$.

Доказательство. Цепочка канонических изоморфизмов

$$\mathrm{End}(V^{\otimes n}) \simeq V^{\otimes n*} \otimes V^{\otimes n} \simeq V^{*\otimes n} \otimes V^{\otimes n} \simeq \left(V^* \otimes V\right)^{\otimes n} \simeq \mathrm{End}(V)^{\otimes n}$$

отождествляет подалгебру $\mathrm{End}_{S_n}\left(V^{\otimes n}\right) \subset \mathrm{End}\left(V^{\otimes n}\right)$ с подпространством симметрических тензоров $\mathrm{Sym}^n\big(\mathrm{End}(V)\big) \subset \mathrm{End}(V)^{\otimes n}$, которое линейно порождается тензорами вида $f^{\otimes n}$ с $f \in \mathrm{GL}(V)$ в силу следующего общего принципа:

Упражнение 5.31 (принцип Аронгольда). Покажите, что для любого конечномерного векторного пространства $W$ над полем характеристики нуль пространство симметрических тензоров $\mathrm{Sym}^n(W) \subset W^{\otimes n}$ линейно порождается тензорами вида $w^{\otimes n} = w \otimes \cdots \otimes w$.

Упражнение 5.32 (усиленный принцип Аронгольда). В условиях упр. 5.31 покажите, что для любого ненулевого многочлена $F$ на $W$ пространство $\mathrm{Sym}^n(W)$ линейно порождается тензорами $w^{\otimes n}$ с $F(w) \neq 0$.

Применяя усиленный принцип Аронгольда к $W = \mathrm{End}(V)$ и $F = \det$, получаем утверждение леммы. □

Предложение 5.5
Все $\mathrm{GL}(V)$-модули Шура $\mathbb{S}^\lambda V = \mathrm{Hom}_{S_n}\left(U_\lambda, V^{\otimes n}\right)$ неприводимы.

Доказательство. Изоморфизм $\mathbb{S}^\lambda V \otimes U_\lambda \simeq V_\lambda^{\otimes n}$ из формулы (5-23) переводит действие $S_n$ на $V_\lambda^{\otimes n}$ в действие $g : \varphi \otimes u \mapsto \varphi \otimes (gu)$. Каждый линейный оператор $F \in \mathrm{End}(\mathbb{S}^\lambda V)$ задаёт линейное преобразование $F : \varphi \otimes u \mapsto F(\varphi) \otimes u$ пространства $\mathbb{S}^\lambda V \otimes U_\lambda$, перестановочное с действием $S_n$. По лем. 5.5 оно лежит в линейной оболочке операторов $f : \varphi \otimes u \mapsto \left(f^{\otimes n} \circ \varphi\right) \otimes u$. Следовательно, образ представления Шура $\mathrm{GL}(V) \to \mathrm{GL}\left(\mathbb{S}^\lambda V\right)$ линейно порождает всю алгебру эндоморфизмов $\mathrm{End}(\mathbb{S}^\lambda V)$ пространства $\mathbb{S}^\lambda(V)$. По упр. 5.13 такое представление неприводимо. □

**5.6.2. Соответствие Шура – Вейля.** Соответствие $U_\lambda \leftrightarrow \mathbb{S}^\lambda V$ между неприводимыми представлениями симметрических групп[1] и неприводимыми представлениями полной линейной группы $\mathrm{GL}(V)$ называется *соответствием Шура – Вейля*. Тривиальному одномерному представлению группы $S_n$ при этом отвечает представление $\mathrm{GL}(V)$ на пространстве $S^n V$, а одномерному знаковому представлению — представление $\mathrm{GL}(V)$ на пространстве $\Lambda^n V$. Можно показать,

[1] Обратите внимание, что количество клеток $n$ в диаграмме $\lambda$ никак не связано с размерностью пространства $V$ и может быть любым, однако некоторые пространства $\mathbb{S}^\lambda V$ при этом могут оказаться нулевыми, как это происходит, к примеру, с внешними степенями $\Lambda^n V$ при $n > \dim V$.

что ненулевые $\mathrm{GL}(V)$-модули $\mathbb{S}^{\lambda}V$ не изоморфны друг другу при разных $\lambda$ и с точностью до тензорных умножений на одномерные представления $\det^m : \mathrm{GL}(V) \to \mathrm{GL}_1(\Bbbk)$, в которых каждый оператор $f \in \mathrm{GL}(V)$ действует умножением на $\det^m(f)$, ими исчерпываются все такие конечномерные неприводимые представления $\varrho : \mathrm{GL}(V) \to \mathrm{GL}(W)$, в которых элементы матрицы $\varrho(f)$ являются рациональными функциями элементов матрицы $f$.

## §6. Представления конечных групп.

Всюду в этом параграфе мы по умолчанию считаем, что $G$ — конечная группа, $\Bbbk$ — алгебраически замкнутое поле, и $\operatorname{char}(\Bbbk) \nmid |G|$.

**6.1. Скалярное произведение и базисные идемпотенты.** Левое регулярное представление

$$L: \Bbbk[G] \hookrightarrow \operatorname{End}(\Bbbk[G]),$$

в котором каждый элемент $f \in \Bbbk[G]$ действует левым умножением $x \mapsto fx$, инъективно вкладывает групповую алгебру в алгебру линейных эндоморфизмов векторного пространства $\Bbbk[G]$. На последней имеется каноническая симметричная билинейная форма — след композиции.

Упражнение 6.1. Убедитесь, что для конечномерного векторного пространства $V$ билинейная форма $\operatorname{End}(V) \times \operatorname{End}(V) \to \Bbbk$, $(A, B) \mapsto \operatorname{tr}(AB)$, принимает на паре разложимых операторов $A = \alpha \otimes a$ и $B = \beta \otimes b$ значение $\alpha(b) \cdot \beta(a)$, и выведите отсюда, что эта форма симметрична и невырождена.

Ограничение следа композиции на образ $L(\Bbbk[G]) \subset \operatorname{End}(\Bbbk[G])$ левого регулярного представления задаёт на $\Bbbk[G]$ симметричное скалярное произведение

$$(f, g) \stackrel{\text{def}}{=} \operatorname{tr}(L_f L_g) = \operatorname{tr}(L_{fg}). \tag{6-1}$$

Так как след левого умножения на единицу группы равен $|G|$, а умножение на любой другой элемент группы бесследно, скалярные произведения элементов группы задаются формулой

$$(g, h) = \begin{cases} |G| & \text{при } h = g^{-1} \\ 0 & \text{при } h \neq g^{-1}. \end{cases} \tag{6-2}$$

Таким образом, скалярное произведение невырождено[1], и двойственным базисом к базису из групповых элементов $g$ является базис из элементов $g^* = g^{-1}/|G|$. В частности, каждый элемент $z \in \Bbbk[G]$ разлагается по базису из групповых элементов в виде

$$z = \frac{1}{|G|} \sum_{g \in G} (g^{-1}, z) \cdot g \tag{6-3}$$

Упражнение 6.2. Покажите, что левое и правое умножение на заданный элемент сопряжены другу другу относительно скалярного произведения: $(fg, h) = (f, gh)$ и выведите отсюда, что ортогональное дополнение к любому левому идеалу в $\Bbbk[G]$ является правым идеалом, а ортогональное дополнение к правому — левым[2].

Изоморфизм $\mathfrak{rep}: \Bbbk[G] \xrightarrow{\sim} \prod_{\lambda \in \operatorname{Ir}(G)} \operatorname{End}(U_\lambda)$ из теоремы Машке[3] позволяет выразить скалярное произведение (6-1) через следы действий в неприводимых представлениях.

Предложение 6.1 (формула Планшереля)
Для всех $f, g \in \Bbbk[G]$ $\quad (f, g) = \sum_{\lambda \in \operatorname{Ir}(G)} \dim(U_\lambda) \cdot \operatorname{tr}\big(\lambda(fg)\big)$.

[1] Отметим, что если характеристика поля делит порядок группы, то это не так.
[2] Тем самым, ортогональное дополнение к любому двустороннему идеалу тоже двусторонний идеал.
[3] См. теор. 5.5 на стр. 77.

Доказательство. Вычислим $\mathrm{tr}(L_{fg})$ в алгебре $\bigoplus_{\lambda\in\mathrm{Ir}(G)}\mathrm{End}(U_\lambda)$. Он равен сумме следов левого умножения на $\lambda(fg)$ в $\mathrm{End}(U_\lambda)$ по всем неприводимым представлениям $\lambda$. След левого умножения на матрицу $M$ в матричной алгебре $\mathrm{Mat}_n(\Bbbk)$ равен $n\cdot\mathrm{tr}(M)$, поскольку каждая матричная единица $E_{ij}$ входит в $ME_{ij}$ с коэффициентом $m_{ii}$. □

Определение 6.1 (базисные идемпотенты)
Элементы $e_\lambda = \mathfrak{rep}^{-1}(0,\dots,0,\mathrm{Id}_{U_\lambda},0,\dots,0)\in I_\lambda\subset\Bbbk[G]$, действующие тождественным оператором в неприводимом представлении $\lambda$ и нулевым оператором во всех остальных неприводимых представлениях, называются *базисными*[1] *идемпотентами.*. Они образуют базис в центре групповой алгебры и перемножаются по правилам

$$e_\lambda e_\varrho = \begin{cases} e_\lambda & \text{при } \varrho=\lambda\\ 0 & \text{при } \varrho\neq\lambda\,.\end{cases} \tag{6-4}$$

В любом представлении $\Bbbk[G]\to\mathrm{End}(V)$ каждый из неприводимых идемпотентов $e_\lambda$ действует как $G$-инвариантный проектор на $\lambda$-изотипную компоненту $V_\lambda\subset V$.

Упражнение 6.3. Проверьте, что главный левый идеал $\Bbbk[G]\cdot e_\lambda$ является минимальным по включению ненулевым левым идеалом и как $G$-модуль[2] изоморфен неприводимому представлению $U_\lambda$. Покажите также, что порождённый $e_\lambda$ двусторонний идеал в $\Bbbk[G]$ равен $I_\lambda$.

Следствие 6.1
Базисные идемпотенты составляют ортогональный базис центра групповой алгебры и имеют скалярные квадраты $(e_\lambda,e_\lambda)=\dim^2 U_\lambda$. □

Следствие 6.2
Разложение $\Bbbk[G]=\bigoplus_{\lambda\in\mathrm{Ir}(G)} I_\lambda$ левого регулярного представления в прямую сумму изотипных подмодулей является *ортогональным* разложением, и неприводимые идемпотенты являются *ортогональными проекциями* единицы $1\in\Bbbk[G]$ на идеалы $I_\lambda$.

Следствие 6.3
Базисный идемпотент $e_\lambda$ выражается через элементы группы по формуле

$$e_\lambda = \frac{\dim U_\lambda}{|G|}\sum_{g\in G}\mathrm{tr}\left(\lambda(g^{-1})\right)\cdot g\,, \tag{6-5}$$

и каждое представление $\Bbbk[G]\to\mathrm{End}(V)$ переводит правую часть этого равенства в $G$-инвариантный проектор на $\lambda$-изотипный подмодуль $V_\lambda\subset V$.

Доказательство. Согласно формуле (6-3) элемент $e_\lambda=|G|^{-1}\sum_{\mu\in\mathrm{Ir}(G)}(g^{-1},e_\lambda)\cdot g$. По формуле Планшереля $(g^{-1},e_\lambda)=\sum_{\mu\in\mathrm{Ir}(G)}\dim(U_\mu)\cdot\mathrm{tr}\big(\mu(g^{-1}e_\lambda)\big)=\dim(U_\lambda)\cdot\mathrm{tr}\big(\lambda(g^{-1})\big)$, так как умножение слева на $e_\lambda$ аннулирует все неприводимые $U_\mu$ с $\mu\neq\lambda$, а на $U_\lambda$ действует тождественным оператором. □

[1] А также *неприводимыми* или *минимальными*

[2] Относительно действия группы $G$ левыми умножениями.

**6.2. Характеры.** Линейная форма на $\Bbbk[G]$, сопоставляющая элементу групповой алгебры след его действия на пространстве $V$ линейного представления $\varrho : G \to \mathrm{GL}(V)$ называется *характером*[1] представления $\varrho$ и обозначается

$$\chi_\varrho : \Bbbk[G] \to \Bbbk\,, \quad \chi_\varrho(f) \overset{\text{def}}{=} \operatorname{tr}\varrho(f)\,. \tag{6-6}$$

Так как след оператора не меняется при сопряжении, характер любого представления постоянен на классах сопряжённых элементов, и изоморфные представления имеют равные характеры. Формула (6-5) для проектора на $\lambda$-изотипную компоненту переписывается в терминах характеров как

$$e_\lambda = \frac{\dim U_\lambda}{|G|} \sum_{g\in G} \chi_\lambda\left(g^{-1}\right)\cdot g\,, \tag{6-7}$$

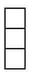
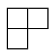
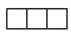
Пример 6.1 (характеры перестановочных представлений)
Если группа $G$ действует на векторном пространстве перестановками базисных векторов, то значение характера такого представления на элементе $g \in G$ равно числу неподвижных элементов перестановки $g$. В частности, характер регулярного представления имеет вид

$$\chi_L(g) = \begin{cases} |G| & \text{если} \quad g = e \\ 0 & \text{если} \quad g \neq e\,. \end{cases}$$

Значение характера тавтологического представления симметрической группы $S_n$ перестановками базисных векторов координатного пространства $\Bbbk^n$ на перестановке циклового типа $\lambda$ равно $m_1(\lambda)$, т. е. числу строк длины 1 в диаграмме $\lambda$. Поскольку это представление является прямой суммой тривиального одномерного, с тождественно единичным характером, и симплициального, мы заключаем, что значение симплициального характера группы $S_n$ на классе сопряжённости $C_\lambda$, состоящем из перестановок циклового типа $\lambda$, равно $\chi_\Delta(C_\lambda) = m_1(\lambda) - 1$.

Упражнение 6.4. Убедитесь, что характеры неприводимых представлений симметрической группы $S_3$ задаются таблицей

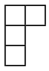
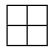
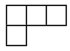
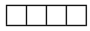
(6-8)

| классы |  |  |  |
|---|---|---|---|
| число элементов | 1 | 3 | 2 |
| значения характеров: | | | |
| тривиального | 1 | 1 | 1 |
| знакового | 1 | −1 | 1 |
| треугольного | 2 | 0 | −1 |

и что проекторы на изотипные компоненты, вычисленные при помощи этой таблицы по формуле (6-7), совпадают с описанными ранее в прим. 5.5 на стр. 77.

[1]Не следует путать эти *аддитивные* характеры с мультипликативными характерами абелевых групп, обсуждавшимися в n° 5.4.1 на стр. 72.

Пример 6.2 (неприводимые характеры $S_4$)
В геометрически заданных представлениях следы можно вычислять складывая собственные значения соответствующих поворотов и отражений. Например, значения характеров пяти представлений симметрической группы $S_4$ из прим. 5.5 задаются таблицей:

| классы |  |  |  |  |  |
|---|---|---|---|---|---|
| число элементов | 1 | 6 | 3 | 8 | 6 |
| значения характеров: | | | | | |
| тривиального | 1 | 1 | 1 | 1 | 1 |
| знакового | 1 | $-1$ | 1 | 1 | $-1$ |
| тетраэдрального | 3 | 1 | $-1$ | 0 | $-1$ |
| кубического | 3 | $-1$ | $-1$ | 0 | 1 |
| треугольного | 2 | 0 | 2 | $-1$ | 0 |

(6-9)

четвёртая строка которой объясняется так: след единицы равен размерности представления; одна транспозиция и пара независимых транспозиций действуют поворотами на 180° вокруг прямой, и собственные числа такого вращения суть 1, $-1$ и $-1$; цикл длины 3 и цикл длины 4 действуют поворотами на 120° и 90° соответственно, и их собственные числа суть 1, $\omega$, $\omega^2$ и 1, $i$, $-i$.

Лемма 6.1
Для любых двух представлений $V$, $W$ группы $G$ с характерами $\chi_U$ и $\chi_V$

$$\chi_{V\oplus W}(g) = \chi_V(g) + \chi_W(g) \tag{6-10}$$
$$\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g) \tag{6-11}$$
$$\chi_{V^*}(g) = \chi_V(g^{-1}) \tag{6-12}$$
$$\chi_{\mathrm{Hom}(V,W)}(g) = \chi_V(g^{-1})\chi_W(g) \tag{6-13}$$

Доказательство. Поскольку любой оператор $g$ из конечной группы полупрост, в пространствах $V$ и $W$ имеются базисы $\{v_i\}$ и $\{w_j\}$ из собственных векторов $g$. Пусть $\alpha_i$ и $\beta_j$ — соответствующие наборы собственных чисел. Набор собственных чисел $g$ в представлении $V \oplus W$ получается объединением этих наборов, откуда следует (6-10). Собственными числами $g$ в представлении $V \otimes W$ являются всевозможные попарные произведения $\alpha_i\beta_j$, что даёт (6-11). Формула (6-12) следует из того, что матрица $g$ в двойственном представлении транспонирована к матрице $g^{-1}$ в исходном (см. n° 5.4). Последняя формула следует из двух предыдущих. □

Упражнение 6.5. Докажите, что производящие функции для характеров симметрических и внешних степеней представления $\varrho :\ G \to \mathrm{GL}(V)$ имеют вид:

$$\sum_{\nu\geqslant 0} \chi_{\Lambda^\nu V}(g)\, t^\nu = \det(1 + t\,\varrho(g)) \quad \text{и} \quad \sum_{\nu\geqslant 0} \chi_{S^\nu V}(g)\, t^\nu = \frac{1}{\det(1 - t\,\varrho(g))}\,.$$

Следствие 6.4
Характер любого представления $V$ выражается через неприводимые характеры $\chi_\lambda$ как

$$\chi_V = \sum_{\lambda\in\mathrm{Ir}(G)} m_\lambda(V)\cdot\chi_\lambda \tag{6-14}$$

где $m_\lambda(V) = \dim V_\lambda / \dim U_\lambda$ обозначает кратность простого $G$-модуля $U_\lambda$ в $V$. □

**6.2.1. Преобразование Фурье.** Поскольку любая линейная форма однозначно задаётся своими значениями на базисных векторах, пространство $\Bbbk[G]^*$ естественно изоморфно пространству $\Bbbk^G$ функций $G \to \Bbbk$. Функция $\varphi : G \to \Bbbk$ задаёт форму $\varphi(\sum x_g \cdot g) = \sum x_g \varphi(g)$, линейно продолжающую $\varphi$ с $G$ на $\Bbbk[G]$. С другой стороны, скалярное произведение на групповой алгебре биективно сопоставляет каждому вектору функционал скалярного умножения на этот вектор:

$$\Bbbk[G] \xrightarrow{\sim} \Bbbk[G]^* , \quad f \mapsto (f, *) . \tag{6-15}$$

Прообразом стандартного базиса в $\Bbbk[G]^*$, двойственного к базису из элементов группы[1], при изоморфизме (6-15) является базис из элементов $g^* = g^{-1}/|G|$. Комбинируя эти два отождествления, получаем изоморфизм векторных пространств

$$\Phi : \Bbbk^G \xrightarrow{\sim} \Bbbk[G] , \quad \varphi \mapsto \widehat{\varphi} \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g\in G} \varphi\left(g^{-1}\right) \cdot g , \tag{6-16}$$

который иногда называют *преобразованием Фурье*. По форм. (6-7) на стр. 84 оно переводит характеры неприводимых представлений в элементы групповой алгебры, пропорциональные неприводимым идемпотентам:

$$\widehat{\chi}_\lambda = \frac{1}{\dim U_\lambda} \cdot e_\lambda . \tag{6-17}$$

Упражнение 6.6. Выясните, в какую операцию на групповой алгебре переходит поточечное умножение значений функций и какая операция над функциями соответствует умножению в групповой алгебре.

Перенесём с помощью изоморфизма (6-16) скалярное произведение из групповой алгебры в пространство функций на группе, т. е. положим

$$(\varphi, \psi) \overset{\text{def}}{=} (\widehat{\varphi}, \widehat{\psi}) = \frac{1}{|G|^2} \sum_{g,h\in G} \varphi(g^{-1})\psi(h^{-1})(g, h) = \frac{1}{|G|} \sum_{g\in G} \varphi(g^{-1})\psi(g) . \tag{6-18}$$

Из (6-17) и сл. 6.1 немедленно вытекают следующие результаты, полностью сводящие анализ представлений к формальным алгебраическим вычислениям с характерами.

Следствие 6.5

Неприводимые характеры образуют ортонормальный базис в пространстве функций, постоянных на классах сопряжённых элементов. □

Следствие 6.6

Для любых $G$-модулей $V$ и $W$ $\quad \dim \mathrm{Hom}_G(V, W) = (\chi_V, \chi_W)$.

Доказательство. Обе части равны $\sum_{\lambda\in \mathrm{Ir}(G)} m_\lambda(V) m_\lambda(W)$: левая — по сл. 5.6, правая — в силу сл. 6.4 и ортонормальности характеров. □

Следствие 6.7

Кратность вхождения неприводимого представления $U_\lambda$ в произвольное представление $V$ равна скалярному произведению их характеров: $m_\lambda(V) = (\chi_\lambda, \chi_V)$.

[1] Ср. с формулами (6-2) и (6-3) на стр. 82.

Доказательство. Скалярно умножаем обе части (6-14) на $\chi_\lambda$ и пользуемся ортонормальностью характеров. □

Следствие 6.8
Представление $V$ неприводимо тогда и только тогда, когда $(\chi_V, \chi_V) = 1$.

Доказательство. В силу ортонормальности неприводимых характеров из сл. 6.4 вытекает, что $(\chi_V, \chi_V) = \sum_{\lambda \in \mathrm{Ir}(G)} m_\lambda^2(V)$, где все $m_\lambda(V)$ целые неотрицательные. Такая сумма равна единице только если она состоит из одного слагаемого, равного единице. □

Упражнение 6.7. Опишите все неприводимые представления и вычислите их характеры для групп: а) $D_n$ б) $A_4$ в) $A_5$ г) $S_5$.

Замечание 6.1. (скалярное произведение комплексных характеров) Так как собственные числа всех операторов из конечной группы $G$ являются корнями $|G|$-й степени из единицы, в любом представлении группы $G$ над полем $\mathbb{C}$ следы обратных друг другу элементов $g$ и $g^{-1}$ комплексно сопряжены. Поэтому $\chi(g^{-1}) = \overline{\chi(g)}$ для любого характера $\chi$. Это позволяет переписать скалярное произведение комплексных характеров в виде стандартной эрмитовой структуры:

$$(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_1(g)} \cdot \chi_2(g)\,.$$

Замечание 6.2. (скалярное произведение характеров группы $S_n$) Обратные друг другу перестановки $g, g^{-1} \in S_n$ имеют одинаковый цикловой тип и, стало быть, сопряжены в $S_n$. Поэтому $\chi(g^{-1}) = \chi(g)$ для любого характера $\chi$. Это позволяет переписать скалярное произведение характеров симметрической группы виде стандартной евклидовой структуры:

$$(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \cdot \chi_2(g)\,.$$

В частности, над полями $\mathbb{Q}$ и $\mathbb{R}$ оно *положительно определено*.

Пример 6.3 (внешние степени симплициального представления $S_n$)
Покажем, что все внешние степени симплициального представления $\varDelta$ симметрической группы $S_n$ неприводимы. Разложение тавтологического представления $\tau$ группы $S_n$ перестановками базисных векторов в $\mathbb{Q}^n$ на неприводимые имеет вид $\tau = \varDelta \oplus \mathbb{1}$. Поэтому его $m$-тая внешняя степень $\varLambda^m \tau \simeq \varLambda^m \varDelta \oplus \varLambda^{m-1} \varDelta$.

Упражнение 6.8. Покажите, что $\varLambda^m (U \oplus W) \simeq \bigoplus_{\alpha+\beta=m} \varLambda^\alpha U \otimes \varLambda^\beta W$.

Достаточно убедиться, что скалярный квадрат $\left(\chi_{\varLambda^m \tau}, \chi_{\varLambda^m \tau}\right) = 2$. В стандартном базисе

$$e_I = e_{i_1} \wedge \ldots \wedge e_{i_m}$$

пространства $\varLambda^m(\Bbbk^n)$ след перестановки $\sigma$ равен сумме знаков $\operatorname{sgn} \sigma|_I$ ограничений перестановки $\sigma$ на все такие подмножества $I$, что $\sigma(I) \subset I$. Поэтому

$$\left(\chi_{\varLambda^k \tau}, \chi_{\varLambda^k \tau}\right) = \frac{1}{n!} \sum_{\sigma \in S_n} \left( \sum_{I : \sigma(I) \subset I} \operatorname{sgn}(\sigma|_I) \right) \cdot \left( \sum_{J : \sigma(J) \subset J} \operatorname{sgn}(\sigma|_J) \right) =$$

$$= \frac{1}{n!} \sum_{\sigma \in S_n} \sum_{\substack{I,J : \sigma(I) \subset I \\ \sigma(J) \subset J}} \operatorname{sgn}(\sigma|_I) \cdot \operatorname{sgn}(\sigma|_J) = \frac{1}{n!} \sum_{I,J} \sum_{\substack{\sigma : \sigma(I) \subset I \\ \sigma(J) \subset J}} \operatorname{sgn}(\sigma|_I) \cdot \operatorname{sgn}(\sigma|_J)\,.$$

Совокупность всех таких перестановок $\sigma$, что $\sigma(I) \subset I$ и $\sigma(J) \subset J$, представляет собою прямое произведение симметрических групп, независимо переставляющих элементы в подмножествах $I \cap J$, $I \smallsetminus (I \cap J)$, $J \smallsetminus (I \cap J)$, $\{1, 2, \dots, n\} \smallsetminus (I \cup J)$ и изоморфное $S_k \times S_{m-k} \times S_{m-k} \times S_{n-2m+k}$, где $k = k(I, J) = |I \cap J|$. Поскольку $\operatorname{sgn}(\sigma|_I) \cdot \operatorname{sgn}(s|_J) = \operatorname{sgn}(\sigma|_{I\cap J})^2 \cdot \operatorname{sgn}(\sigma|_{I \smallsetminus (I\cap J)}) \cdot \operatorname{sgn}(\sigma|_{J\smallsetminus(I\cap J)}) = \operatorname{sgn}(\sigma|_{I\smallsetminus(I\cap J)}) \cdot \operatorname{sgn}(\sigma|_{J\smallsetminus(I\cap J)})$, предыдущую сумму можно переписать как

$$\frac{1}{n!}\sum_{I,J} k! \cdot (n-2m+k)! \cdot \Big(\sum_{g\in S_{m-k}} \operatorname{sgn}(g)\Big) \cdot \Big(\sum_{h \in S_{m-k}} \operatorname{sgn}(h)\Big). \tag{6-19}$$

Последние два множителя отличны от нуля только при $k = m$ и $k = m-1$. Проверим, что вклад всех слагаемых с такими значениями $k = |I \cap J|$ в сумму (6-19) равен по единице в каждом из двух случаев. В первом случае $I = J$ и соответствующий кусок суммы (6-19) имеет вид

$$\frac{1}{n!}\sum_I m! \cdot (n-m)!\,.$$

Он состоит из $\binom{n}{m}$ одинаковых слагаемых $\binom{m}{n}^{-1}$, сумма которых равна 1. Во втором случае $|I \cap J| = (m-1)$ и соответствующий кусок суммы (6-19) равен

$$\frac{1}{n!}\sum_{I\cap J}\ \sum_{\substack{i\neq j\\ i,j\notin I\cap J}} (m-1)! \cdot (n-m-1)!\,.$$

Он состоит из $\binom{n}{m-1} \cdot (n-m+1)(n-m)$ одинаковых слагаемых вида

$$\frac{(m-1)! \cdot (n-m-1)!}{n!} = \binom{n}{m-1}^{-1} \cdot \frac{1}{(n-m+1)(n-m)}\,,$$

сумма которых тоже равна 1.

**6.2.2. Кольцо представлений.** Целочисленные линейные комбинации неприводимых характеров конечной группы $G$ образуют коммутативное подкольцо с единицей в алгебре $\Bbbk[G]$ всех функций $G \to \Bbbk$ с операциями поточечного сложения и умножения значений. Это подкольцо называется *кольцом представлений* группы $G$ и обозначается

$$\mathfrak{rep}(G) \overset{\text{def}}{=} \bigoplus_{\lambda \in \operatorname{Irr}(G)} \mathbb{Z} \cdot \chi_\lambda \subset \Bbbk^G\,.$$

Название связано с тем, что в силу предыдущего линейные комбинации неприводимых характеров с неотрицательными коэффициентами взаимно однозначно соответствуют представлениям группы $G$. При этом сложению и умножению в $\mathfrak{rep}(G)$ отвечают прямая сумма и тензорное произведение соответствующих представлений. Элементы кольца $\mathfrak{rep}(G)$, содержащие отрицательные кратности неприводимых характеров, называются *виртуальными представлениями*.

**6.3. Индуцированные представления.** Пусть ассоциативная $\Bbbk$-алгебра $A$ с единицей является подалгеброй ассоциативной $\Bbbk$-алгебры $B$ с той же единицей, что и в $A$. Любое представление $W$ алгебры $B$ одновременно является и представлением алгебры $A$. Пространство $W$, рассматриваемое как модуль над $A$, называется *ограничением* $B$-модуля $W$ на $A$ и обозначается $\operatorname{res} W$ или $\operatorname{res}_A^B W$, если важно указать, о каких $B$ и $A$ идёт речь. Простейшим примером этой ситуации является овеществление комплексных векторных пространств: если $\Bbbk = A = \mathbb{R}$, а $B = \mathbb{C}$, то $n$-

мерное векторное пространство $W$ над полем $\mathbb{C}$ может рассматриваться как вещественное векторное пространство $W_{\mathbb{R}} = \operatorname{res}^{\mathbb{C}}_{\mathbb{R}} W$ размерности $2n$.

Наоборот, по любому $A$-модулю $V$ можно построить $B$-модуль $\operatorname{ind} V = B \otimes_A V$, который называется *индуцированным* с $A$-модуля $V$ и определяется как фактор тензорного произведения векторных пространств $B \otimes V$ по подпространству, порождённому всевозможными разностями

$$ba \otimes v - b \otimes av\,, \text{ где } b \in B\,,\ a \in A\,,\ v \in V\,.$$

По построению, в пространстве $B \otimes_A V$ выполняются равенства $ba \otimes_A v = b \otimes_A av$, т. е. элементы алгебры $A$ «проносятся» через знак тензорного произведения. Поэтому такое произведение называется *тензорным произведением над* $A$. Структура модуля над $B$ задаётся правилом

$$b\,(b' \otimes v) \overset{\text{def}}{=} (bb') \otimes v\,.$$

Простейшим примером этой ситуации является комплексификация вещественного векторного пространства: если $\Bbbk = A = \mathbb{R}$, а $B = \mathbb{C}$, то из $n$-мерного вещественного векторного пространства $V$ можно изготовить комплексное векторное пространство $\mathbb{C} \otimes V$ той же размерности $n$, но уже над полем $\mathbb{C}$. Если важно указать алгебры $B$ и $A$ явно, мы пишем $\operatorname{ind}^B_A V$.

Предложение 6.2

Отображение $\tau_A : V \to B \otimes_A V$, $v \mapsto 1 \otimes_A v$, является $A$-гомоморфизмом, и для любого $A$-гомоморфизма $\varphi : V \to W$ в любой $B$-модуль $W$ существует единственный такой $B$-гомоморфизм $\psi : B \otimes_A V \to W$, что $\psi \circ \tau_A = \varphi$. Иначе говоря, для всех $A$-модулей $V$ и $B$-модулей $W$ имеется канонический изоморфизм

$$\operatorname{Hom}_B(\operatorname{ind} V, W) \xrightarrow{\sim} \operatorname{Hom}_A(V, \operatorname{res} W)\,, \quad \psi \mapsto \psi \circ \tau_A\,. \tag{6-20}$$

Доказательство. Для каждого $B$-гомоморфизма $\psi : B \otimes_A U \to V$ композиция

$$\varphi = \psi \circ \tau_A : V \to W\,, \quad v \mapsto \psi(1 \otimes_A u)$$

является $A$-гомоморфизмом, поскольку $\varphi(av) = \psi(1 \otimes_A av) = \psi(a \otimes_A v) = a\psi(1 \otimes_A v) = a\varphi(v)$. Тем самым, отображение (6-20) определено корректно. Для данного $A$-гомоморфизма $\varphi : V \to W$ такой $B$-гомоморфизм $\psi : B \otimes_A V \to W$, что $\varphi = \psi \circ \tau_A$, обязан действовать на разложимые тензоры по правилу $b \otimes v \mapsto b\varphi(v)$. Тем самым, он единствен. Будучи билинейным по $b$ и $v$, это правило корректно задаёт линейный оператор $B \otimes V \to W$, который переводит соотношения $ba \otimes v - b \otimes av$ в нуль: $ba\psi(v) - b\psi(av) = 0$ в силу $A$-линейности $\psi$. Поэтому он корректно спускается до линейного отображения $B \otimes_A V \to W$, перестановочность которого с левым умножением на элементы $b \in B$ очевидна. □

Упражнение 6.9. Убедитесь, что универсальное свойство из предл. 6.2 определяет $B$-модуль $B \otimes_A V$ вместе с $A$-линейным отображением $\tau_A$ однозначно с точностью до единственного $B$-линейного изоморфизма, перестановочного с $\tau_A$, и проверьте, что ограничение и индуцирование представлений перестановочны с прямыми суммами и с тензорными произведениями представлений.

**6.3.1. Индуцированные представления групп.** В ситуации, когда $B = \Bbbk[G]$ и $A = \Bbbk[H]$ являются групповыми алгебрами конечной группы $G$ и произвольной её подгруппы $H \subset G$, ограничение и индуцирование сопоставляют каждому линейному представлению $\varrho : G \to \mathrm{GL}(W)$ его *ограничение* $\operatorname{res}\varrho \overset{\text{def}}{=} \varrho|_H : H \to \mathrm{GL}(W)$ на подгруппу $H$, а каждому линейному представлению $\lambda : H \to \mathrm{GL}(V)$ — *индуцированное* им представление $\operatorname{ind}\lambda : G \to \mathrm{GL}(\Bbbk[G]\otimes_{k[H]} V)$ группы $G$, так что имеет место канонический изоморфизм $\mathrm{Hom}_G(\operatorname{ind} V, W) \simeq \mathrm{Hom}_H(V, \operatorname{res} W)$. Если нужно подчеркнуть, о каких $G$ и $H \subset G$ идёт речь, мы пишем $\operatorname{res}^G_H$ и $\operatorname{ind}^G_H$. На языке характеров сопряжение и индуцирование являются встречными гомоморфизмами колец представлений

$$\mathfrak{rep}(H) \underset{\text{res}}{\overset{\text{ind}}{\rightleftarrows}} \mathfrak{rep}(G)$$

сопряжёнными относительно канонического скалярного произведения (6-18) на $\Bbbk^G$

$$(\chi_{\operatorname{ind} V}, \chi_W)_{\Bbbk^G} = (\chi_V, \chi_{\operatorname{res} W})_{\Bbbk^H} .$$

В частности, кратность неприводимого $G$-модуля $\lambda : G \to \mathrm{GL}(U)$ в разложении представления, индуцированного с неприводимого $H$-модуля $\mu : H \to \mathrm{GL}(S)$, равна кратности $S$ в разложении ограничения $V$ на подгруппу $H$:

$$m_\lambda(\operatorname{res}\mu) = m_\mu(\operatorname{ind}\lambda) . \tag{6-21}$$

Это равенство называется *законом взаимности Фробениуса*[1].

Предложение 6.3 (транзитивность индуцирования)
Для пары вложенных подгрупп $K \subset H \subset G$ и любого представления $\varrho : K \to \mathrm{GL}(U)$ имеется канонический изоморфзм $G$-модулей $\operatorname{ind}^G_H \operatorname{ind}^H_K U \xrightarrow{\sim} \operatorname{ind}^G_H U$ .

Доказательство. Поскольку для любого $G$-модуля $W$ имеется канонический изоморфизм

$$\mathrm{Hom}_K(U, W) \xrightarrow{\sim} \mathrm{Hom}_H(\operatorname{ind}^H_K U, W) \xrightarrow{\sim} \mathrm{Hom}_G(\operatorname{ind}^G_H \operatorname{ind}^H_K U, W) , \quad \psi \mapsto \psi \circ \tau_K \circ \tau_H ,$$

отображение $\tau_K \circ \tau_H : U \to \operatorname{ind}^G_H \operatorname{ind}^H_K U$ универсально в смысле предл. 6.2. По упр. 6.9 оно отождествляется с отображением $U \to \operatorname{ind}^G_K U$ единственным изоморфизмом. □

**6.3.2. Строение индуцированного представления.** Тензорное произведение

$$\Bbbk[G] \otimes U = \bigoplus_{g\in G} (\Bbbk \cdot g) \otimes V$$

представляет собою прямую сумму $|G|$ копий пространства $V$, занумерованных элементами $g \in G$. Факторизация по соотношениям $(gh)\otimes v = g \otimes (vu)$ склеивает между собою все прямые слагаемые, занумерованные элементами из одного смежного класса $gH$ так, что $gh \otimes v$ отождествляется с $g \otimes hv$. В результате тензорное произведение над $\Bbbk[H]$ оказывается изоморфно прямой сумме $r = [G : H]$ копий пространства $V$ занумерованных какой-либо фиксированной системой $\{g_1, \dots, g_r\}$ представителей классов смежности

$$\Bbbk[G] \bigoplus_{\Bbbk[H]} V \simeq g_1 V \oplus g_2 V \oplus \cdots \oplus g_r V . \tag{6-22}$$

[1] Или *двойственностью Фробениуса*.

В этом разложении каждое $g_\nu V$ представляет собой копию пространства $V$, а стоящий слева значок $g_\nu$ указывает, что данная копия соответствует смежному классу $g_\nu H$. Если писать $g_\nu v$ для обозначения вектора $v \in V$, лежащего в $g_\nu$-й копии $g_\nu V$ пространства $V$, то каждый вектор $w \in \Bbbk[G] \otimes_{k[H]} V$ однозначно запишется в виде суммы $\sum_{\nu=1}^{r} g_\nu v_\nu$, где $v_\nu \in V$. Левое умножение на элемент $g \in G$ в группе $G$ осуществляет перестановку смежных классов: для каждых $g \in G$ и $\nu \in \{1, \dots, r\}$ найдутся единственные такие $h = h(g, \nu) \in H$ и $\mu = \mu(g, \nu) \in \{1, \dots, r\}$, что $gg_\nu = g_\mu h$. В этих обозначениях действие элемента $g \in G$ на вектор $g_\nu v \in g_\nu V$ происходит по правилу $gg_\nu v \overset{\text{def}}{=} g_\mu hv \in g_\mu V$, где $hv \in V$ есть результат действия оператора $h \in H$ на вектор $v \in V$ согласно представлению подгруппы $H$ в $\mathrm{GL}(V)$.

Пример 6.4

Пусть $G = S_3$ и $H \simeq S_2$ — подгруппа, порождённая транспозицией $\sigma = |12\rangle$. В качестве представителей смежных классов $G/H$ выберем $e$, $\tau$ и $\tau^2$, где $\tau = |123\rangle$. Представление $W = \operatorname{ind} \mathbb{1}$, индуцированное тривиальным одномерным представлением, трёхмерно с базисом $e, \tau, \tau^2$ и образующие $\sigma, \tau \in S_3$ действуют на этот базис матрицами

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

соответственно. Тем самым, $W$ изоморфно тавтологическому представлению $S_3$ и является суммой тривиального одномерного представления и двумерного представления группой треугольника. Представление $W' = \operatorname{ind} \operatorname{sgn}$, индуцированное одномерным знаковым представлением, также трёхмерно с тем же базисом, но $\sigma$ и $\tau$ теперь действуют на него матрицами

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Это представление является прямой суммой знакового представления в одномерном пространстве, натянутом на $e + \tau + \tau^2$ и треугольного представления в ортогональной плоскости. Представление, индуцированное с двумерного левого регулярного представления $\Bbbk[S_2]$, это 6-мерное левое регулярное представление группы $S_3$ в $\Bbbk[S_3] = e \cdot \Bbbk[S_2] \oplus \tau \cdot \Bbbk[S_2] \oplus \tau^2 \cdot \Bbbk[S_2]$.

Упражнение 6.10. Убедитесь, что регулярное представление любой подгруппы всегда индуцирует регулярное представление объемлющей группы.

Предложение 6.4

Если группа $G$ имеет абелеву подгруппу $H \subset G$, то размерность любого неприводимого представления группы $G$ не превышает[1] индекса $[G : H]$.

Доказательство. Пусть представление $U$ группы $G$ неприводимо, и $L$ — одномерный $H$-подмодуль в $\operatorname{res} U$. В силу взаимности Фробениуса $\operatorname{ind} L$ содержит $U$ с ненулевой кратностью, откуда $\dim U \leqslant \dim \operatorname{ind} L = [G : H]$. □

[1] Ниже, в теор. 9.1 на стр. 131 мы увидим, что если абелева подгруппа $H$ нормальна в $G$, то размерности всех неприводимых группы $G$ делят индекс $[G : H]$.

Предложение 6.5
Пусть пересечение класса сопряжённых элементов $C \subset G$ с подгруппой $H \subset G$ раскладывается в объединение $C \cap H = D_1 \sqcup D_2 \sqcup \ldots \sqcup D_m$ различных классов $H$-сопряжённости. Тогда для любого представления $V$ подгруппы $H$ характер индуцированного им представления принимает на классе $C$ значение $\chi_{\operatorname{ind} V}(C) = [G : H] \cdot \sum_{i=1}^m \chi_V(D_i) \cdot |D_i| / |C|$. В частности, для тривиального одномерного представления $V = \mathbb{1}$ имеем

$$\chi_{\operatorname{ind} \mathbb{1}}(C) = [G : H] \cdot |C \cap H| / |C| . \tag{6-23}$$

Доказательство. Поскольку элемент $g \in C$ переставляет слагаемые $g_\nu V$ разложения (6-22), след его действия равен сумме следов действий на тех слагаемых $g_\nu V$, которые остаются при этой перестановке на месте, что означает равенство $gg_\nu = g_\nu h$ для некоторого $h = g_\nu^{-1} g g_\nu \in H$. При этом действие элемента $g$ на таком слагаемом $g_\nu V$ совпадает с действием элемента $h$ на пространстве $V$, и его след равен $\chi_V(h) = \chi_V(g_\nu^{-1} g g_\nu)$. Поэтому

$$\chi_{\operatorname{ind} V}(g) = \sum_{\substack{\nu:\\ g_\nu^{-1} g g_\nu \in H}} \chi_V(g_\nu^{-1} g g_\nu) = \frac{1}{|H|} \sum_{\substack{s \in G:\\ s^{-1} g s \in H}} \chi_V(s^{-1} g s) = \frac{1}{|H|} \sum_{i=1}^{m} \sum_{\substack{s \in G:\\ s^{-1} g s \in D_i}} \chi_V(D_i) .$$

Во втором равенстве мы заменили каждое слагаемое левой суммы на $|H|$ равных друг другу слагаемых, получающихся заменой $g_\nu$ на всевозможные $s \in g_\nu H$, а в третьем — собрали вместе все слагаемые, у которых $s^{-1} g s$ лежит в одном классе $H$-сопряжённости $D_i$. Так как различных произведений $s^{-1} g s \in D_i$ имеется $|D_i|$ штук и по формуле для длины орбиты каждое из них получается из $|G|/|C|$ различных $s \in G$, характер $\chi_{\operatorname{ind} V}(g) = |H|^{-1} \sum_{i=1}^m \chi_V(D_i) \cdot |D_i| \cdot |G|/|C|$. □

Упражнение 6.11 (формула проекции). Убедитесь, что для любых $G$-модуля $W$ и $H$-модуля $V$ имеется канонический изоморфизм $G$-модулей[1] $\operatorname{ind}\big((\operatorname{res} W) \otimes V\big) \simeq W \otimes \operatorname{ind} V$.

**6.3.3. Коиндуцированные представления.** В теории представлений ассоциативных алгебр имеется ещё один способ сопоставить $A$-модулю $V$ модуль над алгеброй $B$, содержащей $A$ в качестве подалгебры, а именно — *коиндуцированный модуль* $\operatorname{coind} V \overset{\text{def}}{=} \operatorname{Hom}_A(B, V)$, на котором имеется *левое* действие алгебры $B$ *правым* умножением аргумента $b : \psi \mapsto b\psi$, где $b\psi(b') \overset{\text{def}}{=} \psi(b'b)$.

Упражнение 6.12. Проверьте равенство $(b_1 b_2)\psi = b_1(b_2\psi)$.

Коиндуцированный модуль обладает двойственным к описанному в предл. 6.2 универсальным свойством: каноническое отображение $\tau^A : \operatorname{Hom}_A(B, V) \to V$, $\varphi \mapsto \varphi(1)$, $A$-линейно, и для любых $B$-модуля $W$ и $A$-гомоморфизма $\varphi : W \to V$ существует единственный такой $B$-гомоморфизм $\psi : W \to \operatorname{Hom}_A(B, V)$, что $\tau^A \circ \psi = \varphi$, т. е. для всех $A$-модулей $V$ и $B$-модулей $W$ имеется канонический изоморфизм

$$\operatorname{Hom}_B(W, \operatorname{coind} V) \xrightarrow{\sim} \operatorname{Hom}_A(\operatorname{res} W, V) , \quad \psi \mapsto \tau^A \circ \psi , \tag{6-24}$$

сопоставляющий $B$-гомоморфизму $\psi : W \to \operatorname{Hom}_A(B, V)$, $w \mapsto \psi_w$, $A$-гомоморфизм

$$\tau^A \circ \psi : W \to V , \quad w \mapsto \psi_w(1) .$$

[1] Тензорные произведения в обеих частях суть тензорные произведения представлений групп $H$ и $G$, описанные в n° 5.4 на стр. 71.

Обратное отображение переводит $A$-гомоморфизм $\varphi : W \to V$ в $B$-гомоморфизм

$$\psi : W \to \mathrm{Hom}_A(B, V), \quad w \mapsto \psi_w, \quad \text{где} \quad \psi_w : B \to V, \quad b \mapsto \varphi(bw).$$

Упражнение 6.13. Убедитесь, что оба гомоморфизма корректно определены и обратны друг другу.

В ситуации, когда $A = \Bbbk[H]$, $B = \Bbbk[G]$ суть групповые алгебры конечной группы $G$ и её подгруппы $H \subset G$, преобразование Фурье[1] индуцирует изоморфизм векторных пространств

$$\Phi \otimes \mathrm{Id}_V : \mathrm{Hom}(\Bbbk[G], V) \simeq \Bbbk[G]^* \otimes V \xrightarrow{\sim} \Bbbk[G] \otimes V,$$

действующий на операторы ранга 1 по правилу

$$\xi \otimes v \mapsto \hat{\xi} \otimes v = \frac{1}{|G|} \sum_{g \in G} \xi\left(g^{-1}\right) \cdot g \otimes v = \frac{1}{|G|} \sum_{g \in G} g \otimes \left(\xi \otimes v(g^{-1})\right)$$

и переводящий произвольный линейный оператор $\varphi : \Bbbk[G] \to V$ в тензор

$$\widehat{\varphi} \overset{\text{def}}{=} \frac{1}{|G|} \sum_{g \in G} g^{-1} \otimes \varphi(g),$$

называемый *преобразованием Фурье* оператора $\varphi$. Преобразование Фурье перестановочно с левым действием $G$, ибо для всех $s \in G$

$$\widehat{s\varphi} = \frac{1}{|G|} \sum_{g \in G} g^{-1} \otimes s\varphi(g) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \otimes \varphi(gs) = \frac{1}{|G|} \sum_{g \in G} sg^{-1} \otimes \varphi(g) = s\widehat{\varphi},$$

а его композиция с проекцией $\Bbbk[G] \otimes V \twoheadrightarrow \Bbbk[G] \otimes_{\Bbbk[H]} V$ устанавливает изоморфизм подпространства $H$-инвариантных операторов $\mathrm{Hom}_H(\Bbbk[G], V) \subset \mathrm{Hom}(\Bbbk[G], V)$ с индуцированным $G$-модулем $\mathrm{ind}\, V = \Bbbk[G] \otimes_{\Bbbk[H]} V$.

Упражнение 6.14. Докажите последнее утверждение.

Таким образом, индуцированное и коиндуцированное представления конечной группы канонически изоморфны друг другу посредством преобразования Фурье.

[1] См. формулу (6-16) на стр. 86.

## §7. Представления симметрических групп

**7.1. Действие $S_n$ на заполненных диаграммах Юнга.** Будем называть диаграмму Юнга $\lambda$, в каждой клетке которой стоит какая-нибудь буква[1] алфавита $\{1, \dots, m\}$ *заполнением* формы $\lambda$. Заполнение $T$ называется *стандартным*, если $m = |\lambda|$, т. е. число букв совпадает с числом клеток диаграммы, и каждая буква используется ровно один раз. Заполнение $T$ называется *таблицей,* если стоящие в клетках диаграммы буквы нестрого возрастают слева направо в каждой строке и строго возрастают сверху вниз в каждом столбце. Число всех таблиц формы $\lambda$ в алфавите $\{1, \dots, m\}$ обозначается через $d_\lambda(m)$, а число всех стандартных таблиц формы $\lambda$ — через $d_\lambda$. Числа $d_\lambda(m) \neq 0$ только для диаграмм из $\leqslant m$ строк. Как мы видели в прим. 4.1 на стр. 54

$$\sum_\lambda d_\lambda d_\lambda(m) = m^n \quad \text{и} \quad \sum_\lambda d_\lambda^2 = n!\,, \tag{7-1}$$

где суммирование в обоих случаях идёт по всем диаграммам Юнга веса $|\lambda| \overset{\text{def}}{=} \sum \lambda_i = n$. С каждым стандартным заполнением $T$ формы $\lambda = (\lambda_1, \dots, \lambda_k)$ и веса $n$ связаны *строчная подгруппа* $R_T \subset S_n$, состоящая из всех перестановок, переводящих элементы каждой строки заполнения $T$ в элементы из той же самой строки, и *столбцовая подгруппа* $C_T \subset S_n$, состоящая из всех перестановок, переводящих элементы каждого столбца заполнения $T$ в элементы из того же самого столбца. Таким образом, $R_T \simeq S_{\lambda_1} \times \ldots \times S_{\lambda_k}$ и $C_T \simeq S_{\lambda_1^t} \times \ldots \times S_{\lambda_m^t}$, где $\lambda^t = (\lambda_1^t, \dots, \lambda_m^t)$ здесь и далее означает транспонированную к $\lambda$ диаграмму.

Упражнение 7.1. Убедитесь, что $S_n$ транзитивно действует на стандартных заполнениях фиксированной формы $\lambda$ и что $R_{gT} = gR_Tg^{-1}$ и $C_{gT} = gC_Tg^{-1}$ для всех $g \in S_n$.

Мы пишем $\lambda \trianglerighteq \mu$ и говорим, что диаграмма $\lambda$ *доминирует* диаграмму $\mu$, если[2]

$$\lambda_1 + \ldots + \lambda_k \geqslant \mu_1 + \ldots + \mu_k \text{ при всех } k \in \mathbb{N}\,.$$

Мы пишем $\lambda > \mu$, если $\lambda = (\lambda_1, \dots, \lambda_k)$ лексикографически больше, чем $\mu = (\lambda_1, \dots, \lambda_m)$. Отметим, что диаграмма $\mu$ не может доминировать никакую диаграмму $\lambda > \mu$, и что в отличие от доминирования лексикографический порядок является линейным.

Лемма 7.1 (ключевая комбинаторная лемма)
Пусть стандартное заполнение $T$ формы $\lambda$ и стандартное заполнение $U$ формы $\mu$ имеют одинаковый вес $|\lambda| = |\mu|$, и диаграмма $\mu$ не является строго доминирующей диаграмму $\lambda$. Тогда имеет место ровно одна из двух взаимоисключающих возможностей:

- либо найдутся два числа, стоящие в одной строке заполнения $T$ и в одном столбце заполнения $U$
- либо $\lambda = \mu$ и $pT = qU$ для некоторых $p \in R_T$ и $q \in C_U$.

Доказательство. Пусть все элементы каждой из строк заполнения $T$ находятся в разных столбцах заполнения $U$. Из того, что все элементы первой строки $T$ лежат в разных столбцах $U$, вытекает неравенство $\lambda_1 \leqslant \mu_1$ и существование перестановки $q_1 \in C_U$, переводящей все элементы из первой строки заполнения $T$ в первую строку заполнения $q_1U$. Из того, что все элементы

[1] При этом могут использоваться не все буквы, а используемые буквы могут повторяться.
[2] См. обсуждение перед упр. 4.3 на стр. 57 и само это упражнение.

второй строки $T$ тоже лежат в разных столбцах $U$, вытекает существование такой не затрагивающей элементов из первой строки заполнения $T$ перестановки $q_2 \in C_{q_1 U} = C_U$, что в заполнении $q_2 q_1 U$ каждый элемент второй строки заполнения $T$ стоит либо во второй строке, либо в первой[1], что влечёт неравенство $\lambda_1 + \lambda_2 \leqslant \mu_1 + \mu_2$. Продолжая в том же духе, мы получим последовательность перестановок $q_1, \dots, q_k \in C_U$, где $k$ — количество строк в диаграмме $\mu$ и каждая перестановка $q_i \in C_{q_{i-1} \dots q_1 U} = C_U$ оставляет на месте все элементы из первых $i-1$ строк заполнения $T$, а также все те элементы из $i$-той строки $T$, которые в заполнении $q_{i-1} \dots q_1 U$ лежат в столбцах меньшей, чем $i$ высоты, а все остальные элементы из $i$-той строки $T$ переводит в $i$-тую строку заполнения $q_i q_{i-1} \dots q_1 U$. В частности, при каждом $i$ выполняется неравенство $\lambda_1 + \ldots + \lambda_i \leqslant \mu_1 + \ldots + \mu_i$, что по условию леммы возможно только при $\lambda = \mu$. Но тогда каждая перестановка $q_i$ переводит элементы $i$-той строки заполнения $T$ в точности в $i$-тую строку заполнения $q_i \dots q_1 U$. Поэтому $q_k \dots q_1 U = pT$ для некоторого $p \in R_T$. □

Следствие 7.1
Перестановка $g \in S_n$ тогда и только тогда имеет вид $g = pq$ для некоторых $p \in R_T$, $q \in C_T$, когда никакие два элемента из одной строки $T$ не лежат в одном столбце $gT$, и в этом случае представление перестановки $g \in S_n$ в виде $g = pq$ с $p \in R_T$ и $q \in C_T$ единственно.

Доказательство. Для любых $p \in R_T$ и $q \in C_T$ элементы из одной строки заполнения $T$ лежат в разных столбцах заполнения $qT$, и $p$ переставляет эти элементы между собою, оставляя их лежать в разных столбцах заполнения $pqT$. Наоборот, если никакие два элемента из одной строки заполнения $T$ не лежат в одном столбце заполнения $U = gT$, то по лем. 7.1 найдутся такие $p \in R_T$ и $q' \in C_U$, что $pT = q'U = q'gT$. Поэтому $p = q'g$. Записывая перестановку $q' \in C_{gT} = gC_T g^{-1}$ в виде $gqg^{-1}$, где $q \in C_T$, получаем $g = pq^{-1}$, как и требовалось. Единственность разложения $g = pq$ вытекает из того, что $R_T \cap C_T = \{e\}$. □

**7.2. Симметризаторы Юнга.** Лежащие в групповой алгебре $\mathbb{C}[S_n]$ элементы

$$r_T = \sum_{\sigma \in R_T} \sigma\,, \quad c_T = \sum_{\sigma \in C_T} \operatorname{sgn}(\sigma)\sigma\,, \tag{7-2}$$

$$s_T = r_T c_T = \sum_{p \in R_T} \sum_{q \in C_T} \operatorname{sgn}(q) pq \tag{7-3}$$

называются, соответственно, *строчным*, *столбцовым* и *полным симметризаторами Юнга*. Они обладают следующими очевидными свойствами:

$$\forall g \in S_n \quad r_{gT} = g r_T g^{-1}\,, \quad c_{gT} = g c_T g^{-1} \quad \text{и} \quad s_{gT} = g s_T g^{-1} \tag{7-4}$$

$$\forall p \in R_T \; p r_T = r_T p = r_T \quad \text{и} \quad \forall q \in C_T \; \operatorname{sgn}(q) q c_T = \operatorname{sgn}(q) c_T q = c_T \tag{7-5}$$

$$\forall p \in R_T \quad \text{и} \quad \forall q \in C_T \quad \operatorname{sgn}(q) p s_T q = s_T\,. \tag{7-6}$$

Замечательно, что полный симметризатор $s_T \in \mathbb{C}[S_n]$ однозначно с точностью до пропорциональности *определяется* свойством (7-6).

Лемма 7.2
Векторное подпространство $E_T = \{ f \in \mathbb{C}[S_n] \mid \forall p \in R_T \; \forall q \in C_T \; \operatorname{sgn}(q) p f q = f \}$ одномерно и линейно порождается симметризатором $s_T$.

[1] Последнее происходит, когда этот элемент изначально находится в столбце высоты 1.

Доказательство. Пусть $f = \sum_{g\in S_n} x_g g \in E_T$. Покажем, что $f = x_e s_T$. Условие $\mathrm{sgn}(q)\, pfq = f$ означает, что $x_{pgq} = \mathrm{sgn}(q)x_g$ для всех $g \in S_n$, $p \in R_T$ и $q \in C_T$. Полагая $g = e$, заключаем, что $x_{pq} = \mathrm{sgn}(q)x_e$ и $f = x_e s_T + \sum_{g\notin R_T C_T} x_g g$. Остаётся убедиться, что в последней сумме все $x_g = 0$. Если $g \notin R_T C_T$, то по сл. 7.1 найдутся два элемента, лежащие в одной строке заполнения $T$ и в одном столбце заполнения $gT$. Транспозиция $\tau \in S_n$ этих двух элементов лежит и в $R_T$, и в $C_{gT} = gC_T g^{-1}$. Из второго вытекает, что $g^{-1}\tau g \in C_T$. Полагая $p = \tau$, $q = g^{-1}\tau g$ в равенстве $x_{pgq} = \mathrm{sgn}(q)x_g$, получаем $x_g = -x_g$, откуда $x_g = 0$. □

Лемма 7.3
Имеют место равенства $s_T\mathbb{C}[S_n]\,s_T = \mathbb{C}\,s_T$ и $s_T^2 = n_\lambda s_T$, где число $n_\lambda = n!/\dim\left(\mathbb{C}[S_n]\,s_T\right)$ рационально, положительно и зависит только от формы $\lambda = \lambda(T)$ заполнения $T$.

Доказательство. Из равенств (7-5) – (7-6) вытекает, что при любом $f \in \mathbb{C}[S_n]$ элемент $s_T f s_T$ обладает свойством (7-6) и, тем самым, лежит в одномерном пространстве $E_T = \mathbb{C}\,s_T$ из лем. 7.2. В частности, $s_T^2 = n_T s_T$ для некоторого $n_T \in \mathbb{C}$. Чтобы найти $n_T$, вычислим двумя способами след оператора $\mathbb{C}[S_n] \to \mathbb{C}[S_n]$ правого умножения на элемент $s_T : f \mapsto fs_T$. С одной стороны, из формулы (7-3) вытекает[1], что для любого $g \in S_n$ коэффициент при $g$ у произведения $gs_T$ равен единице, откуда $\mathrm{tr}(s_T) = |S_n| = n!$. С другой стороны, левый идеал $\mathbb{C}[S_n]\,s_T$ является $S_n$-подмодулем левого регулярного представления $S_n$. Так как последнее вполне приводимо, существует такой $S_n$-подмодуль $W \subset \mathbb{C}[S_n]$, что $\mathbb{C}[S_n] = W \oplus \mathbb{C}[S_n]\,s_T$. Правое умножение на $s_T$ переводит $W \subset \mathbb{C}[S_n]$ внутрь $\mathbb{C}[S_n]\,s_T$, а на идеале $\mathbb{C}[S_n]\,s_T$ действует как умножение на $n_T$. Поэтому $\mathrm{tr}(s_T) = n_T \dim(\mathbb{C}[S_n]\,s_T)$. Следовательно, число $n_T = n!/\dim(\mathbb{C}[S_n]\,s_T)$ рационально и положительно. Наконец, из равенства $s_{gT} = gs_T g^{-1}$ вытекает, что $s_{gT}^2 = gs_T^2 g^{-1} = n_T g s_T g^{-1} = n_T s_{gT}$. Поэтому число $n_T = n_{\lambda(T)}$ зависит только от формы $\lambda = \lambda(T)$ заполнения $T$. □

Лемма 7.4
Если форма стандартного заполнения $T$ лексикографически больше, чем форма стандартного заполнения $U$, то $r_T\mathbb{C}[S_n]\,c_U = c_U\mathbb{C}[S_n]\,r_T = s_T\mathbb{C}[S_n]\,s_U = 0$.

Доказательство. Достаточно убедиться, что $r_T g c_U = c_U g r_T = 0$ для всех $g \in S_n$. Пусть для начала $g = e$. По лем. 7.1 какие-то два элемента из одной строки заполнения $T$ лежат в одном столбце заполнения $U$. Транспозиция $\tau \in S_n$ этих двух элементов лежит как в $R_T$, так и в $C_U$. Поэтому $r_T c_U = (r_T\tau)c_U = r_T(\tau c_U) = -r_T c_U$ и $c_U r_T = -(c_U\tau)r_T = -c_U(\tau r_T) = -c_U r_T$, откуда $r_T c_U = c_U r_T = 0$. Теперь и для любого $g \in S_n$ получаем $r_T g c_U = r_T g c_U g^{-1} g = \left(r_T c_{gU}\right) g = 0$ и $c_U g r_T = c_U g r_T g^{-1} g = \left(c_U r_{gT}\right) g = 0$. □

Теорема 7.1
Представление $S_n$ левыми умножениями в идеале $V_T = \mathbb{C}[S_n]\,s_T$ неприводимо. Два таких представления $V_T$ и $V_U$ изоморфны тогда и только тогда, когда заполнения $T$ и $U$ имеют одинаковую форму $\lambda = \lambda(T) = \lambda(U)$. Если для каждой $n$-клеточной диаграммы Юнга $\lambda$ произвольным образом зафиксировать некоторое стандартное заполнение $T_\lambda$, то неприводимые представления $V_\lambda = V_{T_\lambda}$ составят полный список попарно неизоморфных неприводимых представлений $S_n$.

[1] Так как $R_T \cap C_T = \{e\}$, все слагаемые в сумме (7-3) являются *различными* элементами группы $S_n$, взятыми со знаком $\pm 1$, причём элемент $e = ee$ берётся с плюсом.

Доказательство. Пусть $W \subset V_T$ является $S_n$-инвариантным подмодулем. Перестановочный с левым умножением на $S_n$ проектор $\pi_W : \mathbb{C}[S_n] \twoheadrightarrow W$ представляет собою оператор правого умножения на элемент $w = \pi_W(1) \in W$, поскольку $\pi_W(x) = x\pi_W(1) = xw$ для всех $x \in \mathbb{C}[S_n]$. Так как $s_T W \subset s_T V_T = s_T \mathbb{C}[S_n]\, s_T = \mathbb{C}\, s_T$, для левого действия элемента $s_T$ на подмодуле $W$ имеются ровно две возможности: либо $s_T W = 0$, либо $s_T W = \mathbb{C}\, s_T$. В первом случае $WW \subset V_T W = \mathbb{C}[S_n]\, s_T W = 0$, откуда $w^2 = 0$, а значит, и $W = 0$, поскольку правое умножение на $w$ тождественно действует на $W = \mathbb{C}[S_n]\, w$. Во втором случае $s_T \in s_T W \subset W$, откуда $V_T = \mathbb{C}[S_n]\, s_T \subset W$, т. е. $W = V_T$. Таким образом, модуль $V_T$ неприводим. Если заполнения $T$ и $U$ имеют разные формы — скажем, форма заполнения $T$ лексикографически больше формы заполнения $U$, то по лем. 7.4 левое умножение на $s_T$ аннулирует модуль $V_U$, тогда как на модуле $V_T$ оно, согласно лем. 7.3, действует нетривиально: элемент $s_T \in V_T$ является собственным вектором левого умножения на $s_T$ с ненулевым собственным значением $n_{\lambda(T)}$. Поэтому представления $V_T$ и $V_U$ не изоморфны. Отсюда следует последнее утверждение теоремы: число попарно неизоморфных неприводимых представлений $V_{T_\lambda}$ равно числу классов сопряжённости в $S_n$. Если заполнение $U$ имеет ту же форму $\lambda$, что и $T_\lambda$, то неприводимое представление $V_U$, будучи неизоморфным ни одному из представлений $V_{T_\mu}$ с $\mu \neq \lambda$, изоморфно именно представлению $V_{T_\lambda}$. □

**7.2.1. Симметризаторы $s'_T = c_T r_T$.** Множества $R_T C_T$ и $C_T R_T$, вообще говоря, различны. Например, для стандартного заполнения $T = \begin{smallmatrix} 1 & 2 \\ 3 & \end{smallmatrix}$ цикл $|132\rangle = |12\rangle \circ |13\rangle$ входит в $R_T C_T$ и не входит в $C_T R_T$, а цикл $|123\rangle = |13\rangle \circ |12\rangle$, наоборот, входит в $C_T R_T$ и не входит в $R_T C_T$. Таким образом, перестановка сомножителей в формуле (7-3) приводит к вообще говоря отличному от $s_T = r_T c_T$ симметризатору

$$s'_T = c_T r_T = \sum_{p \in R_T} \sum_{q \in C_T} \operatorname{sgn}(q) qp\,, \tag{7-7}$$

который является образом симметризатора $s_T$ при *антиподальном антиавтоморфизме*

$$\alpha : \mathbb{C}[S_n] \xrightarrow{\sim} \mathbb{C}[S_n]\,, \quad \sum_{g \in G} x_g g \mapsto \sum_{g \in G} x_g g^{-1}\,, \tag{7-8}$$

оборачивающем порядок сомножителей в произведениях переводящем строчный и столбцовый симметризаторы $r_T$ и $c_T$ в себя.

Упражнение 7.2. Сформулируйте и докажите для $s'_T$ аналоги равенств (7-6), лем. 7.4, лем. 7.3 и теор. 7.1.

Предложение 7.1
Представления $S_n$ левыми умножениями в идеалах $V_T = \mathbb{C}[S_n]\, s_T$ и $V'_T = \mathbb{C}[S_n]\, s'_T$ изоморфны.

Доказательство. Правые умножения на $c_T$ и $r_T$ задают гомоморфизмы левых $S_n$-модулей

$$V'_T = \mathbb{C}[S_n]\, c_T r_T \underset{x r_T \leftarrow x}{\overset{x \mapsto x c_T}{\rightleftarrows}} \mathbb{C}[S_n]\, r_T c_T = V_T$$

Композиция $x \mapsto x r_T c_T = x s_T$ действует на $V_T = \mathbb{C}[S_n]\, s_T$ умножением на ненулевую константу $n_{\lambda(T)}$. Таким образом, операторы правого умножения на $n_\lambda^{-1/2} c_T$ и $n_\lambda^{-1/2} r_T$ являются взаимно обратными изоморфизмами представлений. □

Следствие 7.2
Неприводимые представления $V_\lambda$ и $V_{\lambda^t}$, отвечающие транспонированным диаграммам $\lambda$ и $\lambda^t$, получаются друг из друга тензорным умножением на одномерное знаковое представление.

Доказательство. Фиксируем какое-либо стандартное заполнение $T$ формы $\lambda$ и транспонированное заполнение $T^t$ транспонированной диаграммы $\lambda^t$. Тогда $R_{T^t} = C_T$, $C_{T^t} = R_T$ и

$$s_{T^t} = \sum_{p\in R_T}\sum_{q\in C_T} \operatorname{sgn}(p)qp = \sum_{p\in R_T}\sum_{q\in C_T} \operatorname{sgn}(q)\operatorname{sgn}(pq)qp = \sigma\left(s'_T\right),$$

где $\sigma:\ \mathbb{C}[S_n] \to \mathbb{C}[S_n]$ обозначает *знаковый автоморфизм* групповой алгебры, действующий на базис из групповых элементов по правилу $g \mapsto \operatorname{sgn}(g)g$. Тензорное произведение представления $V_\lambda$ на одномерное знаковое представление изоморфно представлению $S_n$ в пространстве $V'_T = \mathbb{C}[S_n]\, s'_T$, заданному правилом $g:\ xs'_T \mapsto \operatorname{sgn}(g)gxs'_T$. Знаковый автоморфизм $\sigma$ изоморфно отображает это пространство на $V_{\lambda^t} = \mathbb{C}[S_n]\, s_{T^t}$, превращая последнее действие в левое умножение на $g:\ \sigma(x)s_{T^t} \mapsto g\sigma(x)s_{T^t}$. □

**7.3. Модуль таблоидов.** Орбита стандартного заполнения $T$ под действием строчной подгруппы $R_T$ называется *таблоидом* формы $\lambda$ и обозначается через $\{T\}$. Действие симметрической группы на заполнениях $g:\ T \mapsto gT$ корректно спускается до действия $g:\ \{T\} \mapsto \{gT\}$ на таблоидах, так как $gR_TT = gR_Tg^{-1}gT = R_{gT}gT$. Возникающее таким образом перестановочное представление группы $S_n$ на пространстве формальных комплексных линейных комбинаций таблоидов формы $\lambda$ называется *модулем таблоидов* и обозначается $M_\lambda$. Так как таблоиды формы $\lambda$ биективно соответствуют левым смежным классам $gR_T \in S_n/R_T$ и действие $S_n$ на таблоидах совпадает с действием на смежные классы, модуль таблоидов $M_\lambda = \operatorname{ind}_{R_T}^{S_n} \mathbb{1}$ индуцирован тривиальным одномерным представлением подгруппы $R_T \subset S_n$. Характер модуля $M_\lambda$ обозначается через $\psi_\lambda$.

Упражнение 7.3. Покажите, что представление $S_n$ в пространстве $M_\lambda$ изоморфно представлению $S_n$ левыми умножениями в идеале $\mathbb{C}[S_n]\, r_T$.

Его значение следующим образом выражается через количества $m_j$ строк длины $j$ в диаграмме $\mu$.

Предложение 7.2
Значение $\psi_\lambda(C_\mu)$ на классе сопряжённости $C_\mu \in \operatorname{Cl}(S_n)$, состоящем из всех перестановок циклового типа $\mu$, равно коэффициенту при $m_\lambda$ в разложении симметрического многочлена Ньютона[1] $p_\mu(x_1, \dots, x_n)$ по стандартному мономиальному базису[2] $m_\lambda(x_1, \dots, x_n)$.

Доказательство. Как обычно, обозначим через $m_i$ количество строк длины $i$ в диаграмме $\mu$. Тогда $p_\mu = p_{\mu_1} \dots p_{\mu_n} = p_1(x)^{m_1} \dots p_n(x)^{m_n}$, где

$$p_i(x)^{m_i} = (x_1^i + \dots + x_n^i)^{m_i} = \sum \frac{m_i!}{\varrho_{i1}! \dots \varrho_{in}!} x_1^{i\varrho_{i1}} \dots x_n^{i\varrho_{in}}$$

и суммирование идёт по всевозможным наборам неотрицательных целых чисел $\varrho_{i1}, \dots, \varrho_{in}$ с суммой $\sum_j \varrho_{ij} = m_i$. Таким образом, коэффициент при $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ у многочлена $p_\mu = p_1^{m_1} \dots p_n^{m_n}$ равен

$$\sum_{\varrho_{ij}} m_1! \dots m_n! / \prod_{ij} \varrho_{ij}!, \tag{7-9}$$

[1] См. формулу (3-14) на стр. 41.
[2] См. формулу (3-3) на стр. 37.

где суммирование идёт по всем таким наборам целых чисел $\varrho_{ij} \geqslant 0$, где $1 \leqslant i,j \leqslant n$, что

$$\sum_j \varrho_{ij} = m_i \quad \text{и} \quad \sum_i i\varrho_{ij} = \lambda_j\,. \tag{7-10}$$

С другой стороны, согласно установленной в предл. 6.5 на стр. 92 формуле (6-23) для характера индуцированного представления,

$$\psi_\lambda(C_\mu) = [S_n : R_T]\,|C_\mu \cap R_T|/|C_\mu|\,, \tag{7-11}$$

где $[S_n : R_T] = n!/\prod_j \lambda_j!$, $|C_\mu| = n!/\prod_i i^{m_i} m_i!$, а пересечение $C_\mu \cap R_T$ распадается в объединение непересекающихся классов $R_T$-сопряжёности $D_\varrho$, каждый из которых состоит из перестановок циклового типа $\mu$, в которых $\varrho_{ij}$ из $m_i$ циклов длины $i$ заполнены элементами $j$-той строки из $T$. Эти классы также нумеруются удовлетворяющими условиям (7-10) наборами неотрицательных целых чисел $\varrho = \{\varrho_{ij}\}$ с $1 \leqslant i,j \leqslant n$. При сопряжении подгруппой $R_T$ стабилизатор перестановки $g \in D_\varrho$ является прямым произведением $\prod \varrho_{ij}!$ перестановок циклов одинаковой длины между собою как единого целого и $\prod i^{m_i}$ циклических сдвигов внутри этих циклов. Тем самым, $|C_\mu \cap R_T| = \sum_\varrho |D_\varrho| = \sum_\varrho \prod_j \lambda_j!/\prod_{ij} i^{m_i}\varrho_{ij}!$. Подставляя всё это в (7-11) и сокращая общие множители числителя и знаменателя, получаем (7-9). □

**7.4. Модуль Шпехта.** Для каждого заполнения $T$ формы $\lambda$ рассмотрим в модуле таблоидов $M_\lambda$ вектор

$$v_T = c_T\{T\} = \sum_{q\in C_T} \operatorname{sgn}(q)\{qT\}\,. \tag{7-12}$$

Поскольку ни при каком $q \in C_T$ никакие два элемента из одного столбца $T$ не могут оказаться в одной строке $qT$, равенство $q_1T = pq_2T$ невозможно ни при каких $q_1, q_2 \in C_T$ и $p \in R_{q_2T}$, т. е. все слагаемые в правой сумме (7-12) суть *различные* базисные векторы пространства таблоидов $M_\lambda$, взятые с коэффициентами $\pm 1$. В частности, каждый из векторов $v_T$ отличен от нуля. Линейная оболочка векторов (7-12), полученных из всех возможных заполнений $T$ формы $\lambda$, является $S_n$-подмодулем в $M_\lambda$, так как $gv_T = gc_T\{T\} = gc_Tg^{-1}\{gT\} = c_{gT}\{gT\} = v_{gT}$ для всех $g \in S_n$. Этот подмодуль обозначается $S_\lambda$ и называется *модулем Шпехта*.

Лемма 7.5
Если форма $\lambda$ заполнения $T$ не является строго доминирующей диаграмму $\mu$, то

$$c_T M_\mu = \begin{cases} 0 & \text{при } \mu \neq \lambda \\ \mathbb{C}v_T & \text{при } \mu = \lambda\,. \end{cases}$$

Доказательство. Если в пересечении $R_U \cap C_T$ имеется хоть одна транспозиция $\tau$, то

$$c_T\{U\} = c_T\{\tau U\} = c_T\tau\{U\} = -c_T\{U\}\,, \tag{7-13}$$

откуда $c_T\{U\} = 0$. Если в условиях нашей леммы такой транспозиции нет, то по лем. 7.1 на стр. 94 заполнения $U$ и $T$ имеют одинаковую форму $\lambda$ и $pU = qT$ для некоторых $p \in R_U$ и $q \in C_T$. В этом случае $c_T\{U\} = c_T\{pU\} = c_T\{qT\} = c_Tq\{T\} = \operatorname{sgn}(q)c_T\{T\} = \pm v_T$. □

Теорема 7.2
Модуль Шпехта $S_\lambda$ изоморфен неприводимому представлению $V_\lambda$ левыми умножениями в идеале $\mathbb{C}[S_n]\,s_T$, построенному по произвольному заполнению $T$ формы $\lambda$.

Доказательство. Покажем сначала, что $S_\lambda$ неприводим. Пусть имеется разложение $S_\lambda = V \oplus W$ в сумму $S_n$-подмодулей. Тогда оператор $c_T$, построенный по заполнению $T$ формы $\lambda$, переводит каждое из слагаемых в себя. Так как по лем. 7.5 $c_T S_\lambda \subset c_T M_\lambda = \mathbb{C} v_T$, ненулевой вектор $v_T$ лежит ровно в одном из слагаемых — скажем, в $V$. Но тогда $V$ содержит и все остальные векторы $v_{gT} = g v_T$, а значит, совпадает с $S_\lambda$. При $\mu \neq \lambda$ неприводимые представления $S_\lambda$ и $S_\mu$ не изоморфны: если $\lambda$ лексикографически меньше $\mu$, то по лем. 7.5 оператор $c_T$ аннулирует подмодуль $S_\mu \subset M_\mu$, а на модуле $S_\lambda$ действует нетривиально, ибо $c_T v_T = c_T c_T\{T\} = |C_T| c_T\{T\} = |C_T| v_T$. Из сказанного вытекает, что модуль $S_\lambda$ изоморфен ровно одному из неприводимых представлений $V_\mu = \mathbb{C}[S_n]\, s_U$, где $U$ — любое заполнение формы $\mu$. Поскольку по лем. 7.4 левое умножение на $c_T$ аннулирует все идеалы $V_\mu$ с лексикографически меньшими, чем $\lambda$ диаграммами $\mu$, мы заключаем, что $S_\lambda \simeq V_\lambda$. □

Следствие 7.3
В разложении представления $M_\lambda$ в сумму неприводимых встречаются только модули $S_\mu$ с $\mu \rhd \lambda$, а также модуль $S_\lambda$, входящий в $M_\lambda$ с кратностью 1.

Доказательство. Так как оператор $c_T$ переводит $M_\lambda$ в подмодуль Шпехта и нетривиально действует на последнем, в разложении модуля $M_\lambda$ в прямую сумму простых есть ровно одно слагаемое, изоморфное $S_\lambda$. Если существует $S_n$-линейное вложение $S_\mu \hookrightarrow M_\lambda$, то оператор $c_U$, отвечающий произвольному заполнению $U$ формы $\mu$, нетривиально действует на $M_\lambda$. Но в силу лем. 7.5 $c_U M_\lambda = 0$, когда $\mu$ не доминирует $\lambda$. □

**7.4.1. Табличный базис модуля Шпехта.** Назовём *столбцовой развёрткой* заполнения $T$ диаграммы $\lambda$ слово, которое получится при прочтении заполнения $T$ по столбцам, так что каждый столбец читается снизу вверх, а сами столбцы перебираются слева направо. Например, столбцовая развёртка стандартной таблицы

$$T = \begin{ytableau} 1 & 3 & 4 \\ 2 & 5 \end{ytableau}$$

это слово 21534. Скажем, что $T \succ U$, если наибольшее из чисел, стоящих в заполнениях $T$ и $U$ в разных клетках, встречается в столбцовой развёртке заполнения $T$ раньше, чем в столбцовой развёртке заполнения $U$.

Упражнение 7.4. Проверьте, что это отношение задаёт линейный порядок на стандартных заполнениях формы $\lambda$.

Например, 120 стандартных заполнений формы $\ydiagram{2,2,1}$ выстроятся по убыванию так:

$$\begin{ytableau} 3 & 1 \\ 4 & 2 \\ 5 \end{ytableau} \succ \begin{ytableau} 3 & 2 \\ 4 & 1 \\ 5 \end{ytableau} \succ \begin{ytableau} 2 & 1 \\ 4 & 3 \\ 5 \end{ytableau} \succ \begin{ytableau} 1 & 2 \\ 4 & 3 \\ 5 \end{ytableau} \succ \begin{ytableau} 2 & 3 \\ 4 & 1 \\ 5 \end{ytableau} \succ \begin{ytableau} 1 & 3 \\ 4 & 2 \\ 5 \end{ytableau} \succ \begin{ytableau} 4 & 1 \\ 3 & 2 \\ 5 \end{ytableau} \succ \ldots$$

$$\ldots \succ \begin{ytableau} 4 & 5 \\ 2 & 3 \\ 1 \end{ytableau} \succ \begin{ytableau} 1 & 5 \\ 2 & 4 \\ 3 \end{ytableau} \succ \begin{ytableau} 2 & 5 \\ 1 & 4 \\ 3 \end{ytableau} \succ \begin{ytableau} 2 & 5 \\ 3 & 4 \\ 1 \end{ytableau} \succ \begin{ytableau} 1 & 5 \\ 3 & 4 \\ 2 \end{ytableau} \succ \begin{ytableau} 3 & 5 \\ 1 & 4 \\ 2 \end{ytableau} \succ \begin{ytableau} 3 & 5 \\ 2 & 4 \\ 1 \end{ytableau}.$$

Главная особенность введённого порядка состоит в том, что для любой *стандартной таблицы*[1] $T$ и любых $p \in R_T$ и $q \in C_T$ выполняются строгие неравенства $pT \succ T \succ qT$. Действительно, самое большое число в любом цикле перестановки $p$ сдвигается влево, а самое большое число в любом цикле перестановки $q$ сдвигается вверх. В частности, каждая стандартная таблица $T$

[1] См. n° 7.1 на стр. 94.

является минимальным элементом своей $R_T$-орбиты $R_T T$. Из этого вытекает, что для любого заполнения $U \prec T$ таблоид $\{U\} \neq \{T\}$ в модуле $M_\lambda$.

Упражнение 7.5. Покажите, что $c_T\{U\} = 0$ для любых стандартных таблиц $U \succ T$.

Теорема 7.3
Векторы $v_T$, где $T$ пробегает множество стандартных таблиц формы $\lambda$, образуют базис модуля Шпехта $S_\lambda$. В частности, $\dim S_\lambda = d_\lambda$.

Доказательство. Покажем, что $d_\lambda$ векторов $v_T$, построенных по всем стандартным таблицам $T$, линейно независимы. Выражение вектора $v_T = \sum_{q \in C_T} \operatorname{sgn}(q)\{qT\}$ через базисные векторы $\{U\}$ пространства $M_\lambda$ имеет вид $v_T = \{T\} + \sum_{U \prec T} \varepsilon_U \{U\}$, где $\varepsilon_U = -1, 0, 1$, а всякая линейная зависимость между ними может быть записана в виде[1] $v_T = \sum_{U \prec T} x_U v_U$. Раскладывая векторы $v_T$ и $v_U$ по базису из таблоидов, мы получаем равенство вида $\{T\} = \sum_{U \prec T} y_U\{U\}$, невозможное в силу того, что $\{T\} \neq \{U\}$ ни для какого $U \prec T$. Из линейной независимости векторов $v_T$ вытекает неравенство $\dim S_\lambda \geqslant d_\lambda$. С другой стороны, второе равенство из форм. (7-1) на стр. 94 и соотношение на сумму квадратов размерностей неприводимых представлений из сл. 5.7 на стр. 77 влекут равенство $\sum d_\lambda^2 = n! = \sum \dim^2 S_\lambda$. Поэтому $\dim S_\lambda = d_\lambda$. □

**7.5. Кольцо представлений симметрических групп.** Обозначим через $\mathfrak{R}_n$ аддитивную группу абелеву кольца представлений[2] группы $S_n$, т. е. свободный $\mathbb{Z}$-модуль с базисом $[V_\lambda]$, где $V_\lambda$ пробегает множество попарно неизоморфных представителей всех неприводимых представлений $S_n$. Иначе $\mathfrak{R}_n$ можно описать как целочисленную линейную оболочку неприводимых характеров группы $S_n$ в пространстве всех функций $S_n \to \mathbb{C}$. Положим $\mathfrak{R}_0 \overset{\text{def}}{=} \mathbb{Z}$. Мы собираемся снабдить прямую сумму $\mathfrak{R} \overset{\text{def}}{=} \bigoplus_{n \geqslant 0} \mathfrak{R}_n$ структурой *градуированного* коммутативного кольца с единицей[3]. Подчеркнём, что *умножение Литтлвуда – Ричардсона* на кольце $\mathfrak{R}$, которое мы для этого введём, *отличается* от обсуждавшегося в n° 6.2.2 на стр. 88 умножения $[U], [W] \mapsto [U \otimes W]$, имеющегося на каждом из $\mathfrak{R}_n$ в отдельности.

**7.5.1. Умножение Литтлвуда – Ричардсона в кольце $\mathfrak{R}$.** Каждая пара линейных представлений $\varphi : S_k \to \mathrm{GL}(U)$ и $\psi : S_m \to \mathrm{GL}(W)$ задаёт представление

$$\varphi \times \psi : S_k \times S_m \to \mathrm{GL}(U \otimes W), \quad (g, h) : u \otimes w \mapsto gu \otimes hw. \tag{7-14}$$

Вложим $S_k \times S_m$ в $S_{k+m}$ в качестве подгруппы, сохраняющей разбиение

$$\{1, \dots, k+m\} = \{1, \dots, k\} \sqcup \{k+1, \dots, k+m\}, \tag{7-15}$$

образуем представление $\operatorname{ind}(\varphi \times \psi)$ группы $S_{k+m}$, индуцированное представлением (7-14), и положим $[\varphi]\,[\psi] \overset{\text{def}}{=} [\operatorname{ind}(\varphi \times \psi)]$. Если вместо разбиения (7-15) воспользоваться другим разбиением $\{1, \dots, k+m\} = I \sqcup J$ на непересекающихся подмножества из $k$ и $m$ элементов, получится другая подгруппа $S_k \times S_m \subset S_{k+m}$, сопряжённая к использованной выше, и представление $\operatorname{ind}(\varphi \times \psi)$, индуцированное с этой подгруппы, будет изоморфно предыдущему.

Упражнение 7.6. Убедитесь в этом.

[1] Для этого надо оставить слева ненулевой член с максимальным индексом $T$, а все остальные члены перенести направо.
[2] См. n° 6.2.2 на стр. 88.
[3] Т. е. ввести на $\mathfrak{R}$ такое умножение, что $\mathfrak{R}_k \mathfrak{R}_m \subset \mathfrak{R}_{k+m}$.

Таким образом, класс $[\varphi][\psi]$ не зависит от выбора разбиения (7-15), используемого для его построения. В частности, умножение (7-14) коммутативно. Его ассоциативность вытекает из того, что для любых трёх представлений $\xi$, $\eta$ и $\zeta$ групп $S_k$, $S_\ell$ и $S_m$, оба класса $([\xi][\eta])[\zeta]$ и $[\xi]([\eta][\zeta])$ совпадают с классом представления $S_{m+n+k}$, индуцированного с представления подгруппы $S_k \times S_\ell \times S_m \subset S_{m+n+k}$ в тензорном произведении пространств представлений $\xi$, $\eta$ и $\zeta$ по правилу $(g_1, g_2, g_3) \mapsto \xi(g_1) \otimes \eta(g_2) \otimes \zeta(g_3)$.

Упражнение 7.7. Убедитесь в этом.

Дистрибутивность умножения по отношению к прямым суммам представлений следует из дистрибутивности тензорных произведений.

Лемма 7.6
Кольцо $\mathfrak{R}$ изоморфно кольцу многочленов с целыми коэффициентами от счётного числа переменных, отвечающих классам тривиальных одномерных представлений $[\mathbb{1}_k]$ групп $S_k$ для всех $k \in \mathbb{N}$. При этом классы модулей таблоидов $[M_\lambda] = [\mathbb{1}_{\lambda_1}] \dots [\mathbb{1}_{\lambda_n}] = [\mathbb{1}_1]^{\ell_1} \dots [\mathbb{1}_n]^{\ell_n}$, где $\ell_i$ означает количество строк длины $i$ в диаграмме $\lambda$, образуют базис кольца $\mathfrak{R}$ как модуля над $\mathbb{Z}$.

Доказательство. Из сл. 7.3 вытекает, что классы таблоидных представлений $[M_\lambda]$ выражаются через неприводимые классы $[S_\lambda]$ при помощи верхней треугольной матрицы с целыми коэффициентами и единицами по главной диагонали. Поэтому классы $[M_\lambda]$ образуют базис $\mathfrak{R}$ как модуля над $\mathbb{Z}$. Поскольку представление $M_\lambda$, отвечающее диаграмме $\lambda = (\lambda_1, \dots, \lambda_n)$, индуцировано с тривиального одномерного представления подгруппы $S_{\lambda_1} \times \dots \times S_{\lambda_n} \subset S_{|\lambda|}$, класс $[M_\lambda]$ является произведением классов тривиальных одномерных представлений $[\mathbb{1}_{\lambda_i}]$ групп $S_{\lambda_i}$. При этом $[\mathbb{1}_{\lambda_i}] = [M_{(\lambda_i)}]$ — это тоже модуль таблоидов, состоящих из одной строки длины $\lambda_i$. Поэтому совокупность мономов от классов тривиальных представлений в точности совпадает с совокупностью классов модулей таблойдов, а их формальное перемножение как мономов, совпадает с умножением в кольце $\mathfrak{R}$. □

**7.5.2. Скалярное произведение в кольце $\mathfrak{R}$.** Обозначим через $([U], [W])$ евклидово скалярное произведение на $\mathfrak{R}$, для которого базис из классов неприводимых представлений $[V_\lambda]$ является ортонормальным. Сумма $\mathfrak{R} = \oplus \mathfrak{R}_k$ является ортогональной относительно такого скалярного произведения, а для любых двух классов $[U] = \sum k_\lambda [V_\lambda]$ и $[W] = \sum m_\lambda [V_\lambda]$, лежащих в одной и той же компоненте $\mathfrak{R}_n$, выполняется равенство

$$([U], [W]) = \sum_{|\lambda|=n} k_\lambda m_\lambda = \dim \operatorname{Hom}_{S_n}(U, W) = (\chi_U, \chi_W)_n \,, \tag{7-16}$$

где $(\chi_U, \chi_W)_n$ означает скалярное произведение характеров в алгебре функций[1] $\mathbb{C}^{S_n}$. Как обычно, для каждой диаграммы $\mu$ обозначим через $m_i$ число её строк длины $i$ и положим

$$z_\mu = \prod_i m_i! \, i^{m_i} \,, \tag{7-17}$$

так что число элементов в классе сопряжённости $C_\mu \subset S_n$, состоящем из всех перестановок циклового типа $\mu$, равно $|C_\mu| = n!/z_\mu$. В силу зам. 6.2. на стр. 87 скалярное произведение характеров в правой части (7-16) переписывается в виде

$$\frac{1}{n!} \sum_{g \in S_n} \chi_U(g) \chi_W(g) = \frac{1}{n!} \sum_\mu |C_\mu| \chi_U(C_\mu) \chi_W(C_\mu) = \sum_\mu z_\mu^{-1} \chi_U(C_\mu) \chi_W(C_\mu) \,.$$

[1]См. зам. 6.2. на стр. 87.

Таким образом, скалярное произведение классов представлений $[U],[W]\in\mathfrak{R}_n$ равно

$$([U],[W]) = \sum_\mu z_\mu^{-1}\chi_U(C_\mu)\chi_W(C_\mu)\,. \tag{7-18}$$

**7.5.3. Изоморфизм кольца $\mathfrak{R}$ с кольцом симметрических функций.** В n° 4.6 на стр. 61 мы ввели на кольце $\Lambda$ симметрических функций с целыми коэффициентами скалярное произведение $\langle *\,,\,*\rangle$, для которого базис из полиномов Шура $s_\lambda$ является ортонормальным, базис из полных симметрических функций $h_\lambda$ является двойственным к мономиальному базису $m_\lambda$, а полиномы Ньютона $p_\lambda$ образуют ортогональный базис векторного пространства $\mathbb{Q}\otimes\Lambda$ со скалярными квадратами $\langle p_\lambda\,,\,p_\lambda\rangle = z_\lambda$. Согласно предл. 7.2 на стр. 98 значения $\psi_\lambda(C_\mu)$ характера $\psi_\lambda$ таблоидного представления $M_\lambda$ совпадают с коэффициентами разложения ньютоновской симметрической функции $p_\mu = \sum_\lambda\psi_\lambda(C_\mu)m_\lambda$ по мономиальному базису $m_\lambda$, а значит, равны скалярным произведениям симметрических функций $p_\lambda$ с элементами двойственного к мономиальному базиса из полных симметрических многочленов: $\psi_\lambda(C_\mu) = \langle p_\mu\,,\,h_\lambda\rangle$, которые в свою очередь являются коэффициентами разложения полных симметрических многочленов $h_\lambda$ по ортогональному базису $z_\mu^{-1}p_\mu$:

$$h_\lambda = \sum_\mu z_\mu^{-1}\langle p_\mu\,,\,h_\lambda\rangle p_\mu = \sum_\mu z_\mu^{-1}\chi_{M_\lambda}(C_\mu)p_\mu\,. \tag{7-19}$$

Сравнение равенств (7-19) и (7-18) подсказывает следующий результат:

Теорема 7.4

Существует изометрический изоморфизм колец $\mathrm{ch}\colon\mathfrak{R}\xrightarrow{\sim}\Lambda$, переводящий классы таблоидных представлений $[M_\lambda]$ в полные симметрические многочлены $h_\lambda$, классы неприводимых представлений $[S_\lambda]$ — в многочлены Шура $s_\lambda$, а инволюцию на классах представлений, заданную тензорным умножением на одномерное знаковое представление, — в каноническую инволюцию[1] $\omega$ на $\Lambda$, переводящую друг в друга $s_\lambda$ и $s_{\lambda^t}$, а также $h_\lambda$ и $e_\lambda$. Этот изоморфизм корректно задаётся формулой[2]

$$\mathrm{ch}([U]) \overset{\text{def}}{=} \sum_\mu z_\mu^{-1}\chi_U(C_\mu)p_\mu\,. \tag{7-20}$$

Доказательство. Отображение (7-20) очевидно линейно по $[U]$:

$$\mathrm{ch}([U]+[W]) = \mathrm{ch}([U\oplus W]) = \sum_\mu z_\mu^{-1}\chi_{U\oplus W}(C_\mu)p_\mu = \\ = \sum_\mu z_\mu^{-1}\left(\chi_U(C_\mu)+\chi_W(C_\mu)\right)p_\mu = \mathrm{ch}([U])+\mathrm{ch}([W])\,.$$

Согласно лем. 7.6 на стр. 102 и сл. 3.4 на стр. 41 оба кольца $\mathfrak{R}$ и $\Lambda$ являются кольцами многочленов от счётного числа переменных: первое — от классов тривиальных одномерных представлений $[\mathbb{1}_k]$ групп $S_k$, второе — от простейших полных симметрических многочленов[3] $h_k$, где в обоих случаях $k$ пробегает $\mathbb{N}$. В силу соотношения (7-19) отображение ch переводит каждый базисный моном $[M_\lambda] = [\mathbb{1}_{\lambda_1}]\dots[\mathbb{1}_{\lambda_n}] = [\mathbb{1}_1]^{\ell_1}\dots[\mathbb{1}_n]^{\ell_n}$, где $\ell_i$ равно количеству строк длины $i$

[1] См. сл. 4.2 на стр. 61.

[2] Не смотря на то, что она содержит знаменатели.

[3] Напомню, что $h_k(x)$ представляет собою сумму всех мономов полной степени $k$, см. n° 3.3 на стр. 40.

в диаграмме $\lambda$, в базисный моном $h_\lambda = h_{\lambda_1} \dots h_{\lambda_n} = h_1^{\ell_1} \dots h_n^{\ell_n}$ с сохранением мультипликативной структуры, ибо $\mathrm{ch}([\mathbb{1}_k]) = h_k$. Тем самым, отображение (7-20) является корректно определённым изоморфизмом колец. Ортогональность отображения ch вытекает из формулы (7-18) и того, что полиномы Ньютона $p_\lambda$ образуют в ортогональный базис $\mathbb{Q} \otimes \Lambda$ со скалярными квадратами[1] $\langle p_\lambda , p_\lambda \rangle = z_\lambda$. А именно:

$$\langle \mathrm{ch}([U]) , \mathrm{ch}([W]) \rangle = \sum_{\lambda,\mu} z_\lambda^{-1} z_\mu^{-1} \chi_U(C_\lambda)\chi_W(C_\mu) \langle p_\mu , p_\lambda \rangle = \sum_\mu z_\mu^{-1} \chi_U(g)\chi_W(g) = ([U], [W]) .$$

Из сл. 7.3 на стр. 100 вытекает, что ортонормальный базис $[S_\lambda]$ выражается через таблоидный базис $[M_\lambda]$ при помощи нижней унитреугольной матрицы: $[S_\lambda] = [M_\lambda] + \sum_{\mu \rhd \lambda} x_{\mu\lambda}[M_\mu]$. По форм. (4-18) на стр. 60 полные симметрические многочлены $h_\lambda$ выражаются через многочлены Шура $s_\lambda$ также при помощи нижней унитреугольной матрицы[2]: $h_\lambda = s_\lambda + \sum_{\mu \rhd \lambda} K_{\mu,\lambda} s_\mu$. Поэтому выражение $\mathrm{ch}\left([S_\lambda]\right)$ через полиномы Шура тоже задаётся некой нижней унитреугольной матрицей:

$$\mathrm{ch}\left([S_\lambda]\right) = \mathrm{ch}\big([M_\lambda] + \sum_{\mu \rhd \lambda} x_{\mu\lambda}[M_\mu]\big) = h_\lambda + \sum_{\mu \rhd \lambda} x_{\mu\lambda} h_\mu = s_\lambda + \sum_{\mu \rhd \lambda} y_{\mu\lambda} s_\mu .$$

Из равенств

$$1 = \big([S_\lambda], [S_\lambda]\big) = \langle \mathrm{ch}([S_\lambda]) , \mathrm{ch}([S_\lambda]) \rangle = \langle s_\lambda , s_\lambda \rangle + \sum_{\mu \rhd \lambda} y_{\mu\lambda}^2 \langle s_\mu , s_\mu \rangle = 1 + \sum_{\mu \rhd \lambda} y_{\mu\lambda}^2$$

мы заключаем, что все $y_{\mu\lambda} = 0$ и $\mathrm{ch}\left([S_\lambda]\right) = s_\lambda$. Утверждение об инволюциях вытекает из сл. 7.2 на стр. 97 и сл. 4.2 на стр. 61. □

Следствие 7.4 (правило Юнга)
Кратность вхождения неприводимого представления $S_\mu$ в модуль таблоидов $M_\lambda$ равна числу Костки $K_{\mu,\lambda}$.

Следствие 7.5 (правило Литтлвуда – Ричардсона)
Кратность вхождения $[S_\nu]$ в $[S_\lambda]\,[S_\mu]$ равна коэффициенту Литтлвуда – Ричардсона[3] $c_{\lambda\mu}^\nu$ из разложения $s_\lambda s_\mu = \sum_\nu c_{\lambda\mu}^\nu s_\nu$ .

Следствие 7.6 (правило ветвления индуцированных представлений)
Представление группы $S_{n+1}$, индуцированное неприводимым представлением $S_\lambda$ подгруппы $S_n \subset S_{n+1}$, является прямой суммой однократных неприводимых представлений $S_\mu$, диаграмма $\mu$ которых получается добавлением одной клетки к диаграмме $\lambda$.

Доказательство. Поскольку $[\mathrm{ind}(S_\lambda)] = [S_\lambda]\,[\mathbb{1}_1]$, утверждение вытекает из предыдущего следствия и формулы Пьери[4] для вычисления $s_\lambda h_1$. □

---

[1] См. предл. 4.2 на стр. 62.

[2] Напомню, что *число Костки* $K_{\mu,\lambda}$ равно количеству таблиц формы $\mu$, заполненных $\lambda_1$ единицами, $\lambda_2$ двойками, и т. д., и отлично от нуля только при $\mu \trianglerighteq \lambda$, а все $K_{\lambda,\lambda} = 1$, см. обсуждение перед упр. 4.3 на стр. 57.

[3] См. теор. 4.2 на стр. 59.

[4] См. упр. 4.5 на стр. 60.

Следствие 7.7 (правило ветвления ограниченных представлений)
Ограничение неприводимого представления $S_\lambda$ группы $S_n$ на подгруппу $S_{n-1} \subset S_n$ является прямой суммой однократных неприводимых представлений $S_\mu$, диаграмма $\mu$ которых получается выкидыванием одной клетки из диаграммы $\lambda$.

Доказательство. Это получается из предыдущего следствия и взаимности Фробениуса: кратность вхождения неприводимого представления $S_\mu$ в res $S_\lambda$ равна кратности вхождения неприводимого представления $S_\lambda$ в ind $S_\mu$. □

Следствие 7.8 (формула Фробениуса для характеров $S_n$)
Значение характера $\chi_\lambda$ неприводимого представления $S_\lambda$ симметрической группы $S_n$ на классе сопряжённости $C_\mu \subset S_n$ равно каждому из следующих трёх чисел:

- коэффициенту при $z_\mu^{-1}p_\mu(x)$ в разложении многочлена Шура $s_\lambda(x)$ по базису $z_\mu^{-1}p_\mu(x)$ в векторном пространстве $\mathbb{Q} \otimes \Lambda$
- коэффициенту при $s_\lambda(x)$ в разложении многочлена Ньютона $p_\mu(x)$ по базису Шура $s_\lambda(x)$ в $\mathbb{Z}$-модуле $\Lambda$
- коэффициенту при одночлене $x^{\lambda+\delta} = x_1^{\lambda_1+n-1}x_2^{\lambda_2+n-2} \dots x_n^{\lambda_n}$ в многочлене
$$p_\mu(x)\Delta_\delta(x) = p_1(x)^{m_1} \dots p_n(x)^{m_n} \prod_{i<j}(x_i - x_j)\,,$$
где $p_k(x) = \sum_i x_i^k$ суть степенные суммы Ньютона, число $m_i$ равно количеству строк длины $i$ в диаграмме $\mu$, а $\Delta_\delta(x) = \det\left(x_j^{n-i}\right)$ — это определитель Вандермонда.

Доказательство. Первое вытекает прямо из теор. 7.4. Второе — из свойств скалярного произведения на кольце симметрических функций: поскольку система многочленов $p_\mu$ ортогональна со скалярными квадратами $z_\mu$, коэффициент при $z_\mu^{-1}p_\mu(x)$ в разложении $s_\lambda$ по базису $p_\mu$ равен скалярному произведению $\langle\, s_\lambda\,,\, p_\mu\,\rangle$, которое в свою очередь равно коэффициенту при $s_\lambda$ в разложении $p_\mu$ по ортонормальному базису $s_\lambda$. Для доказательства третьего запишем $s_\lambda$ по формуле Якоби – Труди как отношение определителей $s_\lambda(x) = \Delta_{\lambda+\delta}(x)\,/\,\Delta_\delta(x)$ и умножим обе части разложения $p_\mu(x) = \sum_\lambda \chi_\lambda(C_\mu)\Delta_{\lambda+\delta}(x)\,/\,\Delta_\delta(x)$ на $\Delta_\delta$. Получим равенство $p_\mu(x)\Delta_\delta(x) = \sum_\lambda \chi_\lambda(C_\mu)\Delta_{\lambda+\delta}(x)$, означающее, что $\chi_\lambda(C_\mu)$ равен коэффициенту разложения кососимметрического многочлена $p_\mu(x)\Delta_\delta(x)$ по стандартному детерминантному базису[1] $\Delta_{\lambda+\delta}(x)$. □

**7.5.4. Размерности неприводимых представлений.** По формуле Фробениуса размерность $\dim S_\lambda = \chi_\lambda(1)$ равна коэффициенту при $x^{\lambda+\delta} = x_1^{\lambda_1+n-1}x_2^{\lambda_2+n-2}\dots x_n^{\lambda_n}$ в многочлене $p_1^n\Delta_\delta = \left(\sum x_i\right)^n \det\left(x_j^{n-i}\right) = \sum_{m_1\dots m_n} \frac{n!}{m_1!\dots m_n!}x_1^{m_1}\dots x_n^{m_n}\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)x_1^{n-\sigma(1)}\dots x_n^{n-\sigma(n)}$. Обозначим строго убывающие длины строк диаграммы $\eta = \lambda + \delta$ через $\eta_i = \lambda_i + n - i$. Коэффициент при $x^\eta = x_1^{\eta_1}\dots x_n^{\eta_n}$ в предыдущем произведении равен
$$\sum_\sigma \frac{\operatorname{sgn}(\sigma)n!}{\prod_j\left(\eta_j - n + \sigma(j)\right)!} = \frac{n!}{\eta_1!\dots\eta_n!}\sum_\sigma \operatorname{sgn}(\sigma)\prod_j \eta_j(\eta_j-1)\dots(\eta_j - n + \sigma(j) + 1)\,,$$

[1] См. n° 3.1.2 на стр. 38.

где суммирование происходит по всем перестановкам $\sigma \in S_n$, для которых каждое из $n$ чисел $\eta_j - n + \sigma(j) \geqslant 0$, и $j$-тый сомножитель последнего произведения сам является произведением $n - \sigma(j)$ последовательно убывающих чисел, начиная с $\eta_j$. Такая сумма равна

$$\det\begin{pmatrix} \eta_1 \dots (\eta_1 - n + 1) & \eta_2 \dots (\eta_2 - n + 1) & \dots & \eta_n \dots (\eta_n - n + 1) \\ \vdots & \vdots & \cdots & \vdots \\ \eta_1(\eta_1 - 1) & \eta_2(\eta_2 - 1) & \cdots & \eta_n(\eta_n - 1) \\ \eta_1 & \eta_2 & \cdots & \eta_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

Упражнение 7.8. Покажите, что этот определитель равен $\prod_{i<j}(\eta_i - \eta_j)$.

Таким образом, нами установлено

Следствие 7.9 (формула Фробениуса для размерностей)
Пусть $\eta = \lambda + \delta$, т. е. $\eta_i = \lambda_i + n - i$. Тогда $\dim S_\lambda = \frac{n!}{\eta_1! \dots \eta_n!} \prod_{i<j}(\eta_i - \eta_j)$. □

Упражнение 7.9 (формула крюков). Назовём *крюком* клетки $a$ в диаграмме Юнга $\lambda$ Г-образную поддиаграмму, состоящую из клетки $a$ и всех клеток ниже $a$ в том же столбце и всех клеток правее $a$ в той же строке. Количество клеток в таком крюке обозначим через $\Gamma(a)$ и назовём *длиной крюка* клетки $a$. Докажите, что $\dim S_\lambda = n! / \prod_{a \in \lambda} \Gamma(a)$.

Например, длины крюков диаграммы $\lambda = (4, 2, 1)$ суть $\begin{array}{|c|c|c|c|}\hline 6&4&2&1\\ \hline 3&1 \\ \cline{1-2} 1 \\ \cline{1-1}\end{array}$, откуда размерность модуля Шпехта $S_{(4,2,1)}$ группы $S_7$ равна $7!/(6 \cdot 4 \cdot 3 \cdot 2) = 7 \cdot 5 = 35$. Довольно нетривиальным следствием из упр. 7.9 и теор. 7.3 на стр. 101 является возможность подсчитать количество стандартных таблиц формы $\lambda$ по формуле крюков. К примеру, только что проделанное вычисление показывает, что стандартных таблиц формы $\begin{array}{|c|c|c|c|}\hline \ & \ & \ & \ \\ \hline \ & \ \\ \cline{1-2} \ \\ \cline{1-1}\end{array}$ имеется ровно 35 штук.

## §8. Категории и функторы

**8.1. Категории.** Категория $\mathcal{C}$ это *класс*[1] объектов, обозначаемый $\operatorname{Ob}\mathcal{C}$, в котором для каждой упорядоченной пары объектов $X, Y \in \operatorname{Ob}\mathcal{C}$ задано *множество* морфизмов

$$\operatorname{Hom}(X,Y) = \operatorname{Hom}_{\mathcal{C}}(X,Y)\,.$$

Для разных пар объектов эти множества не пересекаются. Морфизмы удобно представлять себе в виде стрелок $\varphi : X \to Y$. Объединение всех стрелок категории $\mathcal{C}$ обозначается

$$\operatorname{Mor}\mathcal{C} = \bigsqcup_{X,Y\in\operatorname{Ob}\mathcal{C}} \operatorname{Hom}_{\mathcal{C}}(X,Y)$$

и тоже является классом, а не множеством. Для каждой тройки объектов $X, Y, Z \in \operatorname{Ob}\mathcal{C}$ имеется отображение $\operatorname{Hom}(Y,Z) \times \operatorname{Hom}(X,Y) \to \operatorname{Hom}(X,Z)$, $(\varphi,\psi) \mapsto \varphi\circ\psi\ (=\varphi\psi)$, именуемое *композицией*[2] и ассоциативное в том смысле, что $(\chi\circ\varphi)\circ\psi = \chi\circ(\varphi\circ\psi)$ всякий раз, когда эти композиции определены. Наконец, у каждого объекта $X \in \operatorname{Ob}\mathcal{C}$ есть *тождественный эндоморфизм* $\operatorname{Id}_X \in \operatorname{Hom}(X,X)$, удовлетворяющий условиям[3] $\varphi\circ\operatorname{Id}_X = \varphi$ и $\operatorname{Id}_X\circ\psi = \psi$ для любых стрелок $\varphi : X \to Y$ и $\psi : Z \to X$.

Подкатегория $\mathcal{D} \subset \mathcal{C}$ это категория, все объекты, стрелки и композиции которой наследуются из $\mathcal{C}$. Подкатегория называется *полной*, если $\operatorname{Hom}_{\mathcal{D}}(X,Y) = \operatorname{Hom}_{\mathcal{C}}(X,Y)$ для всех $X, Y \in \operatorname{Ob}\mathcal{D}$.

Категория $\mathcal{C}$ называется *малой*, если $\operatorname{Ob}\mathcal{C}$ это *множество*, а не больший класс. В этом случае $\operatorname{Mor}\mathcal{C}$ тоже является множеством.

Пример 8.1 (категории, не являющиеся малыми)

Примеры категорий, которые *не* являются малыми, это категория $\mathcal{S}et$ всех множеств и всех отображений, категория $\mathcal{T}op$ топологических пространств и непрерывных отображений, категория $\mathcal{V}ec_{\Bbbk}$ векторных пространств над полем $\Bbbk$ и $\Bbbk$-линейных отображений и её полная подкатегория $vec_{\Bbbk}$ конечномерных пространств, категории $R$-$\mathcal{M}od$ и $\mathcal{M}od$-$R$ левых и правых модулей над кольцом $R$ и $R$-линейных отображений и их полные подкатегории $R$-$mod$ и $mod$-$R$ конечно представимых[4] модулей, категория абелевых групп $\mathcal{A}b = \mathbb{Z}$-$\mathcal{M}od$, категория $\mathcal{G}rp$ всех групп и групповых гомоморфизмов, категория $\mathcal{C}mr$ коммутативных колец с единицей и гомоморфизмов, переводящих единицу в единицу, и т. п.

Пример 8.2 (предпорядки, чумы и топологии)

Каждое множество $M$ с предпорядком[5] $\leqslant$ может рассматриваться как малая категория, объекты которой суть элементы $m \in M$, стрелки суть неравенства:

$$\operatorname{Hom}_M(n,m) = \begin{cases} \text{одноэлементное множество, когда } n \leqslant m, \\ \varnothing \text{ в остальных случаях}\,, \end{cases}$$

[1] Не хотелось бы вдаваться в точную формализацию этого термина (содержательную в той же мере, как формализация арифметики и теории множеств, изучаемые в стандартном курсе математической логики). Для наших нужд достаточно, что такая формализация существует и позволяет говорить, например, о «категории множеств», объекты которой, по понятным причинам, множества не образуют.

[2] Значок композиции «$\circ$», как и знак умножения, принято опускать, когда ясно, о чём речь.

[3] Выкладка $\operatorname{Id}' = \operatorname{Id}'\circ\operatorname{Id}'' = \operatorname{Id}''$ показывает, что тождественный морфизм единствен.

[4] Модуль называется *конечно представимым*, если он изоморфен фактору свободного модуля конечного ранга по конечно порождённому подмодулю.

[5] Т. е. рефлексивным и транзитивным бинарным отношением.

а композиция стрелок $k \leqslant \ell$ и $\ell \leqslant n$ это стрелка $k \leqslant n$. Наличие композиции и тождественных морфизмов обеспечиваются транзитивностью и рефлексивностью отношения $\leqslant$.

Если предпорядок $\leqslant$ на $M$ является частичным порядком[1], то при $m \neq n$ как минимум одно из множеств $\mathrm{Hom}(m,n)$, $\mathrm{Hom}(n,m)$ пусто. Важным примером такой категории-чума[2] является категория $\mathcal{U}(X)$ всех открытых подмножеств топологического пространства $X$, стрелками в которой являются включения:

$$\mathrm{Hom}_{\mathcal{U}(X)}(U,W) = \begin{cases} \text{вложение } U \hookrightarrow W, \text{ если } U \subseteq W \\ \text{пустое множество, когда } U \not\subseteq W. \end{cases}$$

Пример 8.3 (малые категории и ассоциативные алгебры)
Всякую ассоциативную алгебру[3] $A$ с единицей можно рассматривать как малую категорию с одним объектом $*$ и множеством стрелок $\mathrm{Hom}(*,*) = A$, композиция на котором задаётся умножением в этой алгебре. Наоборот, со всякой малой категорией $\mathcal{C}$ и коммутативным кольцом $K$ с единицей можно связать *алгебру стрелок* $K[\mathcal{C}]$, состоящую из формальных конечных линейных комбинаций стрелок категории $\mathcal{C}$ с коэффициентами в $K$. Условимся для заданного множества $M$ обозначать через $K \otimes M$ свободный $K$-модуль с базисом $M$, образованный всеми конечными формальными линейными комбинациями элементов множества $M$ с коэффициентами из $K$. Тогда $K[\mathcal{C}] \overset{\text{def}}{=} \bigoplus_{X,Y \in \mathrm{Ob}\,\mathcal{C}} K \otimes \mathrm{Hom}(X,Y) = \left\{ \sum x_i \varphi_i \,\middle|\, x_i \in K\,,\ \varphi_i \in \mathrm{Mor}(\mathcal{C}) \right\}$. Умножение стрелок в алгебре $K[\mathcal{C}]$ определяется их композицией в категории $\mathcal{C}$

$$\varphi\psi \overset{\text{def}}{=} \begin{cases} \varphi \circ \psi & \text{если конец } \psi \text{ совпадает с началом } \varphi \\ 0 & \text{во всех прочих случаях} \end{cases}$$

и по дистрибутивности распространяется на произвольные конечные линейные комбинации стрелок. Алгебру $K[\mathcal{C}]$ можно представлять себе как алгебру финитных квадратных матриц[4], строки и столбцы которых занумерованы объектами категории, и в каждой клетке $(Y,X)$ стоят элементы из своего $K$-модуля $K \otimes \mathrm{Hom}(X,Y)$. Эта алгебра, вообще говоря, некоммутативна и без единицы, однако, для всякого $f \in K[\mathcal{C}]$ существует такой идемпотент $e_f = e_f^2$, что $e_f \circ f = f \circ e_f = f$: например, можно взять сумму тождественных эндоморфизмов $\mathrm{Id}_X$ всех объектов $X$, служащих началами или концами стрелок, линейной комбинацией которых является стрелка $f$.

**8.1.1. Мономорфизмы, эпиморфизмы и изоморфизмы.** Стрелка $\varphi$ называется *мономорфизмом*[5] (соотв. *эпиморфизмом*[6]), если на неё можно сокращать слева (соотв. справа), т. е. когда $\varphi\alpha = \varphi\beta \Rightarrow \alpha = \beta$ (соотв. $\alpha\varphi = \beta\varphi \Rightarrow \alpha = \beta$). По умолчанию мы используем стрелки $\hookrightarrow$ для обозначения мономорфизмов, и стрелки $\twoheadrightarrow$ для эпиморфизмов. Стрелка $\varphi : X \to Y$ называется *изоморфизмом* (или *обратимой* стрелкой) и обозначается $\xrightarrow{\sim}$, если существует такая стрелка $\psi : Y \to X$, что $\varphi\psi = \mathrm{Id}_Y$ и $\psi\varphi = \mathrm{Id}_X$. В этой ситуации объекты $X$ и $Y$ называются *изоморфными*, а морфизмы $\varphi$ и $\psi$ — *обратными* друг к другу. Например, в предупорядоченном множестве $M$,

[1] Т. е. кососимметричен в том смысле, что одновременное выполнение неравенств $x \leqslant y$ и $y \leqslant x$ влечёт равенство $x = y$.

[2] Т. е. частично упорядоченного множества.

[3] Более общим образом — любой ассоциативный моноид, т. е. полугруппу с единицей.

[4] Возможно, бесконечного размера, но с конечным числом ненулевых элементов.

[5] А также *вложением* или *инъективным* морфизмом.

[6] А также *наложением* или *сюрьективным* морфизмом.

рассматриваемом как категория[1], изоморфность элементов $m$ и $n$ означает, что $m \leqslant n$ и $n \leqslant m$, т. е. $m$ и $n$ принадлежат одному классу эквивалентности, ассоциированному с предпорядком.

**8.1.2. Подобъекты и фактор объекты.** Класс инъективной стрелки с концом в $X$ по модулю её умножения справа на обратимые стрелки называется *подобъектом* объекта $X$, а класс сюрьективной стрелки с началом в $X$ по модулю левого умножения на обратимые стрелки — *фактор объектом* объекта $X$. Категория называется *умеренно мощной*[2], если подобъекты любого её объекта образуют множество. Все категории из прим. 8.3 умеренно мощны.

Упражнение 8.1 (частичный порядок на под- и фактор объектах). Проверьте, что в умеренно мощной категории отношение $\varphi \subseteq \psi$, означающее, что существует такая стрелка $\xi$, что $\varphi = \psi\xi$, задаёт частичный порядок на множестве подобъектов, а отношение $\varphi \geqslant \psi$, означающее наличие такой стрелки $\xi$, что $\psi = \xi\varphi$, задаёт частичный порядок на множестве фактор объектов.

Пример 8.4 (конечные упорядоченные множества и комбинаторные симплексы)
Обозначим через $\Delta_{\text{big}}$ категорию, объектами которой являются конечные упорядоченные множества $X$, а морфизмами — сохраняющие порядок[3] отображения. Категория $\Delta_{\text{big}}$ не является малой[4], но содержит полную малую подкатегорию $\Delta \subset \Delta_{\text{big}}$, объектами которой являются конечные подмножества в $\mathbb{Z}$ вида

$$[n] \overset{\text{def}}{=} \{0, 1, \dots, n\}, \quad n \geqslant 0, \tag{8-1}$$

со стандартным порядком. Множество (8-1) называется $n$-мерным *комбинаторным симплексом*, а категория $\Delta$ — *симплициальной категорией*. Для любого $X \in \operatorname{Ob}\Delta_{\text{big}}$ имеется *единственный* изоморфизм $n_X : X \xrightarrow{\sim} [n]$ с *единственным* $[n] \in \operatorname{Ob}\Delta$, а именно нумерация элементов $X$ в порядке возрастания.

Упражнение 8.2. Сколько всего стрелок в множестве $\operatorname{Hom}_\Delta([n],[m])$? Сколько среди них инъективных? Сколько сюрьективных? Покажите, что алгебра стрелок $\mathbb{Z}[\Delta]$, как абстрактная ассоциативная алгебра, порождается стрелками

$$e_n = \operatorname{Id}_{[n]} \qquad \text{(тождественное отображение)} \tag{8-2}$$

$$\partial_n^{(i)} : [n-1] \hookrightarrow [n] \qquad \text{(вложение, образ которого не содержит } i) \tag{8-3}$$

$$s_n^{(i)} : [n] \twoheadrightarrow [n-1] \qquad \text{(наложение, склеивающее } i \text{ с } (i+1)) \tag{8-4}$$

и опишите образующие идеала соотношений между этими стрелками.

**8.1.3. Обращение стрелок.** С каждой категорией $\mathcal{C}$ связана *противоположная* категория $\mathcal{C}^{\text{opp}}$ с теми же объектами, но с обращённым направлением всех стрелок:

$$\operatorname{Ob}\mathcal{C}^{\text{opp}} = \operatorname{Ob}\mathcal{C}, \quad \operatorname{Hom}_{\mathcal{C}^{\text{opp}}}(X,Y) = \operatorname{Hom}_{\mathcal{C}}(Y,X), \quad \varphi^{\text{opp}} \circ \psi^{\text{opp}} = (\psi \circ \varphi)^{\text{opp}}.$$

На языке алгебр такое обращение стрелок означает переход от алгебры $C = K[\mathcal{C}]$ к противоположной алгебре $C^{\text{opp}}$ из тех же элементов, но с происходящим в противоположном порядке умножением. Мономорфизмы и подобъекты категории $\mathcal{C}$ являются эпиморфизмами и фактор объектами категории $\mathcal{C}^{\text{opp}}$ и наоборот.

---

[1] См. прим. 8.2 на стр. 107.
[2] По-английски: *well powered*.
[3] Т. е. такие отображения $\varphi : X \to Y$, что $x_1 \leqslant x_2 \Rightarrow \varphi(x_1) \leqslant \varphi(x_2)$ для всех $x_1, x_2 \in X$.
[4] По упомянутым выше логическим причинам, см. сноску на стр. 107.

**8.2. Функторы.** Функтор[1] $F : \mathcal{C} \to \mathcal{D}$ из категории $\mathcal{C}$ в категорию $\mathcal{D}$ это отображение классов $\operatorname{Ob}\mathcal{C} \to \operatorname{Ob}\mathcal{D}$, $X \mapsto F(X)$, и набор таких отображений множеств[2]

$$\operatorname{Hom}_{\mathcal{C}}(X, Y) \to \operatorname{Hom}_{\mathcal{D}}(F(X), F(Y)), \quad \varphi \mapsto F(\varphi), \tag{8-5}$$

что $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$ для всех $X \in \operatorname{Ob}\mathcal{C}$ и $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$ всякий раз, когда композиция $\varphi \circ \psi$ определена. На языке ассоциативных алгебр, каждый функтор $F : \mathcal{C} \to \mathcal{D}$ задаёт *гомоморфизм* алгебр стрелок $F : K[\mathcal{C}] \to K[\mathcal{D}]$. Если все отображения (8-5) сюрьективны, функтор $F$ называется *полным*[3]. Образ такого функтора является полной подкатегорией. Если все отображения (8-5) инъективны, функтор $F$ называется *строгим*[4]. Такой функтор задаёт вложение алгебр стрелок. Полные строгие функторы иначе называются *вполне строгими*.

Простейшие функторы — это *тождественный функтор* $\mathrm{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$, тождественно действующий на объектах и морфизмах, и *забывающие функторы*, действующие из какой-либо категории множеств с дополнительной структурой[5], морфизмы в которой суть сохраняющие эту структуру отображения множеств, в категорию $\mathcal{S}et$ всех множеств — такие функторы просто забывают о структуре. Забывающий функтор не строг, если имеются различные морфизмы структур, одинаково действующие на подлежащих множествах, и не полон, если не всякое отображение множеств сохраняет рассматриваемую структуру.

Пример 8.5 (геометрическая реализация комбинаторных симплексов)
Зададим функтор $\Delta \to \mathcal{T}op$ из категории комбинаторных симплексов в категорию топологических пространств, сопоставляя $n$-мерному комбинаторному симплексу $[n]$ стандартный $n$-мерный симплекс[6]

$$\Delta^n = \left\{ (x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1} \;\middle|\; \sum x_\nu = 1\,,\ x_\nu \geqslant 0 \right\} \subset \mathbb{R}^{n+1}, \tag{8-6}$$

а стрелке $\varphi : [n] \to [m]$ — единственное аффинное отображение $\varphi_* : \Delta^n \to \Delta^m$, действующее на базисные векторы по правилу $e_\nu \mapsto e_{\varphi(\nu)}$. Это строгий, но не полный функтор. Образующие элементы (8-3) и (8-4) алгебры стрелок категории $\Delta$ переводятся этим функтором, соответственно, во *вложение $i$-той грани* $\Delta^{(n-1)} \hookrightarrow \Delta^n$ и в *вырождение вдоль $i$-того ребра*[7] $\Delta^n \twoheadrightarrow \Delta^{(n-1)}$.

**8.2.1. Предпучки.** Функтор $F : \mathcal{C}^{\mathrm{opp}} \to \mathcal{D}$ называется *контравариантным функтором* из $\mathcal{C}$ в $\mathcal{D}$ или *предпучком*[8] объектов категории $\mathcal{D}$ на категории $\mathcal{C}$. Такой функтор оборачивает композицию: $F(\varphi \circ \psi) = F(\psi) \circ F(\varphi)$ и на языке ассоциативных алгебр является *антигомоморфизмом* алгебр стрелок.

[1]Иногда вместо «функтор» говорят *ковариантный функтор*.

[2]По одному отображению для каждой упорядоченной пары объектов $X, Y \in \operatorname{Ob}\mathcal{C}$.

[3]По-английски: *full*.

[4]По-английски: *faithful*.

[5]Например, геометрической — такой, как топология или структура гладкого многообразия, или алгебраической — такой, как структура группы, кольца или модуля.

[6]Т. е. выпуклую оболочку концов стандартных базисных векторов $e_0, e_1, \dots, e_n$ в $\mathbb{R}^{n+1}$.

[7]Т. е. в проекцию симплекса на симплекс на единицу меньшей размерности вдоль ребра, соединяющего $i$-тую вершину с $(i+1)$-й.

[8]Термин «предпучок» употребляется чаще в ситуациях, когда категоря $\mathcal{C}$ малая.

Пример 8.6 (триангулированные пространства)
Обозначим через $\varDelta_s \subset \varDelta$ неполную подкатегорию, объектами которой тоже являются комбинаторные симплексы, $\operatorname{Ob}\varDelta_s = \operatorname{Ob}\varDelta$, но в качестве морфизмов допускаются только *строго возрастающие*[1] отображения. Категория $\varDelta_s$ называется *полусимплициальной категорией*.

Упражнение 8.3. Убедитесь, что алгебра стрелок $\mathbb{Z}[\varDelta_s]$ порождается тождественными стрелками $e_n = \mathrm{Id}_{[n]}$ и отображениями вложения граней $\partial_n^{(i)}$ из (8-3).

Предпучок множеств $X : \varDelta_s^{\mathrm{opp}} \to \mathcal{S}et$ на полусимплициальной категории $\varDelta_s$ называется *полусимплициальным множеством* и является ни чем иным, как комбинаторным описанием *триангулированного топологического пространства* $|X|$, которое называется *геометрической реализацией* полусимплициального множества $X$. В самом деле, функтор $X$ задаёт для каждого целого неотрицательного $n$ множество $X_n = X([n])$, каждый элемент которого мы будем воспринимать как стандартный $n$-мерный симплекс (8-6). Таким образом, каждое множество $X_n$ представляет собою набор одинаковых $n$-мерных симплексов $\varDelta^n$. Пространство $|X|$ склеивается из них так. Стрелки $\varphi : [n] \to [m]$ категории $\varDelta_s$ биективно соответствуют $n$-мерным граням $m$-мерного симплекса $\varDelta^m$. Будем воспринимать отображение $X(\varphi) : X_m \to X_n$, которое функтор $X$ сопоставляет стрелке $\varphi$, как *правило склейки*: оно указывает каждому $m$-мерному симплексу $x \in X_m$, какой именно $n$-мерный симплекс $X(\varphi)x \in X_n$ надлежит приклеить к $x$ в качестве $\varphi$-той $n$-мерной грани.

Так, на рис. 8◇1 показана стандартная триангуляция двумерного тора, склеенного из прямоугольника, изображённого на рис. 8◇2. Эта триангуляция состоит из одного 0-мерного симплекса, в который склеятся все вершины прямоугольника, трёх 1-мерных симплексов, в которые склеятся, соответственно, две горизонтальных стороны, две вертикальных стороны, и диагональ прямоугольника, а также пары 2-мерных симплексов, на которые прямоугольник разрезается диагональю. Стрелки на рис. 8◇2 изображают порядок на множестве вершин каждого симплекса и направлены от меньших вершин к большим. Вертикальные рёбра $e_2$ с рис. 8◇2 изображаются на рис. 8◇1 меридианом тора, а горизонтальные рёбра $e_1$ — экватором тора. Соответствующее полусимплициальное множество $X$ имеет $X_0 = \{v\}$, $X_1 = \{e_1, e_2, e_3\}$, $X_2 = \{f_1, f_2\}$, и $X_i = \varnothing$ для всех $i \geqslant 3$, а отображения склейки $X(\varphi)$ действуют по правилам

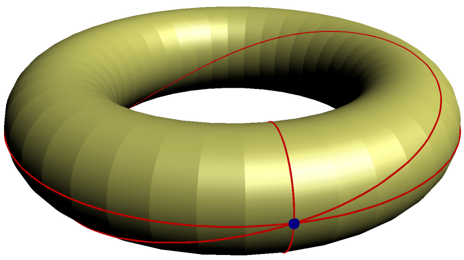


**Рис. 8◇1.** Триангуляция тора.

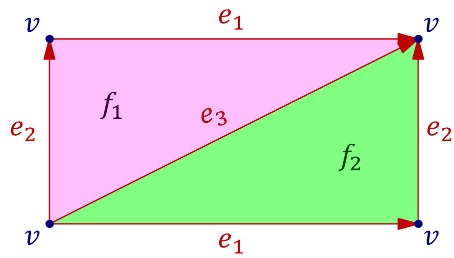



**Рис. 8◇2.** Симплексы триангуляции.

$$
\begin{aligned}
X(\partial_1^0) = X(\partial_1^1) : X_1 \to X_0\,, &\quad e_i \mapsto v \text{ для всех } i = 1,2,3\\
X(\partial_2^0) : X_2 \to X_1\,, &\quad f_1 \mapsto e_1\,,\ f_2 \mapsto e_2\,,\\
X(\partial_2^1) : X_2 \to X_1\,, &\quad f_1 \mapsto e_3\,,\ f_2 \mapsto e_3\,,\\
X(\partial_2^2) : X_2 \to X_1\,, &\quad f_1 \mapsto e_2\,,\ f_2 \mapsto e_1\,.
\end{aligned}
\tag{8-7}
$$

[1] Т. е. сохраняющие порядок и инъективные.

Упражнение 8.4. Существует ли триангуляция окружности $S^1$ а) тремя 0-мерными и тремя 1-мерным симплексами[1] б) одним 0-мерным и одним 1-мерным симплексом? Существует ли триангуляция двумерной сферы $S^2$ в) четырьмя 0-мерными, шестью 1-мерными и четырьмя 2-мерным симплексами г) двумя 0-мерными, одним 1-мерным и одним 2-мерным симплексом? Если да, задайте все отображения $X(\varphi)$ явно, если нет, объясните почему.

Пример 8.7 (симплициальные множества)
Предпучок множеств $X : \Delta^{\mathrm{opp}} \to \mathcal{S}et$ на всей симплициальной категории называется *симплициальным множеством*. Из каждого симплициального множества $X$ также, как и в предыдущем примере, можно изготовить топологическое пространство $|X|$, называемое его *геометрической реализацией*. Для этого, как и выше, сопоставим каждой точке $x \in X_n$ стандартный $n$-мерный симплекс $\Delta^n_x$ и обозначим через $\varphi^* \overset{\text{def}}{=} X(\varphi)$ отображение $X_m \to X_n$, которое функтор $X$ сопоставляет каждому неубывающему отображению $\varphi : [n] \to [m]$ из категории $\Delta$, а через $\varphi_* : \Delta^n \to \Delta^m$ — аффинное отображение симплексов, переводящее вершины симплекса $\Delta^n$ в вершины симплекса $\Delta^m$ так, как предписывает $\varphi$. После чего для каждого $m$, каждого $x \in X_m$ и каждой стрелки $\varphi : [n] \to [m]$ склеим каждую точку $s \in \Delta^n_{\varphi^*(x)}$ с точкой $\varphi_*(s) \in \Delta^m_x$. На языке формул результат такой склейки описывается как топологическое фактор пространство дизъюнктного объединения[2] $\bigsqcup_{n\geqslant 0} X_n \times \Delta^n$ по наименьшему отношению эквивалентности, содержащему отождествления $\left(\varphi^* x, s\right) \simeq \left(x, \varphi_* s\right)$ для всех точек $x \in X_m$, $s \in \Delta^n$ и стрелок $\varphi : [n] \to [m]$.

Если стрелка $\varphi : [n] \to [m]$ является композицией наложения $\sigma : [n] \twoheadrightarrow [k]$ и вложения $\delta : [k] \hookrightarrow [m]$, то каждый $n$-мерный симплекс $\Delta^n_z$, лежащий в образе $\varphi^*$ и помеченный точкой $z = \sigma^* y = \sigma^* \delta^* x$, вклеится в пространство $|X|$ в виде $k$-мерного симплекса $\Delta^k_y = \sigma_* \Delta^n_z$, полученного из $\Delta^n_z$ аффинно линейной проекцией $\sigma_* : \Delta^n \twoheadrightarrow \Delta^k$. При этом он окажется $\delta$-той $k$-мерной гранью $m$-мерного симплекса $\Delta^m_x$. Таким образом, каждый симплекс $z \in X_n$, лежащий в образе отображения $\sigma^*$, отвечающего какой-нибудь стрелке $\sigma : [n] \to [k]$ с $k < n$, виден в итоговом пространстве $|X|$ как симплекс меньшей, чем $n$ размерности. Такие симплексы называются *вырожденными*. Их использование позволяет описывать более общие клеточные структуры, чем стандартные триангуляции. Платой за это является громоздкость получающегося описания: для любого функтора $X : \Delta^{\mathrm{opp}} \to \mathcal{S}et$ каждое из множеств $X_n$ непусто.

Например, $n$-мерная сфера $S^n$ гомеоморфна топологическому фактору стандартного $n$-мерного симплекса по его границе[3] $S^n \simeq \Delta^n / \partial \Delta^n$. Этот гомеоморфизм задаёт на сфере $S^n$ клеточную структуру, состоящую из одной нульмерной вершины, в которую склеится граница симплекса, и одной $n$-мерной клетки, в которую превратится весь симплекс. Она описывается предпучком $X : \Delta^{\mathrm{opp}} \to \mathcal{S}et$, у которого при всех $k$ множество $X_k = X([k])$ получается из множества $\mathrm{Hom}_\Delta([k],[n])$ отождествлением всех неэпиморфных стрелок в один элемент, а правило склейки $\varphi^* : X_m \to X_k$, отвечающее неубывающему отображению $\varphi : [k] \to [m]$, переводит класс стрелки $\zeta : [m] \to [n]$ в класс стрелки $\zeta\varphi : [k] \to [n]$.

Упражнение 8.5. Убедитесь, что это описание корректно задаёт предпучок $X$ с геометрической

[1] Т. е. можно ли получить окружность в качестве геометричекой реализации полусимплициального множества $X$, у которого $X_0$ и $X_1$ состоят из трёх элементов, а все остальные $X_i$ пусты.

[2] В котором множества $X_n$ рассматриваются с *дискретной*, а симплексы $\Delta^n \subset \mathbb{R}^{n+1}$ со стандартной топологией объемлющего вещественного аффинного пространства.

[3] Т. е. склеивании всех точек границы в одну. Например, двумерная сфера $S^2$ получается таким способом из треугольника.

реализацией $|X| \simeq S^n$, и найдите количество элементов в каждом множестве $X_k$, $k \in \mathbb{Z}_{\geqslant 0}$.

Пример 8.8 (предпучки и пучки на топологических пространствах)
Исторически, термин «предпучок» впервые возник применительно к категории $\mathcal{C} = \mathcal{U}(X)$ открытых множеств $U \subset X$ топологического пространства $X$. Предпучок $F : \mathcal{U}(X)^{\mathrm{opp}} \to \mathcal{D}$ сопоставляет каждому открытому множеству $U \subset X$ объект $F(U) \in \operatorname{Ob}\mathcal{D}$, который называется *сечениями* предпучка $F$ над $U$. В зависимости от категории $\mathcal{D}$ сечения могут образовывать множество, кольцо, алгебру, векторное или топологическое пространство и т. п. В таком контексте морфизм $F(W) \to F(U)$, отвечающий включению $U \subset W$, называется *ограничением сечений*, определённых над $W$, на подмножество $U \subset W$, и результат его применения к сечению $s \in F(W)$ обозначается через $s|_U$. Вот несколько типичных примеров таких предпучков:

1) предпучок $\varGamma_E$ локальных сечений непрерывного отображения $p : E \to X$ имеет в качестве $\varGamma_E(U)$ множество таких непрерывных отображений $s : U \to E$, что[1] $p \circ s = \mathrm{Id}_U$, а его отображения ограничения — это обычные ограничения сечений с большего подмножества на меньшее

2) беря в предыдущем примере в качестве отображения проекцию $p : X \times Y \to X$, получаем предпучок локальных непрерывных отображений $\mathcal{C}^0(X, Y)$ пространства $X$ в пространство $Y$, имеющий в качестве сечений над $U \subset X$ непрерывные отображения $s : U \to Y$

3) дальнейшими специализациями являются так называемые *структурные предпучки* $\mathcal{O}_X$: предпучок дифференцируемых функций $X \to \mathbb{R}$ на гладком вещественном многообразии $X$, предпучок локальных голоморфных функций $X \to \mathbb{C}$ на комплексно аналитическом многообразии $X$, предпучок локальных рациональных функций $X \to \Bbbk$ на алгебраическом многообразии $X$ над полем $\Bbbk$ и т. п. (все они являются предпучками алгебр над соответствующим полем)

4) постоянный *предпучок* $S$ имеет в качестве $S(U)$ одно и то же фиксированное множество $S$ для всех $U \subset X$, и все его отображения ограничения — тождественные морфизмы $\mathrm{Id}_S$.

Предпучок $F$ называется *пучком*, если для любого семейства открытых подмножеств $U_i$ и любого набора таких локальных сечений $s_i \in F(U_i)$, что $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ при всех $i, j$, существует единственное такое сечение $s \in F(\bigcup_i U_i)$, что $s|_{U_i} = s_i$ при всех $i$. В случае, когда имеется не более одного такого сечения (но может не быть и ни одного), предпучок $F$ называется *отделимым*. Все предпучки (1) – (4) отделимы, и только последний из них — постоянный *предпучок* — не является пучком, поскольку для непересекающихся открытых множеств $U_1, U_2$ не всякая пара констант $s_i \in S(U_i)$ является ограничением одной константы $s \in S(U_1 \sqcup U_2)$. Тем не менее, наряду с постоянным предпучком в природе имеется и

5) постоянный *пучок* $S^{\sim}$, у которого $S^{\sim}(U)$ это *непрерывные* отображения $U \to S$ в множество $S$, рассматриваемое с *дискретной* топологией, или — что то же самое — *локально* постоянные функции со значениями в $S$.

Упражнение 8.6. Опишите множество первообразных действительной функции $1/x$.

[1]Это требование означает, что каждая точка $x \in U$ отображается в слой $p^{-1}(x)$ над нею.

**8.2.2. Функторы Hom.** С каждым объектом $X \in \mathrm{Ob}\,\mathcal{C}$ любой категории $\mathcal{C}$ связаны функтор $h^X : \mathcal{C} \to \mathcal{S}et$, который переводит объект $Y$ в множество морфизмов $h^X(Y) \stackrel{\text{def}}{=} \mathrm{Hom}(X,Y)$, а стрелку $\varphi : Y_1 \to Y_2$ в отображение $\varphi_* : \mathrm{Hom}(X,Y_1) \to \mathrm{Hom}(X,Y_2)$, $\psi \mapsto \varphi\circ\psi$, левого умножения на эту стрелку, а также предпучок $h_X : \mathcal{C} \to \mathcal{S}et$, который переводит объект $Y$ в множество морфизмов $h_X(Y) \stackrel{\text{def}}{=} \mathrm{Hom}(Y,X)$, а стрелку $\varphi : Y_1 \to Y_2$ в отображение $\varphi^* : \mathrm{Hom}(Y_2,X) \to \mathrm{Hom}(Y_1,X)$, $\psi \mapsto \psi \circ \varphi$, правого умножения на эту стрелку.

Например, предпучок $h_{[n]} : \varDelta_s \to \mathcal{S}et$ на полусимплициальной категории $\varDelta_s$ задаёт стандартную триангуляцию стандартного $n$-мерного симплекса: множество её $k$-мерных симплексов $h_{[n]}([k]) = \mathrm{Hom}([k],[n])$ это в точности множество всех $k$-мерных граней. На топологическом пространстве $X$ предпучок $h_U : \mathcal{U}(X) \to \mathcal{S}et$ имеет ровно одно сечение над всеми $W \subseteq U$ и пустое множество сечений над любым $W \nsubseteq U$. Вот ещё несколько примеров.

Пример 8.9 (двойственность в категории векторных пространств)
Предпучок $h_{\Bbbk} : \mathcal{V}ec_{\Bbbk}^{\mathrm{opp}} \to \mathcal{V}ec_{\Bbbk}$ сопоставляет векторному пространству $V$ двойственное векторное пространство $h_{\Bbbk}(V) = \mathrm{Hom}(V,\Bbbk) = V^*$, а линейному отображению $\varphi : V \to W$ — двойственное отображение $\varphi^* : W^* \to V^*$, переводящее линейную форму $\xi : W \to \Bbbk$ в линейную форму $\xi \circ \varphi : V \to \Bbbk$.

Пример 8.10 (двойственность конечных упорядоченных множеств)
Это комбинаторная версия предыдущего примера. Обозначим через через $\nabla_{\mathrm{big}}$ категорию конечных упорядоченных множеств из не менее двух элементов, морфизмами в которой являются неубывающие отображения, переводящие минимальный элемент в минимальный, а максимальный — в максимальный[1]. Тавтологическое включение $\nabla_{\mathrm{big}} \hookrightarrow \varDelta_{\mathrm{big}}$ является строгим, но не полным функтором. Предпучки

$$h_{[1]} : \varDelta_{\mathrm{big}}^{\mathrm{opp}} \to \nabla_{\mathrm{big}} \quad \text{и} \quad h_{[1]} : \nabla_{\mathrm{big}}^{\mathrm{opp}} \to \varDelta_{\mathrm{big}}$$

переводят упорядоченные множества $X \in \mathrm{Ob}\,\varDelta_{\mathrm{big}}$ и $Y \in \mathrm{Ob}\,\nabla_{\mathrm{big}}$ в множества

$$X^* \stackrel{\text{def}}{=} \mathrm{Hom}_{\varDelta_{\mathrm{big}}}(X,[1]) \quad \text{и} \quad Y^* \stackrel{\text{def}}{=} \mathrm{Hom}_{\nabla_{\mathrm{big}}}(Y,[1])\,,$$

порядок на которых задаётся поточечным сравнением значений:

$$\varphi \leqslant \psi\,, \quad \text{если } \varphi(x) \leqslant \psi(x) \text{ для всех } x.$$

Стрелка $\varphi : Z_1 \to Z_2$ переводится обоими функторами в морфизм правого умножения

$$\varphi^* : \mathrm{Hom}(Z_2,[1]) \to \mathrm{Hom}(Z_1,[1])\,, \quad \xi \mapsto \xi \circ \varphi\,.$$

Иначе можно сказать, что множество $Z^*$ это множество «дедекиндовых сечений» множества $Z$, т. е. множество таких разбиений $Z = Z_0 \sqcup Z_1$, что $z_0 < z_1$ для всех $z_0 \in Z_0$, $z_1 \in Z_1$, причём оба множества $Z_i$ должны быть непусты, когда $Z \in \mathrm{Ob}\,\nabla_{\mathrm{big}}$, но одно из них может быть пусто, когда $Z \in \mathrm{Ob}\,\varDelta_{\mathrm{big}}$. Обратите внимание, что сечения ведут себя *контра*вариантно по отношению к морфизмам: при наличии неубывающего отображения $Z_1 \to Z_2$ разбиение множества $Z_2$ индуцирует разбиение на $Z_1$, но не наоборот.

[1]Отметим, что минимальный и максимальный элементы различны.

**8.3. Естественные преобразования.** Для пары функторов $F, G : \mathcal{C} \to \mathcal{D}$ *естественным* (или *функториальным*) *преобразованием* функтора $F$ в функтор $G$ называется такое занумерованное объектами $X \in \operatorname{Ob}\mathcal{C}$ семейство стрелок $f_X : F(X) \to G(X)$ в категории $\mathcal{D}$, что для любой стрелки $\varphi : X \to Y$ из $\mathcal{C}$ возникающая в категории $\mathcal{D}$ диаграмма

$$\begin{tikzcd} F(X) \arrow[r, "F(\varphi)"] \arrow[d, "f_X"'] & F(Y) \arrow[d, "f_Y"] \\ G(X) \arrow[r, "G(\varphi)"'] & G(Y) \end{tikzcd} \tag{8-8}$$

коммутативна. На языке алгебр, гомоморфизм $F : K[\mathcal{C}] \to K[\mathcal{D}]$ наделяет алгебру $K[\mathcal{D}]$ структурой модуля над алгеброй $K[\mathcal{C}]$, в которой умножение элемента $b \in K[\mathcal{D}]$ на элемент $a \in K[\mathcal{C}]$ определяется правилом $a \cdot b \stackrel{\text{def}}{=} F(a) \cdot b$. Пара функторов $F$, $G$ задаёт на алгебре $K[\mathcal{D}]$ две различных структуры $K[\mathcal{C}]$-модуля, и естественное преобразование $f : F \to G$ это гомоморфизм $K[\mathcal{C}]$-модулей, переводящий стрелку $\psi$ с концом в $F(X)$ в стрелку $f_X \circ \psi$ с концом в $G(X)$, а все не заканчивающиеся в объектах вида $F(X)$ стрелки — в нуль.

Упражнение 8.7. Убедитесь, что $K[\mathcal{C}]$-линейность описанного отображения и впрямь означает, что для любого $\varphi \in K[\mathcal{C}]$ действие на $K[\mathcal{D}]$ операторов $F(\varphi)$ и $G(\varphi)$ удовлетворяет соотношению $f \circ F(\varphi) = G(\varphi) \circ f$.

**8.3.1. Категории функторов.** Функторы из малой категории $\mathcal{C}$ в произвольную категорию $\mathcal{D}$ образуют категорию $\mathcal{F}un(\mathcal{C}, \mathcal{D})$, объектами которой являются функторы $\mathcal{C} \to \mathcal{D}$, а морфизмами — естественные преобразования $f : F \to G$. Для малой категории $\mathcal{C}$ мы будем обозначать категорию предпучков $\mathcal{F}un(\mathcal{C}^{\text{opp}}, \mathcal{D})$ через $p\mathcal{S}h(\mathcal{C}, \mathcal{D})$. Опущенная буква $\mathcal{D}$ в этой записи по умолчанию означает, что $\mathcal{D} = \mathcal{S}et$, т. е. $p\mathcal{S}h(\mathcal{C}) \stackrel{\text{def}}{=} \mathcal{F}un(\mathcal{C}^{\text{opp}}, \mathcal{S}et)$.

Упражнение 8.8. Проверьте, что описанное в n° 8.2.2 сопоставление $X \mapsto h_X$ задаёт функтор $\mathcal{C} \to p\mathcal{S}h(\mathcal{C})$, а сопоставление $X \mapsto h^X$ — предпучок $\mathcal{C}^{\text{opp}} \to \mathcal{F}un(\mathcal{C}, \mathcal{S}et)$.

Пример 8.11 (категория предпучков)

Предпучки на категории $\mathcal{U}(X)$ открытых множеств топологического пространства $X$ обычно называются просто предпучками на $X$. Они образуют категорию, обозначаемую $p\mathcal{S}h(X)$. Морфизм предпучков $f : F \to G$ на $X$ задаётся набором согласованных с ограничениями отображений между множествами сечений $f_U : F(U) \to G(U)$, по одному отображению для каждого открытого $U \subset X$. Согласованность с ограничениями означает, что $f_W(s)|_U = f_U(s|_U)$ для любой пары вложенных открытых множеств $U \subset W$ и любого сечения $s \in F(W)$. Пучки и отделимые предпучки[1] образуют полные подкатегории $\mathcal{S}h(X)$ и $sp\mathcal{S}h(X)$ категории предпучков $p\mathcal{S}h(X)$.

Пример 8.12 (категория симплициальных множеств)

Предпучки $X : \varDelta \to \mathcal{S}et$ на симплициальной категории[2] $\varDelta$, образуют категорию, морфизмами $X \to Y$ в которой являются наборы отображений $f_n : X_n \to Y_n$, согласованные со склейкой, т. е. такие, что для любого симплекса $x \in X_m$ и неубывающего отображения $\varphi : [n] \to [m]$ из $\varDelta$ в $Y_n$ выполняется равенство $f_n(\varphi^* x) = \varphi^* f_m(x)$. На геометрическом языке такому отображению отвечает непрерывное отображение $f : |X| \to |Y|$, при котором образ каждого симплекса $\varDelta_x^n$ в

[1] См. прим. 8.8 на стр. 113.
[2] См. прим. 8.7 на стр. 112.

пространстве[1] $|X|$ отображается на образ симплекса $\varDelta^n_{f_n(x)}$ в пространстве $|Y|$ так, что все соотношения инцидентности[2] между симплексами при этом сохраняются.

**8.3.2. Эквивалентности категорий.** Категории $\mathcal{C}$ и $\mathcal{D}$ называются *эквивалентными*, если между ними есть такие функторы $F : \mathcal{C} \to \mathcal{D}$ и $G : \mathcal{D} \to \mathcal{C}$, что композиция $GF$ естественно изоморфна тождественному функтору $\mathrm{Id}_{\mathcal{C}}$, а композиция $FG$ естественно изоморфна $\mathrm{Id}_{\mathcal{D}}$, т. е. имеются функториальные по $X \in \mathrm{Ob}\,\mathcal{C}$ и $Y \in \mathrm{Ob}\,\mathcal{D}$ преобразования

$$GF(X) \simeq X \quad \text{и} \quad FG(Y) \simeq Y\,, \tag{8-9}$$

являющиеся для всех $X$ и $Y$ изоморфизмами в категориях $\mathcal{C}$ и $\mathcal{D}$ соответственно. Такие функторы $F$ и $G$ называются *квазиобратными* друг другу *эквивалентностями категорий*. Подчеркнём, что наличие изоморфизмов (8-9) не означает равенств $FG = \mathrm{Id}_{\mathcal{D}}$ или $GF = \mathrm{Id}_{\mathcal{C}}$: объекты $GF(X)$ и $X$ могут быть различны, как и объекты $FG(Y)$ и $Y$.

Пример 8.13 (выбор базиса)

Зафиксируем поле $\Bbbk$ и обозначим через $\mathcal{vec}$ категорию конечномерных векторных пространств над $\Bbbk$, а через $\mathcal{crd} \subset \mathcal{vec}$ — её полную малую подкатегорию со счётным множеством объектов, коими являются *координатные* пространства $\Bbbk^n$, где $n \geqslant 0$ и $\Bbbk^0 = \{0\}$. Выберем в каждом пространстве $V \in \mathrm{Ob}\,\mathcal{vec}$ какой-нибудь базис, т. е. зафиксируем изоморфизм[3]

$$f_V : V \simeq \Bbbk^{\dim(V)}\,, \tag{8-10}$$

и для координатных пространств положим $f_{\Bbbk^n} = \mathrm{Id}_{\Bbbk^n}$. Рассмотрим функтор $F : \mathcal{vec} \to \mathcal{crd}$, переводящий векторное пространство $V$ в координатное пространство $\Bbbk^{\dim V}$, а стрелку $\varphi : V \to W$ — в стрелку $F(\varphi) = f_W \circ \varphi \circ f_V^{-1}$, которую можно воспринимать как матрицу оператора $\varphi$ в выбранных базисах пространств $V$ и $W$. Покажем, что $F$ является эквивалентностью категорий, квазиобратной к тавтологическому вложению $G : \mathcal{crd} \hookrightarrow \mathcal{vec}$. По построению мы имеем точное равенство[4] $FG = \mathrm{Id}_{\mathcal{crd}}$. Противоположная композиция $GF : \mathcal{vec} \to \mathcal{vec}$ принимает значения в несопоставимой с $\mathcal{vec}$ по мощности малой подкатегории $\mathcal{crd} \subset \mathcal{vec}$. Однако изоморфизмы (8-10) задают естественное преобразование из $\mathrm{Id}_{\mathcal{vec}}$ в $GF$, т. к. в силу определения действия функтора $F$ на стрелки все диаграммы (8-8) коммутативны:

$$\begin{tikzcd}
\mathrm{Id}_{\mathcal{vec}}(V) = V \arrow[r, "\varphi = \mathrm{Id}_{\mathcal{vec}}(\varphi)"] \arrow[d, "f_V"'] & W = \mathrm{Id}_{\mathcal{vec}}(W) \arrow[d, "f_W"] \\
GF(V) = \Bbbk^{\dim V} \arrow[r, "GF(\varphi) = f_W \circ \varphi \circ f_V^{-1}"] & \Bbbk^{\dim W} = GF(W).
\end{tikzcd}$$

Тем самым, тождественный функтор $\mathrm{Id}_{\mathcal{vec}}$ естественно изоморфен композиции $GF$.

Упражнение 8.9. Покажите, что категория $\varDelta_{\mathrm{big}}$ канонически эквивалентна симплициальной подкатегории $\varDelta \subset \varDelta_{\mathrm{big}}$ (см. прим. 8.4 на стр. 109).

[1] Этот образ, вообще говоря, может быть симплексом меньшей, чем $n$, размерности.
[2] Т. е. отношения вида «симплекс $a$ является $\varphi$-той гранью (или $\psi$-тым вырождением) симплекса $b$».
[3] Переводящий выбранный базис в стандартный базис пространства $\Bbbk^n$.
[4] А не просто изоморфизм функторов.

Предложение 8.1
Функтор $G : \mathcal{C} \to \mathcal{D}$ тогда и только тогда задаёт эквивалентность категорий, когда он вполне строг[1] и каждый объект $Y \in \operatorname{Ob}\mathcal{D}$ изоморфен объекту вида $G(X)$ для некоторого (зависящего от $Y$) объекта[2] $X = X(Y) \in \operatorname{Ob}\mathcal{C}$.

Доказательство. Пусть для каждого $Y \in \operatorname{Ob}\mathcal{D}$ указаны объект $X = X(Y) \in \operatorname{Ob}\mathcal{C}$ и изоморфизм $f_Y : Y \xrightarrow{\sim} G(X)$, причём если $Y = G(Z)$, то мы полагаем $X(Y) = Z$ и $f_Y = \mathrm{Id}_Y$. Зададим функтор $F : \mathcal{D} \to \mathcal{C}$ на объектах правилом $F(Y) = X(Y)$, а для стрелки $\varphi : Y_1 \to Y_2$ положим $F(\varphi)$ равным такой стрелке[3] $\psi : X(Y_1) \to X(Y_2)$, что $G(\psi) = f_{Y_2} \circ \varphi \circ f_{Y_1}^{-1}$. Тогда $FG = \mathrm{Id}_{\mathcal{C}}$ и для любой стрелки $\varphi : Y_1 \to Y_2$ диаграмма

$$\begin{tikzcd}
\mathrm{Id}_{\mathcal{D}}(Y_1) = Y_1 \arrow[r, "\varphi"] \arrow[d, "f_{Y_1}"'] & Y_2 = \mathrm{Id}_{\mathcal{D}}(Y_2) \arrow[d, "f_{Y_2}"] \\
GF(Y_1) = X_1 \arrow[r, "GF(\varphi)=G(\psi)"] & X_2 = GF(Y_2)
\end{tikzcd}$$

коммутативна, т. е. $f_Y : Y \xrightarrow{\sim} G(X) = GF(Y)$ задают естественный изоморфизм тождественного функтора $\mathrm{Id}_{\mathcal{D}}$ с композицией $GF$. □

Упражнение 8.10. Покажите, что функтор дуализации из прим. 8.10 и ограничение функтора дуализации из прим. 8.9 на полную подкатегорию конечномерных пространств являются квазиобратными самим себе антиэквивалентностями[4] категорий.

**8.4. Представимые функторы.** Предпучок $F : \mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$, естественно изоморфный предпучку $h_X : Y \mapsto \operatorname{Hom}_{\mathcal{C}}(Y, X)$ для некоторого $X \in \operatorname{Ob}\mathcal{C}$, называется *представимым*, и объект $X$ в этом случае называют *представляющим* предпучок $F$. Двойственным образом, ковариантный функтор $F : \mathcal{C} \to \mathcal{S}et$ называется *копредставимым*, если он естественно изоморфен функтору $h^X : Y \mapsto \operatorname{Hom}_{\mathcal{C}}(X, Y)$ для некоторого объекта $X$, который в этом случае называется *копредставляющим* функтор $F$.

Упражнение 8.11. Убедитесь, что для произвольным образом зафиксированных конечномерных векторных пространств $U$ и $W$ функтор $\mathcal{V}ec \to \mathcal{S}et$, сопоставляющий векторному пространству $W$ множество билинейных отображений $U \times V \to W$ копредставим тензорным произведением $U \otimes V$.

Множество $X_n = X([n])$ всех $n$-мерных симплексов триангулированного топологического пространства $X : \Delta_{\mathrm{s}}^{\mathrm{opp}} \to \mathcal{S}et$ можно описать как $\operatorname{Hom}_{p\mathcal{S}h(\Delta_{\mathrm{s}})}\big(h_{[n]}, X\big)$, т. е. как множество «согласованных с триангуляциями» отображений стандартным образом триангулированного $n$-мерного симплекса $\Delta^n = h_{[n]}$ в триангулированное пространство $X$. Прямым обобщением этого наблюдения является

Лемма 8.1 (лемма Ионеды I)
Для любого предпучка множеств $F : \mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$ на произвольной категории $\mathcal{C}$ имеется функториальная по $F \in p\mathcal{S}h(\mathcal{C})$ и по $A \in \mathcal{C}$ биекция $F(A) \xrightarrow{\sim} \operatorname{Hom}_{p\mathcal{S}h(\mathcal{C})}(h_A, F)$, переводящая элемент

[1] Т. е. все отображения $G : \operatorname{Hom}_{\mathcal{C}}(X, Y) \to \operatorname{Hom}_{\mathcal{D}}(G(X), G(Y))$ являются изоморфизмами.

[2] Функторы $G$, обладающие этим свойством, называются *по существу сюрьективными* (по-английски: *essentially surjective*).

[3] Поскольку $G : \operatorname{Hom}(X_1, X_2) \xrightarrow{\sim} \operatorname{Hom}(G(X_1), G(X_2))$ является изоморфизмом, стрелка $\psi$ существует и единственна.

[4] Т. е. контравариантными эквивалентностями: устанавливают эквивалентность не $\mathcal{C}$ с $\mathcal{D}$, а $\mathcal{C}^{\mathrm{opp}}$ с $\mathcal{D}$.

$a \in F(A)$ в естественное преобразование

$$f_X:\ \mathrm{Hom}(X,A) \to F(X)\,, \tag{8-11}$$

которое посылает стрелку $\varphi:\ X \to A$ в значение отображения $F(\varphi):\ F(A) \to F(X)$ на элементе $a$. Обратная биекция сопоставляет каждому естественному преобразованию (8-11) значение отображения $f_A:\ h_A(A) \to F(A)$ на элементе $\mathrm{Id}_A \in h_A(A)$.

Доказательство. Для любого естественного преобразования (8-11), любого объекта $X \in \mathrm{Ob}\,\mathcal{C}$ и любой стрелки $\varphi:\ X \to A$ мы имеем коммутативную диаграмму (8-8)

$$\begin{tikzcd} h_A(A) = \mathrm{Hom}(A,A) \arrow[r, "h_A(\varphi)"] \arrow[d, "f_A"'] & \mathrm{Hom}(X,A) = h_A(X) \arrow[d, "f_X"] \\ F(A) \arrow[r, "F(\varphi)"] & F(X)\,, \end{tikzcd} \tag{8-12}$$

верхняя строка которой переводит $\mathrm{Id}_A$ в $\varphi$, так что $f_X(\varphi) = F(\varphi)\big(f_A(\mathrm{Id}_A)\big)$. Это означает, что естественное преобразование $f:\ h_A \to F$ однозначно восстанавливается по элементу

$$a = f_A(\mathrm{Id}_A) \in F(A)\,.$$

Преобразование (8-11), отвечающее произвольно заданному элементу $a \in F(A)$, переводит стрелку $\varphi \in \mathrm{Hom}(X,A)$ в $f_X(\varphi) = F(\varphi)(a) \in F(X)$. Оно функториально, поскольку для любой стрелки $\psi:\ Y \to X$ и всех $\varphi \in h_A(X)$ имеем $f_Y\left(h_A(\psi)\varphi\right) = f_Y(\varphi\psi) = F(\varphi\psi)a = F(\psi)F(\varphi)a = F(\psi)\left(f_X(\varphi)\right)$, т. е. $f_Y \circ h_A(\psi) = F(\psi) \circ f_X$ как отображения $h_A(X) \to F(Y)$. □

Упражнение 8.12 (лемма Ионеды 2). Для ковариантного функтора $F:\ \mathcal{C} \to \mathcal{S}et$ постройте функториальную по $F$ и $A \in \mathrm{Ob}\,\mathcal{C}$ биекцию $F(A) \simeq \mathrm{Hom}_{\mathcal{F}un(\mathcal{C},\mathcal{S}et)}(h^A, F)$.

Следствие 8.1

Функторы $X \mapsto h_X$ и $X \mapsto h^X$ задают вполне строгие ковариантное и контравариантное вложения категории $\mathcal{C}$ в категории предпучков и ковариантных функторов соответственно. Иными словами, имеются функториальные по $A, B \in \mathrm{Ob}\,\mathcal{C}$ изоморфизмы

$$\mathrm{Hom}_{p\mathcal{S}h(\mathcal{C})}(h_A, h_B) = \mathrm{Hom}_{\mathcal{C}}(A,B) \quad \text{и} \quad \mathrm{Hom}_{\mathcal{F}un(\mathcal{C})}(h^A, h^B) = \mathrm{Hom}_{\mathcal{C}}(B,A)\,.$$

Доказательство. Применяем леммы Ионеды к функторам $F = h_B$ и $F = h^B$. □

Следствие 8.2

Если объект $A \in \mathrm{Ob}\,\mathcal{C}$, копредставляющий функтор $F:\ \mathcal{C} \to \mathcal{S}et$ (соотв. представляющий предпучок $F:\ \mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$) существует, то он единствен с точностью до канонического изоморфизма.

Доказательство. Если имеются два таких объекта $A, B$, что $h^A \simeq F \simeq h^B$ (соотв. $h_A \simeq F \simeq h_B$), то беря подходящую композицию этих естественных изоморфизмов, мы получаем естественный изоморфизм $h^B \simeq h^A$ (соотв. $h_A \simeq h_B$), которому по лемме Ионеды отвечает естественный по $A$ и $B$ изоморфизм $A \simeq B$. □

**8.4.1. Описание объектов универсальными свойствами.** При помощи сл. 8.2 можно пытаться переносить в произвольную категорию $\mathcal{C}$ естественные[1] операции над множествами, имеющиеся в категории $\mathcal{S}et$. А именно, будем называть результатом применения такой операции к набору объектов $X_i \in \operatorname{Ob}\mathcal{C}$ представляющий объект $X$ предпучка $\mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$, переводящего каждый объект $Y \in \operatorname{Ob}\mathcal{C}$ в результат применения этой операции к множествам $\operatorname{Hom}(Y, X_i)$ в категории $\mathcal{S}et$. Разумеется, такое неявное описание не даёт никаких гарантий *существования* определяемого объекта, т. к. рассматриваемый функтор может оказаться непредставимым. Однако, если он представим, то представляющий объект $X$, во-первых, автоматически обладает некоторыми «универсальными свойствами», а во-вторых, единствен с точностью до *единственного* изоморфизма, сохраняющего эти свойства. Вдобавок, у каждой такого рода конструкции есть двойственная версия, получающаяся из предыдущей обращением стрелок и объявляющая результатом теоретико множественной операции над объектами $X_i \in \operatorname{Ob}\mathcal{C}$ копредставляющий объект ковариантного функтора $\mathcal{C} \to \mathcal{S}et$, переводящего $Y \in \operatorname{Ob}\mathcal{C}$ в результат применения операции к множествам $\operatorname{Hom}(X_i, Y)$.

Пример 8.14 (произведение $A \times B$)
Определим *произведение* $A \times B$ объектов $A, B \in \operatorname{Ob}\mathcal{C}$ произвольной категории $\mathcal{C}$ как объект, представляющий предпучок $\mathcal{C}^{\mathrm{opp}} \to \mathcal{S}et$, $Y \mapsto \operatorname{Hom}(Y, A) \times \operatorname{Hom}(Y, B)$. Если произведение существует, то имеется функториальный по $Y$ изоморфизм

$$\beta_Y : \operatorname{Hom}(Y, A \times B) \xrightarrow{\sim} \operatorname{Hom}(Y, A) \times \operatorname{Hom}(Y, B)\,.$$

Полагая в нём $Y = A \times B$, получаем пару стрелок

$$A \xleftarrow{\pi_A} A \times B \xrightarrow{\pi_B} B\,, \tag{8-13}$$

изображающих элемент $\beta_{A\times B}(\mathrm{Id}_{A\times B}) \in \operatorname{Hom}(A \times B, A) \times \operatorname{Hom}(A \times B, B)$. Пара стрелок (8-13) универсальна в том смысле, что для любой пары стрелок

$$A \xleftarrow{\varphi} Y \xrightarrow{\psi} B\,, \quad (\varphi, \psi) \in \operatorname{Hom}(Y, A) \times \operatorname{Hom}(Y, B)\,, \tag{8-14}$$

существует единственная стрелка $\varphi\times\psi : Y \to A\times B$, такая что $\beta_Y(\varphi\times\psi) = (\varphi, \psi)$. Коммутативная диаграмма[2]

$$\begin{tikzcd}
\operatorname{Hom}(A \times B, A \times B) \arrow[r, "h_{A\times B}(\varphi\times\psi)"] \arrow[d, "\beta_{A\times B}"'] & \operatorname{Hom}(Y, A \times B) \arrow[d, "\beta_Y"] \\
\operatorname{Hom}(A \times B, A) \times \operatorname{Hom}(A \times B, B) \arrow[r, "h_A(\varphi\times\psi)\times h_B(\varphi\times\psi)"] & \operatorname{Hom}(Y, A) \times \operatorname{Hom}(Y, B)\,,
\end{tikzcd}$$

верхняя горизонтальная стрелка которой переводит $\mathrm{Id}_{A\times B}$ в $\varphi\times\psi$, а композиция нижней и левой стрелок действуют на $\mathrm{Id}_{A\times B}$ как

$$\mathrm{Id}_{A\times B} \xmapsto{\beta_{A\times B}} (\pi_A, \pi_B) \xmapsto{h_A(\varphi\times\psi)\times h_B(\varphi\times\psi)} \big(\pi_A \circ (\varphi \times \psi), \pi_B \circ (\varphi \times \psi)\big)\,,$$

[1] Т. е. функториальные по всем участвующим множествам.
[2] Ср. с использованной в доказательстве леммы Ионеды диаграммой из форм. (8-12) на стр. 118

показывает, что равенство $\beta_Y(\varphi\times\psi) = (\varphi,\psi)$ равносильно равенствам $\varphi = \pi_A\circ(\varphi\times\psi)$ и $\psi = \pi_B\circ(\varphi\times\psi)$.

Упражнение 8.13. Пусть диаграмма $A \xleftarrow{\pi'_A} C \xrightarrow{\pi'_B} B$ тоже универсальна в том смысле, что для любой пары стрелок (8-14) существует единственная такая стрелка $Y\to C$, композиции которой с $\pi'_A$ и $\pi'_B$ равны $\varphi$ и $\psi$ соответственно. Убедитесь, что существует единственный такой изоморфизм $\gamma : C \xrightarrow{\sim} A\times B$, что $\pi_A\circ\gamma=\pi'_A$ и $\pi_B\circ\gamma=\pi'_B$. Покажите также, что любая пара стрелок $\alpha : A_1\to A_2$, $\beta : B_1\to B_2$ задаёт единственный такой морфизм

$$\alpha\times\beta : A_1\times B_1\to A_2\times B_2\,,$$

что $\alpha\circ\pi_{A_1}=\pi_{A_2}\circ(\alpha\times\beta)$ и $\beta\circ\pi_{B_1}=\pi_{B_2}\circ(\alpha\times\beta)$.

В категории множеств произведение $A\times B=\{(a,b)\mid a\in A,\ b\in B\}$. Снабжённое слабейшей топологией, в которой $\pi_A$ и $\pi_B$ непрерывны, это множество задаёт произведение и в категории топологических пространств. Снабжённое покомпонентными операциями, оно же является произведением групп, колец и модулей над кольцами.

Пример 8.15 (копроизведение $A\otimes B$)
Двойственным образом, копроизведение $A\otimes B$ объектов $A, B\in \operatorname{Ob}\mathcal{C}$ произвольной категории $\mathcal{C}$ определяется как объект, копредставляющий ковариантный функтор

$$\mathcal{C}\to\mathcal{S}et\,,\quad Y\mapsto \operatorname{Hom}(A,Y)\times\operatorname{Hom}(B,Y)\,.$$

Обращая все стрелки в предыдущем примере, мы можем охарактеризовать копроизведение как объект, включающийся в диаграмму $A\xrightarrow{\iota_A} A\otimes B \xleftarrow{\iota_B} B$, универсальную в том смысле, что для любой пары стрелок $A\xrightarrow{\varphi} Y\xleftarrow{\psi} B$ в $\mathcal{C}$ имеется единственный такой морфизм

$$\varphi\otimes\psi : A\otimes B\to Y\,,$$

что $\varphi=(\varphi\otimes\psi)\circ\iota_A$ и $\psi=(\varphi\otimes\psi)\circ\iota_B$.

Упражнение 8.14. Убедитесь, что если универсальная диаграмма существует, то она единственна с точностью до единственного изоморфизма, перестановочного со стрелками $\iota_A$, $\iota_B$, и что любая пара стрелок $\alpha : A_1\to A_2$, $\beta : B_1\to B_2$ задаёт единственный такой морфизм $\alpha\otimes\beta : A_1\otimes B_1\to A_2\otimes B_2$, что $\iota_{A_2}\circ\alpha=(\alpha\otimes\beta)\circ\iota_{A_1}$ и $\iota_{B_2}\circ\beta=(\alpha\otimes\beta)\circ\iota_{B_1}$.

Копроизведение в категории множеств и топологических пространств это дизъюнктное объединение $A\otimes B=A\sqcup B$. В категории групп это свободное произведение групп[1] $A\otimes B=A*B$. В категории модулей над кольцом[2] копроизведение совпадает с произведением и равно прямой сумме модулей $A\otimes B=A\times B=A\oplus B$. В категории коммутативных колец с единицей копроизведение $A\otimes B$ это тензорное произведение колец[3].

[1] Т. е. фактор свободной группы, порождённой дизъюнктным объединением $A\sqcup B$, по наименьшей нормальной подгруппе соотношений, позволяющих заменять пару соседних лежащих в одной группе букв их произведением. К примеру, $\mathbb{Z}*\mathbb{Z}\simeq\mathbb{F}_2$ это свободная (некоммутативная) группа с двумя образующими.

[2] В частности, в категории $\mathcal{A}b$ абелевых групп.

[3] Т. е. тензорное произведение подлежащих абелевых групп, как модулей над $\mathbb{Z}$, с покомпонентным умножением: $(a_1\otimes b_1)\cdot(a_2\otimes b_2)\stackrel{\text{def}}{=}(a_1\cdot a_2)\otimes(b_1\cdot b_2)$.

Пример 8.16 (свободные модули)
Обозначим через $R$-$\mathcal{M}od$ категорию левых модулей над фиксированным кольцом $R$. Для любого множества $E \in \mathrm{Ob}\,\mathcal{S}et$ ковариантный функтор $R$-$\mathcal{M}od \to \mathcal{S}et$, $M \mapsto \mathrm{Hom}_{\mathcal{S}et}(E, M)$, копредставим *свободным* $R$-модулем с базисом $E$. Мы будем обозначать такой свободный модуль через $R \otimes E$. По определению, он состоит из формальных линейных комбинаций $\sum_{e \in E} x_e e$ элементов множества $E$ с коэффициентами $x_e \in R$, лишь конечное число из которых отлично от нуля.

Упражнение 8.15. Установите функториальный по $M$ и $E$ изоморфизм

$$\mathrm{Hom}_{R\text{-}\mathcal{M}od}(R \otimes E, M) \simeq \mathrm{Hom}_{\mathcal{S}et}(E, M)\,. \tag{8-15}$$

**8.5. Сопряжённые функторы.** Функторы $F : \mathcal{C} \to \mathcal{D}$ и $G : \mathcal{D} \to \mathcal{C}$ между категориями $\mathcal{C}$ и $\mathcal{D}$ называются, соответственно, *левым* и *правым сопряжёнными* друг другу, если имеется функториальная по $X \in \mathrm{Ob}\,\mathcal{C}$ и $Y \in \mathrm{Ob}\,\mathcal{D}$ биекция

$$\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, G(Y))\,. \tag{8-16}$$

С каждой парой сопряжённых функторов связаны естественные преобразования

$$t : F \circ G \to \mathrm{Id}_{\mathcal{D}} \quad \text{и} \quad s : \mathrm{Id}_{\mathcal{C}} \to G \circ F\,. \tag{8-17}$$

Стрелка $t_Y : FG(Y) \to Y$, задающая действие преобразования $t$ над $Y \in \mathrm{Ob}\,\mathcal{D}$, является образом элемента $\mathrm{Id}_{G(Y)}$ при изоморфизме (8-16), написанном для $X = G(Y)$:

$$\mathrm{Hom}_{\mathcal{D}}(FG(Y), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(G(Y), G(Y)) \ni \mathrm{Id}_{G(Y)}\,.$$

Двойственным образом, стрелка $s_X : X \to GF(X)$ получается из $\mathrm{Id}_{F(X)}$ при изоморфизме (8-16), написанном для $Y = F(X)$:

$$\mathrm{Id}_{F(X)} \in \mathrm{Hom}_{\mathcal{D}}(F(X), F(X)) \simeq \mathrm{Hom}_{\mathcal{C}}(X, GF(X))\,.$$

Упражнение 8.16. Убедитесь в естественности этих преобразований.

Пример 8.17 (продолжение прим. 8.16 про свободные модули)
Изоморфизм из форм. (8-15) на стр. 121 означает, что функтор $F : \mathcal{S}et \to R$-$\mathcal{M}od$, $E \mapsto R \otimes E$, сопоставляющий произвольному множеству $E$ свободный левый $R$-модуль с базисом $E$, сопряжён слева к забывающему функтору $G : R$-$\mathcal{M}od \to \mathcal{S}et$, переводящему модуль в множество его элементов, т. е. $\mathrm{Hom}_{R\text{-}\mathcal{M}od}(R \otimes E, M) \simeq \mathrm{Hom}_{\mathcal{S}et}\big(E, G(M)\big)$ функториально по модулю $M$ и множеству $E$. Естественное преобразование $s_E : E \hookrightarrow G(A \otimes E)$ вкладывает $E$ в качестве множества базисных векторов в множество всех векторов свободного модуля $R \otimes E$. Естественное преобразование $t_M : R \otimes G(M) \twoheadrightarrow M$ — это $R$-линейный эпиморфизм огромного свободного модуля, базисом которого служит множество всех векторов модуля $M$, на модуль $M$. Он переводит каждый базисный вектор $m$ в элемент $m \in M$, а формальную линейную комбинацию базисных векторов — в результат её вычисления внутри модуля $M$. Так, при $M = R = \mathbb{R}$ векторное пространство $\mathbb{R} \otimes G(\mathbb{R})$ состоит из формальных линейных комбинаций $\sum_{x \in \mathbb{R}} f(x) \cdot x$, в которых лишь конечное множество коэффициентов $f(x)$ отлично от нуля. Оно изоморфно пространству всех функций $f : \mathbb{R} \to \mathbb{R}$ с конечным носителем, и преобразование $t_{\mathbb{R}}$ сопоставляет такой функции $f$ вещественное число $\sum_{x \in \mathbb{R}} f(x) \cdot x$.

Пример 8.18 (самосопряжённость представимых функторов на категории $\mathcal{A}b$)
Для любых трёх абелевых групп $A$, $B$, $C$ имеется канонический изоморфизм

$$\mathrm{Hom}_{\mathcal{A}b}\big(A, \mathrm{Hom}_{\mathcal{A}b}(B, C)\big) \simeq \mathrm{Hom}_{\mathcal{A}b}\big(B, \mathrm{Hom}_{\mathcal{A}b}(A, C)\big)\,, \tag{8-18}$$

переводящий семейство гомоморфизмов $\varphi_a : B \to C$, запараметризованное элементами $a \in A$ так, что $\varphi_{a'+a''} = \varphi_{a'} + \varphi_{a''}$ для всех $a', a'' \in A$, в запараметризованное элементами $b \in B$ семейство гомоморфизмов $\psi_b : A \to C$, $a \mapsto \varphi_a(b)$.

Упражнение 8.17. Проверьте, что каждое отображение $\psi_b$ является гомоморфизмом абелевых групп и что $\psi_{b'+b''} = \psi_{b'} + \psi_{b''}$ для всех $b', b'' \in B$. Постройте обратное отображение из правой части (8-18) в левую.

Изоморфизм (8-18) можно переписать как $\mathrm{Hom}_{\mathcal{A}b^{\mathrm{opp}}}\big(h_C(B), A\big) \simeq \mathrm{Hom}_{\mathcal{A}b}\big(B, h_C(A)\big)$. Это означает, что для любой абелевой группы $C$ представимый функтор

$$h_C : \mathcal{A}b^{\mathrm{opp}} \to \mathcal{A}b\,, \quad X \mapsto \mathrm{Hom}_{\mathcal{A}b}(X, C)\,,$$

самосопряжён. Естественное преобразование $s_X : X \to \mathrm{Hom}_{\mathcal{A}b}\big(\mathrm{Hom}_{\mathcal{A}b}(X, C), C\big)$ сопоставляют элементу $x \in X$ гомоморфизм вычисления $s_X(x) = \mathrm{ev}_x : \mathrm{Hom}(X, C) \to C$, $\varphi \mapsto \varphi(x)$. Естественное преобразование $t_X$ представляет собою стрелку $h_C\big(h_C(X)\big) \to X$ в категории $\mathcal{A}b^{\mathrm{opp}}$, т. е. стрелку $X \to h_C\big(h_C(X)\big)$ в категории $\mathcal{A}b$, и в таком виде совпадает с преобразованием $s_X$.

Предложение 8.2
Для существования левого сопряжённого функтора $F : \mathcal{C} \to \mathcal{D}$ к данному функтору $G : \mathcal{D} \to \mathcal{C}$ необходимо и достаточно, чтобы для любого $X \in \mathrm{Ob}\,\mathcal{C}$ функтор

$$h_G^X : \mathcal{D} \to \mathcal{S}et\,, \quad Y \mapsto \mathrm{Hom}_{\mathcal{C}}\big(X, G(Y)\big)\,, \tag{8-19}$$

был копредставим, и в этом случае $F(X)$ является его копредставляющим объектом.

Доказательство. Необходимость очевидна из определений. Докажем достаточность. Пусть для каждого $X \in \mathrm{Ob}\,\mathcal{C}$ функтор (8-19) представляется объектом $F(X)$, т. е. имеется естественный изоморфизм функторов $f^X : h^{F(X)} \xrightarrow{\sim} h_G^X$. Чтобы продолжить соответствие $X \mapsto F(X)$ до функтора $F : \mathcal{C} \to \mathcal{D}$ заметим, что морфизм $\varphi : X_1 \to X_2$ задаёт естественное преобразование правого умножения $\varphi^* : h_G^{X_2} \to h_G^{X_1}$ на стрелку $\varphi$, которое переводит стрелку $\psi : X_2 \to G(Y)$ в композицию $\psi\varphi : X_1 \to G(Y)$. Из леммы Ионеды вытекает[1], что композиция естественных преобразований $\big(f^{X_1}\big)^{-1} \circ \varphi^* \circ f^{X_2} : h^{F(X_2)} \to h^{F(X_1)}$ задаётся правым умножением на единственную стрелку $F(X_1) \to F(X_2)$, которую мы и объявим образом $F(\varphi)$ стрелки $\varphi$ под действием функтора $F$. Прямо по построению мы получаем функториальный по $X$ изоморфизм $\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \simeq \mathrm{Hom}_{\mathcal{C}}(X, G(Y))$. □

Следствие 8.3 (из доказательства предл. 8.2)
Если функтор $F$, сопряжённый слева к функтору $G$, существует, то он определяется по $G$ однозначно с точностью до естественного изоморфизма функторов. □

Упражнение 8.18. Докажите двойственные утверждения: для существования правого сопряжённого функтора $G$ к функтору $F : \mathcal{C} \to \mathcal{D}$ необходимо и достаточно, чтобы для любого

[1] См. сл. 8.1 на стр. 118.

$Y \in \operatorname{Ob}\mathcal{D}$ предпучок $h_Y^F : \mathcal{C} \to \mathcal{S}et$, $X \mapsto \operatorname{Hom}_{\mathcal{D}}(F(X), Y)$ был представим, и в этом случае объект $G(Y)$ его представляет, а функтор $G$ определяется по $F$ однозначно с точностью до естественного изоморфизма функторов.

Предложение 8.3

Функтор $F : \mathcal{C} \to \mathcal{D}$ тогда и только тогда сопряжён слева к функтору $G : \mathcal{D} \to \mathcal{C}$, когда существуют такие естественные преобразования $t : F \circ G \to \operatorname{Id}_{\mathcal{D}}$ и $s : \operatorname{Id}_{\mathcal{C}} \to G \circ F$, что композиции $F \xrightarrow{F \circ s} FGF \xrightarrow{t \circ F} F$ и $G \xrightarrow{s \circ G} GFG \xrightarrow{G \circ t} G$ являются тождественными эндоморфизмами функторов $F$ и $G$.

Доказательство. Если имеются функториальные по $X$ и $Y$ изоморфизмы

$$\begin{tikzcd} \operatorname{Hom}_{\mathcal{D}}\big(F(X), Y\big) \arrow[r, bend left, "\varrho"] & \operatorname{Hom}_{\mathcal{C}}\big(X, G(Y)\big) \arrow[l, bend left, "\lambda"] \end{tikzcd} \tag{8-20}$$

то для любой стрелки $\varphi : X_1 \to X_2$ в $\mathcal{C}$ и любого $Y$ из $\mathcal{D}$ коммутативна диаграмма

$$\begin{tikzcd} \operatorname{Hom}_{\mathcal{D}}(F(X_1), Y) & \operatorname{Hom}_{\mathcal{C}}(X_1, G(Y)) \arrow[l, "\lambda"', "\sim"] \\ \operatorname{Hom}_{\mathcal{D}}(F(X_2), Y) \arrow[u, "F(\varphi)^*"'] & \operatorname{Hom}_{\mathcal{C}}(X_2, G(Y)) \arrow[l, "\lambda"', "\sim"] \arrow[u, "\varphi^*"'] \end{tikzcd}$$

вертикальные стрелки которой задаются правым умножением на $F(\varphi)$ и на $\varphi$ соответственно. Рисуя это для $Y = F(X)$ и морфизма $\varphi = s_X : X \to GF(X)$, который задаёт действие над объектом $X$ естественного преобразования $s : \operatorname{Id}_{\mathcal{C}} \to GF$ из форм. (8-17) на стр. 121, получаем коммутативную диаграмму

$$\begin{tikzcd} \operatorname{Hom}_{\mathcal{D}}(F(X), F(X)) & \operatorname{Hom}_{\mathcal{C}}(X, GF(X)) \arrow[l, "\lambda"', "\sim"] \\ \operatorname{Hom}_{\mathcal{D}}(FGF(X), F(X)) \arrow[u, "F(s_X)^*"'] & \operatorname{Hom}_{\mathcal{C}}(GF(X), GF(X)) \arrow[l, "\lambda"', "\sim"] \arrow[u, "s_X^*"'] \end{tikzcd}$$

верхняя стрелка $\lambda$ которой переводит $s_X$ в $\operatorname{Id}_{F(X)}$, а нижняя стрелка $\lambda$ переводит $\operatorname{Id}_{GF(X)}$ в морфизм $t_{F(X)} : FGF(X) \to F(X)$, задающий второе естественное преобразование $t : FG \to \operatorname{Id}_{\mathcal{D}}$ из формулы (8-17) над объектом $F(X)$. Таким образом,

$$\operatorname{Id}_{F(X)} = \lambda(s_X) = \lambda s_X^* \left(\operatorname{Id}_{GF(X)}\right) = F(s_X)^* \lambda \left(\operatorname{Id}_{GF(X)}\right) = F(s_X)^* \left(t_{F(X)}\right) = t_{F(X)} \circ F(s_X),$$

а это и значит, что композиция $F \xrightarrow{F \circ s} FGF \xrightarrow{t \circ F} F$ задаёт тождественное преобразование функтора $F$. Проверка того, что $G \xrightarrow{s \circ G} GFG \xrightarrow{G \circ t} G$ совпадает с $\operatorname{Id}_G$ полностью симметрична. Наоборот, если имеются преобразования $s : \operatorname{Id}_{\mathcal{C}} \to GF$ и $t : FG \to \operatorname{Id}_{\mathcal{D}}$, зададим в (8-20) действие $\lambda$ и $\varrho$ на стрелки $\varphi : F(X) \to Y$ и $\psi : X \to G(Y)$ правилами:

$$\varrho(\varphi) = G(\varphi) \circ s_X \quad \text{и} \quad \lambda(\psi) = t_Y \circ F(\psi),$$

в правых частях которых стоят сквозные отображения вдоль стрелок

$$X \xrightarrow{s_X} GF(X) \xrightarrow{G(\varphi)} G(Y) \quad \text{и} \quad F(X) \xrightarrow{F(\psi)} FG(Y) \xrightarrow{t_Y} Y.$$

Композиция $\lambda\varrho(\varphi) = t_Y \circ FG(\varphi) \circ F(s_X) : F(X) \to Y$ представляет собою путь из левого нижнего угла в правый верхний на диаграмме

$$\begin{tikzcd}
 & F(X) \arrow[rr, "\varphi"] & & Y & \\
F(X) \arrow[ur, equal, "\mathrm{Id}_{F(X)}"] \arrow[rr, "F(s_X)"] & & FGF(X) \arrow[ul, "t_{F(X)}"'] \arrow[rr, "FG(\varphi)"] & & FG(Y) \arrow[ul, "t_Y"']
\end{tikzcd}$$

правый параллелограмм которой коммутативен в силу естественности преобразования $t$, а левый треугольник — в силу того, что композиция $F \xrightarrow{F\circ s} FGF \xrightarrow{t\circ F} F$ совпадает с $\mathrm{Id}_F$. Поэтому $\lambda\varrho(\varphi) = \varphi$. Равенство $\varrho\lambda(\psi) = \psi$ проверяется симметричным образом. $\square$

Пример 8.19 (эквивалентности категорий как сопряжённые функторы)
Пусть функторы $F : \mathcal{C} \to \mathcal{D}$ и $G : \mathcal{D} \to \mathcal{C}$ являются квазиобратными эквивалентностями[1], т. е. имеются естественные изоморфизмы $g : \mathrm{Id}_{\mathcal{C}} \xrightarrow{\sim} GF$ и $f : \mathrm{Id}_{\mathcal{D}} \xrightarrow{\sim} FG$. Как и в доказательстве предл. 8.3, рассмотрим естественные по $X$, $Y$ отображения

$$\begin{aligned}
\varrho_{FG} &: \ \mathrm{Hom}_{\mathcal{D}}\big(F(X), Y\big) \to \mathrm{Hom}_{\mathcal{C}}\big(X, G(Y)\big)\,, \quad \varphi \mapsto G(\varphi)\circ g_X = (g_X^* \circ G)\varphi \\
\varrho_{GF} &: \ \mathrm{Hom}_{\mathcal{C}}\big(G(Y), X\big) \to \mathrm{Hom}_{\mathcal{D}}\big(Y, F(X)\big)\,, \quad \psi \mapsto F(\psi)\circ f_Y = (f_Y^* \circ F)\psi\,.
\end{aligned}$$

Поскольку оба отображения

$$\begin{aligned}
g_X^* &: \ \mathrm{Hom}_{\mathcal{C}}\big(GF(X), G(Y)\big) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}\big(X, G(Y)\big)\,, \quad \xi \mapsto \xi \circ f_X\,, \\
G &: \ \mathrm{Hom}_{\mathcal{D}}\big(F(X), Y\big) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}\big(GF(X), G(Y)\big)\,, \quad \xi \mapsto G(\xi)\,,
\end{aligned}$$

являются биективными[2], их композиция $\varrho_{FG}$ тоже биективна. Это означает, что функтор $F$ сопряжён слева к функтору $G$. По аналогичной причине биективно и преобразование $\varrho_{GF}$, т. е. функтор $F$ сопряжён к функтору $G$ также и справа. Тем самым, квазиобратные эквивалентности категорий сопряжены друг другу с обеих сторон. Отметим, что по сл. 8.3 и упр. 8.18 на стр. 122 отсюда вытекает, что если один из двух сопряжённых друг другу функторов является эквивалентностью категорий, то и другой тоже таковою является.

Пример 8.20 (соответствие предпорядков, продолжение прим. 8.2 на стр. 107)
Функтор $F : N \to M$ между предупорядоченными множествами, рассматриваемыми как категории, это просто отображение, сохраняющее предпорядок: $n_1 \leqslant n_2 \Rightarrow F(n_1) \leqslant F(n_2)$. Левая сопряжённость такого отображения сохраняющему порядок отображению $G : M \to N$ означает, что неравенства $F(n) \leqslant m$ и $n \leqslant G(m)$ равносильны друг другу. Наличие естественных преобразований $t : F\circ G \to \mathrm{Id}_M$ и $s : \mathrm{Id}_N \to G\circ F$ означает неравенства $FG(m) \leqslant m$ и $n \leqslant GF(n)$ для всех $n \in N$, $m \in M$, а тождественность сквозных преобразований $F \to FGF \to F$ и $G \to GFG \to G$ — неравенства $F(n) \leqslant FGF(n) \leqslant F(n)$ и $G(m) \leqslant GFG(m) \leqslant G(m)$.

Упражнение 8.19. Убедитесь непосредственно, что условие $F(n) \leqslant m \iff n \leqslant G(m)$ на сохраняющие предпорядок отображения $F$, $G$ эквивалентно системе неравенств $FG(m) \leqslant m$ и $n \leqslant GF(n)$ для всех $m \in M$, $n \in N$, причём если эти неравенства выполнены, то неравенства $F(n) \leqslant FGF(n) \leqslant F(n)$ и $G(m) \leqslant GFG(m) \leqslant G(m)$ выполняются автоматически.

---

[1]См. n° 8.3.2 на стр. 116.

[2]Первое — в силу того, что является правым умножением на обратимую стрелку $g_X$, второе — потому что функтор $F$ вполне строг.

Если оба предпорядка являются частичными порядками, последние два неравенства превращаются в равенства $F(n) = FGF(n)$ и $G(m) = GFG(m)$. Примером такой ситуации является *соответствие Галуа*. Пусть группа $H$ действует слева на множестве $X$, а $\mathcal{S}(H)$ и $\mathcal{S}(X)$ обозначают частично упорядоченные по включению множества подгрупп в $H$ и подмножеств в $X$ соответственно. Функтор

$$F : \mathcal{S}(H) \to \mathcal{S}(X)^{\mathrm{opp}}, \quad S \mapsto X^S = \{x \in X \mid \forall h \in S \; hx = x\},$$

сопоставляет подгруппе $S \subset G$ множество её неподвижных точек. Функтор

$$G : \mathcal{S}(X)^{\mathrm{opp}} \to \mathcal{S}(H), \quad T \mapsto Z_T = \{h \in H \mid \forall x \in T \; hx = x\},$$

сопоставляет подмножеству $T \subset X$ его *централизатор*[1].

Упражнение 8.20. Убедитесь, что эти функторы сопряжены, т. е. $X^S \supset T \iff S \subset Z(T)$ для любых подмножества $T \subset X$ и подгруппы $S \subset H$, и что при этом выполняются равенства

$$Z_{X^{Z_T}} = Z_T \quad \text{и} \quad X^{Z_{X^S}} = X^S.$$

**8.6. Тензорные произведения и Hom.** Пусть $R$ — произвольное кольцо. Тензорным произведением $M \otimes_R N$ правого $R$-модуля $M$ на левый $R$-модуль $N$ называется фактор тензорного произведения абелевых групп[2] $M \otimes N$ по подгруппе, порождённой всевозможными разностями $(mx) \otimes n - m \otimes (xn)$, где $m \in M$, $x \in R$ и $n \in N$. Это абелева группа, на которой кольцо $R$, вообще говоря, больше уже не действует, но в которой выполняются соотношения

$$(mx) \otimes_R n = m \otimes_R (xn).$$

Тензорное умножение на фиксированный левый $R$-модуль $N$ задаёт функтор

$$\mathcal{M}od\text{-}R \to \mathcal{A}b, \quad X \mapsto X \otimes_R N, \tag{8-21}$$

из категории правых $R$-модулей в абелевы группы. Он переводит стрелку $\varphi : X_1 \to X_2$ в стрелку

$$\varphi \otimes \mathrm{Id}_N : m \otimes_R n \mapsto \varphi(m) \otimes_R n.$$

Если левый $R$-модуль $N$ одновременно является правым модулем над ещё одним кольцом $S$, и правое действие $S$ коммутирует с левым действием[3] $R$, функтор (8-21) действует из $\mathcal{M}od\text{-}R$ в $\mathcal{M}od\text{-}S$, поскольку кольцо $S$ действует на $M \otimes N$ справа по правилу $(m \otimes n)y = m \otimes (ny)$. Вместе с этим, представимый функтор $h^N : \mathcal{M}od\text{-}S \to \mathcal{A}b$, $Y \mapsto \mathrm{Hom}_S(N, Y)$, принимает значения в $\mathcal{M}od\text{-}R$. Правое действие $x \in R$ на $\mathrm{Hom}_S(N, Y)$ переводит $S$-линейную справа стрелку $\varphi : N \to Y$ в стрелку $\varphi x : n \mapsto \varphi(xn)$, так что выполняется равенство $(\varphi x)n = \varphi(xn)$.

Предложение 8.4
Тензорное умножение на $R$-$S$-бимодуль $N$ сопряжено слева функтору $h^N$, т. е. имеется естественный по $X \in \mathrm{Ob}\,\mathcal{M}od\text{-}R$ и $Y \in \mathrm{Ob}\,\mathcal{M}od\text{-}S$ изоморфизм абелевых групп

$$\mathrm{Hom}_{\mathcal{M}od\text{-}S}\big(X \otimes_R N, Y\big) \simeq \mathrm{Hom}_{\mathcal{M}od\text{-}R}\big(X, \mathrm{Hom}_{\mathcal{M}od\text{-}S}(N, Y)\big). \tag{8-22}$$

[1] Т. е. поточечный стабилизатор. Обратите внимание, что оба функтора оборачивают включения.
[2] Или, что то же самое, $\mathbb{Z}$-модулей.
[3] Такие модули $N$ называются $R$-$S$ *бимодулями*.

Доказательство. Отображение из левой части (8-22) в правую сопоставляет $S$-линейному справа гомоморфизму $\varphi : X \otimes_R N \to Y$ зависящее от $x \in X$ семейство гомоморфизмов $\varphi_x : N \to Y$, $n \mapsto \varphi(x \otimes n)$. Каждый из них $S$-линеен справа: $\varphi_x(ns) = \varphi(x \otimes_R ns) = \varphi(x \otimes_R n)s = \varphi_x(n)s$, а сопоставление $x \mapsto \varphi_x$, как отображение $X \to \mathrm{Hom}_{\mathcal{M}od\text{-}S}(N, Y)$, $R$-линейно справа: $\varphi_{xr}n = = \varphi(xr \otimes_R n) = \varphi(x \otimes_R rn) = \varphi_x(rn) = (\varphi_x r)n$. Обратное отображение из правой части (8-22) в левую переводит семейство $S$-линейных справа гомоморфизмов $\varphi_x : N \to Y$, которые $R$-линейно справа зависят от $x \in X$, в $S$-линейный справа гомоморфизм $\varphi : x \otimes_R n \mapsto \psi_x(n)$. □

Упражнение 8.21. Явно опишите естественные преобразования

$$t_Y : \mathrm{Hom}_{\mathcal{M}od\text{-}S}(N, Y) \otimes_R N \to Y \quad \text{и} \quad s_X : X \to \mathrm{Hom}_{\mathcal{M}od\text{-}S}\big(N, X \otimes_R N\big) .$$

Пример 8.21 (индуцирование и коиндуцирование)
Если кольцо $A$ содержится в кольце $B$ и они имеют общую единицу, каждый правый $B$-модуль $X$ одновременно является и правым $A$-модулем, что задаёт *функтор ограничения*

$$\mathrm{res} : \mathcal{M}od\text{-}B \to \mathcal{M}od\text{-}A . \tag{8-23}$$

Рассмотрим $B$ как $A$-$B$ бимодуль и положим в предл. 8.4 $S = N = B$, $R = A$. Абелева группа $\mathrm{Hom}_{\mathcal{M}od\text{-}B}(B, Y)$ канонически отождествляется с $Y$ гомоморфизмом $\varphi \mapsto \varphi(1)$, и как правый $A$-модуль изоморфна $\mathrm{res}\, Y$.

Упражнение 8.22. Убедитесь в этом.

Поэтому изоморфизм (8-22) из предл. 8.4 превращается в функториальный по $A$-модулю $X$ и $B$-модулю $Y$ изоморфизм

$$\mathrm{Hom}_{\mathcal{M}od\text{-}B}(X \otimes_A B, Y) \simeq \mathrm{Hom}_{\mathcal{M}od\text{-}A}(X, \mathrm{res}\, Y) .$$

Правый $B$-модуль $\mathrm{ind}\, X \overset{\text{def}}{=} X \otimes_A B$ называется *индуцированным* с $A$-модуля $X$. Таким образом, функтор индуцирования $\mathrm{ind} : \mathcal{M}od\text{-}A \to \mathcal{M}od\text{-}B$ сопряжён слева к функтору ограничения.

Упражнение 8.23. Явно опишите естественные преобразования

$$t_Y : \mathrm{res}\,\mathrm{ind}\, Y \to Y \quad \text{и} \quad s_X : X \to \mathrm{ind}\,\mathrm{res}\, X .$$

Теперь рассмотрим $B$ как $B$-$A$ бимодуль и положим в предл. 8.4 $S = A$, $N = R = B$. Канонический гомоморфизм $X \otimes_B B \xrightarrow{\sim} X$, $x \otimes_B b \mapsto xb$, является изоморфизмом абелевых групп и отождествляет правый $A$-модуль $X \otimes_B B$ с $\mathrm{res}\, X$.

Упражнение 8.24. Убедитесь в этом.

Поэтому изоморфизм (8-22) из предл. 8.4 превращается в функториальный по $B$-модулю $X$ и $A$-модулю $Y$ изоморфизм абелевых групп

$$\mathrm{Hom}_{\mathcal{M}od\text{-}A}(\mathrm{res}\, X, Y) \simeq \mathrm{Hom}_{\mathcal{M}od\text{-}B}\big(X, \mathrm{Hom}_{\mathcal{M}od\text{-}A}(B, Y)\big) .$$

Правый $B$-модуль $\mathrm{coind}\, Y \overset{\text{def}}{=} \mathrm{Hom}_{\mathcal{M}od\text{-}A}(B, Y)$ называется *коиндуцированным* с $A$-модуля $Y$. Таким образом, функтор коиндуцирования $\mathrm{coind} : \mathcal{M}od\text{-}A \to \mathcal{M}od\text{-}B$ сопряжён справа к функтору ограничения.

Упражнение 8.25. Явно опишите естественные преобразования

$$t_Y : \mathrm{res}\,\mathrm{coind}\, Y \to Y \quad \text{и} \quad s_X : X \to \mathrm{coind}\,\mathrm{res}\, X .$$

В ситуации, когда $A = \Bbbk[H]$ и $B = \Bbbk[G]$ являются групповыми алгебрами группы $G$ и её подгруппы $H \subset G$ с коэффициентами в поле $\Bbbk$, мы получаем обсуждавшиеся нами в n° 6.3 на стр. 88 функторы (ко)индуцирования линейных представлений группы $G$ над полем $\Bbbk$ с представлений её подгруппы $H \subset G$.

Упражнение 8.26*. Покажите, что функторы ind, coind : $\mathcal{M}od\text{-}H \to \mathcal{M}od\text{-}G$ естественно изоморфны, если индекс $[G : H]$ конечен.

Пример 8.22 (сингулярные симплексы)
Свяжем с топологическим пространством $Y$ симплициальное множество его *сингулярных симплексов* $S(Y) : \Delta^{\mathrm{opp}} \to \mathcal{S}et$, которое сопоставляет комбинаторному симплексу $[n] \in \operatorname{Ob}\Delta$ множество $S_n(Y) \overset{\text{def}}{=} \operatorname{Hom}_{\mathcal{T}op}(\Delta^n, Y) = h_Y(\Delta^n)$ всех непрерывных отображений правильного $n$-мерного симплекса $\Delta^n \subset \mathbb{R}^{n+1}$ в $Y$, а неубывающему отображению $\varphi : [n] \to [m]$ — правое умножение $f \mapsto f \circ \varphi^*$ на аффинное отображение $\varphi^* : \Delta^m \to \Delta^n$, действие которого на вершины симплекса совпадает с $\varphi$. Возникающий таким образом функтор $S : \mathcal{T}op \to p\mathcal{S}h(\Delta)$ сопряжён справа функтору геометрической реализации $p\mathcal{S}h(\Delta) \to \mathcal{T}op$, $X \mapsto |X|$, из прим. 8.7 на стр. 112, т. е. имеется естественный по симплициальному множеству $X : \Delta^{\mathrm{opp}} \to \mathcal{S}et$ и топологическому пространству $Y$ изоморфизм

$$\operatorname{Hom}_{\mathcal{T}op}(|X|, Y) \simeq \operatorname{Hom}_{p\mathcal{S}h}(X, S(Y)), \tag{8-24}$$

который является категорным аналогом изоморфизма из форм. (8-22) на стр. 125. В самом деле, функтор геометрической реализации вкладывает категорию $\Delta$ в категорию $\mathcal{T}op$ в виде дизъюнктного набора $D = \bigsqcup_{n\geqslant 0} \Delta^n$ правильных симплексов всех размерностей. На пространстве $D$ имеется левое действие стрелок $\varphi$ категории $\Delta$ аффинными отображениями $\varphi_*$. Оно задаёт правое действие стрелок из $\Delta$ на множестве $S(Y) = \operatorname{Hom}_{\mathcal{T}op}(D, Y)$ сингулярных симплексов топологического пространства $Y$. С другой стороны, каждое симплициальное множество $X : \Delta^{\mathrm{opp}} \to \mathcal{S}et$ по определению снабжено правым действием стрелок категории $\Delta$ на множества $X_n = X([n])$, и геометрическая реализация $|X|$, представляющая собою фактор дизъюнктного объединения $\bigsqcup_{n\geqslant 0} X_n \times \Delta^n$ по соотношениям $(x\varphi, s) = (x, \varphi s)$, является прямым аналогом «тензорного произведения $X \otimes_\Delta D$». Таким образом, изоморфизм (8-24) имеет вид

$$\operatorname{Hom}_{\mathcal{T}op}\big(X \otimes_\Delta D, Y\big) \simeq \operatorname{Hom}_{\mathcal{M}od\text{-}\Delta}\big(X, \operatorname{Hom}_{\mathcal{T}op}(D, Y)\big), \tag{8-25}$$

ничем не отличающийся от изоморфизма (8-22) со стр. 125.

Упражнение 8.27. Явно постройте взаимно обратные изоморфизмы между левой и правой частями формулы (8-25) и опишите естественные преобразования[1]

$$t_Y : |S(Y)| \to Y \quad \text{и} \quad s_X : X \to S\big(|X|\big).$$

[1] Первое является непрерывным отображением топологических пространств, второе — естественным преобразованием функторов $\Delta^{\mathrm{opp}} \to \mathcal{S}et$, переводящих комбинаторный симплекс $[n]$ в множества $X_n$ и $\operatorname{Hom}_{\mathcal{T}op}\big(\Delta^n, |X|\big)$ соответственно.

## §9. Расширения коммутативных колец

**9.1. Целые элементы.** Всюду этом параграфе термин «кольцо» по умолчанию подразумевает *коммутативное кольцо с единицей*, а все гомоморфизмы колец предполагаются отображающими единицу в единицу. Если кольцо $A$ является подкольцом кольца $B$, то мы называем $B$ *расширением* кольца $A$. В этой ситуации элемент $b \in B$ называется *целым* над $A$, если он удовлетворяет перечисленным в лем. 9.1 условиям.

Лемма 9.1 (характеризация целых элементов)
Следующие три свойства элемента $b \in B$ попарно эквивалентны:

(1) $b^m = a_1\, b^{m-1} + \dots + a_{m-1}\, b + a_m$ для некоторых $m \in \mathbb{N}$ и $a_1, \dots, a_m \in A$

(2) $A$-линейная оболочка всех целых неотрицательных степеней $b^m$ линейно порождается над $A$ конечным числом элементов

(3) существует конечно порождённый $A$-подмодуль $M \subset B$, который не аннулируется умножением ни на какой ненулевой элемент из $B$, и такой, что $bM \subset M$.

Доказательство. Импликации (1) $\Rightarrow$ (2) $\Rightarrow$ (3) очевидны. Покажем, что (3) $\Rightarrow$ (1). Пусть элементы $e_1, \dots, e_m$ линейно порождают $M$ над $A$ и $A$-линейный оператор $b : M \to M$, $m \mapsto bm$, умножения на $b$ действует на эти образующие по правилу

$$(be_1, \dots, be_m) = (e_1, \dots, e_m) \cdot Y\,, \tag{9-1}$$

где $Y \in \mathrm{Mat}_m(A)$ — некоторая матрица. Для любой квадратной матрицы $X$ над любым коммутативным кольцом с единицей выполняется тождество $\det X \cdot E = X \cdot X^{\vee}$, где $X^{\vee}$ — присоединённая к $X$ матрица[1], а $E$ — единичная матрица того же размера, что $X$. Согласно этому тождеству, образ оператора умножения на $\det X$ содержится в линейной оболочке столбцов матрицы $X$. Мы заключаем, что $\det(bE - Y) \cdot M$ содержится в линейной оболочке векторов $(e_1, \dots, e_m) \cdot (bE - Y)$, которая равна нулю в силу (9-1). Поскольку умножение на ненулевой элемент кольца $B$ не может аннулировать модуль $M$, равенство $\det(bE - Y) \cdot M = 0$ влечёт равенство $\det(bE - Y) = 0$. Так как все элементы матрицы $Y$ лежат в $A$, последнее равенство имеет требуемый в условии (1) вид. □

Определение 9.1
Множество всех $b \in B$, целых над подкольцом $A \subset B$, называется *целым замыканием* $A$ в $B$. Если оно совпадает с $A$, подкольцо $A$ называется *целозамкнутым* в $B$. Если оно совпадает с $B$, расширение колец $A \subset B$ называется *целым* и кольцо $B$ называется *целой $A$-алгеброй*.

Пример 9.1 (целозамкнутость $\mathbb{Z}$ в $\mathbb{Q}$)
Покажем, что кольцо $\mathbb{Z}$ целозамкнуто в поле $\mathbb{Q} \supset \mathbb{Z}$. Если дробь $p/q$ с взаимно простыми $p, q \in \mathbb{Z}$ такова, что

$$\frac{p^m}{q^m} = a_1\,\frac{p^{m-1}}{q^{m-1}} + \dots + a_{m-1}\frac{p}{q} + a_m$$

с $a_i \in \mathbb{Z}$, то $p^m = a_1 q p^{m-1} + \dots + a_{m-1} q^{m-1} p + a_m q^m$ делится на $q$, что при взаимно простых $p$ и $q$ возможно только если $q = \pm 1$.

[1] Она состоит из алгебраических дополнений $x^{\vee}_{ij} = (-1)^{i+j} X_{ji}$ к элементам матрицы $X^t$, см. теорему 8.1 на стр. 114 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_08.pdf.

Пример 9.2 (инварианты действия конечной группы)
Пусть конечная группа $G$ действует на кольце $B$ кольцевыми автоморфизмами. Покажем, что кольцо $B$ цело над *подкольцом инвариантов* $B^G \overset{\text{def}}{=} \{a \in B \mid \forall g \in G \;\; ga = a\}$. Если $G$-орбита элемента $b \in B$ состоит из элементов $b_1, \dots, b_n$, где $b = b_1$, то элемент $b$ является корнем приведённого[1] многочлена $B(t) = \prod(t - b_i) \in B^G[t]$.

Предложение 9.1
Целое замыкание любого подкольца $A \subset B$ является подкольцом в $B$. В любом расширении колец $C \supset B$ всякий элемент $c \in C$, целый над целым замыканием $A$ в $B$, цел и над $A$.

Доказательство. Если элементы $p, q \in B$ таковы, что

$$p^m = x_1 p^{m-1} + \dots + x_{m-1} p + x_m \quad \text{и} \quad q^n = y_1 q^{n-1} + \dots + y_{n-1} q + y_n$$

для некоторых $x_\nu, y_\mu \in A$, то произведения $p^i q^j$ с $0 \leqslant i \leqslant m-1$ и $0 \leqslant j \leqslant n-1$ порождают $A$-модуль, который выдерживает умножение и на $p$, и на $q$, а значит, и на $p+q$, и на $pq$. Поскольку он содержит единицу, его нельзя аннулировать умножением ни на какой элемент из $B$. Аналогично, если $z_0^r = z_1 z_0^{r-1} + \dots + z_{r-1} z_0 + z_r$, где каждый $z_k$ с $k > 0$ удовлетворяет равенству

$$z_k^{m_k} = a_{k,1}\, z_k^{m_k - 1} + \dots + a_{k,m_k-1}\, z_k + a_{k,m_k}$$

для некоторых $a_{k,\ell} \in A$, то умножение на элемент $z_0$ переводит в себя $A$-линейную оболочку всех произведений $z_0^{j_0} z_1^{j_1} \cdots z_r^{j_r}$, где $0 \leqslant j_0 \leqslant r-1$ и $0 \leqslant j_k \leqslant m_k - 1$ при $k > 0$. □

Следствие 9.1 (лемма Гаусса – Кронекера – Дедекинда)
Для любого расширения колец $A \subset B$ и произвольных приведённых многочленов $f, g \in B[x]$ положительной степени все коэффициенты произведения $f(x)g(x)$ целы над $A$ если и только если все коэффициенты обоих многочленов $f(x)$ и $g(x)$ целы над $A$.

Доказательство. Если коэффициенты многочленов $f$ и $g$ целы над $A$, то коэффициенты их произведения $h = fg$ тоже целы над $A$, поскольку целые элементы образуют кольцо. Чтобы показать обратное, рассмотрим какое-нибудь кольцо $C \supset B$, над которым $f$ и $g$ полностью разлагаются на линейные множители[2], т. е. $f(x) = \prod(x - \alpha_\nu)$ и $g(x) = \prod(x - \beta_\mu)$ в $C[x]$ для некоторых $\alpha_\nu, \beta_\mu \in C$. Если все коэффициенты многочлена $h(x) = \prod(x - \alpha_\nu)\prod(x - \beta_\mu)$ целы над $A$, то все его корни $\alpha_\nu$ и $\beta_\mu$ целы над целым замыканием $A$ в $C$, а значит, и над самим $A$. Поскольку коэффициенты многочленов $f$ и $g$ являются многочленами от $\alpha_\nu$ и $\beta_\mu$, они тоже целы над $A$. □

Предложение 9.2
Пусть кольцо $B$ цело над подкольцом $A \subset B$. Если $B$ — поле, то $A$ также является полем. Наоборот, если $A$ — поле, и в $B$ нет делителей нуля, то $B$ — поле.

[1] Напомню, что многочлен называется *приведённым*, если его старший коэффициент равен единице.

[2] Кольцо $C \supset B$, над которым заданный приведённый многочлен $f \in B[x]$ полностью раскладывается на линейные множители, строится индукцией по $\deg f$. Если $\deg f > 0$, то $B$ вкладывается в фактор кольцо $F = B[x]/(f)$ как подкольцо, образованное классами констант. В кольце $F$ многочлен $f$ имеет корень $\gamma = x \pmod{f}$. Поэтому $f(x) = (x - \gamma) \cdot f_1(x)$, где $f_1 \in F[x]$ тоже приведён и $\deg f_1 < \deg f$. По индукции, $f_1 = \prod(x - \gamma_i)$ для подходящих элементов $\gamma_i$ из подходящего расширения $C \supset F \supset B$.

Доказательство. Если $B$ — поле, целое над $A$, то обратный к произвольному ненулевому $a \in A$ элемент $a^{-1} \in B$ удовлетворяет уравнению $a^{-m} = \alpha_1 a^{1-m} + \dots + \alpha_{m-1} a^{-1} + \alpha_0$, где $\alpha_\nu \in A$. Умножая обе части на $a^{m-1}$, заключаем, что $a^{-1} = \alpha_1 + \dots + \alpha_{m-1} a^{m-2} + \alpha_0 a^{m-1} \in A$.

Обратно, если $A$ — поле, и $B$ — целая $A$-алгебра, то все неотрицательные целые степени $b^i$ любого ненулевого элемента $b \in B$ порождают конечномерное векторное пространство $V$ над полем $A$. Если в $B$ нет делителей нуля, то линейный оператор $b : V \to V$, $x \mapsto bx$, сюрьективен, так как имеет нулевое ядро. Обратный к $b$ элемент $b^{-1}$ является прообразом единицы $1 \in V$. □

Пример 9.3 (целые алгебраические числа)
Пусть поле $K \supset \mathbb{Q}$ конечномерно как векторное пространство над $\mathbb{Q}$. Элементы таких полей называются *алгебраическими числами*. По предл. 9.1 целые над $\mathbb{Z}$ алгебраические числа образуют в поле $K$ подкольцо. Оно называется *кольцом целых* поля $K$ и обозначается $\mathcal{O}_K$. Поскольку целые неотрицательные степени $\xi^m$ любого числа $\xi \in K$ линейно зависимы над $\mathbb{Q}$, каждое алгебраическое число $\xi$ удовлетворяет уравнению $a_0\xi^n + a_1\xi^{n-1} + \dots + a_{n-1}\xi + a_n = 0$ с коэффициентами $a_i \in \mathbb{Z}$, откуда вытекает, что число $a_0\xi$ цело[1] над $\mathbb{Z}$. Таким образом, для каждого алгебраического числа $\xi$ и для любого базиса $e_1, \dots, e_d$ поля $K$ как векторного пространства над $\mathbb{Q}$ существует такое $n \in \mathbb{N}$, что $n\xi$ и все $ne_i$ целы над $\mathbb{Z}$. В частности, каждое конечномерное над $\mathbb{Q}$ поле $K \supset \mathbb{Q}$ является полем частных своего кольца целых $\mathcal{O}_K$.

Упражнение 9.1. Покажите, что кольцо целых $\mathcal{O}_K \subset K$ является свободным $\mathbb{Z}$-модулем ранга $d = \dim_{\mathbb{Q}} K$, а число $\zeta \in K$ является целым над $\mathbb{Z}$ если и только если оператор умножения на $\zeta$ записывается в подходящем базисе $K$ над $\mathbb{Q}$ целочисленной матрицей[2].

Пример 9.4 (целые квадратичные иррациональности)
Расширение $K \supset \mathbb{Q}$ называется *квадратичным*, если $K$ двумерно как векторное пространство над $\mathbb{Q}$. В этом случае для любого $\zeta \in K \smallsetminus \mathbb{Q}$ числа 1 и $\zeta$ образуют базис $K$ над $\mathbb{Q}$, и $\zeta^2 = b\zeta + c$ для некоторых $b, c \in \mathbb{Q}$, откуда $\zeta = x + y\sqrt{d}$ для подходящих $x, y \in \mathbb{Q}$ и свободного от квадратов[3] целого $d$. Поэтому $K = \mathbb{Q}[\sqrt{d}] = \mathbb{Q}[x]/(x^2 - d)$. Таким образом, каждое квадратичное расширение получается присоединением к $\mathbb{Q}$ квадратного корня из свободного от квадратов целого числа.

Упражнение 9.2. Покажите, что $\mathbb{Q}[\sqrt{d_1}] \not\simeq \mathbb{Q}[\sqrt{d_2}]$ для свободных от квадратов $d_1 \neq d_2$.

Пусть число $\xi = a + b\sqrt{d}$, где $a, b \in \mathbb{Q}$, цело над $\mathbb{Z}$. Обозначим через $t = \operatorname{tr}(\xi)$ и $n = N(\xi)$ след и определитель оператора умножения на $\xi$ в поле $K = \mathbb{Q}[\sqrt{d}]$. Так как в подходящем базисе поля $K$над $\mathbb{Q}$ этот оператор имеет целочисленную матрицу, оба числа $t, n \in \mathbb{Z}$. В базисе $1, \sqrt{d}$ умножение на $\xi$ имеет матрицу

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Поэтому $t = 2a \in \mathbb{Z}$ и $n = a^2 - db^2 = t^2/4 - db^2 \in \mathbb{Z}$. Полагая $s = 2b$, мы заключаем, что $s \in \mathbb{Z}$ и $t^2 - ds^2 \equiv 0 \pmod 4$. Если $d \equiv 1 \pmod 4$, то $t^2 \equiv s^2 \pmod 4$, откуда $t \equiv s \pmod 2$. Пусть $s = t + 2r$, где $r \in \mathbb{Z}$. Тогда $\xi = t + r(1 + \sqrt{d})/2$.

Упражнение 9.3. Убедитесь, что $(1 + \sqrt{d})/2 \in \mathcal{O}_K$ при $d \equiv 1 \pmod 4$.

[1] Ибо $\zeta = a_0\xi$ удовлетворяет уравнению $\zeta^n = -a_1 \cdot \zeta^{n-1} - a_0a_2 \cdot \zeta^{n-2} - \dots - a_0^{n-1}a_n$.

[2] Именно так целые алгебраические числа были впервые определены Дедекиндом в XIX веке.

[3] Целое число называется *свободным от квадратов*, если оно отлично от нуля и единицы и не делится на отличные от единицы целые квадраты.

Мы заключаем, что при $d \equiv 1 \pmod 4$ базис $\mathbb{Z}$-модуля $\mathcal{O}_K$ образуют 1 и $(1+\sqrt{d})/2$. В частности, *числа Кронекера*, т. е. целые элементы поля $\mathbb{Q}[\sqrt{-3}] = \mathbb{Q}[\omega]/(\omega^2+\omega+1)$, исчерпываются целочисленными линейными комбинациями вида $a + b\omega$, где $\omega = (-1+\sqrt{-3})/2$ — первообразный комплексный кубический корень из единицы. Если $d \equiv 2 \pmod 4$ или $d \equiv 3 \pmod 4$, то соответственно $t^2 \equiv 2s^2 \pmod 4$ или $t^2 + s^2 \equiv 0 \pmod 4$, и оба числа $t, s$ чётны, а $\xi = a + b\sqrt{d}$ имеет $a, b \in \mathbb{Z}$. Так как $\sqrt{d} \in \mathcal{O}_K$, базис $\mathbb{Z}$-модуля $\mathcal{O}_K$ при $d \equiv 2, 3 \pmod 4$ составляют 1 и $\sqrt{d}$. В частности, *гауссовы числа*, т. е. целые элементы поля $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]/(i^2+1)$исчерпываются целочисленными линейными комбинациями вида $a + bi$, где $i = \sqrt{-1}$ — первообразный комплексный корень четвёртой степени из единицы.

**9.2. Приложения к теории представлений.** Пусть $G$ — конечная группа. Значение характера $\chi_\varrho$ любого конечномерного представления $\varrho$ группы $G$ на любом элементе $g \in G$ цело над $\mathbb{Z}$ в силу того, что оператор $\varrho(g)$ аннулируется многочленом $t^{|G|} - 1$, все корни которого целы над $\mathbb{Z}$, а значение $\chi_\varrho(g)$ равно сумме некоторых из этих корней[1].

Теорема 9.1

Если конечная группа $G$ имеет нормальную абелеву подгруппу $A \lhd G$, то размерности всех комплексных неприводимых линейных представлений группы $G$ делят индекс $[G : A]$.

Доказательство. Пусть $\varrho : \mathbb{C}[G] \to \operatorname{End} W$ — неприводимое комплексное представление. Сначала докажем теорему для единичной подгруппы $A = \{e\}$, т. е. покажем, что $\dim W$ делит $|G|$. В силу прим. 9.1 достаточно убедиться, что рациональное число $|G|/\dim W$ цело над $\mathbb{Z}$. Так как представление $\varrho$ неприводимо, скалярный квадрат его характера равен единице:

$$1 = (\chi_\varrho, \chi_\varrho) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \varrho(g^{-1}) \cdot \operatorname{tr} \varrho(g)\,. \tag{9-2}$$

Функция $g \mapsto \operatorname{tr} \varrho(g^{-1})$ постоянна на классах сопряжённости, и её значения целы над $\mathbb{Z}$. Обозначим через $\tau(K) \in \mathbb{C}$ её значение на классе $K \in \operatorname{Cl}(G)$ и перепишем (9-2) как

$$\frac{|G|}{\dim W} = \frac{1}{\dim W} \sum_{g \in G} \operatorname{tr} \varrho(g^{-1}) \cdot \operatorname{tr} \varrho(g) = \sum_{K \in \operatorname{Cl} G} \frac{\tau(K)}{\dim W}\, \operatorname{tr} \sum_{g \in K} \varrho(g)\,.$$

Достаточно проверить, что каждое из чисел

$$\frac{1}{\dim W}\, \operatorname{tr} \sum_{g \in K} \varrho(g) = \frac{\operatorname{tr} \varrho(g_K)}{\dim W}\,, \quad \text{где} \quad g_K \overset{\text{def}}{=} \sum_{g \in K} g \in Z(\mathbb{Z}[G])\,,$$

цело над $\mathbb{Z}$. Неприводимое представление $\varrho$ переводит конечно порождённый $\mathbb{Z}$-модуль центральных элементов подкольца $\mathbb{Z}[G] \subset \mathbb{C}[G]$ в конечно порождённый $\mathbb{Z}$-подмодуль кольца $\operatorname{End} W$. По лемме Шура все элементы последнего подмодуля являются скалярными гомотетиями, ибо перестановочны со всеми элементами группы. Коэффициенты этих гомотетий образуют конечно порождённый $\mathbb{Z}$-подмодуль в $\mathbb{C}$, выдерживающий умножение на каждый из коэффициентов. Следовательно, все эти коэффициенты целы над $\mathbb{Z}$. Но коэффициент гомотетии $\varrho(g_K)$ как раз и равен $\operatorname{tr} \varrho(g_K)/\dim W$. Итак, $|G|/\dim W \in \mathbb{Z}$.

[1] Напомню, что собственные числа оператора содержатся среди корней любого аннулирующего этот оператор многочлена.

Теперь рассмотрим случай, когда $A = Z(G)$ является центром группы $G$, т. е. покажем, что рациональное число $q = [G : Z(G)]/\dim W$ тоже цело над $\mathbb{Z}$. Для этого достаточно убедиться, что все его натуральные степени $q^n$ лежат в конечно порождённом $\mathbb{Z}$-подмодуле поля $\mathbb{Q}$. Рассмотрим действие группы $G^n = G \times \dots \times G$ на $W^{\otimes n}$ по правилу

$$(g_1, \dots, g_n) : w_1 \otimes \dots \otimes w_n \mapsto \varrho(g_1)w_1 \otimes \dots \otimes \varrho(g_n)w_n .$$

Упражнение 9.4. Убедитесь, что это неприводимое линейное представление.

Подгруппа $C \subset G^n$, состоящая из таких элементов $(c_1, \dots, c_n)$, что все $c_i \in Z(G)$ и произведение $c_1 \dots c_n = 1$, содержится в ядре этого представления, поскольку по лемме Шура каждый центральный элемент $c_i$ действует в неприводимом представлении $\varrho$ умножением на некоторую константу, и произведение этих констант равно единице в силу равенства $\prod \varrho(c_i) = \varrho(c_1 \dots c_n) = \varrho(1) = 1$. Подгруппа $C$ имеет порядок $|Z(G)|^{n-1}$ и нормальна, поскольку лежит в центре группы $G^n$. Таким образом, пространство $W^{\otimes n}$ размерности $\dim^n W$ является неприводимым представлением фактор группы $G^n/C$ порядка $|G|^n/|Z(G)|^{n-1}$. По уже доказанному

$$\frac{|G|^n}{(\dim W)^n |Z(G)|^{n-1}} = |Z(G)| \cdot q^n \in \mathbb{Z} .$$

Тем самым, все степени $q^n$ лежат в $\mathbb{Z}$-модуле $|Z(G)|^{-1}\,\mathbb{Z} \subset \mathbb{Q}$ ранга 1.

Наконец, рассмотрим произвольную нормальную абелеву подгруппу $A \lhd G$ и изотипное разложение $\operatorname{res}_A W = \bigoplus W_\chi$ ограничения представления $\varrho$ на $A$. Каждая изотипная компонента $W_\chi$ является прямой суммой одномерных представлений абелевой группы $A$, отвечающих некоторому мультипликативному характеру[1] $\chi : A \to \mathbb{C}^*$, т. е. $aw = \chi(a)w$ для всех $a \in A$ и $w \in W_\chi$. Поскольку подгруппа $A$ нормальна в $G$, группа $G$ действует на её мультипликативных характерах: элемент $g \in G$ переводит характер $\chi : A \to \mathbb{C}^*$ в композицию $\chi^g = \chi \circ \mathrm{Ad}_{g^{-1}}$, принимающую на элементах $a \in A$ значения $\chi^g(a) = \chi(g^{-1}ag)$. Так как $agw = gg^{-1}agw = g\chi^g(a)w = \chi^g(a)gw$ для всех $w \in W_\chi$, $a \in A$, $g \in G$, в представлении $\varrho$ каждый элемент $g \in G$ изоморфно отображает изотипную компоненту $W_\chi$ в компоненту $W_{\chi^g}$. Поскольку представление $\varrho$ неприводимо, действие $G$ на изотипных компонентах $W_\chi$ транзитивно. Поэтому все компоненты имеют одну и ту же размерность, которая делит $\dim W$. Если компонента всего одна, то все элементы подгруппы $A$ действуют на $W$ скалярно, и образ $\varrho(A)$ лежит в центре $Z(\varrho(G))$ образа всего представления. По уже доказанному индекс центра $[\varrho(G) : Z(\varrho(G))]$ делится на $\dim W$. Но этот индекс делит индекс $[\varrho(G) : \varrho(A)]$ центральной подгруппы $\varrho(A)$, а последний в свою очередь делит индекс[2] $[G : A]$. Остаётся рассмотреть случай, когда изотипных компонент несколько. Пусть $W_\chi$ — одна из них. Обозначим через $H = \{g \in G \mid g(W_\chi) = W_\chi\}$ её стабилизатор в $G$. Тогда общее число изотипных компонент равно $[G : H]$, подгруппа $H \subsetneq G$ является собственной, содержит $A$, и её линейное представление в пространстве $W_\chi$ неприводимо.

Упражнение 9.5. Убедитесь в этом.

Применяя индукцию по порядку $|G|$, мы можем считать, что $\dim W_\chi$ делит индекс $[H : A]$. Но тогда и $\dim W = [G : H]\,\dim W_\chi$ делит $[G : A] = [G : H]\,[H : A]$. □

[1]См. n° 5.4.1 на стр. 72.

[2]Ибо гомоморфизм $\varrho$ корректно задаёт эпиморфизм фактор групп $G/A \twoheadrightarrow \varrho(G)/\varrho(A)$.

**9.3. Алгебраические элементы.** Коммутативная $\Bbbk$-алгебра $B$ называется *конечно порождённой*, если существует эпиморфизм $\Bbbk$-алгебр $\pi : \Bbbk[x_1, \dots, x_m] \twoheadrightarrow B$. В этом случае образы переменных $b_i = \pi(x_i) \in B$ называются *образующими* алгебры $B$, а ядро $\ker\pi \subset \Bbbk[x_1, \dots, x_m]$ называется *идеалом соотношений* между ними. Элемент $b \in B$ цел над полем $\Bbbk$ если и только если *гомоморфизм вычисления* $\mathrm{ev}_b : \Bbbk[x] \to B$, $f \mapsto f(b)$, имеет ненулевое ядро, т. е. $f(b) = 0$ для какого-нибудь ненулевого $f \in \Bbbk[x]$. Такие элементы $b$ также называют *алгебраическими* над полем $\Bbbk$. Поскольку все идеалы в $\Bbbk[x]$ главные, $\ker(\mathrm{ev}_b) = (\mu_b)$, где образующая $\mu_b \in \Bbbk[x]$ однозначно определяется алгебраическим элементом $b$ как приведённый многочлен наименьшей степени, аннулирующий $b$. Этот многочлен называется *минимальным многочленом* элемента $b$ над $\Bbbk$. Элемент $b \in B$, не являющийся алгебраическим, называется *трансцендентным* над $\Bbbk$.

Обозначим через $\Bbbk[b] = \mathrm{im}\,\mathrm{ev}_b \subset B$ наименьшую $\Bbbk$-подалгебру в $B$, содержащую элементы 1 и $b$. Если $b$ трансцендентен, подалгебра $\Bbbk[b]$ изоморфна кольцу многочленов $\Bbbk[x]$. В частности, она бесконечномерна как векторное пространство над $\Bbbk$ и не является полем. Когда $b$ алгебраичен, алгебра $\Bbbk[b] \simeq \Bbbk[x]/(\mu_b)$ имеет размерность $\deg \mu_b$ как векторное пространство над $\Bbbk$. Она является полем если и только если многочлен $\mu_b$ неприводим в $\Bbbk[x]$.

Упражнение 9.6. Убедитесь, что следующие три свойства алгебраического над полем $\Bbbk$ элемента $b \in B$ с минимальным многочленом $\mu_b \in \Bbbk[x]$ эквивалентны друг другу: а) $\Bbbk[b]$ является полем б) $\Bbbk[b]$ не имеет делителей нуля в) $\mu_b$ неприводим в $\Bbbk[x]$.

Теорема 9.2

Если конечно порождённая $\Bbbk$-алгебра является полем, то все её элементы алгебраичны над $\Bbbk$.

Доказательство. Пусть алгебра $B$ является полем и порождается над $\Bbbk$ элементами $b_1, \dots, b_m$. Воспользуемся индукцией по $m$. Случай $m = 1$ был разобран перед упр. 9.6 выше. Пусть $m > 1$. Если $b_m$ алгебраичен над $\Bbbk$, то алгебра $\Bbbk[b_m]$ является полем. Тогда по предположению индукции поле $B$ алгебраично над $\Bbbk[b_m]$, а значит и над $\Bbbk$ по предл. 9.1 на стр. 129. Остаётся убедиться, что образующая $b_m$ не может быть трансцендентна над $\Bbbk$. Допустим противное. Тогда изоморфизм $\Bbbk[x] \xrightarrow{\sim} \Bbbk[b_m]$ продолжается до изоморфизма поля рациональных функций $\Bbbk(x)$ с наименьшим содержащим элемент $b_m$ подполем $\Bbbk(b_m) \subset B$. По предположению индукции поле $B$ алгебраично над полем $\Bbbk(b_m)$, т. е. каждая из образующих $b_1, \dots, b_{m-1}$ удовлетворяет некоторому полиномиальному уравнению с коэффициентами из $\Bbbk(b_m)$. Умножая эти уравнения на подходящие многочлены от $b_m$, сделаем их коэффициенты лежащими в $\Bbbk[b_m]$, а все старшие коэффициенты — равными одному и тому же многочлену $p(b_m) \in \Bbbk[b_m]$. Поле $B$ цело над подалгеброй $F \subset B$, порождённой над $\Bbbk$ элементами $b_m$ и $1/p(b_m)$. По предл. 9.2 подалгебра $F$ является полем. Покажем, что элемент $1 + p(b_m) \in F$ не обратим в $F$. Пусть это не так, и

$$\big(1 + p(b_m)\big)\, g\big(b_m, 1/p(b_m)\big) = 1 \tag{9-3}$$

для некоторого многочлена $g \in \Bbbk[x_1, x_2]$. Записывая рациональную функцию $g\big(x, 1/p(x)\big)$ в виде $h(x)/p^k(x)$, где $h \in \Bbbk[x]$ не делится в $\Bbbk[x]$ на $p$, и умножая обе части (9-3) на $p^k(b_m)$, мы получим на $b_m$ полиномиальное уравнение $h(b_m)\,(1 + p(b_m)) = p^{k+1}(b_m)$. Оно нетривиально, поскольку $h(1 + p) = h + hp$ не делится на $p$. □

Следствие 9.2

Всякое поле $\mathbb{F}$, являющееся конечно порождённой алгеброй над подполем $\Bbbk \subset \mathbb{F}$, конечномерно как векторное пространство над $\Bbbk$.

Доказательство. Индукция по числу образующих: добавление очередной алгебраической образующей приводит к конечномерному пространству над полем, порождённым предыдущими образующими. □

Определение 9.2 (нормальные кольца)
Коммутативное кольцо $A$ без делителей нуля называется *нормальным*, если оно целозамкнуто в своём поле частных $Q_A$. В частности, каждое поле нормально.

Пример 9.5 (факториальные кольца нормальны)
Дословно то же рассуждение, что и в прим. 9.1, показывает, что любое факториальное[1] кольцо $A$ нормально: многочлен $a_0t^m + a_1t^{m-1} + \dots + a_{m-1}t + a_m \in A[t]$ аннулирует дробь $p/q \in Q_A$ с $\text{нод}(p,q) = 1$, только если $q|a_0$ и $p|a_m$, поэтому из $a_0 = 1$ вытекает, что $q = 1$. В частности, кольцо многочленов от любого числа переменных над факториальным кольцом нормально.

Следствие 9.3 (лемма Гаусса)
Пусть $A$ — нормальное кольцо с полем частных $Q_A$. Если в $Q_A[x]$ многочлен $f \in A[x]$ раскладывается в произведение приведённых множителей, то все эти множители лежат в $A[x]$.

Доказательство. Это вытекает из сл. 9.1 на стр. 129. □

Следствие 9.4
Пусть $A$ — целостное[2] кольцо с полем частных $Q_A$, и $B$ — произвольная $Q_A$-алгебра. Если элемент $b \in B$ цел над $A$, то все коэффициенты его минимального многочлена над полем $Q_A$ целы над $A$.

Доказательство. Поскольку $b$ цел над $A$, он аннулируется приведённым многочленом $f \in A[x]$, который делится в $Q_A[x]$ на минимальный многочлен элемента $b$ над полем $Q_A$. Поэтому все коэффициенты минимального многочлена целы над $A$ в силу сл. 9.1 на стр. 129. □

Следствие 9.5
Пусть $A$ — нормальное кольцо с полем частных $Q_A$, и $B$ — произвольная $Q_A$-алгебра. Если элемент $b \in B$ цел над $A$, то его минимальный многочлен над полем $Q_A$ лежит в $A[x]$. □

**9.4. Базисы трансцендентности.** Пусть $\Bbbk$-алгебра $A$ не имеет делителей нуля. Обозначаем через $Q_A$ её поле частных, а через $\Bbbk(a_1, \dots, a_m) \subset Q_A$ — наименьшее подполе, содержащее заданные элементы $a_1, \dots, a_m \in A$.

Элементы $a_1, \dots, a_m \in A$ называются *алгебраически независимыми* над $\Bbbk$, если гомоморфизм вычисления $\text{ev}_{(a_1,\dots,a_m)} : \Bbbk[x_1, \dots, x_m] \to A$, $f \mapsto f(a_1, \dots, a_m)$ инъективен, т. е. на элементы $a_1, \dots, a_m$ нет нетривиальных полиномиальных соотношений. В этом случае гомоморфизм вычисления продолжается до изоморфизма полей $\Bbbk(x_1, \dots, x_m) \xrightarrow{\sim} \Bbbk(a_1, \dots, a_m) \subset Q_A$, переводящего рациональную функцию $f(x_1, \dots, x_m)$ в её значение на элементах $a_i$.

[1] Напомню, что кольцо называется *факториальным*, если в нём нет делителей нуля, каждый необратимый элемент является произведением конечного числа неприводимых, и если $p_1 \dots p_n = q_1 \dots q_m$, где все $p_i$ и $q_j$ неприводимы, то $m = n$ и после надлежащей перенумерации $p_i = s_iq_i$, где все $s_i$ обратимы. Поля, кольца главных идеалов и кольца многочленов с коэффициентами в факториальном кольце факториальны. См. лекцию http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_05.pdf.

[2] Т. е. без делителей нуля.

Элементы $a_1, \dots, a_m \in A$ называются *алгебраически порождающими* $A$ над $\Bbbk$, если каждый элемент алгебры $A$ алгебраичен над $\Bbbk(a_1, \dots, a_m)$. В этом случае поле $Q_A$ тоже алгебраично над $\Bbbk(a_1, \dots, a_m)$, так как целое замыкание $\Bbbk(a_1, \dots, a_m)$ в $Q_A$ является полем по предл. 9.2 на стр. 129 и содержит $A$, а значит, и $Q_A$.

Алгебраически независимый набор элементов $a_1, \dots, a_m$ алгебры $A$, алгебраически порождающий $A$ над $\Bbbk$, называется *базисом трансцендентности* алгебры $A$ над $\Bbbk$. Поскольку собственные подмножества любого базиса трансцендентности алгебраически независимы, но не являются базисами трансцендентности, базис трансцендентности можно иначе охарактеризовать либо как такой минимальный по включению набор $a_1, \dots, a_m$, что алгебра $A$ алгебраична над $\Bbbk(a_1, \dots, a_m)$, либо как максимальный по включению алгебраически независимый набор. Доказательство того, что все базисы трансцедентности состоят из одинакового числа элементов совершенно аналогично доказательству оответствующей теоремы о базисах векторных пространств.

Лемма 9.2 (о замене)
Если $b_1, \dots, b_n \in A$ алгебраически независимы, а $a_1, \dots, a_m \in A$ алгебраически порождают $A$ над $\Bbbk$, то $n \leqslant m$ и элементы $a_i$ можно перенумеровать так, что набор $b_1, \dots, b_n, a_{n+1}, \dots, a_m$ будет алгебраически порождать $A$ над $\Bbbk$.

Доказательство. Поскольку $b_1$ алгебраичен над $\Bbbk(a_1, \dots, a_m)$, имеется содержащее $b_1$ полиномиальное соотношение $f(b_1, a_1, \dots, a_m) = 0$, и так как $b_1$ трансцендентен над $\Bbbk$, в это соотношение входит какое-нибудь $a_i$. Перенумеруем $a_i$ так, чтобы это было $a_1$. Тогда алгебра $A$ алгебраична над $\Bbbk(b_1, a_2, \dots, a_m)$. Пусть по индукции элементы $b_1, \dots, b_k, a_{k+1}, \dots, a_m$ алгебраически порождают алгебру $A$ над $\Bbbk$, и при этом $k < n$. Поскольку $b_{k+1}$ алгебраичен над полем $\Bbbk(b_1, \dots, b_k, a_{k+1}, \dots, a_m)$, имеется содержащее $b_{k+1}$ полиномиальное соотношение

$$f(b_1, \dots, b_{k+1}, a_{k+1}, \dots, a_m) = 0\,.$$

Так как $b_1, \dots, b_n$ алгебраически независимы над $\Bbbk$, в это соотношение входит какое-нибудь $a_i$. Поэтому $m > k$, и после надлежащей перенумерации можно считать, что в последнем соотношении участвует элемент $a_{k+1}$. Тогда этот элемент, а с ним и вся алгебра $A$ алгебраичны над полем $\Bbbk(b_1, \dots, b_{k+1}, a_{k+2}, \dots, a_m)$, что воспроизводит индуктивное предположение. □

Следствие 9.6 (теорема о базисе)
Все базисы трансцендентности конечно порождённой $\Bbbk$-алгебры состоят из одинакового числа элементов, не превосходящего число образующих, причём любой набор элементов, алгебраически порождающий $A$ над $\Bbbk$, содержит в себе базис трансцендентности, а любой алгебраически независимый набор элементов можно дополнить до базиса трансцендентности. □

Определение 9.3
Число элементов в базисе трансцендентности конечно порождённой алгебры $A$ над $\Bbbk$ называется *степенью трансцендентности* этой алгебры и обозначается $\operatorname{tr}\deg_{\Bbbk} A$.

Пример 9.6 (теорема Люрота)
Степень трансцендентности любой отличной от поля $\Bbbk$ подалгебры $A \subset \Bbbk(t)$ в поле рациональных функций $\Bbbk(t)$ равна единице. В самом деле, если $\psi = f(t)/g(t) \in A \smallsetminus \Bbbk$, то элемент $t$ алгебраичен над наименьшим содержащим $\psi$ подполем $\Bbbk(\psi) \subset \mathbb{Q}_A$, ибо удовлетворяет уравнению $\psi \cdot g(x) - f(x) = 0$ с коэффициентами в $\Bbbk(\psi)$.

Упражнение 9.7. Убедитесь, что многочлен $\psi \cdot g(x) - f(x)$ отличен от нуля в $\Bbbk(\psi)[x]$.

Поэтому $\psi$ трансцендентен над $\Bbbk$ (иначе $t$ был бы алгебраичен над $\Bbbk$), и поле $\Bbbk(t)$ алгебраично над полем $\Bbbk(\psi)$, причём последнее поле изоморфно полю рациональных функций. Это наблюдение известно как *теорема Люрота*.

## §10. Аффинная алгебраическая геометрия

**10.1. Системы полиномиальных уравнений.** Каждая система полиномиальных уравнений

$$f_\nu(x_1,\dots,x_n)=0\,,\quad f_\nu\in\Bbbk[x_1,\dots,x_n]\,, \tag{10-1}$$

может быть расширена до бесконечной системы уравнений, левые части которых пробегают идеал $J\subset\Bbbk[x_1,\dots,x_n]$, порождённый левыми частями $f_\nu$ системы (10-1). При таком расширении множество решений системы не изменится. Так как кольцо многочленов нётерово[1], идеал $J$ порождается конечным набором многочленов $f_1,\dots,f_m$, которые можно выбрать среди левых частей исходной системы (10-1). Мы заключаем, что любая (в том числе бесконечная) система полиномиальных уравнений равносильна, с одной стороны, некоторой своей конечной подсистеме, а с другой стороны — системе, левые части которой образуют в кольце многочленов идеал. Множество всех решений системы полиномиальных уравнений вида (10-1), левые части которых пробегают идеал $J\subset\Bbbk[x_1,\dots,x_n]$, обозначается

$$V(J)\stackrel{\text{def}}{=}\{a\in\mathbb{A}^n\mid\forall\,f\in J\;f(a)=0\}$$

и называется *аффинным алгебраическим многообразием*, задаваемым идеалом $J$. Это множество вполне может оказаться пустым, что происходит, к примеру, когда идеал $J=(1)=\Bbbk[x_1,\dots,x_n]$ содержит уравнение $1=0$.

Для произвольной фигуры $\Phi\subset\mathbb{A}^n$ множество всех многочленов, тождественно зануляющихся на $\Phi$, образует в кольце многочленов идеал, который обозначается

$$I(\Phi)\stackrel{\text{def}}{=}\{\,f\in\Bbbk[x_1,\dots,x_n]\mid f(p)=0\;\forall\,p\in\Phi\}$$

и называется *идеалом фигуры* $\Phi$. Множество нулей $V(I(\Phi))$ такого идеала — это наименьшее аффинное алгебраическое многообразие, содержащее $\Phi$. Для любого идеала $J\subset\Bbbk[x_1,\dots,x_n]$ имеется тавтологическое включение $J\subset I(V(J))$. Вообще говоря, оно строгое: например, при $n=1$ для идеала $J=(x^2)$ многообразие $V(J)=\{0\}$, тогда как идеал $I(V(J))=(x)\supsetneq(x^2)=J$.

Теорема 10.1 (Nullstellensatz, или теорема Гильберта о нулях)
Над алгебраически замкнутым полем $\Bbbk$ для любого идеала $J\subset\Bbbk[x_1,\dots,x_n]$ имеют место *слабая теорема о нулях*: $V(J)=\varnothing\iff 1\in J$ и *сильная теорема о нулях*:

$$f\in I(V(J))\iff f^m\in J\text{ для некоторого }m\in\mathbb{N}\,.$$

Доказательство. Чтобы доказать первое утверждение, достаточно для каждого собственного[2] идеала $J\subset\Bbbk[x_1,\dots,x_n]$ указать точку $p\in\mathbb{A}^n$, в которой зануляются все многочлены из $J$. Если имеется необратимый по модулю $J$ многочлен $g\notin J$, идеал $J'=(J,g)$ не содержит 1 и строго больше, чем $J$. Так как увеличение идеала $J$ только усложняет нашу задачу, мы можем заменить $J$ на $J'$. В силу нётеровости кольца многочленов конечное число таких расширений приведёт к *максимальному* собственному идеалу $J$, фактор по которому $\Bbbk[x_1,\dots,x_n]/J$ является

[1] См. раздел 5.1.1 на стр. 65 и следствие 5.1 на стр. 66 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_05.pdf.

[2] Т. е. отличного от всего кольца многочленов.

полем. Поскольку это поле конечно порождено как $\Bbbk$-алгебра, каждый его элемент $\vartheta$ алгебраичен[1] над $\Bbbk$, т. е. удовлетворяет уравнению $\mu(\vartheta) = 0$, где $\mu(t) \in \Bbbk[t]$ — неприводимый приведённый многочлен. Так как поле $\Bbbk$ алгебраически замкнуто, многочлен $\mu$ линеен, и $\vartheta \in \Bbbk$. Тем самым, $\Bbbk[x_1, \dots, x_n]/J = \Bbbk$, т. е. любой многочлен $f \in \Bbbk[x_1, \dots, x_n]$ сравним по модулю идеала $J$ с некоторой константой. Пусть переменная $x_i$ сравнима с $p_i \in \Bbbk$. Так как редукция по модулю $J$ является гомоморфизмом, каждый многочлен $f(x_1, \dots, x_n) \equiv f(p_1, \dots, p_n) \pmod J$. Следовательно, все многочлены $f \in J$ зануляются в точке $p = (p_1, \dots, p_n) \in \mathbb{A}^n$.

Для доказательства второго утверждения вложим $\mathbb{A}^n$ в большее пространство $\mathbb{A}^{n+1}$ с координатами $(t, x_1, \dots, x_n)$ в качестве гиперплоскости $t = 0$. Так как многочлен $f(x)$ тождественно обращается в нуль на $V(J) \subset \mathbb{A}^n$, многочлен $g(t, x) = 1 - t\,f(x)$ тождественно равен единице на цилиндре $\mathbb{A}^1 \times V(J) \subset \mathbb{A}^{n+1}$. Поэтому порождённый многочленами из идеала $J \subset \Bbbk[x_1, \dots, x_n] \subset \Bbbk[t, x_1, \dots, x_n]$ и многочленом $g(t, x)$ идеал в $\Bbbk[t, x_1, \dots, x_n]$ имеет пустое множество нулей в $\mathbb{A}^{n+1}$. По слабой теореме о нулях он содержит единицу, т. е. существуют такие $q_0, q_1, \dots, q_s \in \Bbbk[t, x_1, \dots, x_n]$ и $f_1, \dots, f_s \in J$, что

$$q_0(x, t) \cdot \bigl(1 - tf(x)\bigr) + q_1(t, x) \cdot f_1(x) + \dots + q_s(x, t) \cdot f_s(x) = 1\,.$$

Применяя к этому равенству гомоморфизм $\Bbbk[t, x_1, \dots, x_n] \to \Bbbk(x_1, \dots, x_n)$, действующий на переменные по правилам $t \mapsto 1/f(x)$, $x_\nu \mapsto x_\nu$, получаем равенство

$$q_1\bigl(1/f(x), x\bigr) \cdot f_1(x) + \dots + q_s\bigl(1/f(x), x\bigr) \cdot f_s(x) = 1$$

в поле рациональных функций $\Bbbk(x_1, \dots, x_n)$. Умножая обе части на подходящую степень $f^m$ получаем равенство $f^m = \tilde q_1 f_1 + \dots + \tilde q_s f_s$, в котором $\tilde q_\nu \in \Bbbk[x_1, \dots, x_n]$. □

**10.2. Аффинный алгебро-геометрический словарик.** Всюду далее мы по умолчанию считаем, что основное поле $\Bbbk$ алгебраически замкнуто. Аффинные алгебраические многообразия, определённые над полем $\Bbbk$, образуют категорию $\mathcal{A}\!f\!f_{\Bbbk}$, морфизмами в которой являются такие отображения $\varphi : X \to Y$ из аффинного алгебраического многообразия $X \subset \mathbb{A}^n$ в аффинное алгебраическое многообразие $Y \subset \mathbb{A}^m$, которые задаются в координатах формулой

$$x = (x_1, \dots, x_n) \mapsto (\varphi_1(x), \dots, \varphi_m(x))\,, \quad \text{где} \quad \varphi_i(x) \in \Bbbk[x_1, \dots, x_n]\,.$$

Такие отображения называются *регулярными* или *полиномиальными*. Функция $f : X \to \Bbbk$ называется *регулярной*, если она является ограничением на $X$ многочлена $f \in \Bbbk[x_1, \dots, x_n]$. Регулярные функции на $X$ образуют конечно порождённую приведённую[2] $\Bbbk$-алгебру, которая называется *координатной алгеброй* аффинного алгебраического многообразия $X$ и обозначается

$$\Bbbk[X] \overset{\text{def}}{=} \operatorname{Hom}_{\mathcal{A}\!f\!f_{\Bbbk}}(X, \Bbbk) \simeq \Bbbk[x_1, \dots, x_n]/I(X)\,, \qquad (10\text{-}2)$$

где $I(X) = \{f \in \Bbbk[x_1, \dots, x_n] \mid f|_X \equiv 0\}$ — идеал всех зануляющихся на $X$ многочленов.

Лемма 10.1

Всякая конечно порождённая приведённая алгебра $A$ над алгебраически замкнутым полем $\Bbbk$ изоморфна координатной алгебре $A = \Bbbk[X]$ некоторого аффинного алгебраического многообразия $X$.

---

[1]См. теор. 9.2 на стр. 133.

[2]Коммутативная алгебра называется *приведённой*, если в ней нет *нильпотентов* — таких ненулевых элементов $a$, что $a^n = 0$ для некоторого $n \in \mathbb{N}$.

Доказательство. Зададим алгебру $A$ образующими и соотношениями, т. е. представим её в виде фактор алгебры $A = \Bbbk[x_1, \dots, x_n]/I$. Приведённость алгебры $A$ означает, что равенство $f^n \in I$ для $f \in \Bbbk[x_1, \dots, x_n]$ возможно только если $f \in I$. По сильной теореме о нулях это означает, что $I = I(V(I))$ является идеалом аффинного алгебраического многообразия $V(I) \subset \mathbb{A}^n$. □

**10.2.1. Максимальный спектр.** С каждой точкой $p \in X$ аффинного алгебраического многообразия $X$ связан *гомоморфизм вычисления* $\mathrm{ev}_p : \Bbbk[X] \to \Bbbk$, $f \mapsto f(p)$. Он эпиморфен, поскольку переводит единицу, а значит, является гомоморфизмом факторицации по модулю своего ядра

$$\mathfrak{m}_p \stackrel{\text{def}}{=} \ker \mathrm{ev}_p = \{ f \in \Bbbk[X] \mid f(p) = 0 \}, \tag{10-3}$$

которое является максимальным идеалом в $\Bbbk[X]$, так как фактор по нему — поле. Идеал (10-3) называется *максимальным идеалом точки* $p \in X$. Итак,

$$\mathrm{ev}_p : \Bbbk[X] \twoheadrightarrow \frac{\Bbbk[X]}{\mathfrak{m}_p} \simeq \Bbbk, \quad f \mapsto f \,(\mathrm{mod}\, \mathfrak{m}_p) = f(p) \in \Bbbk.$$

Множество всех максимальных идеалов произвольной $\Bbbk$-алгебры $A$ называется её *максимальным спектром* и обозначается $\mathrm{Spec}_{\mathrm{m}}(A)$. Каждой точке $\mathfrak{m} \in \mathrm{Spec}_{\mathrm{m}} A$ отвечает гомоморфизм факторизации $A \twoheadrightarrow A/\mathfrak{m}$, $a \mapsto a \,(\mathrm{mod}\ \mathfrak{m})$, принимающий значения в поле $A/\mathfrak{m} \supset \Bbbk$. Если алгебра $A$ конечно порождена, поле $A/\mathfrak{m}$ тоже конечно порождено $\Bbbk$-алгеброй, а значит, является конечным алгебраическим расширением[1] поля $\Bbbk$. Над алгебраически замкнутым полем $\Bbbk$ это влечёт равенство $A/\mathfrak{m} = \Bbbk$, что позволяет интерпретировать элементы *любой* конечно порождённой алгебры $A$ над алгебраически замкнутым полем как функции $\mathrm{Spec}_{\mathrm{m}} A \to \Bbbk$.

Лемма 10.2

Для любого аффинного алгебраического многообразия $X$ над алгебраически замкнутым полем $\Bbbk$ соответствия $p \mapsto \mathrm{ev}_p \mapsto \mathfrak{m}_p = \ker(\mathrm{ev}_p)$ устанавливают биекции между точками многообразия $X$, гомоморфизмами $\Bbbk[X] \to \Bbbk$, тождественными на $\Bbbk$, и максимальными идеалами алгебры $\Bbbk[X]$.

Доказательство. Биективность второго соответствия мы уже проверили выше[2]. Сопоставление точке $p \in X \subset \mathbb{A}^n$ её максимального идеала $\mathfrak{m}_p = \ker \mathrm{ev}_p$ вкладывает множество точек в множество максимальных идеалов, поскольку для $p \neq q$ всегда[3] можно указать аффинно линейную функцию $f : \mathbb{A}^n \to \Bbbk$ зануляющуюся в $p$ и отличную от нуля в $q$. Чтобы показать, что над алгебраически замкнутым полем $\Bbbk$ любой максимальный идеал $\mathfrak{m} \subset \Bbbk[X]$ имеет вид $\mathfrak{m}_p = \ker \mathrm{ev}_p$ для некоторой точки $p \in X$, рассмотрим полный прообраз $\widetilde{\mathfrak{m}} \subset \Bbbk[x_1, \dots, x_n]$ идеала $\mathfrak{m} \subset \Bbbk[x_1, \dots, x_n]/I(X)$. Так как $\Bbbk[x_1, \dots, x_n]/\widetilde{\mathfrak{m}} = \Bbbk[X]/\mathfrak{m} = \Bbbk$, идеал $\widetilde{\mathfrak{m}}$ является собственным, максимальным и содержит $I(X)$. По слабой теореме о нулях $V(\widetilde{\mathfrak{m}}) \neq \varnothing$, т. е. $\widetilde{\mathfrak{m}} \subset \mathfrak{m}_p$ для некоторой точки $p \in \mathbb{A}^n$. Поскольку $I(X) \subset \widetilde{\mathfrak{m}}$, точка $p \in X$. Так как $\mathfrak{m}$ максимален, включение $\mathfrak{m} \subset \mathfrak{m}_p$ влечёт равенство $\mathfrak{m} = \mathfrak{m}_p$. □

---

[1] См. теор. 9.2 на стр. 133 и сл. 9.2 на стр. 133.

[2] Над алгебраически не замкнутым полем $\Bbbk$ сопоставление $\varphi \mapsto \ker \varphi$ вкладывает множество тождественных на поле $\Bbbk$ гомоморфизмов $\varphi : A \to \Bbbk$ в множество максимальных идеалов алгебры $A$, однако над незамкнутым полем *не все* максимальные идеалы в $A$ являются ядрами гомоморфизмов вычисления со значениями в поле $\Bbbk$: например, ядро гомоморфизма вычисления $\mathrm{ev}_i : \mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(i)$, где $i = \sqrt{-1} \in \mathbb{C}$, является максимальным идеалом $\mathbb{R}$-алгебры $\mathbb{R}[x]$, но его нельзя реализовать как ядро вычисления $\mathbb{R}[x] \to \mathbb{R}$, поскольку $\mathrm{codim}_{\mathbb{R}} \ker \mathrm{ev}_i = 2$.

[3] Даже над не замкнутым полем.

Определение 10.1
Множество нильпотентных элементов[1] $\mathfrak{n}(A) \overset{\text{def}}{=} \{a \in A \mid \exists n \in \mathbb{N} : a^n = 0\}$ произвольного коммутативного кольца $A$ называется *нильрадикалом* этого кольца.

Упражнение 10.1. Убедитесь, что нильрадикал является идеалом в $A$.

Следствие 10.1
Для любой конечно порождённой алгебры $A$ над алгебраически замкнутым полем $\Bbbk$

$$\mathfrak{n}(A) = \bigcap_{\mathfrak{m} \in \operatorname{Spec}_{\mathrm{m}} A} \mathfrak{m}\,.$$

Иначе говоря, $\mathfrak{n}(A)$ — это ядро гомоморфизма из алгебры $A$ в алгебру функций на $\operatorname{Spec}_{\mathrm{m}} A$, сопоставляющего элементу $a \in A$ функцию $a\colon \operatorname{Spec}_{\mathrm{m}} A \to \Bbbk \simeq A/\mathfrak{m}$, $\mathfrak{m} \mapsto a \,(\operatorname{mod} \mathfrak{m})$.

Доказательство. Для любого максимального идеала $\mathfrak{m}$ фактор $A/\mathfrak{m}$ является полем, поэтому класс любого нильпотента в нём равен нулю. Тем самым, нильрадикал лежит в пересечении всех максимальных идеалов. Для доказательства обратного включения рассмотрим приведённую алгебру $A_{\mathrm{red}} \overset{\text{def}}{=} A/\mathfrak{n}(A)$. Достаточно убедиться, что каждый элемент $a \in A_{\mathrm{red}}$, задающий нулевую функцию на $\operatorname{Spec}_{\mathrm{m}} A_{\mathrm{red}} = \operatorname{Spec}_{\mathrm{m}} A$, является нулевым в $A_{\mathrm{red}}$. Но редуцированная алгебра $A_{\mathrm{red}}$ изоморфна координатной алгебре $\Bbbk[X] = \Bbbk[x_1, \dots, x_n]/I(X)$ некоторого аффинного алгебраического многообразия $X \subset \mathbb{A}^n$ и точки $\mathfrak{m} \in \operatorname{Spec}_{\mathrm{m}} A_{\mathrm{red}}$ находятся в биекции с точками многообразия $X$. Если многочлен $f \in \Bbbk[x_1, \dots, x_n]$ задаёт нулевую функцию на $X$, то он лежит в $I(X)$ и задаёт нулевой класс в $\Bbbk[X]$. $\square$

Упражнение 10.2*. Покажите, что нильрадикал произвольного коммутативного кольца совпадает с пересечением всех простых идеалов этого кольца.

**10.2.2. Антиэквивалентность категорий.** Со всяким отображением множеств $\varphi\colon X \to Y$ связан *гомоморфизм поднятия* $\varphi^*\colon \Bbbk^Y \to \Bbbk^X$, $f \mapsto f \circ \varphi$, действующий из алгебры $\Bbbk^Y$ всех функций $Y \to \Bbbk$ в алгебру $\Bbbk^X$ всех функций $X \to \Bbbk$. Если аффинные многообразия $X \subset \mathbb{A}^n$ и $Y \subset \mathbb{A}^m$ имеют координатные алгебры $\Bbbk[X] = \Bbbk[x_1, \dots, x_n]/I(X)$ и $\Bbbk[Y] = \Bbbk[y_1, \dots, y_m]/I(Y)$, а отображение $\varphi\colon X \to Y$ задаётся в координатах формулой $(x_1, \dots, x_n) \mapsto \big(\varphi_1(x), \dots, \varphi_m(x)\big)$, то поднятия $\varphi^*(y_i) = \varphi_i$. Регулярность отображения $\varphi$, по определению означающая, что $\varphi_i(x) \in \Bbbk[x_1, \dots, x_n]$, равносильна включению[2] $\varphi^*(\Bbbk[Y]) \subset \Bbbk[X]$, т. е. тому, что поднятие регулярной функции на $Y$ является регулярной функцией на $X$.

Упражнение 10.3. Проверьте, что теоретико множественное отображение топологических (соотв. гладких или аналитических) многообразий $X \to Y$ является непрерывным (соотв. гладким или аналитическим) если и только если его гомоморфизм поднятия переводит непрерывные (соотв. гладкие или аналитические) функции $Y \to \mathbb{R}$ в непрерывные (соотв. гладкие или аналитические) функции $X \to \mathbb{R}$.

Теорема 10.2
Над алгебраически замкнутым полем $\Bbbk$ контравариантный функтор

$$\mathcal{A\!f\!f}_{\Bbbk} \to \mathcal{A\ell g}_{\Bbbk}^{\mathrm{opp}}\,, \quad X \mapsto \Bbbk[X] = \operatorname{Hom}_{\mathcal{A\!f\!f}_{\Bbbk}}(X, \mathbb{A}^1)\,, \tag{10-4}$$

[1] Вместе с нулевым элементом.

[2] Обратите внимание, что включение $\varphi(X) \subset Y$ гарантирует включение $\varphi^*\big(I(Y)\big) \subset I(X)$, означающее, что правило $y_i \mapsto \varphi_i$ корректно задаёт гомоморфизм фактор алгебр $\Bbbk[Y] = \Bbbk[y_1, \dots, y_m]/I(Y) \to \Bbbk[x_1, \dots, x_n] = \Bbbk[X]$.

переводящий регулярный морфизм $\varphi : X \to Y$ аффинных многообразий в гомоморфизм поднятия $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$, является эквивалентностью категорий.

Доказательство. Согласно предл. 8.1 на стр. 117 достаточно убедиться, что функтор (10-4) посуществу сюрьективен и вполне строг. Первое было установлено в лем. 10.1 на стр. 138. Для доказательства второго рассмотрим функтор

$$\mathcal{A}\ell g_{\Bbbk} \to \mathcal{S}et\,, \quad A \mapsto \operatorname{Spec_m} A = \operatorname{Hom}_{\mathcal{A}\ell g_{\Bbbk}}(A, \Bbbk)\,, \tag{10-5}$$

переводящий гомоморфизм алгебр $\psi : A \to B$ в отображение поднятия

$$\psi^* : \operatorname{Spec_m} B \to \operatorname{Spec_m} A\,,$$

сопоставляющее эпиморфизму $\operatorname{ev} : B \twoheadrightarrow \Bbbk$ с ядром $\mathfrak{m} \in \operatorname{Spec_m} B$ композицию $\psi^*(\operatorname{ev}) = \operatorname{ev} \circ \psi$, которая является эпиморфизмом с ядром $\psi^{-1}(\mathfrak{m}) \in \operatorname{Spec_m} \Bbbk[X]$. Отображения множеств

$$\operatorname{Hom}_{\mathcal{A}ff_{\Bbbk}}(X, Y) \underset{\psi^* \leftarrow\!\shortmid \psi}{\overset{\varphi \mapsto \varphi^*}{\rightleftarrows}} \operatorname{Hom}_{\mathcal{A}\ell g_{\Bbbk}}(\Bbbk[Y], \Bbbk[X])$$

являются взаимно обратными биекциями, т. е. $\varphi^{**} = \varphi$ и $\psi^{**} = \psi$ для любых аффинных многообразий $X \subset \mathbb{A}^n$ и $Y \subset \mathbb{A}^m$ с координатными алгебрами $\Bbbk[X] = \Bbbk[x_1, \dots , x_n] / I(X)$ и $\Bbbk[Y] = \Bbbk[y_1, \dots , y_m] / I(Y)$. В самом деле, если регулярный морфизм $\varphi : X \to Y$ задаётся формулой $(x_1, \dots , x_n) \mapsto \big(\varphi_1(x), \dots , \varphi_m(x)\big)$, где $\varphi_i(x) \in \Bbbk[x_1, \dots , x_n]$, то $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ действует на образующие алгебры $\Bbbk[Y]$ по правилу $y_i \mapsto \varphi_i \pmod{I(X)}$, причём включение $\varphi(X) \subset Y$ гарантирует включение $\varphi^*\big(I(Y)\big) \subset I(X)$, обеспечивающее корректное действие $\varphi^*$ на фактор алгебру $\Bbbk[Y] = \Bbbk[y_1, \dots , y_m] / I(Y)$. Дважды двойственное отображение $\varphi^{**} : \operatorname{Spec_m} \Bbbk[X] \to \operatorname{Spec_m} \Bbbk[Y]$ переводит гомоморфизм вычисления $\operatorname{ev}_p : \Bbbk[X] \to \Bbbk$, $f(x) \mapsto f(p)$, в точке $p = (p_1, \dots , p_n) \in X$, в его композицию с $\varphi^*$. Эта композиция переводит образующую $y_i \in \Bbbk[Y]$ в число $\varphi_i(p)$, т. е. является гомоморфизмом вычисления в точке $\varphi(p)$. Тем самым, $\varphi^{**} = \varphi$. Равенство $\psi^{**} = \psi$ для любого гомоморфизма алгебр $\psi : \Bbbk[Y] \to \Bbbk[X]$ проверяется аналогично. □

Упражнение 10.4. Сделайте эту проверку.

Замечание 10.1. Согласно лем. 10.2 функтор (10-5) почти квазиобратен к функтору (10-4): применяя его к координатной алгебре $A = \Bbbk[X]$, мы получаем *множество* $\operatorname{Spec_m} A$ точек многообразия $X$. Однако на этом множестве имеется много *разных* изоморфных друг другу структур аффинного алгебраического многообразия, если понимать такую структуру как вложение $\varphi : \operatorname{Spec_m} A \hookrightarrow \mathbb{A}^n$ с сюрьективным гомоморфизмом поднятия $\varphi^* : \Bbbk[\mathbb{A}^n] \twoheadrightarrow A$, отождествляющее $\operatorname{Spec_m} A$ с аффинным алгебраическим многообразием $V\left(\ker \varphi^*\right) \subset \mathbb{A}^n$. Фиксация таковой структуры равносильна выбору конкретного задания алгебры $A$ образующими и соотношениями, т. е. фиксации изоморфизма $A \simeq \Bbbk[x_1, \dots , x_n] / I$.

Пример 10.1 (прямая и гипербола)

Так как гомоморфизм $\operatorname{ev} : \Bbbk[t] \to \Bbbk$ однозначно определяется своим значением $\operatorname{ev}(t) = p \in \Bbbk$ на образующей $t$, точки спектра $\operatorname{Spec_m} \Bbbk[t]$ биективно соответствуют точкам $p \in \mathbb{A}^1 = \Bbbk$. Соответственно, максимальные идеалы $\mathfrak{m} \subset \Bbbk[t]$ суть главные идеалы вида $(t - p)$. Аналогично, спектр алгебры полиномов Лорана $\operatorname{Spec_m} \Bbbk[t, t^{-1}]$ находятся в биекции с точками $p \in \mathbb{A}^1 \smallsetminus \{0\} = \Bbbk^*$, поскольку значение $p = \operatorname{ev}(t) = 1/(\operatorname{ev}(t^{-1})$ должно быть обратимым элементом поля $\Bbbk$. Алгебру полиномов Лорана можно задать образующими и соотношениями при помощи изоморфизма $\varphi^* : \Bbbk[t,t^{-1}] \xrightarrow{\sim} \Bbbk[x,y]/(xy-1)$, $t \mapsto x$, $t^{-1} \mapsto y$. Алгебра $\Bbbk[x,y]/(xy-1)$ является координатной алгеброй гиперболы $xy = 1$ в $\mathbb{A}^2$. Отображение поднятия $\varphi : V(xy-1) \to \mathbb{A}^1 \smallsetminus \{0\}$, отвечающее предыдущему гомоморфизму алгебр $\varphi^*$, проектирует гиперболу на координатную ось, биективно отождествляя точки гиперболы с отличными от нуля точками этой оси.

Пример 10.2 (копроизведение многообразий)
Так как алгебра $\Bbbk[X]\times\Bbbk[Y]$ конечно порождена и приведена, она является прямым произведением[1] алгебр $\Bbbk[X]$ и $\Bbbk[Y]$ в категории $\mathcal{Alg}_{\Bbbk}$. Поэтому максимальный спектр $\operatorname{Spec_m}\big(\Bbbk[X]\times\Bbbk[Y]\big) \simeq X \sqcup Y$ является прямым копроизведением[2] $X$ и $Y$ в категории $\mathcal{Aff}_{\Bbbk} \simeq \mathcal{Alg}_{\Bbbk}^{\mathrm{opp}}$. Таким образом, дизъюнктное объединение аффинных алгебраических многообразий $X$ и $Y$ также является аффинным алгебраическим многообразием.

Пример 10.3 (произведение многообразий)
Тензорное произведение $\Bbbk$-алгебр $A \otimes B$ определяется как тензорное произведение векторных пространств над $\Bbbk$. Умножение разложимых тензоров задаётся правилом $(a_1 \otimes b_1)\cdot(a_2 \otimes b_2) = (a_1a_2) \otimes (b_1b_2)$ и по дистрибутивности продолжается на их линейные комбинации.

> Упражнение 10.5. Убедитесь, что такое продолжение корректно и задаёт на $A \otimes B$ структуру коммутативной $\Bbbk$-алгебры с единицей и что эта алгебра является копроизведением алгебр $A$ и $B$ в категории всех[3] коммутативных $\Bbbk$-алгебр с единицами.

Универсальное свойство тензорного произведения задаёт теоретико множественную биекцию $\operatorname{Spec_m}(A)\times\operatorname{Spec_m}(B) \xrightarrow{\sim} \operatorname{Spec_m}(A\otimes B)$, переводящую пару гомоморфизмов вычисления $\mathrm{ev}_p : A \to \Bbbk$, $\mathrm{ev}_q : B \to \Bbbk$ в гомоморфизм $A\otimes B \to \Bbbk$, $a\otimes b \mapsto a(p)b(q)$. Если алгебры $A$ и $B$ конечно порождены, их тензорное произведение порождается конечным множеством всех попарных тензорных произведений образующих алгебр $A$ и $B$. Покажем, что если алгебры $A$ и $B$ приведены, то их тензорное произведение $A \otimes B$ тоже приведено. По сл. 10.1 на стр. 140 достаточно убедиться, что всякий элемент $h \in A \otimes B$, задающий нулевую функцию на $\operatorname{Spec_m}(A \otimes B)$, равен нулю. Запишем $h$ как $\sum f_\nu \otimes g_\nu$, где $g_\nu \in B$ линейно независимы над $\Bbbk$. Если $(\mathrm{ev}_p \otimes \mathrm{ev}_q)h = 0$ для всех $(p,q) \in \operatorname{Spec_m}(A \otimes B)$, то при каждом $p \in \operatorname{Spec_m} A$ линейная комбинация $\sum f_\nu(p)\cdot g_\nu \in B$ является тождественно нулевой функцией на $\operatorname{Spec_m} B$, а значит, равна нулю, так как алгебра $B$ приведена. Поэтому каждое $f_\nu \in A$ является нулевой функцией на $\operatorname{Spec_m} A$. Поскольку $A$ приведена, все $f_\nu = 0$, а с ними и $h = 0$. Мы заключаем, что $\Bbbk[X] \otimes \Bbbk[Y]$ является прямым копроизведением в категории $\mathcal{Alg}_{\Bbbk}$. Поэтому аффинное многообразие $\operatorname{Spec_m}\big(\Bbbk[X] \otimes \Bbbk[Y]\big)$ является прямым произведением $X \times Y$ в категории $\mathcal{Aff}_{\Bbbk}$. Выше мы видели, что как множество оно совпадает с прямым произведением в $\mathcal{Set}$.

**10.3. Топология Зарисского.** На множестве $X = \operatorname{Spec_m} A$ имеется каноническая топология, отражающая алгебраические свойства алгебры $A$. Эта топология называется *топологией Зарисского* и имеет в качестве замкнутых подмножеств алгебраические подмногообразия в $X$, т. е. множества вида $V(I) = \{x \in X \mid f(x) = 0\ \forall f \in I\} = \{\mathfrak{m} \in \operatorname{Spec_m} A \mid I \subset \mathfrak{m}\}$ для всевозможных идеалов $I \subset A$.

> Упражнение 10.6. Убедитесь, что а) $\varnothing = V(1)$ б) $X = V(0)$ в) $\bigcap_\nu V(I_\nu) = V\Big(\sum_\nu I_\nu\Big)$, где $\sum_\nu I_\nu$ означает идеал, образованный всевозможными конечными суммами $\sum_\nu f_\nu$ с $f_\nu \in I_\nu$

[1] В смысле прим. 8.14 на стр. 119.
[2] В смысле прим. 8.15 на стр. 120.
[3] Не обязательно приведённых.

г) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$, где $IJ$ означает идеал, представляющий собою $\Bbbk$-линейную оболочку всевозможных произведений[1] $ab$ с $a \in I$, $b \in J$.

Топология Зарисского имеет чисто алгебраическую природу: окрестности Зарисского отражают скорее отношения делимости, нежели «близости», и многие её свойства довольно далеки от интуитивно привычных свойств метрической топологии. Скажем, топология Зарисского на произведении $X \times Y$ тоньше произведения топологий Зарисского на $X$ и $Y$, поскольку замкнутые подмножества $Z \subset X \times Y$ не исчерпываются произведениями замкнутых подмножеств в $X, Y$. Например, при $X = Y = \mathbb{A}^1$ гипербола $V(xy - 1)$ замкнута в топологии Зарисского на $\mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2$, а отличные от всей плоскости произведения замкнутых подмножеств в $\mathbb{A}^1$ исчерпываются конечными объединениями изолированных точек и прямых, параллельных координатным осям.

Предложение 10.1 (база открытых множеств и компактность)
Каждое открытое подмножество аффинного алгебраического многообразия $X$ является объединением конечного числа *главных* открытых множеств $\mathcal{D}(f) \overset{\text{def}}{=} X \smallsetminus V(f) = \{x \in X \mid f(x) \neq 0\}$, где $f \in \Bbbk[X]$, и *компактно* в том смысле, что в каждое его открытое покрытие содержит конечное подпокрытие.

Доказательство. Пусть $U = X \smallsetminus V(I)$. Так как алгебра $\Bbbk[X]$ нётерова, идеал $I = (f_1, \dots, f_m)$ конечно порождён. Поэтому $V(I) = \bigcap V(f_i)$ и $U = \bigcup \big(X \smallsetminus V(f_i)\big) = \bigcup_\nu \mathcal{D}(f_i)$. Это доказывает первое утверждение. Для доказательства второго заметим, что семейство главных открытых множеств $\mathcal{D}(f_\nu)$ покрывает открытое множество $U$ если и только если общие нули всех функций $f_\nu$ лежат вне $U$, т. е. $V(I) \subset X \smallsetminus U$, где $I$ — идеал, порождённый функциями $f_\nu$. Поскольку $I = (f_1, \dots, f_m)$ для некоего конечного набора функций $f_1, \dots, f_m$, множество $U$ покрывается множествами $\mathcal{D}(f_i)$, на которых отличны от нуля функции из этого набора. □

Предложение 10.2 (непрерывность регулярных морфизмов)
Всякий регулярный морфизм алгебраических многообразий $\varphi : X \to Y$ непрерывен в топологии Зарисского.

Доказательство. Прообраз $\varphi^{-1}\big(V(I)\big)$ замкнутого подмножества $V(I) \subset Y$ состоит из всех таких точек $x \in X$, что $f(\varphi(x)) = 0$ для всех $f \in I$. Тем самым, он является множеством нулей идеала, порождённого в $\Bbbk[X]$ образом $\varphi^*(I)$ идеала $I$ при гомоморфизме поднятия $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$. □

**10.3.1. Неприводимые компоненты.** Топологическое пространство $X$, представимое в виде объединения $X = X_1 \cup X_2$ своих собственных замкнутых подмножеств $X_1, X_2 \subsetneq X$, называется *приводимым*. В обычной метрической топологии практически все пространства приводимы. В топологии Зарисского приводимость многообразия $X$ равносильна наличию делителей нуля в алгебре $\Bbbk[X]$, и неприводимые алгебраические многообразия являются грубыми аналогами степеней простых чисел в арифметике.

Предложение 10.3
Аффинное алгебраическое многообразие неприводимо тогда и только тогда, когда в его координатной алгебре $\Bbbk[X]$ нет делителей нуля.

Доказательство. Разложение $X = X_1 \cup X_2$, где каждое $X_i$ замкнуто, непусто и отлично от $X$, означает наличие таких ненулевых необратимых функций $f_1 \in I(X_1)$, $f_2 \in I(X_2)$, что произведение

[1] Обратите внимание, что последнее равенство равносильно равенству $\sqrt{I \cap J} = \sqrt{IJ}$.

$f_1 f_2$ тождественно зануляется на всём $X$. Последнее означает, что $f_1 f_2 = 0$ в $\Bbbk[X]$. Наоборот, если $f_1 f_2 = 0$ в $\Bbbk[X]$ для ненулевых $f_1, f_2 \in \Bbbk[X]$, то $f_1$ и $f_2$ необратимы в $\Bbbk[X]$, а значит, замкнутые подмножества $V(f_1)$ и $V(f_2)$ непусты и отличны от $X$. При этом $X = V(f_1) \cup V(f_2)$. □

Упражнение 10.7. Убедитесь, что $V(f)$ непусто и отлично от $X$ для всякого ненулевого необратимого многочлена $f \in \Bbbk[X]$.

Следствие 10.2
Аффинная гиперповерхность $\{g(x) = 0\} \subset \mathbb{A}^n$ неприводима тогда и только тогда, когда $g$ является степенью неприводимого многочлена.

Доказательство. Поскольку алгебра $\Bbbk[x_1, \dots , x_n]$ факториальна, радикал $\sqrt{(f)}$ любого главного идеала $(f)$ тоже является главным идеалом, порождённым произведением всех попарно неассоциированных неприводимых делителей многочлена $f$. Алгебра $\Bbbk[V(f)] = \Bbbk[x_1, \dots , x_n]/\sqrt{(f)}$ не имеет делителей нуля если и только если $f$ имеет ровно один неприводимый делитель с точностью до умножения на константы. □

Теорема 10.3
Каждое аффинное алгебраическое многообразие $X$ является конечным объединением

$$X = X_1 \cup \ldots \cup X_k$$

таких неприводимых замкнутых подмножеств $X_i \subset X$, что $X_i \not\subset X_j$ при $i \neq j$, и это разложение единственно с точностью до перестановки его элементов.

Доказательство. Сначала докажем существование разложения. Если $X$ неприводимо, доказывать нечего. Если $X$ приводимо, представим его в виде $X = Z_1 \cup Z_2$, где $Z_{1,2}$ — собственные замкнутые подмножества. Каждую приводимую компоненту этого разложения снова разложим в объединение двух собственных замкнутых подмножеств, и так далее. Если на каком-то шаге получится разложение $X = \bigcup Z_\nu$ в котором все $Z_\nu$ неприводимы, мы выкинем из этого объединения все неприводимые компоненты, которые содержатся в других неприводимых компонентах, и получим требуемое разложение. Если процесс не остановится через конечное число шагов, мы сможем построить бесконечную цепочку строго вложенных замкнутых подмножеств $X \supsetneq Y_1 \supsetneq Y_2 \supsetneq \ldots$, идеалы которых $(0) \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$ образуют бесконечную возрастающую цепочку, противоречащую нётеровости алгебры $\Bbbk[X]$.

Единственность доказывается индукцией по $k$. При $k = 1$ многообразие $X$ неприводимо и является единственной своей неприводимой компонентой. Пусть $X$ раскладывается в объединение $k \geqslant 2$ неприводимых компонент и для всех многообразий, раскладывающихся на меньшее число компонент, разложение в объединение неприводимых компонент единственно. Если неприводимое замкнутое подмножество $Y \subset X$ лежит в объединении замкнутых подмножеств $Z_1 \cup Z_2$, то $Y = (Y \cap Z_1) \cup (Y \cap Z_2)$, а значит, $Y \subset Z_1$ или $Y \subset Z_2$. Поэтому равенство двух разложений на неприводимые компоненты $X_1 \cup \ldots \cup X_k = Y_1 \cup \ldots \cup Y_m$ влечёт включение $X_1 \subset Y_\alpha \subset X_\beta$ для некоторых $\alpha, \beta$, что означает равенство $X_1 = Y_\alpha = X_\beta$. Выкинем из обоих разложений компоненты $X_1$ и $Y_\alpha$ и применим предположение индукции к объединению замыканий оставшихся компонент. □

Упражнение 10.8. Пусть $Z \subsetneq Y \subset X$ замкнуты и $Y$ неприводимо. Убедитесь, что $Y = \overline{Y \smallsetminus Z}$, где замыкание берётся в $X$, и что неприводимость $Y$ для этого существенна.

Определение 10.2
Неприводимые замкнутые подмножества $X_i \subset X$ из теор. 10.3, называются *неприводимыми компонентами* многообразия $X$.

Следствие 10.3
Элемент $f \in \Bbbk[X]$ является ненулевым делителем нуля если и только если он обращается в нуль на некоторой неприводимой компоненте многообразия $X$, но не на всём $X$.

Пример 10.4 («большие» открытые множества)
Топология Зарисского нехаусдорфова. Если $X$ неприводимо, любые два непустых открытых подмножества $U_1, U_2 \subset X$ имеют непустое пересечение, поскольку в противном случае возникает разложение $X = (X \smallsetminus U_1) \cup (X \smallsetminus U_2)$. Иначе говоря, каждое непустое открытое подмножество неприводимого многообразия всюду плотно в нём.

Упражнение 10.9. Пусть $X$ неприводимо и $f, g \in \Bbbk[X]$. Докажите, что если $f|_U = g|_U$ для некоторого непустого открытого $U \subset X$, то $f = g$ в $\Bbbk[X]$.

**10.4. Рациональные функции.** Элементы из $\Bbbk[X]$, не являющиеся делителями нуля, образуют *мультипликативную систему*[1] $S_X \subset \Bbbk[X]$. Кольцо частных[2] $\Bbbk[X]S_X^{-1}$ называется *кольцом рациональных функций* на $X$ и обозначается $\Bbbk(X)$. Если $X$ неприводимо, то $\Bbbk(X) = Q_{\Bbbk[X]}$ — это поле частных целостного кольца $\Bbbk[X]$. Скажем, что рациональная функция $f \in \Bbbk(X)$ *определена* в точке $x \in X$, если существует такое её представление дробью $f = p/q$, где $p, q \in \Bbbk[X]$ и $q$ не делит нуль, что $q(x) \neq 0$. Число $f(x) = p(x)/q(x) \in \Bbbk$ называется *значением* $f$ в точке $x$.

Упражнение 10.10. Убедитесь, что $f(x)$ не зависит от способа записи $f$ в виде дроби $f = p/q$, где $p, q \in \Bbbk[X]$, $q$ не делит нуль, и $q(x) \neq 0$.

Множество точек $x$, в которых определена рациональная функция $f$, называется *областью определения* функции $f$ и обозначается $\mathrm{Dom}(f)$. Из сл. 10.3 и прим. 10.4 вытекает, что $\mathrm{Dom}(f)$ является плотным открытым подмножеством в $X$.

Упражнение 10.11. Убедитесь, что для совпадения двух рациональных функций как элементов кольца $\Bbbk(X)$ достаточно поточечного совпадения их значений на каком-нибудь плотном открытом подмножестве в $X$.

Для открытого $U \subset X$ положим $\Bbbk[U] \stackrel{\text{def}}{=} \{f \in \Bbbk(X) \mid \mathrm{Dom}(f) \supset U\}$ и будем называть его кольцом *рациональных функций, регулярных в* $U$.

Предложение 10.4
Если $h \in \Bbbk[X]$ не делит нуля, то $\Bbbk\big[\mathcal{D}(h)\big] = \Bbbk[X][h^{-1}]$ является кольцом частных $\Bbbk[X]$ со знаменателями из мультипликативной системы $\{h^k\}_{k \geqslant 0}$.

[1] Напомню, что подмножество $S$ в коммутативном кольце $A$ с единицей называется *мультипликативной системой*, если $1 \in S$ и $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$, см. раздел 4.1 на стр. 52 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_04.pdf.

[2] Напомню, что кольцом частных $AS^{-1}$ со знаменателями из мультипликативной системы $S$ коммутативного кольца $A$ с единицей (или *локализацией* $A$ относительно $S$) называется фактор декартова произведения $A \times S$, элементы которого принято обозначать $a/s$ и называть *дробями*, по наименьшему отношению эквивалентности, содержащему равенства $a/s = (at)/(st)$ со всевозможными $a \in A$ и $s, t \in S$ (если Вы впервые с этим сталкиваетесь, то Вам следует убедиться, что $a_1/s_1 = a_2/s_2$ тогда и только тогда, когда $t(a_1 s_2 - a_2 s_1) = 0$ для некоторого $t \in S$, и что обычные правила сложения и умножения дробей задают на $AS^{-1}$ структуру коммутативного кольца), см. там же.

Доказательство. Для рациональной функции $f \in \Bbbk(X)$ положим

$$\left(f^{-1}\right) \overset{\text{def}}{=} \{g \in \Bbbk[X] \mid gf \in \Bbbk[X]\}\,. \tag{10-6}$$

Это идеал в $\Bbbk[X]$, и лежащие в нём неделители нуля суть все возможные знаменатели, встречающиеся в разнообразных представлениях $f$ в виде дроби. Множество делителей нуля в $(f^{-1})$ представляет собою пересечение этого идеала с объединением идеалов $I(X_i)$ неприводимых компонент $X_i$ многообразия $X$. Так как неделители нуля в $(f^{-1})$ по определению имеются, каждое пересечение $(f^{-1}) \cap I(X_i) \subsetneq (f^{-1})$ является собственным векторным подпространством в $(f^{-1})$, и весь идеал $(f^{-1})$ является объединением этих подпространств и подпространства, порождённого неделителями нуля. Если последнее подпространство тоже собственное, пространство $(f^{-1})$ оказалось бы объединением конечного набора собственных подпространств, что невозможно над бесконечным полем[1].

Упражнение 10.12. Убедитесь в этом.

Мы заключаем, что неделители нуля линейно порождают $(f^{-1})$ как векторное пространство над $\Bbbk$, и $X \smallsetminus \mathrm{Dom}(f) = V((f^{-1}))$. Включение $\mathcal{D}(h) \subset \mathrm{Dom}(f)$ означает, что $V(h) \supset V((f^{-1}))$, т. е. функция $h$ зануляется на $V((f^{-1}))$. По теореме Гильберта о нулях $h^d \in (f^{-1})$ для некоторого $d \in \mathbb{N}$. Тем самым, $f = p/h^d$, где $p \in \Bbbk[X]$. □

**10.4.1. Аффинность главных открытых множеств.** Если $h \in \Bbbk[X]$ не делит нуль, то главное открытое подмножество $\mathcal{D}(h) = \mathrm{Spec_m}\,\Bbbk[X][h^{-1}] = \mathrm{Spec_m}\,\Bbbk[X][t]/(1-ht)$ всюду плотно в $X$ и является аффинным алгебраическим многообразием: например, его можно реализовать замкнутой гиперповерхностью $V(1-ht) \subset X \times \mathbb{A}^1$. Вложение $i: \mathcal{D} \hookrightarrow X$ является регулярным морфизмом аффинных многообразий: его гомоморфизм подъёма задаёт каноническое вложение $i^*: \Bbbk[X] \hookrightarrow \Bbbk[X][h^{-1}] \simeq \Bbbk[\mathcal{D}(h)]$ и продолжается до изоморфизма колец частных $i^*: \Bbbk(X) \xrightarrow{\sim} \Bbbk\big(\mathcal{D}(h)\big)$.

Замечание 10.2. Два *разных* толкования обозначения $\Bbbk[\mathcal{D}(h)]$ — как координатной алгебры аффинного алгебраического многообразия $\mathcal{D}(h)$ и как алгебры рациональных функций, регулярных на открытом множестве $\mathcal{D}(h) \subset X$, — *согласованы* друг с другом. В частности, согласованы друг с другом и два разных толкования обозначения $\Bbbk[X]$ — как координатной алгебры аффинного многообразия $X$ и как алгебры рациональных функций, регулярных всюду на $X$, т. е. $\Bbbk[x_1,\dots,x_n]/I(X) = \{f \in \Bbbk(X) \mid \mathrm{Dom}(f) = X\}$. Это вытекает из предл. 10.4 при $h = 1$, что отвечает несобственному главному открытому множеству $\mathcal{D}(h) = X$.

Предостережение 10.1. Неглавное открытое подмножество $U \subset X$, вообще говоря, *не является* аффинным подмногообразием: каноническое вложение $U \hookrightarrow \mathrm{Spec_m}\,\Bbbk[U]$, сопоставляющее точке $u \in U$ её максимальный идеал $\mathfrak{m}_u = \ker \mathrm{ev}_u \subset \Bbbk[U]$, может быть не биективно.

Упражнение 10.13. Пусть $n \geqslant 2$ и $U = \mathbb{A}^n \smallsetminus O$ — дополнение к началу координат в аффинном пространстве. Покажите, что $\Bbbk[U] = \Bbbk[\mathbb{A}^n]$ и, тем самым, $\mathrm{Spec_m}\,\Bbbk[U] = \mathbb{A}^n \neq U$.

Предложение 10.5

Пусть разложение аффинного алгебраического многообразия $X$ на неприводимые компоненты имеет вид $X = X_1 \cup \ldots \cup X_k$. Тогда $\Bbbk(X) = \Bbbk(X_1) \times \ldots \times \Bbbk(X_k)$.

[1] А алгебраически замкнутое поле бесконечно.

Доказательство. Объединение $Z = \bigcup_{i\neq j}(X_i \cap X_j)$ попарных пересечений неприводимых компонент замкнуто в $X$. Выберем в его идеале $I(Z) \subset \Bbbk[X]$ какую-нибудь ненулевую функцию $f \in I(Z)$, не делящую нуль в $\Bbbk[X]$.

Упражнение 10.14. Убедитесь, что $I(Z)$ линейно порождается такими функциями как векторное пространство над $\Bbbk$.

Главное открытое подмножество $W = \mathcal{D}(f) = \operatorname{Spec_m} \Bbbk[X][f^{-1}] \subset X$ аффинно и является дизъюнктным объединением подмножеств $W_i = W \cap X_i \subset X_i$. Каждое $W_i$ является главным открытым подмножеством многообразия $X_i$ и тоже аффинно: $W_i = \mathcal{D}(f_i) = \operatorname{Spec_m} \Bbbk[X_i][f_i^{-1}] \subset X_i$, где $f_i = f \pmod{I(X_i)} \in \Bbbk[X_i]$. Согласно прим. 10.2 $\Bbbk[W] \simeq \Bbbk[W_1] \times \dots \times \Bbbk[W_k]$.

Упражнение 10.15. Проверьте, что кольцо частных прямого произведения коммутативных колец с единицами изоморфно прямому произведению колец частных сомножителей:

$$(K_1 \times \ldots \times K_k)S^{-1}_{K_1\times\ldots\times K_k} \simeq K_1 S^{-1}_{K_1} \times \ldots \times K_k S^{-1}_{K_k}\,.$$

Таким образом, $\Bbbk(X) \simeq \Bbbk(W) \simeq \prod \Bbbk(W_i) \simeq \prod \Bbbk(X_i)$. $\square$

**10.5. Геометрические свойства гомоморфизмов алгебр.** Всякий гомоморфизм $\Bbbk$-алгебр

$$\varphi^* : \Bbbk[Y] \to \Bbbk[X]$$

канонически разлагается в композицию эпиморфизма и вложения:

$$\Bbbk[Y] \xrightarrow{\varphi_1^*} \Bbbk[Y]/\ker(\varphi^*) = \operatorname{im}(\varphi^*) \xhookrightarrow{\varphi_2^*} \Bbbk[X]\,. \tag{10-7}$$

Поскольку алгебра $\Bbbk[Y]$ конечно порождена, а алгебра $\Bbbk[X]$ приведена, алгебра

$$\Bbbk[Y]/\ker(\varphi^*) = \operatorname{im}(\varphi^*) \subset \Bbbk[X]$$

тоже конечно порождена и приведена. Она является координатной алгеброй аффинного алгебраического многообразия $Z = \operatorname{Spec_m}\left(\operatorname{im}(\varphi^*)\right) \simeq V\left(\ker(\varphi^*)\right) \subset Y$. Инъективность гомоморфизма $\varphi_1^* : \Bbbk[Z] \to \Bbbk[X]$ означает отсутствие ненулевых функций $f \in \Bbbk[Z]$, зануляющихся на $\varphi_1(X) \subset Z$, т. е. *всюду плотность* образа $\varphi_1(X)$ в многообразии $Z$. Тем самым, $Z = \overline{\varphi(X)} \subset Y$ есть замыкание образа $\varphi(X)$ в многообразии $Y$, вложенное в $Y$ как замкнутое подмножество $V(\ker\varphi^*)$ нулей идеала $\ker\varphi^*$. Иначе говоря, алгебраическое разложение (10-7) на геометрическом языке означает разложение регулярного морфизма многообразий $\varphi : X \to Y$ в композицию регулярного морфизма $\varphi_1 : X \to Z$ с плотным образом и регулярного вложения $\varphi_2 : Z \hookrightarrow Y$ в качестве замкнутого подмногообразия.

**10.5.1. Замкнутые вложения.** Морфизм $\varphi : X \to Y$ называется *замкнутым вложением*, если его гомоморфизм поднятия $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ сюрьективен. Это означает, что $\varphi$ является изоморфизмом между $X$ и замкнутым подмногообразием $V(\ker\varphi^*) \subset Y$. Если замкнутое подмножество $Z \subset X$ неприводимо, гомоморфизм поднятия $i^* : \Bbbk[X] \twoheadrightarrow \Bbbk[Z]$, отвечающий замкнутому вложению $i : Z \hookrightarrow X$, принимает значения в целостном кольце $\Bbbk[Z]$, которое канонически вложено в своё поле частных $\Bbbk(Z)$. По универсальному свойству кольца частных[1] эпиморфизм $i^*$

[1]См. теорему 4.1 на стр. 53 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_04.pdf.

однозначно продолжается до эпиморфизма $\mathrm{ev}_Z : \Bbbk(X) \twoheadrightarrow \Bbbk(Z)$, который ограничивает рациональные функции с $X$ на $Z$ и может интуитивно восприниматься как гомоморфизм вычисления рациональных функций на $X$ в «в общей точке» неприводимого подмногообразия $Z \subset X$, где вычисляемая функция всегда определена, а результат такого вычисления лежит в поле $\Bbbk(Z)$.

В частности, когда $Z \subset X$ является неприводимой компонентой приводимого аффинного многообразия $X$, из сюрьективности гомоморфизма $\mathrm{ev}_Z : \Bbbk(X) \twoheadrightarrow \Bbbk(Z)$ вытекает, что всякая рациональная функция на $Z$ является ограничением некоторой рациональной функции на $X$, т. е. записывается дробью вида $p/q$, знаменатель которой $q \pmod{I(X_i)} \in \Bbbk[X_i] = \Bbbk[X]/I(X_i)$ представляется не делящим нуль в $\Bbbk[X]$ элементом $q \in \Bbbk[X]$.

Упражнение 10.16. Укажите такого представителя для функции $1/x \in \Bbbk\big(\mathrm{Spec_m}\,\Bbbk[x]\big)$ на прямой $Z = \mathrm{Spec_m}\,\Bbbk[x] = V(y)$ координатного креста $X = \mathrm{Spec_m}\,\Bbbk[x,y]/(xy)$ на плоскости $\mathbb{A}^2 = \mathrm{Spec_m}\,\Bbbk[x,y]$.

**10.5.2. Доминантные морфизмы.** Регулярный морфизм $\varphi : X \to Y$ неприводимого многообразия $X$ называется *доминантным*, если гомоморфизм алгебр $\varphi^* : \Bbbk[Y] \to \Bbbk[X]$ инъективен. Как мы уже видели выше, инъективность гомоморфизма поднятия означает, что $\overline{\varphi(X)} = Y$. Если $X$ приводимо, то морфизм $\varphi : X \to Y$ называется *доминантным*, если доминантно его ограничение на *каждую* неприводимую компоненту многообразия $X$. В этом случае каждое из ограничений $\varphi_i = \varphi|_{X_i}$ задаёт вложение $\varphi_i^* : \Bbbk[Y] \hookrightarrow \Bbbk[X_i] \subset \Bbbk(X_i)$ координатной алгебры многообразия $Y$ в *поле* рациональных функций на $X_i$. По универсальному свойству кольца частных такое вложение однозначно продолжается до вложения $\Bbbk(Y) \hookrightarrow \Bbbk(X_i)$ кольца рациональных функций на $Y$. Поэтому каждый доминантный морфизм $X \to Y$ задаёт вложение $\Bbbk(Y) \hookrightarrow \prod \Bbbk(X_i) = \Bbbk(X)$.

Упражнение 10.17. Покажите, что любой доминантный морфизм неприводимых аффинных многообразий $\varphi : X \to Y$ является композицией некоторого (не единственного) замкнутого вложения $\psi : X \hookrightarrow Y \times \mathbb{A}^m$ и проекции $\pi : Y \times \mathbb{A}^m \twoheadrightarrow Y$ вдоль $\mathbb{A}^m$.

**10.5.3. Конечные морфизмы.** Морфизм $\varphi : X \to Y$ называется *конечным*, если алгебра $\Bbbk[X]$ цела над подалгеброй $\varphi^*(k[Y]) \subset \Bbbk[X]$. Это означает, что $\Bbbk[X]$ линейно порождается над $\varphi^*(k[Y])$ конечным набором функций $f_1, \dots , f_m$, т. е. любая функция $h \in \Bbbk[X]$ может быть записана как $h = \sum \varphi^*(g_i)\, f_i$ с подходящими $g_i \in \Bbbk[Y]$.

Лемма 10.3

Любой конечный морфизм $\varphi : X \to Y$ аффинных алгебраических многообразий переводит каждое замкнутое подмножество $Z \subset X$ в замкнутое подмножество $\varphi(Z) \subset Y$, причём индуцированный морфизм $\varphi|_Z : Z \to \varphi(Z)$ тоже конечен. Если $X$ неприводимо и $Z \neq X$, то $\varphi(Z) \neq Y$.

Доказательство. обозначим через $I = I(Z) \subset \Bbbk[X]$ идеал замкнутого подмножества $Z \subset X$. Ограничение $\varphi|_Z : Z \to Y$ отвечает сквозному гомоморфизму алгебр $f_Z^* : \Bbbk[Y] \xrightarrow{\varphi^*} \Bbbk[X] \to \Bbbk[X]/I$. Поскольку алгебра $\Bbbk[X]$ конечно порождена как $\varphi^*(\Bbbk[Y])$-модуль, алгебра $\Bbbk[Z] = \Bbbk[X]/I$ тоже конечно порождена как модуль над $\varphi|_Z^*(\Bbbk[Y]) = \varphi^*(\Bbbk[Y])/(I \cap \varphi^*(\Bbbk[Y]))$. Тем самым, морфизм $f|_Z : Z \to Y$ конечен. Индуцированный морфизм $f|_Z : Z \to \overline{\varphi(Z)}$ тоже конечен, поскольку $\Bbbk[\overline{\varphi(Z)}] = \varphi^*(\Bbbk[Y])$. Поэтому при доказательстве первого утверждения можно считать, что $Z = X$ и $Y = \overline{\varphi(X)}$. Так как равенство $\varphi(X) = \overline{\varphi(X)}$ достаточно проверить отдельно для каждой неприводимой компоненты многообразия $X$, мы можем считать $X$ неприводимым. Таким образом, достаточно доказать, что каждый конечный доминантный морфизм $\varphi : X \to Y$ из неприводимого аффинного многообразия $X$ сюрьективен. На алгебраическом языке это означает, что если в расширении алгебр $\Bbbk[Y] \subset \Bbbk[X]$ большая алгебра не имеет делителей нуля и линейно порождается над меньшей конечным набором элементов $f_1, \dots, f_m$, то каждый максимальный идеал $\mathfrak{m} \subset \Bbbk[Y]$ имеет вид $\widetilde{\mathfrak{m}} \cap \Bbbk[Y]$ для некоторого максимального идеала $\widetilde{\mathfrak{m}} \subset \Bbbk[X]$. Если идеал $\mathfrak{m}\,\Bbbk[X]$, порождённый $\mathfrak{m}$ в $\Bbbk[X]$, является собственным в $\Bbbk[X]$, то в качестве $\widetilde{\mathfrak{m}}$ можно взять любой максимальный идеал, содержащий $\mathfrak{m}\,\Bbbk[X]$. Таким образом, достаточно показать, что $\mathfrak{m}\,\Bbbk[X] \neq \Bbbk[X]$ ни для какого максимального идеала $\mathfrak{m} \subset \Bbbk[Y]$. Предположим противное: пусть $\mathfrak{m}\,\Bbbk[X] = \Bbbk[X]$. Тогда каждая из образующих $f_i$, линейно порождающих $\Bbbk[X]$ над $\Bbbk[Y]$, запишется в виде $f_i = \sum_\nu f_\nu \beta_{\nu i}$ с $\beta_{\nu i} \in \mathfrak{m}$. Мы получаем матричное равенство

$$(f_1, \dots, f_m)\,(E - B) = 0\,,$$

где $B = \left(\beta_{\nu i}\right) \in \mathrm{Mat}_{m\times m}(\mathfrak{m})$, а $E$ — единичная матрица. Следовательно[1]

$$(f_1, \dots, f_m) \cdot \det(E - B) = (f_1, \dots, f_m)\,(E - B)(E - B)^\vee = 0\,.$$

Так как в $\Bbbk[Z]$ нет делителей нуля, $\det(E - B) = 0$. Раскрывая этот определитель, заключаем, что $1 \in \mathfrak{m}$, т. е. идеал $\mathfrak{m} = \Bbbk[Y]$ не является собственным.

Чтобы доказать, что $\varphi(Z) \neq Y$ при $Z \subsetneq X$ рассмотрим какую-нибудь ненулевую функцию $f \in \Bbbk[X]$, тождественно зануляющуюся на $Z$. Поскольку она цела над $\varphi^*(\Bbbk[Y])$

$$f^m + \varphi^*(g_1)\,f^{m-1} + \ldots + \varphi^*(g_{m-1})\,f + \varphi^*(g_m) = 0$$

для некоторых $g_1, \dots, g_m \in \Bbbk[Y]$. Рассмотрим такое соотношение с наименьшим возможным $m$. В нём $g_m \neq 0$, иначе его можно было бы сократить на $f$, ибо в $\Bbbk[X]$ нет делителей нуля. Вычисляя левую часть в точках $z \in Z$, видим, что $\varphi^*(g_m)|_Z = g_m|_{\varphi(Z)} \equiv 0$. Поэтому $\varphi(Z) \subset V(g_m) \subsetneq Y$ является собственным замкнутым подмножеством. □

**10.5.4. Нормальные многообразия.** Аффинное алгебраическое многообразие $Y$ называется *нормальным*, если оно неприводимо и его координатная алгебра $\Bbbk[Y]$ целозамкнута в поле рациональных функций $\Bbbk(Y) = Q_{\Bbbk[Y]}$, т. е. является *нормальным кольцом* в смысле опр. 9.2. Например, любое аффинное многообразие с факториальной координатной алгеброй нормально. В частности, все аффинные пространства $\mathbb{A}^n$ нормальны[2].

Лемма 10.4

Всякий сюрьективный конечный морфизм $\varphi : X \to Y$ в нормальное многообразие $Y$ открыт[3] и сюрьективно отображает каждую неприводимую компоненту $X$ на $Y$.

Доказательство. Вложение $\varphi^* : \Bbbk[Y] \hookrightarrow \Bbbk[X]$ позволяет рассматривать $\Bbbk[Y]$ как подалгебру в $\Bbbk[X]$. Открытость морфизма $\varphi$ означает, что образ каждого главного открытого множества из $X$ содержит вместе с каждой точкой какую-нибудь её главную открытую окрестность в $Y$, т. е. для любой функции $f \in \Bbbk[X]$ и каждой точки $p \in X$, в которой $f(p) \neq 0$, мы должны указать такую функцию $a \in \Bbbk[Y]$, что $\varphi(p) \in \mathcal{D}(a) \subset \varphi(\mathcal{D}(f))$. Для этого рассмотрим отображение

$$\psi = \varphi \times f : X \to Y \times \mathbb{A}^1\,, \quad p \mapsto \big(\varphi(p), f(p)\big)\,.$$

Его гомоморфизм поднятия $\psi^* : \Bbbk[Y \times \mathbb{A}^1] = \Bbbk[Y][t] \to k[X]$ вычисляет полиномы от $t$ с коэффициентами в $\Bbbk[Y]$ на элементе $f \in \Bbbk[X]$. По сл. 9.5 минимальный многочлен $\mu_f$ элемента $f$ над

[1] Ср. с доказательством лем. 9.1 на стр. 128.

[2] Включая точку $\mathbb{A}^0 = \mathrm{Spec}_{\mathrm{m}}\,\Bbbk$.

[3] Т. е. $\varphi(U)$ открыто в $Y$ для любого открытого $U \subset X$.

полем $\Bbbk(Y)$ лежит в $\Bbbk[Y]$. Поэтому гомоморфизм $\psi^*$ представляет собою факторизацию по главному идеалу $(\mu_f) = \ker\psi^*$. Мы заключаем, что морфизм $\psi$ конечен и сюрьективно отображает $X$ на гиперповерхность, заданную в $Y\times\mathbb{A}^1$ уравнением $\mu_f(y;t) = t^m + a_1(y)\,t^{m-1} + \dots + a_m(y) = 0$, а морфизм $\varphi$ является композицией $\psi$ и проекции $Y\times\mathbb{A}^1 \twoheadrightarrow Y$. Образ $\varphi(\mathcal{D}(f)) \subset Y$ состоит из всех таких точек $y \in Y$, что у многочлена $\mu_f(y;t) \in \Bbbk[t]$ есть ненулевой корень. Поскольку над точкой $\varphi(p) \in Y$ многочлен $\mu_f(\varphi(p);t) \in \Bbbk[t]$ имеет ненулевой корень $t = f(p)$, хоть один из коэффициентов, пусть это будет $a_i$, отличен от нуля в точке $\varphi(p)$. Над всеми точками $q \in \mathcal{D}(a_i) \subset Y$ коэффициент $a_i(q)$ тоже отличен от нуля, а значит, у многочлена $\mu_f(q;t) \in \Bbbk[t]$ также есть ненулевой корень. Поэтому все эти точки $q$ лежат в образе множества $\mathcal{D}(f)$, т. е. $\varphi(p) \in \mathcal{D}(a_i) \subset \varphi(\mathcal{D}(f))$, как и требовалось.

Что касается ограничения $\varphi$ на неприводимые компоненты $X_i \subset X$, то для каждого $i$ множество $U_i = X \smallsetminus \bigcup_{\nu\neq i} X_\nu = X_i \smallsetminus \bigcup_{\nu\neq i}(X_i \cap X_\nu)$ открыто в $X$ и плотно в $X_i$. Поскольку $\varphi(U_i)$ открыто, а $Y$ неприводимо, $\varphi(U_i)$ плотно в $Y$, откуда $\varphi(X_i) = \overline{\varphi(U_i)} = Y$. $\square$

## §11. Алгебраические многообразия

Всюду в этом параграфе мы по умолчанию считаем основное поле $\Bbbk$ алгебраически замкнутым.

**11.1. Определения и примеры.** В дифференциальной геометрии и топологии многообразия определяются как топологические пространства, в которых каждая точка обладает открытой окрестностью, гомеоморфной некой стандартной модели — «локальной карте», и любые две такие карты должны быть регулярно согласованы на их пересечении. Алгебраические многообразия определяются аналогичным образом, только в качестве стандартных локальных карт допускаются произвольные[1] аффинные алгебраические многообразия, а регулярность согласования двух таких карт на их пересечении означает, что переход от одной карты к другой задаётся рациональными функциями. Точные определения таковы. Алгебраической аффинной картой на топологическом пространстве $X$ называется гомеоморфизм $\varphi_U : X_U \xrightarrow{\sim} U$, где $X_U$ — аффинное алгебраическое многообразие, рассматриваемое с топологией Зарисского, а $U \subset X$ — открытое подмножество, рассматриваемое с индуцированной из $X$ топологией. Две алгебраических аффинных карты $\varphi_U : X_U \xrightarrow{\sim} U$ и $\varphi_W : X_W \xrightarrow{\sim} W$ на $X$ называются *совместимыми*, если *гомеоморфизм склейки* $\varphi_{WU} \stackrel{\text{def}}{=} \varphi_W^{-1} \circ \varphi_U\big|_{\varphi_U^{-1}(U\cap W)} : \varphi_U^{-1}(U \cap W) \xrightarrow{\sim} \varphi_W^{-1}(U \cap W)$, который отождествляет между собою лежащие в аффинных алгебраических многообразиях $X_U$ и $X_W$ прообразы пересечения $U \cap W$, регулярен в том смысле, что его гомоморфизм поднятия

$$\varphi_{WU}^* : \Bbbk\left[\varphi_W^{-1}(U \cap W)\right] \xrightarrow{\sim} \Bbbk\left[\varphi_U^{-1}(U \cap W)\right] , \quad f \mapsto f \circ \varphi_{WU} ,$$

является изоморфизмом алгебры регулярных на $\varphi_U^{-1}(U\cap W)$ рациональных функций на $X_U$ с алгеброй регулярных на $\varphi_W^{-1}(U\cap W)$ рациональных функций на $X_W$. Открытое покрытие $X = \bigcup U_\nu$ попарно совместимыми алгебраическими картами называется *алгебраическим атласом* на $X$. Два алгебраических атласа называются *эквивалентными*, если их объединение также представляет собой алгебраический атлас. Топологическое пространство $X$, с зафиксированным на нём классом эквивалентных алгебраических атласов называется *алгебраическим многообразием*. Алгебраические многообразия, обладающие конечным атласом, называются многообразиями *конечного типа*.

Пример 11.1 (проективные пространства)
Проективное пространство $\mathbb{P}_n = \mathbb{P}\left(\Bbbk^{n+1}\right)$ с однородными координатами $(x_0 : x_1 : \ldots : x_n)$ обладает алгебраическим атласом из $n+1$ стандартных аффинных карт

$$U_i = \{(x_0 : x_1 : \ldots : x_n) \mid x_i \neq 0\} , \quad 0 \leqslant i \leqslant n .$$

Обозначим через $X_i \simeq \mathbb{A}^n$ аффинное пространство, координаты в котором будем записывать как[2] $t_i = (t_{i,0}, \ldots, t_{i,i-1}, t_{i,i+1}, \ldots, t_{i,n})$. Отображение

$$\varphi_i : X_i \xrightarrow{\sim} U_i , \quad t_i \mapsto (t_{i,0} : \ldots : t_{i,i-1} : 1 : t_{i,i+1} : \ldots : t_{i,n}) , \tag{11-1}$$

биективно, и прообраз $\varphi_i^{-1}(U_i \cap U_j) \subset X_i$ представляет собою главное открытое множество

$$\mathcal{D}(t_{i,j}) = \operatorname{Spec_m} \Bbbk[t_{i,j}^{-1}, t_{i,0}, \ldots, t_{i,i-1}, t_{i,i+1}, \ldots, t_{i,n}] .$$

[1] В том числе не гладкие — такие, как крест $\operatorname{Spec_m}(\Bbbk[x, y]/(xy))$.

[2] Первый индекс $i$ является номером карты, а сами координаты $t_{i,\nu}$ в $i$-той карте нумеруются вторым индексом $\nu \neq i$, $0 \leqslant \nu \leqslant n$.

Отображение склейки $\varphi_{ji} = \varphi_j^{-1}\varphi_i : \mathcal{D}(t_{i,j}) \xrightarrow{\sim} \mathcal{D}(t_{j,i})$ действует по формуле $t_i \mapsto t_{i,j}^{-1} \cdot t_j$ и является изоморфизмом аффинных алгебраических многообразий.

Упражнение 11.1. Убедитесь в этом.

Поэтому перенос топологии Зарисского с $X_i \simeq \mathbb{A}^n$ на $U_i$ посредством биекции (11-1) задаёт на пересечениях $U_i \cap U_j$ согласованные индуцированные топологии и корректно наделяет $\mathbb{P}_n$ топологией, в которой все отображения (11-1) становятся гомеоморфизмами.

Пример 11.2 (грассманианы)
Точками грассманова многообразия $\mathrm{Gr}(k, m)$ являются $k$-мерные векторные подпространства в координатном векторном пространстве $\Bbbk^m$. Иначе их можно воспринимать как орбиты матриц ранга $k$ из $k$ строк ширины $m$ под действием полной линейной группы $\mathrm{GL}_k(\Bbbk)$ левыми умножениями. При этом подпространству $W \subset \Bbbk^n$ отвечает орбита матрицы, по строкам которой записаны координаты в стандартном базисе пространства $\Bbbk^m$ базисных векторов какого-нибудь базиса в $W$, и действие $\mathrm{GL}_k(\Bbbk)$ заключается в замене базиса в $W$. Грассманиан $\mathrm{Gr}(k, m)$ покрывается $\binom{m}{k}$ стандартными аффинными картами $U_I$, занумерованными строго возрастающими наборами индексов $I = (i_1, \dots, i_k)$, $1 \leqslant i_1 < \dots < i_k \leqslant m$. Если обозначить через $s_I(x)$ подматрицу матрицы $x$, образованную столбцами с номерами из $I$, то $U_I = \{x \in \mathrm{Mat}_{k\times m}(\Bbbk) \mid \det s_I(x) \neq 0\}$.

Упражнение 11.2. Убедитесь, что карта $U_I$ состоит из всех $k$-мерных подпространств $W \subset \Bbbk^m$, которые изоморфно проектируются на $k$-мерную координатную плоскость, натянутую на стандартные базисные векторы $e_i$ с $i \in I$ пространства $\Bbbk^m$, вдоль дополнительной $(m-k)$-мерной координатной плоскости, натянутой на остальные базисные векторы.

Обозначим через $X_I \simeq \mathrm{Mat}_{k\times(m-k)}(\Bbbk) \simeq \mathbb{A}^{k(m-k)}$ аффинное пространство всех матриц из $k$ строк ширины $m-k$ и будем нумеровать столбцы этих матриц индексами $\nu$ из дополнительного к $I$ набора $\hat{I} = \{1, \dots, m\} \smallsetminus I$. Отображение $\varphi_I : X_I \xrightarrow{\sim} U_I$, превращающее $k\times(m-k)$-матрицу $t \in X_I$ в $k\times m$-матрицу $\varphi_I(t)$ дописыванием к ней единичной $k\times k$-матрицы в столбцы с номерами из $I$, биективно, и $\varphi_I^{-1}(U_I \cap U_J) = \mathcal{D}\Big(\det s_J\big(\varphi_I(t)\big)\Big)$ является главным открытым подмножеством в $X_I$.

Упражнение 11.3. Убедитесь, что отображение $\varphi_J^{-1}\varphi_I : \mathcal{D}\Big(\det s_J\big(\varphi_I(t)\big)\Big) \to \mathcal{D}\Big(\det s_I\big(\varphi_J(t)\big)\Big)$ действует по формуле $t \mapsto s_{\hat{J}}\Big(s_J^{-1}\big(\varphi_I(t)\big) \cdot \varphi_I(t)\Big)$ и является изоморфизмом аффинных алгебраических многообразий.

Отсюда мы как и в предыдущем примере заключаем, что грассманиан $\mathrm{Gr}(k, n)$ является алгебраическим многообразием конечного типа. Отметим, что $\mathrm{Gr}(1, n+1) = \mathbb{P}_n$.

Пример 11.3 (прямое произведение многообразий)
Структура алгебраического многообразия на прямом произведении алгебраических многообразий $X$ и $Y$ задаётся атласом, состоящим из всех попарных произведений $U \times W$ аффинных карт $U \subset X$ и $W \subset X$ на $X$, $Y$.

**11.1.1. Структурный пучок и регулярные морфизмы.** Функция $f : X \to \Bbbk$ называется *регулярной* в точке $p$ алгебраического многообразия $X$, если существуют такие аффинная карта $\varphi_U : X_U \xrightarrow{\sim} U$ и рациональная функция $\tilde{f} \in \Bbbk(X_U)$, что $p \in U$, $\varphi_U^{-1}(p) \in \mathrm{Dom}\,\tilde{f}$ и $\tilde{f}(x) = \varphi_U^* f(x)$ для всех $x \in \mathrm{Dom}\,\tilde{f}$. Функции $U \to \Bbbk$ на открытом подмножестве $U \subset X$, регулярные в каждой точке $p \in U$, образуют коммутативное кольцо, которое обозначается $\mathcal{O}_X(U)$ и называется кольцом *локальных регулярных функций* на $U$. Сопоставление $U \mapsto \mathcal{O}_X(U)$ является пучком $\Bbbk$-алгебр на топологическом пространстве $X$ в смысле прим. 8.8 на стр. 113. Он называется *структурным пучком* алгебраического многообразия $X$.

Отображение алгебраических многообразий $\varphi : X \to Y$ называется *регулярным*, если для каждой точки $x \in X$ и любой локальной регулярной функции $f \in \mathcal{O}_Y(W)$, определённой в какой-либо окрестности $W \ni \varphi(x)$, существует такая окрестность $U \subset \varphi^{-1}(W)$ точки $x$, что $\varphi^*(f) \in \mathcal{O}_X(U)$. Иными словами, над каждым открытом $U \subset Y$ гомоморфизм поднятия должен переводить локальные регулярные функции на $U$ в локальные регулярные функции на $\varphi^{-1}(U)$, т. е. быть гомоморфизмом $\varphi^* : \mathcal{O}_Y(U) \to \mathcal{O}_X\left(\varphi^{-1}(U)\right)$. Например, множество регулярных морфизмов $X \to \mathbb{A}^1$ совпадает с $\mathcal{O}_X(X)$.

Упражнение 11.4. Покажите, что для каждой аффинной карты $\varphi_U : X_U \xrightarrow{\sim} U$ гомоморфизм подъёма $\varphi_U^* : \mathcal{O}_X(U) \xrightarrow{\sim} \Bbbk[X_U]$ отождествляет кольцо локальных регулярных на $U$ функций с координатной алгеброй аффинного многообразия $X_U$.

**11.1.2. Замкнутые подмногообразия.** Каждое замкнутое подмножество $Z$ алгебраического многообразия $X$ имеет естественную структуру алгебраического многообразия. А именно, для каждой аффинной карты $\varphi_U : X_U \xrightarrow{\sim} U$ прообраз пересечения $\varphi_U^{-1}(Z \cap U)$ является замкнутым подмножеством в $X_U$, т. е. аффинным алгебраическим многообразием с координатным кольцом $\Bbbk[X_U]/\varphi_U^* I(Z \cap U) \simeq \mathcal{O}_X(U)/I(Z \cap U)$, где идеал $I(Z \cap U) \subset \mathcal{O}_X(U)$ состоит из всех локальных регулярных на $U$ функций[1], тождественно зануляющихся на $Z \cap U$. Аффинные карты

$$\varphi_U^{-1}(Z \cap U) \xrightarrow{\sim} Z \cap U \subset Z$$

образуют алгебраический атлас на $Z$. Сопоставление $U \mapsto I(Z \cap U)$ является подпучком идеалов в структурном пучке $\Bbbk$-алгебр $\mathcal{O}_X$. Он называется *пучком идеалов* замкнутого подмногообразия $Z \subset X$ и обозначается $\mathcal{I}_Z \subset \mathcal{O}_X$. В этой ситуации пишут, что $Z = V\left(\mathcal{I}_Z\right)$.

Регулярный морфизм $\varphi : X \to Y$ называется *замкнутым вложением*, если его образ $\varphi(X)$ является замкнутым подмногообразием в $Y$ и $\varphi : X \xrightarrow{\sim} \varphi(X)$ является изоморфизмом алгебраических многообразий. В частности, алгебраическое многообразие $X$ тогда и только тогда допускает замкнутое вложение в аффинное пространство, когда оно является аффинным алгебраическим многообразием в смысле n° 10.1 на стр. 137, т. е. является множеством нулей системы полиномиальных уравнений в аффинном пространстве.

Пример 11.4 (семейства подмногообразий)
Каждый регулярный морфизм $\pi : X \to Y$ может восприниматься как семейство замкнутых подмногообразий $X_y = \pi^{-1}(y) \subset X$, параметризованное точками $y \in Y$. Если $\pi : X \to Y$, $\pi' : X' \to Y$ — два семейства с одной и той же базой, то регулярный морфизм $\varphi : X \to X'$ называется *морфизмом семейств*[2], если он переводит $X_y$ в $X'_y$ для каждого $y \in Y$, т. е. если $\pi = \pi' \circ \varphi$. Семейство $\pi : X \to Y$ называется *постоянным* или *тривиальным*, если оно изоморфно над $Y$ прямому произведению $\pi_Y : X_0 \times Y \to Y$ для некоторого многообразия $X_0$.

**11.1.3. Отделимость.** Стандартный атлас на $\mathbb{P}_1$ состоит из двух карт $\varphi_i : \mathbb{A}^1 \xrightarrow{\sim} U_i$, $i = 0, 1$. Пересечение $U_0 \cap U_1$ видно внутри каждой карты как дополнение к началу координат:

$$\varphi_0^{-1}(U_0 \cap U_1) = \varphi_1^{-1}(U_0 \cap U_1) = \mathbb{A}^1 \smallsetminus \{O\} = \{t \in \mathbb{A}^1 \mid t \neq 0\}\,.$$

[1] Ср. с упр. 11.4.
[2] Или *морфизмом над* $Y$.

Карты склеены по этому пересечению посредством отображения склейки

$$\varphi_{01} : t \mapsto 1/t . \tag{11-2}$$

Если вместо этого отображения воспользоваться тождественным отображением

$$\tilde{\varphi}_{01} : t \mapsto t , \tag{11-3}$$

получится другое многообразие — «прямая с раздвоенной точкой»:

————:———— .

Такая патология называется *неотделимостью*. Она возникла потому, что правило склейки (11-3) не замкнуто и продолжается по непрерывности с $\mathbb{A}^1 \smallsetminus \{O\}$ на всё $\mathbb{A}^1 = \overline{\mathbb{A}^1 \smallsetminus \{O\}}$. Говоря более формально, включения $U_0 \hookleftarrow U_0 \cap U_1 \hookrightarrow U_1$ задают вложение $U_0 \cap U_1 \hookrightarrow U_0 \times U_1$, образ которого является пересечением аффинной карты $U_0 \times U_1 \subset X \times X$ с диагональю $\Delta = \{(x, x) \mid x \in X\} \subset X \times X$. Правило (11-2) задаёт вложение $(\mathbb{A}^1 \smallsetminus O) \hookrightarrow \mathbb{A}^2$ по формуле $t \mapsto (t, t^{-1})$ и таким образом отождествляет пересечение $U_0 \cap U_1 \simeq \left(U_0 \times U_1\right) \cap \Delta$ с гиперболой $xy = 1$, которая является *замкнутым* подмножеством в $U_0 \times U_1 \simeq \mathbb{A}^2$. Правило (11-3) задаёт вложение $(\mathbb{A}^1 \smallsetminus O) \hookrightarrow \mathbb{A}^2$ по формуле $t \mapsto (t, t)$, образ которого не замкнут в $\mathbb{A}^2$.

Алгебраическое многообразие $X$ называется *отделимым*, если для любой пары аффинных карт $U, W$ на $X$ образ канонического вложения $U \cap W \hookrightarrow U \times W$ замкнут, или, что то же самое, если диагональ $\Delta \subset X \times X$ замкнута в $X \times X$.

Например, $\mathbb{A}^n$ и $\mathbb{P}_n$ отделимы, поскольку диагонали в $\mathbb{A}^n \times \mathbb{A}^n$ и в $\mathbb{P}_n \times \mathbb{P}_n$ задаются, соответственно, уравнениями $x_i = y_i$ и $x_i y_j = x_j y_i$. Замкнутое подмногообразие $X \subset Y$ отделимого многообразия $Y$ тоже отделимо, ибо диагональ в $X \times X$ является прообразом диагонали в $Y \times Y$ при вложении $X \times X \hookrightarrow Y \times Y$. В частности, всякое аффинное или проективное многообразие отделимо и имеет конечный тип.

Пример 11.5 (график морфизма)
Пусть $\varphi : X \to Y$ — регулярный морфизм. Прообраз диагонали $\Delta \subset Y \times Y$ при индуцированном морфизме $\varphi \times \mathrm{Id}_Y : X \times Y \to Y \times Y$ называется *графиком* $\varphi$ и обозначается

$$\Gamma_\varphi \overset{\text{def}}{=} \{(x, f(x)) \in X \times Y \mid x \in X\} .$$

Если $Y$ отделимо, то график замкнут. Например, график регулярного морфизма аффинных многообразий $\varphi : \operatorname{Spec_m}(A) \to \operatorname{Spec_m}(B)$ задаётся в $A \otimes B$ системой уравнений $1 \otimes f = \varphi^*(f) \otimes 1$, где $f$ пробегает $B$.

**11.1.4. Рациональные отображения.** Регулярный морфизм $\varphi : U \to Y$, определённый на некотором открытом плотном подмножестве $U$ алгебраического многообразия $X$, называется *рациональным отображением* из $X$ в $Y$. Рациональное отображение $\psi : W \to Y$, заданное на открытом множестве $W \supset U$ и совпадающее с $\varphi$ на $U$, называется *продолжением* рационального отображения $\varphi : U \to Y$. Объединение всех открытых множеств $W \supset U$, на которые продолжается $\varphi$, называется *областью определения* рационального отображения $\varphi : X \dashrightarrow Y$.

Упражнение 11.5 (квадратичная инволюция Кремоны). Покажите, что правило

$$(x_0 : x_1 : x_2) \mapsto (x_0^{-1} : x_1^{-1} : x_2^{-1})$$

задаёт рациональное отображение $\varkappa : \mathbb{P}_2 \dashrightarrow \mathbb{P}_2$, определённое всюду, кроме трёх точек. Найдите эти точки и опишите образ $\varkappa$.

Рациональные отображения $\varphi : X \dashrightarrow Y$ не являются отображениями «из $X$» в теоретико-множественном смысле, ибо определены не везде. В частности, композиция рациональных отображений не определена, когда образ первого отображения оказывается целиком вне области определения второго. Тем не менее, рациональные отображения часто возникают и играют важную роль в алгебраической геометрии. Например, естественная проекция $\mathbb{A}(V) \dashrightarrow \mathbb{P}(V)$, переводящая точку пространства $\mathbb{A}(V)$, представленную вектором $v \in V$, в точку пространства $\mathbb{P}(V)$, представленную тем же самым вектором $v$, является сюрьективным рациональным отображением определённым всюду, кроме нуля.

**11.2. Проективные многообразия.** Алгебраическое многообразие $X$ называется *проективным*, если оно допускает замкнутое вложение в проективное пространство, т. е. изоморфно замкнутому подмногообразию в $\mathbb{P}_n$ для некоторого $n \in \mathbb{N}$.

Упражнение 11.6. Покажите, что множество решений системы однородных полиномиальных уравнений на однородные координаты пространства $\mathbb{P}_n$ является замкнутым подмногообразием в $\mathbb{P}_n$.

Поскольку грассманиан $\mathrm{Gr}(k, V)$ вкладывается в проективное пространство $\mathbb{P}(\Lambda^k V)$ отображением Плюккера[1] и образ этого вложения описывается однородными квадратными уравнениями[2], все грассманианы являются проективными алгебраическими многообразиями.

Упражнение 11.7. Покажите, что прямое произведение проективных многообразий проективно, и выведите из этого, что подмножество в $\mathbb{P}_{n_1} \times \dots \times \mathbb{P}_{n_m}$, задаваемое набором однородных по координатам каждого сомножителя полиномиальных уравнений на однородные координаты, является проективными алгебраическим многообразием.

Пример 11.6 (раздутие точки в $\mathbb{P}_n$)

Прямые, проходящие через заданную точку $p \in \mathbb{P}_n$, находятся в естественной биекции с точками проективного пространства $E \simeq \mathbb{P}_{n-1}$. График инцидентности $\mathcal{B}_p = \{(q, \ell) \in \mathbb{P}_n \times E \mid q \in \ell\}$ называется *раздутием* точки $p \in \mathbb{P}_n$. Проекция $\sigma_p : \mathcal{B}_p \twoheadrightarrow \mathbb{P}_n$ биективна всюду над $\mathbb{P}_n \smallsetminus \{p\}$, однако слой $\sigma_p^{-1}(p) = \{p\} \times E \subset \mathcal{B}_p$. Он называется *исключительным дивизором*[3] в $\mathcal{B}_p$. Таким образом, раздутие точки $p$ можно представлять себе как результат вклеивания проективного пространства $E$ вместо точки $p$ в пространство $\mathbb{P}_n$ таким образом, что приход в точку $p$ вдоль прямой $\ell \subset \mathbb{P}_n$ приводит в точку $\ell \in E$. Вторая проекция $\varrho_E : \mathcal{B}_p \twoheadrightarrow E$ реализует многообразие $\mathcal{B}_p$ как *линейное расслоение* над проективным пространством $E$, слоем которого над точкой $q \in E$ служит прямая $(pq) \subset \mathbb{P}_n$. Это расслоение называется *тавтологическим* линейным расслоением над $E$. Покажем, что $\mathcal{B}_p$ является проективным многообразием. Для этого выберем однородные координаты на $\mathbb{P}_n$ так, чтобы точка $p = (1 : 0 : \dots : 0)$, и отождествим $E$ с гиперплоскостью $V(x_0) \subset \mathbb{P}_n$, сопоставляя прямой $\ell \ni p$ точку $t = \ell \cap V(x_0) = (0 : t_1 : \dots : t_n)$.

[1] См. формулу (2-40) на стр. 35.

[2] См. формулу (2-38) на стр. 34.

[3] Вообще *дивизорами* (*Вейля*) на алгебраическом многообразии называются элементы свободной абелевой группы, порождённой неприводимыми замкнутыми подмногообразиями коразмерности 1 (размерности алгебраических многообразий обсуждаются в n° 11.5 ниже).

Тогда коллинеарность точек $p$, $q$, $t$ запишется системой однородных квадратичных уравнений

$$\mathrm{rk}\begin{pmatrix} 1 & 0 & \cdots & 0 \\ q_0 & q_1 & \cdots & q_n \\ 0 & t_1 & \cdots & t_n \end{pmatrix} = 2\,, \quad \text{или} \quad q_i t_j = q_j t_i \quad \forall\; 1 \leqslant i < j \leqslant n$$

на пару точек $(q,t) \in \mathbb{P}_n \times E$. По упр. 11.7 множество решений таких уравнений является проективным алгебраическим многообразием.

Лемма 11.1
Каждое замкнутое подмногообразие $X \subset \mathbb{P}_n$ является множеством решений конечной системы полиномиальных уравнений на однородные координаты пространства $\mathbb{P}_n$.

Доказательство. В обозначениях из прим. 11.1 на стр. 151 пересечение $X \cap U_i$ со стандартной открытой картой $U_i \subset \mathbb{P}_n$ является множеством нулей некоторого идеала $I_i$ в кольце многочленов от $n$ переменных $t_{i,\nu} = x_\nu / x_i$, где $0 \leqslant \nu \leqslant n$ и $\nu \neq i$. Каждый такой многочлен $f$ можно переписать как $\overline{f}(x_0, x_1, \dots, x_n)/x_i^d$, где $d = \deg f$, а $\overline{f} \in \Bbbk[x_0, x_1, \dots, x_n]$ — такой однородный многочлен степени $d$, что $\overline{f}\left(t_{i,0}, \dots, t_{i,i-1}, 1, t_{i,i+1}, \dots, t_{i,n}\right) = f\left(t_{i,0}, \dots, t_{i,i-1}, t_{i,i+1}, \dots, t_{i,n}\right)$. Для каждого $i$ рассмотрим какое-нибудь конечное множество образующих $f_{i,\alpha}$ идеала $I_i$ и построим по ним однородные многочлены $\overline{f}_{i,\alpha} \in \Bbbk[x_0, x_1, \dots, x_n]$. Покажем, что многообразие $X$ совпадает с множеством $Z$ решений системы однородных полиномиальных уравнений

$$x_i \cdot \overline{f}_{i,\alpha}(x_0, x_1, \dots, x_n) = 0\,,$$

где $0 \leqslant i \leqslant n$ и при каждом $i$ второй индекс $\alpha$ нумерует образующие $f_{i,\alpha}$ идеала $I_i$. Достаточно для каждого $i$ установить равенство $Z \cap U_i = X \cap U_i$. Поскольку пересечение множества нулей однородного многочлена $x_i \cdot \overline{f}(x_0, x_1, \dots, x_n)$ с картой $U_i \subset \mathbb{P}_n$ задаётся в аффинных координатах $t_i$ на $U_i$ уравнением $\overline{f}\left(t_{i,0}, \dots, t_{i,i-1}, 1, t_{i,i+1}, \dots, t_{i,n}\right) = f\left(t_{i,0}, \dots, t_{i,i-1}, t_{i,i+1}, \dots, t_{i,n}\right) = 0$, пересечение карты $U_i$ с множеством общих нулей однородных многочленов $x_i \cdot \overline{f}_{i,\alpha}$, индекс $i$ которых равен номеру карты, совпадает с $X \cap U_i$. Тем самым, $Z \cap U_i \subset X \cap U_i$ и для завершения доказательства остаётся убедиться, что каждый однородный многочлен $x_j \cdot \overline{f}_{j,\beta}$ с $j \neq i$ также зануляется на $X \cap U_i$. Но множитель $x_j$ зануляется на гиперплоскости $V(t_{i,j}) \subset U_i$, а множитель $\overline{f}_{j,\beta}$ зануляется на дополнительном к этой гиперплоскости главном открытом множестве $\mathcal{D}(t_{i,j}) = X \cap U_i \cap U_j \subset X \cap U_i$, ибо оно содержится в пересечении $X \cap U_j$, на котором многочлен $\overline{f}_{j,\beta}$ равен нулю. □

Пример 11.7 (иллюстрация доказательства лем. 11.1)
Проективное многообразие $X = V(x_0 x_1 x_2) \subset \mathbb{P}_2$ представляет собою объединение трёх координатных прямых. В стандартных картах $U_0$, $U_1$, $U_2$ оно задаётся, соответственно, уравнениями $t_{0,1} t_{0,2} = 0$, $t_{1,0} t_{1,2} = 0$, $t_{2,0} t_{2,1} = 0$. В предыдущем доказательстве этим уравнениям отвечают однородные многочлены $\overline{f}_{0,1} = x_1 x_2$, $\overline{f}_{1,1} = x_0 x_2$, $\overline{f}_{2,1} = x_0 x_1$, а задающее $X$ глобальное однородное уравнение $x_0 x_1 x_2 = 0$ имеет в левой части многочлен $x_0 x_1 x_2 = x_0 \cdot \overline{f}_{0,1} = x_1 \cdot \overline{f}_{1,1} = x_0 \cdot \overline{f}_{2,1}$.

**11.3. Системы результатнтов.** Рассматриваемые с точностью до пропорциональности ненулевые решения системы однородных полиномиальных уравнений

$$\begin{cases} f_1(x_0, x_1, \dots, x_n) = 0 \\ f_2(x_0, x_1, \dots, x_n) = 0 \\ \quad \dots\dots\dots\dots\dots\dots \\ f_m(x_0, x_1, \dots, x_n) = 0\,, \end{cases} \tag{11-4}$$

где каждый $f_i \in \Bbbk[x_0, x_1, \dots, x_n]$ однороден степени $d_i$, образуют проективное многообразие — пересечение проективных гиперповерхностей $S_i = V(f_i) \subset \mathbb{P}(V)$. Проективные гиперповерхности степени $d$ являются точками проективного пространства $\mathbb{P}(S^d V^*)$. Наборы гиперповерхностей $(S_1, \dots, S_m)$ заданных степеней $d_1, \dots, d_m$ с непустым пересечением $\bigcap_i S_i \neq \varnothing$, составляют фигуру

$$\mathcal{R}(n+1;\ d_1, \dots, d_m) \subset \mathbb{P}(S^{d_1}V^*) \times \dots \times \mathbb{P}(S^{d_m}V^*)\,, \tag{11-5}$$

которая называется *результантным множеством* системы (11-4). Например, когда число уравнений равно числу переменных и все уравнения линейны, система (11-4) превращается в систему однородных линейных уравнений $Ax = 0$ с квадратной матрицей $A = (a_{ij})$ и имеет ненулевое решение если и только если $\det(a_{ij}) = 0$. Поэтому для $m = n+1$ и $d_1 = \dots = d_{n+1} = 1$ результантное множество является проективным алгебраическим многообразием, заданным одним полиномиальным уравнением на коэффициенты $a_{i,j}$ линейных форм $f_1, \dots, f_{n+1}$.

Покажем, что результантное множество (11-5) всегда является проективным алгебраическим многообразием, т. е. задаётся конечной системой полиномиальных уравнений на коэффициенты многочленов $f_i$, однородных по коэффициентам каждого из многочленов и зависящих только от числа переменных и набора степеней. Для этого рассмотрим идеал

$$J = (f_1, \dots, f_m) \subset \Bbbk[x_0, x_1, \dots, x_n]\,.$$

Отсутствие у системы (11-4) ненулевых решений означает, что аффинное алгебраическое многообразие $V(J) \subset \mathbb{A}(V)$ пусто или совпадает с началом координат. В обоих случаях каждая из координатных функций $x_i$ тождественно зануляется на $V(J)$, и по теореме Гильберта о нулях существует такое $m \in \mathbb{N}$, что $x_i^m \in J$ для все $i$. Наоборот, если $J$ содержит некоторую степень каждой из переменных, то система уравнений с левыми частями из идеала $J$ включает в себя уравнения $x_0^m = x_1^m = \dots = x_n^m = 0$, имеющие только нулевое решение. Таким образом, отсутствие ненулевых решений у системы (11-4) равносильно тому, что для некоторого $m$ идеал $J$ содержит все $x_i^m$. Последнее означает, что любой многочлен, степень которого больше $(n+1)(m-1)$, лежит в $J$, т. е. $J$ содержит все $S^d V^*$ с $d \gg 0$. Пересечение $J \cap S^d V^*$ является образом линейного отображения

$$\mu_d :\ S^{d-d_1}V^* \oplus \dots \oplus S^{d-d_m}V^* \to S^d\,, \quad (g_1, \dots, g_m) \mapsto \sum g_\nu f_\nu\,, \tag{11-6}$$

задаваемого в стандартных базисах из мономов матрицей, ненулевые элементы которой суть коэффициенты многочленов $f_\nu$. При $d \gg 0$ размерность левой части (11-6) ведёт себя как $\sum_{\nu=1}^m \binom{n+d-d_\nu}{n} \sim \frac{m}{n!}\, d^n$ и становится больше, чем размерность правой части, ведущая себя как $\binom{n+d}{n} \sim \frac{1}{n!}\, d^n$. Для всех таких $d$ неэпиморфность отображения (11-6), т. е. неравенство $J \cap S^d V^* \neq S^d V^*$, равносильно обнулению всех максимальных миноров матрицы $\mu_d$.

Итак, наличие ненулевых решений у системы (11-4) эквивалентно обращению в нуль всех максимальных миноров матриц $\mu_d$ для всех таких $d$, что размерность левой части (11-6) не меньше, чем размерность правой. В силу нётеровости кольца многочленов, эта бесконечная система полиномиальных уравнений эквивалентна некоторой конечной подсистеме, называемой *системой результантов*.

Пример 11.8 (результант пары бинарных форм)
Над алгебраически замкнутым полем $\Bbbk$ каждый однородный многочлен степени $d$ от двух переменных $A(t_0,t_1) = a_0\,t_1^d + a_1\,t_0t_1^{d-1} + \dots + a_{d-1}\,t_0^{d-1}t_1 + a_d\,t_0^d$ полностью раскладывается на линейные множители:

$$A(t_0,t_1) = \prod_{i=0}^{d}(\alpha_i''t_0 - \alpha_i't_1) = \prod_{i=0}^{d}\det\begin{pmatrix} t_0 & t_1 \\ \alpha_i' & \alpha_i'' \end{pmatrix}$$

биективно соответствующие $d$ нулям[1] $\alpha_i = (\alpha_i' : \alpha_i'')$ многочлена $A$ на проективной прямой $\mathbb{P}_1 = \mathbb{P}_1(\Bbbk)$. Коэффициенты многочлена $A$ выражаются через однородные координаты его нулей по *формулам Виета* $a_k = (-1)^{d-k}\sigma_k(\alpha',\alpha'') \overset{\text{def}}{=} (-1)^{d-k}\sum_{\#I=k}\left(\prod_{i\in I}\alpha_i' \cdot \prod_{j\notin I}\alpha_j''\right)$, где $I$ пробегает все строго возрастающие подмножества из $k$ индексов. В частности, $a_k$ биоднороден бистепени $(k, d-k)$ по $(\alpha',\alpha'')$. Для фиксированных степеней $m,n\in\mathbb{N}$ рассмотрим в кольце многочленов $\Bbbk[\alpha',\alpha'',\beta',\beta'']$ от четырёх наборов переменных

$$\alpha' = (\alpha_1',\dots,\alpha_n'),\ \alpha'' = (\alpha_1'',\dots,\alpha_n''),\ \beta' = (\beta_1',\dots,\beta_m'),\ \beta'' = (\beta_1'',\dots,\beta_m'')$$

произведение $R_{AB} \overset{\text{def}}{=} \prod_{i,j}\left(\alpha_i'\beta_j'' - \alpha_i''\beta_j'\right) = \prod_{j=1}^n A(\beta_j) = (-1)^{mn}\prod_{i=1}^m B(\alpha_i)$. Оно обращается в нуль если и только если многочлены $A(t_0,t_1) = \sum_{i=0}^n a_i\,t_0^it_1^{n-i}$ и $B(t_0,t_1) = \sum_{j=0}^m b_j\,t_0^jt_1^{m-j}$ с коэффициентами $a_i = (-1)^{n-i}\sigma_i(\alpha',\alpha'')$ и $b_j = (-1)^{m-j}\sigma_j(\beta',\beta'')$ имеют общий нуль на $\mathbb{P}_1$. Многочлен $R_{A,B}$ биоднороден бистепени $(mn,mn)$ по $(\alpha,\beta)$ и явно выражается через коэффициенты форм $A$, $B$ по *формуле Сильвестра*

$$R_{AB} = \det \underbrace{\begin{pmatrix} a_0 & a_1 & \cdots & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & \cdots & a_n & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & \cdots & b_m & & \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ & & & b_0 & b_1 & \cdots & \cdots & b_m \end{pmatrix}}_{m+n} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \end{array} \tag{11-7}$$

В самом деле, линейное отображение (11-6) для векторного пространства $V^*$ с базисом $t_0,t_1$ переводит пару однородных многочленов $(h_1,h_2)$ в $Ah_1 + Bh_2$. При $d = m+n-1$ оно имеет вид $\mu_{m+n-1} : S^{m-1}V^* \oplus S^{n-1}V^* \to S^{m+n-1}V^*$ и в стандартных базисах из мономов задаётся квадратной матрицей, транспонированной к матрице Сильвестра (11-7).

Упражнение 11.8. Убедитесь в этом.

[1] Эти нули не обязательно различны.

Если точка $(\alpha, \beta)$ лежит на квадрике $\alpha_i' \beta_j'' - \alpha_i'' \beta_j' = 0$, то с точностью до постоянного множителя $(\alpha_i'' t_0 - \alpha_i' t_1) = (\beta_i'' t_0 - \beta_i' t_1)$. Так как эта линейная форма делит все многочлены вида $Ah_1 + Bh_2$, образ $\operatorname{im} \mu_{m+n-1} \neq S^{m+n-1}V^*$. Поэтому определитель Сильвестра (11-6) зануляется на каждой квадрике $\alpha_i' \beta_j'' - \alpha_i'' \beta_j' = 0$. По теореме о нулях, некоторая степень многочлена $R_{A,B}$ делится на произведение уравнений квадрик. В силу неприводимости этих уравнений и факториальности кольца многочленов такое возможно только когда $R_{A,B}$ делится на произведение уравнений квадрик. Сравнение степеней и коэффициента при старшем мономе показывает, что частное равно 1.

Упражнение 11.9. Убедитесь в этом.

Таким образом, для пары бинарных форм результантное многообразие задаётся одним уравнением[1] $R_{AB} = 0$ на коэффициенты многочленов $A, B$. Многочлен $R_{A,B}$ называется *результантом* форм $A$ и $B$. Если положить $t_0 = 1$, $t_1 = x$, мы получим результант двух неоднородных многочленов $A(x)$ и $B(x)$. В предположении, что $a_0 b_0 \neq 0$, такой результант обращается в нуль если и только если неоднородные многочлены $A$ и $B$ имеют общий корень в $\mathbb{A}^1 = \mathbb{P}_1 \smallsetminus \{(0:1)\}$.

**11.4. Замкнутость проективных морфизмов.** Геометрическим следствием алгебраичности результантного множества является замкнутость любого морфизма из проективного многообразия в любое отделимое алгебраическое многообразие. Неформально говоря, это означает, что проективные многообразия занимают в алгебраической геометрии примерно такое же место, как компактные многообразия в дифференциальной геометрии.

Лемма 11.2

Проекция $\pi : \mathbb{P}_m \times \mathbb{A}^n \twoheadrightarrow \mathbb{A}^n$ *замкнута*, т. е. переводит замкнутые множества в замкнутые.

Доказательство. Зафиксируем на $\mathbb{P}_m$ однородные координаты $x$, а на $\mathbb{A}^n$ — аффинные координаты $t$. Замкнутое подмножество $X \subset \mathbb{P}_m \times \mathbb{A}^n$ задаётся системой однородных по $x$ полиномиальных уравнений $f_\nu(x, t) = 0$. Его образ $\pi(X) \subset \mathbb{A}^n$ состоит из всех точек $p$, при подстановке которых в эти уравнения вместо $t$ получается имеющая ненулевое решение система однородных уравнений $f_\nu(x, p) = 0$ на $x$. Это означает, что коэффициенты форм $f_\nu(x, p)$, являющиеся полиномами от $p$, удовлетворяют системе результантных полиномиальных уравнений. □

Следствие 11.1

Если многообразие $X$ проективно, то проекция $X \times Y \twoheadrightarrow Y$ замкнута для любого многообразия $Y$.

Доказательство. Ограничиваясь на аффинные карты в $Y$, мы можем считать $Y$ аффинным. Тогда $X \times Y$ является замкнутым подмногообразием в $\mathbb{P}_m \times \mathbb{A}^n$, и наша проекция получается ограничением замкнутой проекции $\mathbb{P}_m \times \mathbb{A}^n \twoheadrightarrow \mathbb{A}^n$ на замкнутое подмножество $X \times Y \subset \mathbb{P}_m \times \mathbb{A}^n$.
□

Следствие 11.2

Если $X$ проективно, а $Y$ отделимо, то любой морфизм $\varphi : X \to Y$ замкнут.

Доказательство. Образ $\varphi(Z) \subset Y$ любого подмножества $Z \subset X$ совпадает с образом пересечения $\Gamma_\varphi \cap (Z \times Y) \subset X \times Y$ при проекции $X \times Y \twoheadrightarrow Y$, где $\Gamma_\varphi \subset X \times Y$ — график отображения $\varphi : X \to Y$. Если $Z$ замкнуто в $X$, произведение $Z \times Y$ замкнуто в $X \times Y$. Если $Y$ отделимо, график $\Gamma_\varphi$ тоже

[1] В прим. 11.10 на стр. 166 ниже мы обобщим этот результат на случай произвольной системы однородных полиномиальных уравнений, в которой число уравнений равно числу неизвестных.

замкнут[1]. Если $X$ проективно, проекция $X \times Y \twoheadrightarrow Y$ замкнута и переводит замкнутое множество $\Gamma_\varphi \cap (Z \times Y) \subset X \times Y$ в замкнутое множество $\varphi(Z) \subset Y$. $\square$

Следствие 11.3

Любое регулярное отображение из связного проективного многообразия $X$ в аффинное многообразие стягивает $X$ в одну точку. В частности, $\mathcal{O}_X(X) = \Bbbk$.

Доказательство. Достаточно доказать утверждение для отображения $\varphi : X \to \mathbb{A}^n$. Беря композицию такого отображения с координатными функциями $x_i : \mathbb{A}^n \to \mathbb{A}^1$, мы сводим утверждение к случаю $n = 1$. Композиция регулярного отображения $X \to \mathbb{A}^1$ с вложением $\mathbb{A}^1 \hookrightarrow \mathbb{P}_1$ в качестве стандартной аффинной карты является регулярном несюрьективным отображением $X \to \mathbb{P}_1$. Так как его образ замкнут и связен, он является точкой. $\square$

**11.4.1. Конечные проекции.** Регулярное отображение $\varphi : X \to Y$ алгебраических многообразий называется *конечным*, если прообраз $W = \varphi^{-1}(U)$ любой аффинной карты $U \subset Y$ является аффинной картой на $X$, и ограничение $\varphi_W : W \to U$ является конечным морфизмом аффинных многообразий в смысле n° 10.5.3 на стр. 148. Из лем. 10.3 на стр. 148 следует, что каждый конечный морфизм замкнут и ограничение конечного морфизма на замкнутое подмногообразие $Z \subset X$ также является конечным морфизмом. Более того, если $X$ неприводимо, то собственное замкнутое подмножество $Z \subsetneq X$ переходит в собственное замкнутое подмножество $\varphi(Z) \subsetneq Y$.

Упражнение 11.10. Проверьте, что композиция конечных морфизмов конечна.

Предложение 11.1

Проекция любого проективного многообразия $X \subsetneq \mathbb{P}_n$ из любой точки $p \notin X$ на любую гиперплоскость $H \not\ni p$ является конечным морфизмом.

Доказательство. Зафиксируем стандартную аффинную карту $U \subset H$ и такие однородные координаты $(x_0 : x_1 : \ldots : x_n)$ на $\mathbb{P}_n$, что $p = (1 : 0 : \ldots : 0)$, гиперплоскость $H = V(x_0)$ состоит из точек $q = (0 : q_1 : \ldots : q_n)$, а карта $U \subset H$ — из точек $u = (0 : u_1 : \ldots : u_{n-1} : 1)$. Пусть многообразие $X$ задаётся в этих координатах системой однородных уравнений $f_\nu(x) = 0$. Поскольку $p \notin X$, прообраз $Y = \pi_p^{-1}(U) \subset X$ является пересечением многообразия $X$ с проколотым конусом $C$ над $U$, образованным всеми прямыми $(pu) \subset \mathbb{P}_n$ с выколотой точкой[2] $p$. Конус $C$ является аффинным алгебраическим многообразием, изоморфным аффинному пространству $\mathbb{A}^n = U \times \mathbb{A}^1$: изоморфизм переводит точку $(u,t) \in U \times \mathbb{A}_1$ в точку $x = tp + u \in \mathbb{P}_n$. Пересечение $Y = C \cap X$ задаётся в координатах $(u,t)$ уравнениями

$$f_\nu(tp + u) = \alpha_0^{(\nu)}(u)\, t^m + \alpha_1^{(\nu)}(u)\, t^{m-1} + \cdots + \alpha_m^{(\nu)}(u) = 0\,, \qquad (11\text{-}8)$$

и является аффинным алгебраическим многообразием с координатной алгеброй $\Bbbk[Y] = \Bbbk[u_1, \ldots, u_{n-1}]/I$, где идеал $I$ порождается многочленами $f_\nu(tp+u)$ из левых частей уравнений (11-8). Покажем, что алгебра $\Bbbk[Y]$ цела над подалгеброй $\Bbbk[U] = \Bbbk[u_1, \ldots, u_{n-1}]$. Для этого достаточно найти в идеале $I$ приведённый многочлен от $t$ с коэффициентами из $\Bbbk[U]$ — тогда класс $t \pmod I$, являющийся его корнем, будет цел над $\Bbbk[U]$. Наличие в $I$ такого многочлена равносильно тому,

[1] См. прим. 11.5 на стр. 154.

[2] Т. е. аффинными прямыми $u + pt$, $t \in \Bbbk$.

что идеал, порождённый в $\Bbbk[U]$ старшими коэффициентами $\alpha_0^{(\nu)}(u)$ всех уравнений (11-8), содержит единицу. По теореме Гильберта это означает отсутствие у многочленов $\alpha_0^{(\nu)}(u)$ общих нулей в $U$. Но если такой общий нуль $u_0$ имеется, то однородные версии уравнений (11-8)

$$f_\nu(\vartheta_0\, p + \vartheta_1\, u_0) = \alpha_0^{(\nu)}(u_0)\,\vartheta_0^m + \alpha_1^{(\nu)}(u_0)\,\vartheta_0^{m-1}\vartheta_1 + \cdots + \alpha_m^{(\nu)}(u_0)\vartheta_1^m = 0\,,$$

которые получаются ограничением задающих $X$ уравнений на проективную прямую $(p, u_0)$, имеют на этой прямой общий корень $(\vartheta_0 : \vartheta_1) = (1 : 0)$, находящийся в самой точке $p$, что противоречит условию $p \notin X$. □

Следствие 11.4
Каждое проективное многообразие допускает конечный сюрьективный морфизм на проективное пространство.

Следствие 11.5
Каждое аффинное многообразие $X$ допускает конечный сюрьективный морфизм на аффинное пространство.

Доказательство. Пусть $X \subsetneq \mathbb{A}^n$. Вложим $\mathbb{A}^n$ в $\mathbb{P}_n$ в виде стандартной аффинной карты $U_0$, положим $H_\infty \overset{\text{def}}{=} \mathbb{P}_n \smallsetminus U_0$ и обозначим через $\overline{X} \subset \mathbb{P}_n$ проективное замыкание аффинного многообразия $X$. Проекция многообразия $\overline{X}$ из любой точки $p \in H_\infty \smallsetminus \overline{X}$ на любую гиперплоскость $L \not\ni p$ выглядит в аффинной карте $U_0$ как параллельная проекция многообразия $X = \overline{X} \smallsetminus H_\infty$ на гиперплоскость $U_0 \cap L = L \smallsetminus H_\infty$ в направлении вектора $p$ и по предл. 11.1 является конечным морфизмом аффинных многообразий. Если он не сюрьективен, повторяем процедуру. □

Упражнение 11.11. Убедитесь, что если $X \neq \mathbb{A}^n$, то $\overline{X} \cap H_\infty \neq H_\infty$.

Пример 11.9 (нормализация Нётер)
Рассмотрим отличный от константы многочлен $f \in \Bbbk[x_1, \dots, x_n]$ и запишем его в виде

$$f = f_0 + f_1 + \cdots + f_d\,,$$

где каждый $f_k$ однороден степени $k$. Замыкание $\overline{X}$ аффинной гиперповерхности $X = V(f) \subset \mathbb{A}^n$ в проективном пространстве $\mathbb{P}_n$ с однородными координатами $(x_0 : x_1 : \dots : x_n)$, куда $\mathbb{A}^n$ вложено в качестве стандартной карты $U_0$, задаётся однородным многочленом

$$\overline{f} = f_0 x_0^d + f_1 x_0^{d-1} + \cdots + f_{d-1}x_0 + f_d\,.$$

Бесконечно удалённая точка $p = (0 : p_1 : \dots : p_n) \notin \overline{X}$ если и только если $f_d(p_1, \dots, p_n) \neq 0$. Над бесконечным[1] полем $\Bbbk$ всегда существует такая точка вида $p = (0, p_1, \dots, p_{n-1}, -1)$. Проекция $\pi_p$ из неё на гиперплоскость $x_n = 0$ выглядит в $\mathbb{A}^n$ как параллельная проекция вдоль вектора $(p_1, \dots, p_{n-1}, -1)$ и действует по правилу $(x_1, \dots, x_n) \mapsto (x_1 + p_1 x_n, \dots, x_{n-1} + p_{n-1}x_n, 0)$. Её гомоморфизм подъёма $\pi_p^* : \Bbbk[t_1, \dots, t_{n-1}] \to \Bbbk[x_1, \dots, x_n]/(f)$ переводит $t_i$ в $x_i + p_i x_n$. По предл. 11.1 алгебра $\Bbbk[X] = \Bbbk[x_1, \dots, x_n]/(f)$ цела[2] над $\Bbbk[t_1, \dots, t_{n-1}]$.

Упражнение 11.12. Явно предъявите уравнения целой зависимости для всех $x_i$.

---

[1] И даже не обязательно алгебраически замкнутым.

[2] Откуда следует, в частности, что $\operatorname{tr}\deg \Bbbk[x_1, \dots, x_n]/(f) = n - 1$.

Проекция $\pi_p$ доминантна, так как точка $q \notin \pi_p(X)$ если и только если многочлен

$$f\left(q_1 + p_1 x_n,\ q_2 + p_2 x_n,\ \dots\ ,\ q_{n-1} + p_{n-1} x_n, x_n\right) \in \Bbbk[x_n]$$

является ненулевой константой, что означает обращение в нуль всех его коэффициентов кроме свободного члена и происходит на собственном замкнутом подмножестве в $\mathbb{A}^{n-1}$. Из лем. 10.3 на стр. 148 следует, что проекция $\pi_p$ сюрьективна. Мы заключаем, что каждая аффинная гиперповерхность над произвольным бесконечным полем допускает конечную сюрьективную параллельную проекцию на гиперплоскость.

Упражнение 11.13. Убедитесь в этом напрямую, без привлечения лем. 10.3.

Этот факт известен как *лемма Нётер о нормализации*.

**11.5. Размерность** алгебраического многообразия $X$ в точке $x \in X$ определяется как максимальное $n \in \mathbb{N}$, для которого существует цепочка неприводимых замкнутых подмногообразий

$$\{x\} = X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_{n-1} \subsetneq X_n \subseteq X\,, \tag{11-9}$$

и обозначается $\dim_x X$. Если многообразие $X$ неприводимо, в максимальная цепочке (11-9) с неизбежностью $X_n = X$. Если $X$ приводимо, размерность $\dim_x X$ равна максимальной из размерностей всех проходящих через точку $x$ неприводимых компонент многообразия $X$.

Упражнение 11.14. Покажите, что $\dim_x X = \dim_x U$ для всякой аффинной окрестности $U$ точки $x$.

Предложение 11.2

Если многообразие $Y$ неприводимо и имеется сюрьективный морфизм $\varphi : Y \twoheadrightarrow X$, то для любой точки $y \in Y$ выполняется неравенство $\dim_y Y \geqslant \dim_{\varphi(y)} X$.

Доказательство. Для любой цепочки (11-9) при каждом $i$ многообразие $\varphi^{-1}(X_i) \subset Y$ имеет неприводимую компоненту $Y_i$, которая отображается в $X_i$ доминантно. Они составляют цепочку $\{y\} = Y_0 \subsetneq Y_1 \subsetneq \dots \subsetneq Y_n = Y$. □

Предложение 11.3

Для любого конечного морфизма $\varphi : X \to Y$ неприводимых многообразий и любой точки $x \in X$ выполняется неравенство $\dim_x X \leqslant \dim_{\varphi(x)} Y$, равенство в котором равносильно сюрьективности $\varphi$.

Доказательство. В силу упр. 11.14 можно считать $X$ и $Y$ аффинными. Каждая цепочка (11-9) в $X$ по лем. 10.3 на стр. 148 порождает цепочку строго вложенных друг в друга замкнутых неприводимых подмногообразий $\varphi(X_i)$ в $Y$, что даёт нужное неравенство, причём когда $\varphi(X) \neq Y$, это неравенство строгое. Если $\varphi(X) = Y$, то по предл. 11.2 имеется и противоположное неравенство. □

Следствие 11.6

В любой точке $x \in \mathbb{A}^n$ выполнено равенство $\dim_x \mathbb{A}^n = n$.

Доказательство. Так как в $\mathbb{A}^n$ имеется цепочка (11-9) из проходящих через $x$ аффинных подпространств, $\dim_x \mathbb{A}^n \geqslant n$. Противоположное неравенство доказывается по индукции. Очевидно, что $\dim \mathbb{A}^0 = 0$. Если $\dim \mathbb{A}^{n-1} = n-1$, то беря конечную проекцию последнего отличного от $\mathbb{A}^n$

элемента максимальной цепочки (11-9), написанной для $X = \mathbb{A}^n$, на гиперплоскость в $\mathbb{A}^n$, мы заключаем из предл. 11.3, что его размерность, а значит и номер, не превосходит $n-1$. Поэтому $\dim_x \mathbb{A}^n = n$. □

Следствие 11.7
Пусть $X$ — неприводимое аффинное многообразие и $\varphi : X \to \mathbb{A}^m$ — сюрьективный конечный морфизм. Тогда $\dim_x X = m$ в каждой точке $x \in X$, и число $m$ не зависит от выбора $\varphi$. □

Следствие 11.8
Размерность аффинного неприводимого многообразия $X$ равна степени трансцендентности[1] алгебры $\Bbbk[X]$ над полем $\Bbbk$.

Доказательство. Гомоморфизм подъёма конечной сюрьекции $\pi : X \twoheadrightarrow \mathbb{A}^m$ задаёт целое расширение алгебр $\pi^* : \Bbbk[u_1, \dots, u_m] = \Bbbk[\mathbb{A}^m] \hookrightarrow \Bbbk[X]$. Поэтому функции $\pi^* u_i$ образуют базис трансцендентности алгебры $\Bbbk[X]$ над полем $\Bbbk$. □

Упражнение 11.15. Докажите, что $\dim(X \times Y) = \dim X + \dim Y$ для любых неприводимых многообразий $X, Y$.

**11.5.1. Размерности подмногообразий.** Если через точка $x$ лежит сразу на нескольких неприводимых компонентах многообразия $X$ и функция $f \in \Bbbk[X]$ тождественно обращается в ноль на одной из них, имеющей максимальную размерность $\dim_x X$, то гиперповерхность $V(f) \subset X$ имеет в точке $x$ ту же размерность, что и объемлющее многообразие $X$. Такое возможно, только когда $f$ делит нуль в $\Bbbk[X]$.

Предложение 11.4
Если $X$ неприводимо, то $\dim_p V(f) = \dim_p(X) - 1$ для любой непостоянной регулярной функции $f \in \mathcal{O}_X(X)$ и любой точки $p \in V(f)$.

Доказательство. Мы можем и будем предполагать $X$ аффинным. Случай $X = \mathbb{A}^n$ был разобран в прим. 11.9. Общий случай сводится к этому рассуждением, аналогичным использованному в доказательстве лем. 10.4 на стр. 149. Зафиксируем конечную сюрьекцию $\pi : X \twoheadrightarrow \mathbb{A}^m$ и рассмотрим отображение $\varphi = \pi \times f : X \to \mathbb{A}^m \times \mathbb{A}^1$, $x \mapsto \big(\pi(x), f(x)\big)$. В лем. 10.4 мы видели, что оно конечно и сюрьективно отображает $X$ на аффинную гиперповерхность $V(\mu_f) \subset \mathbb{A}^m \times \mathbb{A}^1$ — множество нулей минимального многочлена $\mu_f(u, t) = t^n + \alpha_1(u)\, t^{n-1} + \dots + \alpha_n(u) \in \Bbbk[u_1, \dots, u_m][t]$ функции $f$ над полем $\Bbbk(\mathbb{A}^m)$. Гиперповерхность $V(f) \subset X$ отображается морфизмом $\varphi$ в пересечение гиперповерхности $V(\mu_f)$ с аффинной гиперплоскостью $t = 0$, внутри которой это пересечение задаётся уравнением $\alpha_n(u) = 0$, т. е. является аффинной гиперповерхностью $V(\alpha_n) \subset \mathbb{A}^m$ размерности $m - 1$. По предл. 11.3 $\dim V(f) = \dim V(\alpha_n) = m - 1 = \dim X - 1$. □

Следствие 11.9
Для любых функций $f_1, \dots, f_m \in \Bbbk[X]$ на аффинном алгебраическом многообразии $X$ в каждой точке $p \in V(f_1, \dots, f_m) \subset X$ выполняется неравенство $\dim_p V(f_1, \dots, f_m) \geqslant \dim_p(X) - m$. Если при каждом $i$ класс функции $f_i$ не делит нуль в $\Bbbk[X]/(f_1, \dots, f_{i-1})$, это неравенство превращается в равенство[2].

[1] См. n° 9.4 на стр. 134.
[2] Последовательности функций с таким свойством называются *регулярными*

Предостережение 11.1. Предыдущее следствие вовсе не утверждает, что $V(f_1,\dots,f_m)\neq\varnothing$, и формально истинно при $V(f_1,\dots,f_m)=\varnothing$. Такое часто случается: например, $V(x,x+1)=\varnothing$ в $\mathbb{A}^3=\operatorname{Spec_m}\Bbbk[x,y,z]$. Из слабой теоремы Гильберта о нулях вытекает, что $V(f_1,\dots,f_m)=\varnothing$ если и только если при некотором $i$ класс $f_i$ в $\Bbbk[X]/(f_1,\dots,f_{i-1})$ равен ненулевой константе.

Предложение 11.5
Для любых аффинных многообразий $X_1,X_2\subset\mathbb{A}^n$ в каждой точке $x\in X_1\cap X_2$ выполняется неравенство $\dim_x(X_1\cap X_2)\geqslant\dim_x(X_1)+\dim_x(X_2)-n$.

Доказательство. Пусть $\varphi_1: X_1\hookrightarrow\mathbb{A}^n$ и $\varphi_2: X_2\hookrightarrow\mathbb{A}^n$ — замкнутые вложения. Тогда $X_1\cap X_2$ является прообразом диагонали $\Delta\subset\mathbb{A}^n\times\mathbb{A}^n$ при отображении $\varphi_1\times\varphi_2: X_1\times X_2\hookrightarrow\mathbb{A}^n\times\mathbb{A}^n$. Внутри $X_1\times X_2$ он задаётся $n$ уравнениями $(\varphi_1\times\varphi_2)^*(x_i)=(\varphi_1\times\varphi_2)^*(y_i)$, которые являются поднятиями линейных уравнений $x_i=y_i$, задающих диагональ $\Delta$ в $\mathbb{A}^n\times\mathbb{A}^n$. Остаётся применить сл. 11.9. □

Предложение 11.6
Если размерности неприводимых проективных многообразий $X_1,X_2\subset\mathbb{P}_n$ удовлетворяют неравенству $\dim(X_1)+\dim(X_2)\geqslant n$, то $X_1\cap X_2\neq\varnothing$.

Доказательство. Пусть $\mathbb{P}_n=\mathbb{P}(V)$. Рассмотрим в $\mathbb{A}^{n+1}=\mathbb{A}(V)$ аффинные конусы $X_1'$, $X_2''$, которые заметаются одномерными векторными подпространствами в $V$, составляющими точки проективных многообразий $X_1$ и $X_2$. Эти конусы задаются теми же самыми уравнениями, что и многообразия $X_1$, $X_2$, только теперь эти уравнения рассматриваются как аффинные. Согласно предл. 11.5 $\dim_O(X_1'\cap X_2'')\geqslant\dim_O(X_1)+1+\dim_O(X_2)+1-n-1\geqslant 1$. Поэтому $X_1'\cap X_2''$ не исчерпывается точкой $O$. □

**11.5.2. Размерности слоёв регулярных морфизмов.** В алгебраической геометрии, в отличие от дифференциальной, размерность прообраза при регулярном отображении контролируется почти столь же жёстко, как в линейной алгебре.

Теорема 11.1
Для любого доминантного морфизма $\varphi: X\to Y$ неприводимых алгебраических многообразий в каждой точке $x\in X$ выполняется неравенство $\dim_x\varphi^{-1}(\varphi(x))\geqslant\dim X-\dim Y$, и существует такое плотное открытое подмножество $U\subset Y$, что для всех точек $y\in U$ в каждой точке $x\in\varphi^{-1}(y)$ имеет место равенство $\dim_x\varphi^{-1}(y)=\dim_x X-\dim_y Y$.

Доказательство. Беря композицию $\varphi$ с конечным сюрьективным морфизмом какой-нибудь аффинной карты $U\ni\varphi(x)$ на пространство $\mathbb{A}^m$ и заменяя $X$ на $\varphi^{-1}(U)$, мы сводим первое утверждение теоремы к случаю $Y=\mathbb{A}^m=\operatorname{Spec_m}\Bbbk[u_1,\dots,u_m]$, $\varphi(x)=0$. Заменяя $X$ аффинной окрестностью точки $x$, мы можем считать $X$ аффинным. В этом случае $\varphi^{-1}(0)$ является непустым пересечением $m$ гиперповерхностей $V(\varphi^*(u_i))\subset X$, и требуемое неравенство вытекает из сл. 11.9. В доказательстве второго утверждения мы также можем и будем считать оба многообразия аффинными, а морфизм $\varphi$ — ограничением проекции $\pi: Y\times\mathbb{A}^m\twoheadrightarrow Y$ на замкнутое подмногообразие $X\subset Y\times\mathbb{A}^m$, как в упр. 10.17 на стр. 148. Мы собираемся применить к слоям этой проекции сл. 11.5. Для этого рассмотрим проективное замыкание $\overline{X}\subset Y\times\mathbb{P}_m$, выберем гиперплоскость $H\subset\mathbb{P}_m$ и точку $p\in\mathbb{P}_m\smallsetminus H$ так, чтобы сечение $Y\times\{p\}\subset Y\times\mathbb{P}_m$ не содержалось в $\overline{X}$. Тогда послойная проекция из $p$ на $H$ удовлетворяет условиям предл. 11.1 во всех слоях, располагающихся над открытым подмножеством $U\subset Y$, дополнительным к $\overline{\pi}\big((Y\times\{p\})\cap\overline{X}\big)$, где

$\overline{\pi} : Y \times \mathbb{P}_m \twoheadrightarrow Y$ — проекция вдоль $\mathbb{P}_m$. Таким образом, заменяя $Y$ любым лежащим в $U$ главным открытым подмножеством (которое, как и $Y$, тоже является аффинным алгебраическим многообразием), мы можем повторить рассуждения из сл. 11.5 одновременно во всех слоях проекции $\pi$. После конечного числа таких итераций мы получим конечный сюрьективный морфизм $\psi : X \twoheadrightarrow Y \times \mathbb{A}^n$, ограничение которого на каждый слой $\varphi^{-1}(y)$ является конечным сюрьективным морфизмом $\varphi^{-1}(y) \twoheadrightarrow \{y\} \times \mathbb{A}^n$. Конечность $\psi$ влечёт равенство $n = \dim X - \dim Y$, а конечность его ограничений на слои — равенство $\dim_x \varphi^{-1}(y) = n$. □

Следствие 11.10 (теорема Шевалле о полунепрерывности)
Для любого морфизма алгебраических многообразий $\varphi : X \to Y$ множества

$$X_k \stackrel{\text{def}}{=} \{\, x \in X \mid \dim_x \varphi^{-1}(\varphi(x)) \geqslant k \,\}$$

замкнуты в $X$ при всех $k \in \mathbb{Z}$.

Доказательство. Если $\dim Y = 0$, то теорема тривиально верна для всех $X$ и $k$. Пусть теперь $\dim Y = m$ и для всех $Y$ меньшей размерности теорема верна для всех $X$ и $k$. Покажем, что она верна для $Y$. Можно считать $X$ и $Y$ неприводимыми. Если $k \leqslant \dim(X) - \dim(Y)$, то $X_k = X$ по теор. 11.1. Для $k > \dim(X) - \dim(Y)$ заменим $Y$ на $Y' = Y \smallsetminus U$, где $U$ взято из теор. 11.1, а $X$ — на $X' = \varphi^{-1}(Y')$. Тогда $X_k \subset X'$, $\dim Y' < \dim Y$, и применимо индуктивное предположение. □

Следствие 11.11
Для любого замкнутого морфизма $\varphi : X \to Y$ множество $Y_k \stackrel{\text{def}}{=} \{y \in Y \mid \dim \varphi^{-1}(y) \geqslant k\}$ замкнуто в $Y$ при каждом $k \in \mathbb{Z}$.

Теорема 11.2 (размерностный критерий неприводимости)
Если регулярный морфизм $\varphi : X \twoheadrightarrow Y$ сюрьективен, а все его слои неприводимы и имеют одинаковые размерности, то неприводимость $Y$ влечёт неприводимость $X$.

Доказательство. Пусть $X = X_1 \cup X_2$ приводимо. Положим

$$Y_1 \stackrel{\text{def}}{=} \{y \in Y \mid \varphi^{-1}(y) \subset X_1\}, \quad Y_2 \stackrel{\text{def}}{=} \{y \in Y \mid \varphi^{-1}(y) \subset X_2\}.$$

Поскольку каждый слой $\varphi$, будучи неприводимым, целиком содержится либо в $X_1$, либо в $X_2$, мы заключаем, что $Y = Y_1 \cup Y_2$, причём оба подмножества $Y_i$ отличны от $Y$, коль скоро оба подмножества $X_i$ отличны от $X$. Так как $Y_i$ совпадает с множеством таких точек в $Y$, над которыми слой отображения $\varphi|_{X_i} X_i \to Y$ достигает своей максимальной размерности, из сл. 11.11 вытекает, что $Y_i$ замкнуто. Тем самым, приводимость $X$ влечёт приводимость $Y$. □

**11.6. Размерности проективных многообразий.** По предл. 11.6 всякое $d$-мерное неприводимое многообразие $X \subset \mathbb{P}_n = \mathbb{P}(V)$ пересекается со всеми проективными подпространствами $H \subset \mathbb{P}_n$ размерности $\dim H \geqslant n - d$. Покажем, что общее подпространство $H$ размерности $\dim H < n - d$ не пересекается с $X$, и, тем самым, $\dim X$ можно охарактеризовать как наибольшее такое $d$, что $X$ пересекается со всеми проективными подпространствами коразмерности $d$. Для этого рассмотрим грассманиан $\mathrm{Gr}(n-d, n+1) = \mathrm{Gr}(n-d, V)$, точками которого являются все $(n-d-1)$-мерные проективные подпространства $H \subset \mathbb{P}(V)$, и образуем многообразие инцидентности

$$\Gamma \stackrel{\text{def}}{=} \{(x, H) \in X \times \mathrm{Gr}(n-d, V) \mid x \in H\} \tag{11-10}$$

Упражнение 11.16. Убедитесь, что $\Gamma$ является проективным алгебраическим многообразием.

Проекция $\pi_1 : \Gamma \twoheadrightarrow X$ сюрьективна: её слой над каждой точкой $x$ состоит из всех проективных подпространств размерности $n-d-1$, проходящих через $x$, и изоморфен грассманиану $\mathrm{Gr}(n-d-1,n) = \mathrm{Gr}(n-d-1, V/\Bbbk x)$ всех векторных $(n-d-1)$-мерных подпространств в фактор пространстве $V/\Bbbk x$. По теор. 11.2 многообразие $\Gamma$ неприводимо и имеет размерность $d + (n-d-1)(d+1) = (n-d)(d+1) - 1$. Образ $\pi_2(\Gamma) \subset \mathrm{Gr}(n-d, V)$ второй проекции $\pi_2 : \Gamma \to \mathrm{Gr}(n-d, V)$ состоит из всех $(n-d-1)$-мерных подпространств, пересекающих $X$. Это неприводимое замкнутое подмногообразие размерности, не превышающей $\dim \Gamma$ и, тем самым, строго меньшей, чем $\dim \mathrm{Gr}(n-d, V) = (n-d)(d+1)$. Поэтому множество не пересекающих $X$ подпространств размерности $(n-d-1)$ содержит в себе открытое по Зарисскому плотное подмножество грассманиана $\mathrm{Gr}(n-d, V)$.

Соображения размерности позволяют сказать и больше. Повторяя предыдущее рассуждение для $(n-d)$-мерных подпространств $H'$ вместо $(n-d-1)$-мерных, мы получим неприводимое проективное многообразие $\Gamma' \stackrel{\text{def}}{=} \{(x, H') \in X \times \mathrm{Gr}(n-d+1, V) \mid x \in H\}$ размерности $\dim X + \dim \mathrm{Gr}(n-d, n) = d + d(n-d) = d(n-d+1)$. Так как $X \cap H' \neq \varnothing$ для всех $H'$, проекция $\pi_2 : \Gamma' \twoheadrightarrow \mathrm{Gr}(n-d+1, V)$ эпиморфна, и её общий слой[1] имеет по теор. 11.1 размерность $\dim \Gamma - \dim \mathrm{Gr}(n-d+1, n+1) = d(n-d+1) - (n-d+1)d = 0$. Это означает, что общая $d$-мерная плоскость $H'$ пересекает $X$ по конечному числу точек.

Беря одну из таких плоскостей $H'$ и проводя внутри неё $(n-d-1)$-мерную плоскость $H$ через одну из точек пересечения $p \in X \cap H'$, мы видим, что $H \cap X$ конечно и непусто. Это означает, что у проекции $\pi_2 : \Gamma \to \mathrm{Gr}(n-d, V)$ первого многообразия инцидентности (11-10) имеется нульмерный слой. Тем самым, минимальная размерность непустого слоя этой проекции нулевая, откуда по теор. 11.1 вытекает, что $\dim \pi_2(\Gamma) = \dim \Gamma = \dim \mathrm{Gr}(n-d, V) - 1$, т. е. пересекающие $X$ подпространства размерности $(n-d-1)$ образуют неприводимую гиперповерхность[2] в грассманиане.

Упражнение 11.17. Выведите отсюда, что существует неприводимый многочлен от плюккеровых координат $(n-d-1)$-мерного подпространства в $\mathbb{P}_n$, обращение которого в нуль на данном подпространстве $H$ равносильно тому, что $H \cap X \neq \varnothing$.

Проделанные рассуждения иллюстрируют стандартный метод подсчёта размерностей при помощи многообразий инцидентности, часто используемый в геометрии.

Пример 11.10 (результант)

Фиксируем $d_0, d_1, \dots, d_n \in \mathbb{N}$ и обозначим через $\mathbb{P}_{N_i} = \mathbb{P}\left(S^{d_i} V^*\right)$ пространство проективных гиперповерхностей степени $d_i$ в $\mathbb{P}_n = \mathbb{P}(V)$, как в n° 11.3 на стр. 157. Покажем, что результантное многообразие $\mathcal{R} = \{(S_0, S_1, \dots, S_n) \in \mathbb{P}_{N_0} \times \mathbb{P}_{N_1} \times \dots \times \mathbb{P}_{N_n} \mid \cap S_i \neq \varnothing\}$ системы из $(n+1)$ однородных полиномиальных уравнений на $n+1$ неизвестных, является неприводимой гиперповерхностью[3] в $\mathbb{P}_{N_0} \times \dots \times \mathbb{P}_{N_n}$. Для этого рассмотрим многообразие инцидентности

$$\Gamma \stackrel{\text{def}}{=} \{(S_1, \dots, S_n,\ p) \in \mathbb{P}_{N_0} \times \dots \times \mathbb{P}_{N_n} \times \mathbb{P}_n \mid p \in \cap S_i\}.$$

[1] Т. е. любой слой над точкой из некоего плотного открытого подмножества в грассманиане.

[2] Т. е. подмногообразие коразмерности 1.

[3] Т. е. существует такой неприводимый многочлен от коэффициентов уравнений, что его обращение в нуль на наборе многочленов $f_0, f_1, \dots, f_n$ равносильно существованию ненулевого решения у системы полиномиальных уравнений $f_i(x_0, x_1, \dots, x_n) = 0$. Этот многочлен называется *результантом* рассматриваемой системы.

Упражнение 11.18. Убедитесь, что $G$ является проективным алгебраическим многообразием.

Поскольку уравнение $f(p) = 0$ линейно по $f$, проективные гиперповерхности степени $d_i$, проходящие через заданную точку $p \in \mathbb{P}_n$, образуют гиперплоскость в пространстве $\mathbb{P}_{N_i}$. Поэтому проекция $\pi_2 : \Gamma \twoheadrightarrow \mathbb{P}_n$ сюрьективна, а все её слои являются произведениями проективных гиперплоскостей и имеют одинаковую размерность $\sum(N_i - 1) = \sum N_i - n - 1$. Поэтому $\Gamma$ является неприводимым проективным многообразием размерности $\sum N_i - 1$.

Упражнение 11.19. Предъявите в $\mathbb{P}_n$ набор из $n + 1$ гиперповерхностей $S_i$ заданных степеней $d_i$, пересекающихся ровно в одной точке.

Из упражнения вытекает, что у проекции $\pi_1 : \Gamma \to \mathbb{P}_{N_0} \times \mathbb{P}_{N_1} \times \cdots \times \mathbb{P}_{N_n}$ имеется нульмерный слой. Поэтому общий непустой слой тоже нульмерен, и $\dim \pi_1(\Gamma) = \dim \Gamma$. Тем самым, $\pi_1(\Gamma)$ является неприводимой гиперповерхностью в $\mathbb{P}_{N_0} \times \cdots \times \mathbb{P}_{N_n}$.

Упражнение 11.20. Покажите, что всякое неприводимое подмногообразие коразмерности 1 в произведении проективных пространств задаётся неприводимым многочленом от однородных координат, однородным по координатам каждого из проективных пространств.

Пример 11.11 (прямые на поверхностях)

Множество всех поверхностей данной степени $d$ в $\mathbb{P}_3 = \mathbb{P}(V)$ образует проективное пространство $\mathbb{P}_N = \mathbb{P}(S^d V^*)$ размерности $N = \frac{1}{6}(d+1)(d+2)(d+3) - 1$. Множество всех прямых в $\mathbb{P}_3 = \mathbb{P}(V)$ представляет собою грассманиан $\mathrm{Gr}(2,4) = \mathrm{Gr}(2,V)$, изоморфный гладкой четырёхмерной квадрике в $\mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$. Обозначим через $\Gamma \overset{\text{def}}{=} \{(S,\ell) \in \mathbb{P}_N \times \mathrm{Gr}(2,4) \mid \ell \subset S\}$ многообразие инцидентности между прямыми и поверхностями.

Упражнение 11.21. Убедитесь, что $\Gamma \subset \mathbb{P}_N \times \mathrm{Gr}(2,4)$ является проективным алгебраическим многообразием.

Покажем, что проекция $\pi_2 : \Gamma \twoheadrightarrow Q_P$ сюрьективна и все её слои являются проективными пространствами одинаковой размерности. Прямая $\ell$, заданная уравнениями $x_0 = x_1 = 0$, лежит на поверхности $V(f)$ если и только если $f = x_2 \cdot g + x_3 \cdot h$ лежит в образе линейного отображения

$$\psi : S^{d-1}V^* \oplus S^{d-1}V^* \to S^d V^* , \ (g,h) \mapsto x_2 g + x_3 h ,$$

который изоморфен фактору пространства $S^{d-1}V^* \oplus S^{d-1}V^*$ размерности $\frac{1}{3} d(d+1)(d+2)$ по подпространству $\ker \psi = \{(g,h) = (x_3 q, -x_2 q) \mid q \in S^{d-2}V^*\}$ размерности $\frac{1}{6}(d-1)d(d+1)$. Поэтому содержащие $\ell$ поверхности составляют проективное пространство размерности

$$\frac{1}{6}\Big( 2\, d(d+1)(d+2) - (d-1)d(d+1) \Big) - 1 = \frac{1}{6}\, d(d+1)(d+5) - 1 .$$

Мы заключаем, что $\Gamma$ является неприводимым проективным многообразием размерности

$$\dim \Gamma = \frac{1}{6}\, d(d+1)(d+5) + 3 .$$

Проекция $\pi_1(\Gamma) \subset \mathbb{P}_N$ представляет собою множество поверхностей, содержащих хотя бы одну прямую. Из предыдущего вытекает, что это замкнутое неприводимое многообразие.

Упражнение 11.22. Для каждого $d \geqslant 3$ предъявите поверхность степени $d$ в $\mathbb{P}_3$, содержащую конечное число прямых.

Из упражнения вытекает, что у проекции $\pi_1$ имеется непустой 0-мерный слой. Поэтому её общий непустой слой тоже нульмерен, и $\dim \pi_1(\Gamma) = \dim \Gamma$. Так как разность

$$N - \dim \Gamma = \frac{1}{6}\left((d+1)(d+2)(d+3) - d(d+1)(d+5)\right) - 4 = d - 3\,,$$

мы заключаем, что на каждой кубической поверхности в $\mathbb{P}_3$ есть прямая, причём на общей кубической поверхности лежит конечное число прямых, а на общей поверхности степени не менее четырёх прямых вообще нет.

**12.1. Конечные расширения.** Поле $\mathbb{F}$, конечномерное как векторное пространство над своим под полем $\Bbbk \subset \mathbb{F}$, называется *конечным расширением* поля $\Bbbk$. Размерность $\dim_{\Bbbk} \mathbb{F}$ этого векторного пространства называется *степенью* поля $\mathbb{F}$ над $\Bbbk$ и обозначается $\deg \mathbb{F}/\Bbbk$ или $[\mathbb{F} : \Bbbk]$.

Упражнение 12.1. Пусть расширения полей $\Bbbk \subset \mathbb{K} \subset \mathbb{F}$ конечны и $f_1, \dots, f_m \in \mathbb{F}$ составляют базис $\mathbb{F}$ как векторного пространства над $\mathbb{K}$, а $t_1, \dots, t_n \in \mathbb{K}$ — базис $\mathbb{K}$ над $\Bbbk$. Покажите, что $mn$ произведений $f_i t_j$ составляют базис $\mathbb{F}$ над $\Bbbk$. В частности,

$$\deg \mathbb{F}/\Bbbk = \deg \mathbb{F}/\mathbb{K} \cdot \deg \mathbb{K}/\Bbbk. \tag{12-1}$$

Поскольку целость и алгебраичность элемента над полем означают одно и то же, из доказанных в n° 9.1 на стр. 128 свойств целых элементов вытекает, что всякая коммутативная $\Bbbk$-алгебра $A$, конечномерная как векторное пространство над $\Bbbk$, алгебраична над $\Bbbk$, и если в $A$ нет делителей нуля, то $A$ является полем. Наоборот, любое поле $\mathbb{K} \supset \Bbbk$, конечно порождённое как $\Bbbk$-алгебра, является конечным расширением поля $\Bbbk$. В частности, любая конечно порождённая $\Bbbk$-подалгебра $\Bbbk[a_1, \dots, a_m]$ в любом поле $\mathbb{F} \supset \Bbbk$ конечной степени над $\Bbbk$ тоже является полем конечной степени над $\Bbbk$, причём эта степень делит $\deg \mathbb{F}/\Bbbk$ по упр. 12.1.

Упражнение 12.2. Убедитесь, что любое конечное поле $\mathbb{F}$ имеет положительную характеристику $\operatorname{char}(\mathbb{F}) = p > 0$, является конечным расширением своего простого подполя[1] $\mathbb{F}_p = \mathbb{Z}/(p)$ и имеет порядок $|\mathbb{F}| = p^{[\mathbb{F}:\mathbb{F}_p]}$.

**12.1.1. Примитивные расширения.** Для любого отличного от константы неприводимого многочлена $f \in \Bbbk[x]$ алгебра $\Bbbk[x]/(f)$ не имеет делителей нуля и $n$-мерна над $\Bbbk$. Поэтому она является полем. Элементы этого поля однозначно записываются в виде $b_0 + b_1\vartheta + \dots + b_{n-1}\vartheta^{n-1}$, где $b_i \in \Bbbk$, а класс $\vartheta = x \pmod f$ является корнем многочлена $f$. Поле $\Bbbk[x]/(f)$ называется *примитивным* расширением поля $\Bbbk$, полученным *присоединением* к полю $\Bbbk$ корня $\vartheta$ неприводимого многочлена $f$. Если понятно, какой многочлен $f$ имеется в виду, примитивное расширение $\Bbbk[x]/(f)$ часто обозначают[2] $\Bbbk[\vartheta]$ или $\Bbbk(\vartheta)$. Так, запись $\Bbbk\left[\sqrt[m]{a}\right]$ по определению означает примитивное расширение $\Bbbk[x]/(x^m - a)$, где $a \in \Bbbk$ таков, что многочлен $x^m - a$ неприводим в $\Bbbk[x]$.

Пример 12.1 (кубические расширения)
Для любого поля $\Bbbk$ и неприводимого над $\Bbbk$ многочлена $f = x^3 + a_1x^2 + a_2x + a_3 \in \Bbbk[x]$ поле $\mathbb{K} = \Bbbk[x]/(f)$ имеет степень 3 над $\Bbbk$ и его элементы однозначно записываются в виде $b_0 + b_1\vartheta + b_2\vartheta^2$, где $b_i \in \Bbbk$, а $\vartheta \in \mathbb{K}$ означает класс $x \pmod f$. Такие записи перемножаются и складываются по стандартным правилам раскрытия скобок с учётом соотношения $f(\vartheta) = 0$.

Упражнение 12.3. Пусть $\Bbbk = \mathbb{Q}$ и $f(x) = x^3 + x + 1$. Запишите $(1 + 2\vartheta)^{-1}$ и $(1 + \vartheta + \vartheta^2)^{-1}$ в виде $b_0 + b_1\vartheta + b_2\vartheta^2$.

Так как $f(\vartheta) = 0$, многочлен $f(x)$ раскладывается в $\mathbb{K}[x]$ в произведение $f(x) = (x - \vartheta) \cdot q(x)$, где квадратный трёхчлен $q(x) = x^2 + c_1x + c_2 \in \mathbb{K}[x]$ либо приводим над $\mathbb{K}$, и тогда

$$q(x) = (x - \vartheta_1)(x - \vartheta_2) \tag{12-2}$$

[1] Напомню, что *простым подполем* поля $\mathbb{F}$ называется наименьшее по включению подполе в $\mathbb{F}$, см. раздел 2.8.1 на стр. 32 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_02.pdf.

[2] Однако без явного указания многочлена $f$ обозначение $\Bbbk[\vartheta]$ мало осмысленно.

для некоторых $\vartheta_1, \vartheta_2 \in \mathbb{K}$, либо неприводим, и тогда разложение (12-2) пишется лишь над квадратичным расширением $\mathbb{L} = \mathbb{K}[x]/(q)$ поля $\mathbb{K}$, степень которого над исходным полем $\Bbbk$ равна 6. Чтобы выяснить, какой из этих двух случаев имеет место, заметим, что *дискриминант*[1]

$$D(f) = (\vartheta - \vartheta_1)^2(\vartheta - \vartheta_2)^2(\vartheta_1 - \vartheta_2)^2 = q^2(\vartheta) \cdot D(q)\,, \tag{12-3}$$

будучи симметрическим многочленом от корней, является многочленом от коэффициентов $f$ и лежит в $\Bbbk$.

Упражнение 12.4. Убедитесь, что $D(x^2 + px + q) = p^2 - 4q$, а $D(x^3 + px + q) = -4\,p^3 - 27\,q^2$.

Приводимость $q$ в $\mathbb{K}[x]$ равносильна тому, что $D(q) = (\vartheta_1 - \vartheta_2)^2$ является квадратом в $\mathbb{K}$. Согласно (12-3), это эквивалентно тому, что квадратом в $\mathbb{K}$ является $D(f)$. Но если $D(f)$ квадрат в $\mathbb{K}$, то он квадрат и в $\Bbbk$: иначе многочлен $x^2 - D(f)$ был неприводим над $\Bbbk$, и квадратичное расширение $\Bbbk[x]/\big(x^2 - D(f)\big)$ поля $\Bbbk$ вкладывалось бы в поле $\mathbb{K}$ по правилу $x \bmod \big(x^2 - D(f)\big) \mapsto \sqrt{D(f)} \in \mathbb{K}$, что невозможно по упр. 12.1, так как $\deg \mathbb{K}/\Bbbk = 3$. Итак, неприводимый кубический многочлен $f \in \Bbbk[x]$ тогда и только тогда полностью разлагается на линейные множители над кубическим расширением $\Bbbk[x]/(f)$, когда $D(f)$ квадрат в $\Bbbk$.

Упражнение 12.5. Покажите, что следующие три условия на вещественный трёхчлен $f(x) = x^3 + px + q \in \mathbb{R}[x]$ попарно эквивалентны: а) $D(f) > 0$ б) все комплексные корни $f$ вещественны в) при некотором $\lambda \in \mathbb{R}$ подстановка $x = \lambda t$ превращает уравнение $f(x) = 0$ в уравнение $4\,t^3 - 3\,t = c$ с $|c| \leqslant 1$, корнем которого является $x = \cos\big(\frac{1}{3}\,\arccos(c)\big)$.

**12.1.2. Сепарабельность.** Если в рассмотренном выше прим. 12.1 характеристика исходного поля $\Bbbk$ равна 3, некоторые из корней $\vartheta$, $\vartheta_1$ и $\vartheta_2$ многочлена $f$ могут совпасть, хотя он и *неприводим* над $\Bbbk$. Скажем, над полем $\Bbbk = \mathbb{F}_3(t)$ рациональных функций с коэффициентами в поле $\mathbb{F}_3 = \mathbb{Z}/(3)$ многочлен $f(x) = x^3 - t \in \Bbbk[x]$ неприводим, так как не имеет корней в $\Bbbk$, однако над примитивным расширением $\mathbb{K} = \Bbbk\big[\sqrt[3]{t}\big] = \Bbbk[x]/(f)$ он становится полным кубом[2]: $x^3 - t = \Big(x - \sqrt[3]{t}\Big)^3$.

Определение 12.1

Многочлен $f \in \Bbbk[x]$ называется *сепарабельным*, если у него нет кратных корней ни в каком расширении $\mathbb{K} \supset \Bbbk$. Алгебраическое расширение $\mathbb{F} \supset \Bbbk$ (возможно, бесконечное) называется *сепарабельным*, если минимальный над $\Bbbk$ многочлен $\mu_\vartheta \in \Bbbk[x]$ любого элемента $\vartheta \in \mathbb{F} \smallsetminus \Bbbk$ сепарабелен.

Упражнение 12.6. Покажите, что корень $\alpha \in \mathbb{F} \supset \Bbbk$ многочлена $f \in \Bbbk[x]$ является кратным если и только если $f'(\alpha) = 0$.

Тем самым, многочлен $f \in \Bbbk[x]$ сепарабелен если и только если нод$(f, f') = 1$, и это условие проверяемо при помощи алгоритма Евклида над исходным полем $\Bbbk$.

Упражнение 12.7. Убедитесь, что все неприводимые многочлены над любым полем характеристики нуль сепарабельны.

[1] Напомню, что *дискриминантом* приведённого многочлена $f(x) = \prod(x - \vartheta_i)$ называется произведение $D(f) \overset{\text{def}}{=} \prod_{i<j}(\vartheta_i - \vartheta_j)^2$ квадратов разностей его корней.

[2] Напомню, что $(a + b)^3 = a^3 + b^3$ в любом поле характеристики 3.

Пример 12.2 (сепарабельность конечных полей)
Если многочлен $f$ неприводим, то он не может иметь отличных от констант общих делителей ни с каким ненулевым многочленом меньшей степени. Поэтому неравенство нод$(f,f') \neq 1$ возможно только когда $f' = 0$. Над полем $\Bbbk$ характеристики $p$ это равенство означает, что показатели всех мономов, входящих в $f$ с ненулевым коэффициентом, делятся на $p$. Для простого поля $\Bbbk = \mathbb{F}_p = \mathbb{Z}/(p)$, в котором $a^p = a$ для каждого $a \in \Bbbk$, последнее условие означает, что многочлен $f(x) = a_n x^{np} + \dots + a_1 x^p + a_0 = a_n^p x^{np} + \dots + a_1^p x^p + a_0^p = (a_n x^n + \dots + a_1 x + a_0)^p$ является чистой $p$-той степенью. Поэтому все неприводимые многочлены над $\mathbb{F}_p$ сепарабельны. В частности, каждое конечное поле сепарабельно над своим простым подполем.

Упражнение 12.8. Пусть $\Bbbk = \mathbb{F}_p(t)$. Покажите что многочлен $f(x) = x^p - t \in \Bbbk[x]$ неприводим над $\Bbbk$ и несепарабелен.

Пример 12.3 (корни из единицы)
Корни уравнения $x^n = 1$ в произвольном поле $\Bbbk$ образуют конечную мультипликативную подгруппу, которая обозначается $\boldsymbol{\mu}_n(\Bbbk)$ и называется *группой корней $n$-той степени из единицы* поля $\Bbbk$. Как и всякая конечная мультипликативная подгруппа в поле, группа $\boldsymbol{\mu}_n(\Bbbk)$ циклическая. Если её порядок равен $n$, то говорят, что поле $\Bbbk$ *содержит все* $\sqrt[n]{1}$, и буде это так, образующие группы $\boldsymbol{\mu}_n(\Bbbk) \simeq \mathbb{Z}/(n)$ называются *первообразными корнями* степени $n$ из единицы. Всего имеется $\varphi(n)$ первообразных корней, и если $\zeta \in \Bbbk$ — один из них, все степени $\zeta^m$ с $0 \leqslant m \leqslant n-1$ различны. Поэтому следующие три условия эквивалентны: (1) поле $\Bbbk$ допускает расширение, содержащее все $\sqrt[n]{1}$; (2) многочлен $x^n - 1$ сепарабелен над $\Bbbk$; (3) $\operatorname{char}(\Bbbk)$ не делит $n$. При выполнении этих условий каждый многочлен $f(x) = x^n - a$ с ненулевым $a \in \Bbbk$ сепарабелен, так как $f'(x) = nx^{n-1}$ имеет единственный корень нуль, не являющийся корнем $f$.

Лемма 12.1
Любое конечное расширение $\mathbb{F} \supset \Bbbk$ можно получить в качестве верхнего этажа башни

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F} \tag{12-4}$$

примитивных расширений $\mathbb{L}_i = \mathbb{L}_{i-1}[x]/(f_i)$, где $f_i \in \mathbb{L}_{i-1}[x]$ неприводим над $\mathbb{L}_{i-1}$.

Доказательство. Пусть поле $\mathbb{L}_i \subset \mathbb{F}$ уже построено. Если $\mathbb{L}_i \neq \mathbb{F}$, возьмём в качестве $f_{i+1} \in \mathbb{L}_i[x]$ минимальный многочлен любого элемента $\vartheta \in \mathbb{F} \smallsetminus \mathbb{L}_i$ над полем $\mathbb{L}_i$ и вложим примитивное расширение $\mathbb{L}_i[x]/(f)$ в поле $\mathbb{F}$ по правилу $x \pmod f \mapsto \vartheta$. Обозначим через $\mathbb{L}_{i+1} \supsetneq \mathbb{L}_i$ образ этого вложения. Поскольку степень поля $\mathbb{F}$ над $\mathbb{L}_{i+1}$ строго меньше, чем над $\mathbb{L}_i$, через конечное число шагов оно исчерпается. □

Лемма 12.2
Для любого многочлена $f \in \Bbbk[x]$ существует конечное расширение $\mathbb{F} \supset \Bbbk$, над которым $f$ полностью раскладывается на линейные множители.

Доказательство. Разложим $f$ в $\Bbbk[x]$ на неприводимые множители. Если хоть один из них, назовём его $q$, не линеен, перейдём от $\Bbbk$ к расширению $\mathbb{K} = \Bbbk[x]/(q) \supset \Bbbk$ и повторим процедуру. Поскольку над $\mathbb{K}$ многочлен $f$ имеет строго большее число линейных множителей, чем над $\Bbbk$, после нескольких таких итераций мы получим требуемое расширение. □

Теорема 12.1 (теорема о примитивном элементе)
Всякое конечное сепарабельное расширение $\mathbb{K} \supset \Bbbk$ примитивно, т. е. имеет вид $\mathbb{K} = \Bbbk[x]/(f)$, где $f \in \Bbbk[x]$ — неприводимый многочлен степени $\deg \mathbb{K}/\Bbbk$.

Доказательство. Если поле $\Bbbk$ конечно, поле $\mathbb{K}$ тоже конечно, и его ненулевые элементы образуют циклическую мультипликативную группу. Если $\vartheta \in \mathbb{K}$ — образующая этой группы[1], то $\mathbb{K} = \Bbbk[\vartheta]$. Поэтому далее мы считаем поле $\Bbbk$ бесконечным. Индукция по длине башни из лем. 12.1 сводит теорему к случаю, когда поле $\mathbb{K} = \Bbbk[\alpha, \beta] \supset \Bbbk[\alpha] \supset \Bbbk$ является башней двух примитивных расширений и как $\Bbbk$-алгебра порождается двумя сепарабельными алгебраическими элементами $\alpha, \beta$. Мы собираемся подобрать $t \in \Bbbk^*$ так, чтобы порождённая над $\Bbbk$ элементом $\vartheta = \alpha + t\beta$ подалгебра $\Bbbk[\vartheta] \subset \mathbb{K}$ совпала со всем полем $\mathbb{K}$. Так как $\vartheta$ алгебраичен над $\Bbbk$, алгебра $\Bbbk[\vartheta]$ является полем. Достаточно добиться того, чтобы в это поле попал элемент $\beta$: тогда и $\alpha = \vartheta - t\beta$ тоже будет в нём лежать. Обозначим через $f_\alpha(x)$ и $f_\beta(x)$ минимальные многочлены элементов $\alpha$ и $\beta$ над полем $\Bbbk$. Элемент $\beta$ является общим корнем многочлена $f_\beta(x) \in \Bbbk[x]$ и многочлена $g(x) = f_\alpha(\vartheta - tx)$, коэффициенты которого лежат в зависящем от параметра $t$ поле $\Bbbk[\vartheta]$. Рассмотрим любое поле $\mathbb{F} \supset \mathbb{K}$, над которым $f_\alpha$ и $f_\beta$, а с ними и $g$, полностью разлагаются на линейные множители. Если $t$ таков, что $\beta$ является единственным общим корнем многочленов $f_\beta$ и $g$ в поле $\mathbb{F}$, то выразив $(x - \beta) = \text{нод}\big(f_\beta(x), g(x)\big)$ через многочлены $f_\beta$ и $g$ по алгоритму Евклида, мы получим искомое представление элемента $\beta$ в виде рациональной функции от лежащих в $\Bbbk[\vartheta]$ коэффициентов этих многочленов. Пусть $\deg f_\alpha = m$, $\deg f_\beta = \deg g = k$. Обозначим через $\alpha_1, \dots, \alpha_m$ и $\beta_1, \dots, \beta_k$ корни многочленов $f_\alpha$ и $f_\beta$ в $\mathbb{F}$, считая, что $\alpha = \alpha_1$ и $\beta = \beta_1$. Тогда корни $g$ суть $(\vartheta - \alpha_i)/t = \beta_1 + (\alpha_1 - \alpha_i)/t$, где $1 \leqslant i \leqslant m$. Мы хотим, чтобы $\beta_j \neq \beta_1 + (\alpha_1 - \alpha_i)/t$ для всех $i, j$ кроме $i = j = 1$. В силу сепарабельности элемента $\alpha$ разность $\alpha_1 - \alpha_i \neq 0$ при $i \neq 1$. Поэтому каждое неравенство с $i \neq 1$ запрещает ровно одно значение $t = (\beta_j - \beta_1)/(\alpha_1 - \alpha_i)$. При $i = 1$ запреты означают, что $\beta_1 \neq \beta_j$ при $j \neq 1$, и это так в силу сепарабельности $\beta$. Тем самым, исключается лишь конечное множество значений $t$, что и доказывает теорему для бесконечного поля $\Bbbk$. □

Следствие 12.1
Если поле $\mathbb{K}$ является сепарабельным алгебраическим расширением поля $\Bbbk$ и степени всех его элементов[2] ограничены, то $\mathbb{K}$ конечно над $\Bbbk$, и $\deg \mathbb{K}/\Bbbk = \max_{\vartheta \in \mathbb{K}} \deg_\Bbbk \vartheta$.

Доказательство. Если $\beta \in \mathbb{K}$ не лежит в примитивном расширении $\Bbbk[\alpha] \supset \Bbbk$, порождённом каким-либо другим элементом $\alpha \in \mathbb{K}$, то $[\Bbbk[a, \beta] : \Bbbk] > \deg_\Bbbk \alpha$, и степень примитивного элемента поля $\Bbbk[\alpha, \beta]$ строго больше $\deg \alpha$. Поэтому подполе в $\mathbb{K}$, порождённое элементом максимальной степени, совпадает со всем $\mathbb{K}$. □

**12.2. Продолжение гомоморфизмов.** Поскольку у полей нет ненулевых собственных идеалов, все ненулевые гомоморфизмы полей в кольца инъективны. Каждое вложение полей $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ продолжается до вложения колец многочленов $\Bbbk[x] \hookrightarrow \mathbb{F}[x]$, переводящего многочлен $f \in \Bbbk[x]$ в многочлен $f^\varphi \in \mathbb{F}[x]$, получающийся из $f \in \Bbbk[x]$ применением $\varphi$ к каждому коэффициенту $f$.

[1] Это рассуждение показывает, что каждое конечное поле как алгебра над любым своим подполем всегда порождается одним элементом — образующей своей мультипликативной группы. Хотя сепарабельность не использовалась в нашем рассуждении явно, в прим. 12.2 мы видели, что все конечные поля сепарабельны над своими простыми подполями.

[2] Напомню, что *степенью* алгебраического элемента называется степень его минимального многочлена.

Лемма 12.3
Пусть $\mathbb{K} = \Bbbk[x]/(f)$ — примитивное расширение поля $\Bbbk$ степени $d = \deg f = [\mathbb{K} : \Bbbk]$, и $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ — любое вложение $\Bbbk$ в произвольное поле. Вложения $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, совпадающие с $\varphi$ на подполе $\Bbbk \subset \mathbb{K}$, находятся в канонической биекции с корнями многочлена $f^{\varphi}$ в поле $\mathbb{F}$. В частности, таких вложений не более $d$, и их ровно $d$ если и только если многочлен $f^{\varphi}$ полностью раскладывается над $\mathbb{F}$ в произведение $d$ попарно разных линейных множителей.

Доказательство. Каждый элемент $\alpha \in \mathbb{F}$ задаёт гомоморфизм $\varphi_\alpha : \Bbbk[x] \to \mathbb{F}$, $g(x) \mapsto g^{\varphi}(\alpha)$. Если $\alpha$ является корнем многочлена $f^{\varphi} \in \mathbb{F}[x]$, то $f \in \ker \varphi_\alpha$, и $\varphi_\alpha$ корректно факторизуется до вложения полей $\widetilde{\varphi}_\alpha : \Bbbk[x]/(f) \hookrightarrow \mathbb{F}$, переводящего примитивный элемент $\vartheta = x \pmod{f}$ поля $\mathbb{K}$ в $\alpha \in \mathbb{F}$. При этом разные корни $\alpha \neq \beta$ задают разные вложения $\widetilde{\varphi}_\alpha \neq \widetilde{\varphi}_\beta$. С другой стороны, любое вложение $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, совпадающее с $\varphi$ на подполе $\Bbbk \subset \mathbb{K}$, переводит $\vartheta$ в некоторый корень многочлена $f^{\varphi}$, так как $f^{\varphi}\left(\widetilde{\varphi}(\vartheta)\right) = \widetilde{\varphi}\big(f(\vartheta)\big) = \varphi(0) = 0$. Поэтому $\widetilde{\varphi}$ совпадает с одним из вложений $\widetilde{\varphi}_\alpha$. □

Лемма 12.4
Пусть алгебраическое расширение[1] $\mathbb{K} \supset \Bbbk$ и вложение $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ таковы, что для любого элемента $\vartheta \in \mathbb{K}$ с минимальным над $\Bbbk$ многочленом $\mu_\vartheta \in \Bbbk[x]$ многочлен $\mu_\vartheta^{\varphi} \in \mathbb{F}[x]$ полностью раскладывается в $\mathbb{F}[x]$ на линейные множители. Тогда для любого элемента $\vartheta \in \mathbb{K}$ и любого корня $\xi \in \mathbb{F}$ многочлена $\mu_\vartheta^{\varphi}$ существует такое совпадающее с $\varphi$ на подполе $\Bbbk$ вложение $\widetilde{\varphi} : \mathbb{K} \hookrightarrow \mathbb{F}$, что $\widetilde{\varphi}(\vartheta) = \xi$.

Доказательство. По лем. 12.3 вложение $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ продолжается до вложения $\varphi_\xi : \Bbbk[\vartheta] \hookrightarrow \mathbb{F}$, переводящего $\vartheta$ в $\xi$. Множество всех продолжений $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$ отображения $\varphi_\xi$ на всевозможные подполя $\Bbbk[\vartheta] \subseteq \mathbb{L} \subseteq \mathbb{K}$ непусто, ибо содержит $\varphi_\xi$, и частично упорядочено отношением $(\mathbb{L}'', \psi'') \geqslant (\mathbb{L}', \psi')$ когда $\mathbb{L}'' \supseteq \mathbb{L}'$ и $\psi''|_{\mathbb{L}'} = \psi'$.

Упражнение 12.9. Убедитесь, что этот чум удовлетворяет условиям леммы Цорна.

Покажем, что его максимальный элемент $\psi : \mathbb{L} \hookrightarrow \mathbb{F}$ имеет область определения $\mathbb{L} = \mathbb{K}$. Если имеется элемент $\vartheta \in \mathbb{K} \smallsetminus \mathbb{L}$, то его минимальный многочлен $\mu_\vartheta \in \Bbbk[x]$ над полем $\Bbbk$ делится в $\mathbb{L}[x]$ на его минимальный многочлен $\mu_{\vartheta,\mathbb{L}}$ над полем $\mathbb{L}$. Коль скоро многочлен $\mu_\vartheta^{\varphi}$ полностью раскладывается в $\mathbb{F}[x]$ на линейные множители, его делитель $\mu_{\vartheta,\mathbb{L}}^{\varphi}$ тоже обладает этим свойством. Поэтому к примитивному расширению $\mathbb{L} \subset \mathbb{L}[\vartheta]$ применима лем. 12.3, и вложение $\psi$ продолжается на строго большее подполе $\mathbb{L}[\vartheta] = \mathbb{L}[x]/(\mu_{\vartheta,\mathbb{L}})$. □

Предложение 12.1
Если расширение $\mathbb{K} \supset \Bbbk$ конечно, то вложение полей $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ продолжается до вложения $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ не более, чем $[\mathbb{K} : \Bbbk]$ различными способами. Наличие ровно $[\mathbb{K} : \Bbbk]$ продолжений равносильно тому, что расширение $\mathbb{K} \supset \Bbbk$ сепарабельно и образ $\mu_\vartheta^{\varphi} \in \mathbb{F}[x]$ минимального над $\Bbbk$ многочлена $\mu_\vartheta \in \Bbbk[x]$ любого элемента $\vartheta \in \mathbb{K}$ полностью раскладывается в $\mathbb{F}[x]$ на линейные множители.

Доказательство. Разложим $\mathbb{K}$ в башню (12-4) примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{F}, \tag{12-5}$$

[1] Не обязательно конечное.

где $\mathbb{L}_i = \mathbb{L}_{i-1}[\vartheta_i] \simeq \mathbb{L}_{i-1}[x]/(f_i)$ и многочлен $f_i \in \mathbb{L}_{i-1}[x]$ является минимальным над $\mathbb{L}_{i-1}$ многочленом элемента $\vartheta_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_{i-1}$. Ограничения продолжающего $\varphi$ вложения $\psi : \mathbb{K} \hookrightarrow \mathbb{F}$ на подполя $\mathbb{L}_i \subset \mathbb{K}$ образуют цепочку последовательно продолжающих друг друга вложений $\psi_i : \mathbb{L}_i \hookrightarrow \mathbb{F}$. Так как по лем. 12.3 каждый шаг этой цепочки можно осуществить не более, чем $\deg f_i = [\mathbb{L}_i : \mathbb{L}_{i-1}]$ способами, продолжающих $\varphi$ вложений $\psi$ имеется не более $\prod_i [\mathbb{L}_i : \mathbb{L}_{i-1}] = [\mathbb{K} : \Bbbk]$, и их будет ровно столько если и только если каждый многочлен $f_i^{\varphi}$ имеет $\deg f_i$ различных корней в поле $\mathbb{F}$. Поскольку башню (12-5) можно начать присоединением любого элемента $\vartheta = \vartheta_1 \in \mathbb{K}$, из наличия $[\mathbb{K} : \Bbbk]$ продолжений вытекает, что образ $\mu_{\vartheta}^{\varphi}$ минимального многочлена $\mu_{\vartheta}$ любого элемента $\vartheta \in \mathbb{K}$ раскладывается над $\mathbb{F}$ в произведение $\deg \mu_{\vartheta}$ различных линейных множителей. В частности, $\mu_{\vartheta}$ сепарабелен. Наоборот, если все элементы $\vartheta \in \mathbb{K}$ сепарабельны, а образы $\mu_{\vartheta}^{\varphi}$ их минимальных многочленов полностью раскладываются над $\mathbb{F}$ на линейные множители, то эти множители будут различны, и в любой цепочке (12-5) каждый многочлен $f_i$, будучи делителем многочлена $\mu_{\vartheta_i}$ в кольце $\mathbb{L}_{i-1}[x]$, переведётся вложением $\psi_{i-1} : \mathbb{L}_{i-1} \hookrightarrow \mathbb{F}$ в многочлен, полностью разлагающийся над $\mathbb{F}$ в произведение попарно различных линейных множителей. Поэтому вложение $\varphi : \Bbbk \hookrightarrow \mathbb{F}$ будет продолжаться вдоль такой цепочки ровно $[\mathbb{K} : \Bbbk]$ способами. □

Упражнение 12.10. Пусть в условиях предл. 12.1 поле $\mathbb{K}$ как алгебра над $\Bbbk$ порождается элементами $\xi_1, \dots, \xi_m$. Покажите, что наличие ровно $[\mathbb{K} : \Bbbk]$ продолжений равносильно тому, что каждый элемент $\xi_\nu$ сепарабелен и его минимальный многочлен полностью раскладывается в $\mathbb{F}[x]$ на линейные множители.

Предложение 12.2

Если поле $\mathbb{K} \supset \Bbbk$ алгебраично[1] над $\Bbbk$, то любое вложение $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$, тождественное на подполе $\Bbbk$, является автоморфизмом поля $\mathbb{K}$.

Доказательство. Достаточно убедиться, что $\varphi(\mathbb{K}) = \mathbb{K}$. Пусть $\vartheta \in \mathbb{K}$ имеет над $\Bbbk$ минимальный многочлен $f \in \Bbbk[x]$. Вложение $\varphi$ переводит корни многочлена $f$ в корни многочлена $f$. Поэтому $\varphi^m \vartheta = \varphi^n \vartheta$ для некоторых $m > n$, где $\varphi^k = \varphi \circ \ldots \circ \varphi$ означает $k$-кратную итерацию вложения $\varphi : \mathbb{K} \hookrightarrow \mathbb{K}$. Из инъективности $\varphi$ вытекает, что $\vartheta = \varphi^{m-n}\vartheta \in \operatorname{im}\varphi$. □

**12.3. Поле разложения и алгебраическое замыкание.** В этом разделе мы установим существование у любого поля $\Bbbk$ некоторых специальных расширений, единственных с точностью до неканонического изоморфизма, тождественно действующего на $\Bbbk$.

Определение 12.2 (поле разложения)

Поле $\mathbb{L}_f \supset \Bbbk$ называется *полем разложения* многочлена $f \in \Bbbk[x]$, если $f$ полностью раскладывается в $\mathbb{L}_f[x]$ на линейные множители, и для любого расширения $\mathbb{F} \supset \Bbbk$, в котором $f$ полностью раскладывается на линейные множители, существует вложение $\mathbb{L}_f \hookrightarrow \mathbb{F}$, тождественное на подполе $\Bbbk$.

Пример 12.4 (поле разложения кубического многочлена)

В прим. 12.1 на стр. 169 мы видели, что полем разложения неприводимого кубического многочлена $f \in \Bbbk[x]$, дискриминант $D(f)$ которого является квадратом в $\Bbbk$, служит примитивное кубическое расширение $\mathbb{K} = \Bbbk[x]/(f)$, а если $D(f)$ не квадрат в $\Bbbk$, то он не квадрат и в $\mathbb{K}$, и полем разложения $f$ в этом случае служит квадратичное расширение поля $\mathbb{K}$ при помощи $\sqrt{D(f)}$, имеющее над полем $\Bbbk$ степень 6.

[1] Но не обязательно конечно.

Теорема 12.2
У любого многочлена $f \in \Bbbk[x]$ есть поле разложения $\mathbb{L}_f$, и между любыми двумя полями разложения многочлена $f$ имеется (не канонический) изоморфизм, тождественно действующий на подполе $\Bbbk$.

Доказательство. Рассмотрим любое конечное расширение $\mathbb{F} \supset \Bbbk$, в котором $f$ полностью раскладывается на линейные множители[1], и обозначим через $\alpha_1, \dots, \alpha_m \in \mathbb{F}$ корни $f$, а через $\mathbb{L}_f$ — наименьшее подполе в $\mathbb{F}$, содержащее $\Bbbk$ и все эти корни. Поле $\mathbb{L}_f$ раскладывается в башню (12-4) примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_{k-1} \subset \mathbb{L}_k = \mathbb{L}_f \,, \tag{12-6}$$

на каждом этаже которой присоединяется какой-нибудь элемент[2] $\vartheta \in \{\alpha_1, \dots, \alpha_m\}$. Если поле $\mathbb{K} \supset \Bbbk$ таково, что $f$ полностью раскладывается над ним на линейные множители, то включение $\Bbbk \subset \mathbb{K}$ продолжается вдоль башни (12-6) до тождественного на $\Bbbk$ вложения $\mathbb{L}_f \hookrightarrow \mathbb{K}$ по лем. 12.4: минимальный многочлен каждого присоединяемого элемента $\vartheta$, будучи делителем многочлена $f$, полностью раскладываются над $\mathbb{K}$ на линейные множители. Тем самым, $\mathbb{L}_f$ является полем разложения. Для любого другого поля разложения $\mathbb{L}'_f$ имеются вложения $\varphi : \mathbb{L}_f \hookrightarrow \mathbb{L}'_f$ и $\varphi' : \mathbb{L}'_f \hookrightarrow \mathbb{L}_f$. По предл. 12.2 обе композиции $\varphi \circ \varphi'$ и $\varphi' \circ \varphi$ биективны. Поэтому каждое из вложений является изоморфизмом. □

Пример 12.5 (классификация конечных полей)
Согласно упр. 12.2 каждое конечное поле $\mathbb{F}$ характеристики $p$ является конечным расширением своего простого подполя $\mathbb{F}_p = \mathbb{Z}/(p)$ и состоит из $q = p^n$ элементов, где $n = [\mathbb{F} : \mathbb{F}_p]$. Так как ненулевые элементы поля $\mathbb{F}$ образуют конечную мультипликативную группу порядка $q-1$, все они удовлетворяют уравнению $x^{q-1} = 1$. Следовательно, элементы поля $\mathbb{F}$ суть $q$ различных корней многочлена $f(x) = x^q - x \in \mathbb{F}_p[x]$, сепарабельного, поскольку $f' = 1$. Таким образом, поле $\mathbb{F}$ является полем разложения многочлена $f$ и единственно с точностью до (не канонического) изоморфизма.

Определение 12.3 (алгебраическое замыкание)
Алгебраическое над $\Bbbk$ алгебраически замкнутое поле $\overline{\Bbbk} \supset \Bbbk$ называется *алгебраическим замыканием поля* $\Bbbk$.

Упражнение 12.11. Покажите, что любое конечное расширение $\mathbb{K} \supset \Bbbk$ допускает тождественное на $\Bbbk$ вложение в любое алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$.

Теорема 12.3
У каждого поля $\Bbbk$ есть алгебраическое замыкание, и между любыми двумя алгебраическими замыканиями поля $\Bbbk$ имеется (не канонический) изоморфизм, тождественно действующий на подполе $\Bbbk$.

---

[1] См. лем. 12.2 на стр. 171.

[2] Отметим, что число $k$ этажей башни может оказаться меньше, чем число корней $m$ многочлена $f$, поскольку присоединение очередного корня может привести к автоматическому присоединению ещё нескольких.

Доказательство. Для любых двух алгебраических замыканий $\mathbb{L}'$, $\mathbb{L}''$ поля $\Bbbk$ включение $\Bbbk \subset \mathbb{L}'$ продолжается до тождественного на $\Bbbk$ вложения $\varphi' : \mathbb{L}' \hookrightarrow \mathbb{L}''$. Симметричным образом имеется тождественное на $\Bbbk$ вложение $\varphi'' : \mathbb{L}'' \hookrightarrow \mathbb{L}'$. По предл. 12.2 композиции $\varphi' \circ \varphi''$ и $\varphi'' \circ \varphi'$ биективны. Поэтому $\varphi'$ и $\varphi''$ тоже биективны, и $\mathbb{L}' \simeq \mathbb{L}''$. Существование алгебраического замыкания устанавливается в несколько итераций. Пусть поле $\Bbbk$ содержится в алгебраически замкнутом поле $\mathbb{K}$. Тогда множество $\overline{\Bbbk}$ алгебраичных над $\Bbbk$ элементов поля $\mathbb{K}$ является полем по предл. 9.2 на стр. 129. Любой многочлен из $\overline{\Bbbk}[x] \subset \mathbb{K}[x]$ имеет корень $\vartheta$ в $\mathbb{K}$. Поскольку $\vartheta$ алгебраичен над $\overline{\Bbbk}$, он алгебраичен и над $\Bbbk$, а значит, лежит в $\overline{\Bbbk}$. Тем самым, поле $\overline{\Bbbk}$ алгебраически замкнуто и является алгебраическим замыканием поля $\Bbbk$. Остаётся убедиться в наличии какого-нибудь алгебраически замкнутого поля $\mathbb{K} \supset \Bbbk$. Сначала построим поле $\mathbb{F}_1 \supset \Bbbk$, над которым каждый многочлен $f \in \Bbbk[x]$ полностью разлагается на линейные множители. Для этого рассмотрим множество $\mathcal{L}$, элементами которого являются следующие наборы данных: (1) линейно упорядоченное множество многочленов $L \subset \Bbbk[x]$ (2) множество таких занумерованных многочленами $f \in L$ полей $\mathbb{L}_f(L) \supset \Bbbk$, что $f$ полностью разлагается на линейные множители над $\mathbb{L}_f(L)$ и $\mathbb{L}_f(L) \subseteq \mathbb{L}_g(L)$ при $f \leqslant g$. Введём на $\mathcal{L}$ частичный порядок, полагая $L_1 \leqslant L_2$ если $L_1 \subseteq L_2$ с сохранением порядка и $L_f(L_1) = L_f(L_2)$ для всех $f \in L_1$.

Упражнение 12.12. Убедитесь, что $\mathcal{L}$ является непустым полным чумом.

По лемме Цорна[1] в $\mathcal{L}$ имеется максимальный элемент $L$. Если существует отличный от константы многочлен $h \notin L$, то множество $L$ можно увеличить, добавив к нему $h$ в качестве максимального элемента и положив $\mathbb{L}_h$ равным полю разложения многочлена $h$ над полем $\bigcup_{f\in L} \mathbb{L}_f$. Таким образом, множество многочленов $L$ содержит все многочлены положительной степени, и все они полностью разлагаются на линейные множители над полем $\mathbb{F}_1 = \bigcup_{f\in L} \mathbb{L}_f$, что и требовалось. Заменяя $\Bbbk$ на $\mathbb{F}_1$ и повторяя процедуру, мы получим бесконечную цепочку вложенных полей $\Bbbk = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \dots$, в которой каждый многочлен из $\mathbb{F}_i[x]$ полностью разлагается на множители над полем $\mathbb{F}_{i+1}$. Поле $\mathbb{K} = \bigcup_i \mathbb{F}_i$ алгебраически замкнуто и содержит $\Bbbk$. ☐

Следствие 12.2

В любой башне конечных расширений $\mathbb{L}_1 \subset \mathbb{L}_2 \subset \mathbb{L}_3$ расширение $\mathbb{L}_1 \subset \mathbb{L}_3$ сепарабельно если и только если сепарабельны оба расширения $\mathbb{L}_1 \subset \mathbb{L}_2$ и $\mathbb{L}_2 \subset \mathbb{L}_3$.

Доказательство. Если поле $\mathbb{L}_3$ сепарабельно над $\mathbb{L}_1$, то сепарабельно и его подполе $\mathbb{L}_2$. Так как минимальный многочлен над $\mathbb{L}_2$ любого элемента $\vartheta \in \mathbb{L}_3$ делит сепарабельный минимальный многочлен элемента $\vartheta$ над $\mathbb{L}_1$, то $\mathbb{L}_3$ сепарабельно над $\mathbb{L}_2$. Наоборот, если оба расширения $\mathbb{L}_1 \subset \mathbb{L}_2$ и $\mathbb{L}_2 \subset \mathbb{L}_3$ сепарабельны, то по предл. 12.1 тождественное вложение $\mathbb{L}_1$ в алгебраическое замыкание $\overline{\mathbb{L}}_1$ допускает ровно $\deg \mathbb{L}_2 / \mathbb{L}_1$ продолжений до вложения $\mathbb{L}_2 \hookrightarrow \overline{\mathbb{L}}_1$, и каждое из них ровно $\deg \mathbb{L}_3 / \mathbb{L}_2$ способами продолжается до вложения $\mathbb{L}_3 \hookrightarrow \overline{\mathbb{L}}_1$, так что всего имеется $\deg \mathbb{L}_2/\mathbb{L}_1 \cdot \deg \mathbb{L}_3/\mathbb{L}_2 = \deg \mathbb{L}_3/\mathbb{L}_1$ продолжений тождественного вложения $\mathbb{L}_1 \hookrightarrow \overline{\mathbb{L}}_1$ до вложения $\mathbb{L}_3 \hookrightarrow \overline{\mathbb{L}}_1$, что по предл. 12.1 означает сепарабельность расширения $\mathbb{L}_1 \subset \mathbb{L}_3$. ☐

**12.4. Нормальные расширения.** Алгебраическое расширение $\Bbbk \subset \mathbb{K}$ называется *нормальным*, если любой неприводимый над $\Bbbk$ многочлен $f \in \Bbbk[x]$, имеющий корень в $\mathbb{K}$, полностью разлагается в $\mathbb{K}[x]$ на линейные множители.

Упражнение 12.13. Покажите, что неприводимый над $\Bbbk$ приведённый многочлен $f \in \Bbbk[x]$,

[1] См. предложение 1.5 на стр. 19 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_01.pdf.

имеющий корень $\vartheta$ в алгебраическом расширении $\mathbb{K} \supset \Bbbk$, является минимальным многочленом элемента $\vartheta$ над $\Bbbk$.

Таким образом, нормальность алгебраического расширения $\Bbbk \subset \mathbb{K}$ равносильна тому, что минимальный любого элемента $\vartheta \in \mathbb{K}$ над $\Bbbk$ полностью раскладывается в $\mathbb{K}[x]$ на линейные множители.

Упражнение 12.14. Убедитесь, что любое квадратичное расширение нормально.

Лемма 12.5
Фиксируем произвольное алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$. Алгебраическое расширение $\Bbbk \subset \mathbb{K}$ нормально тогда и только тогда, когда образы всех тождественных на $\Bbbk$ вложений $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ совпадают друг с другом.

Доказательство. По лем. 12.4 на стр. 173 существует тождественное на подполе $\Bbbk$ вложение $\mathbb{K} \hookrightarrow \overline{\Bbbk}$. Поэтому мы можем считать, что $\Bbbk \subset \mathbb{K} \subset \overline{\Bbbk}$. Любое тождественное на $\Bbbk$ вложение $\psi : \mathbb{K} \hookrightarrow \overline{\Bbbk}$ переводит каждый элемент $\vartheta \in \mathbb{K}$ в один из корней его минимального над полем $\Bbbk$ многочлена $\mu_\vartheta \in \Bbbk[x]$. Если все эти корни лежат в $\mathbb{K}$, то $\psi(\mathbb{K}) \subset \mathbb{K}$. Наоборот, по лем. 12.4 для каждого корня $\xi$ минимального многочлена $\mu_\vartheta \in \Bbbk[x]$ любого элемента $\vartheta \in \mathbb{K}$ имеется такое вложение $\psi_{\vartheta,\xi} : \mathbb{K} \hookrightarrow \overline{\Bbbk}$, что $\psi_{\vartheta,\xi}(\vartheta) = \xi$. Если образы всех этих вложений лежат в $\mathbb{K}$, то все корни минимальных многочленов элементов поля $\mathbb{K}$ лежат в $\mathbb{K}$. □

Лемма 12.6
Пусть в башне алгебраических расширений $\Bbbk \subset \mathbb{L} \subset \mathbb{K}$ поле $\mathbb{K}$ нормально над $\Bbbk$. Тогда $\mathbb{K}$ нормально и над $\mathbb{L}$, а вот $\mathbb{L}$ нормально над $\Bbbk$ если и только если образ любого тождественного на $\Bbbk$ вложения $\mathbb{L} \hookrightarrow \mathbb{K}$ совпадает с $\mathbb{L}$.

Доказательство. Минимальный над $\mathbb{L}$ многочлен любого элемента $\vartheta \in \mathbb{K}$ делит в $\mathbb{L}[x]$ минимальный многочлен элемента $\vartheta$ над $\Bbbk$, и если в $\mathbb{K}[x]$ второй из них полностью раскладывается на линейные множители, то и первый раскладывается. Поэтому $\mathbb{K}$ нормально над $\mathbb{L}$. Второе утверждение вытекает из лем. 12.5: фиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \mathbb{K} \supset \mathbb{L} \supset \Bbbk$ и заметим, что образы всех вложений $\mathbb{L} \hookrightarrow \overline{\Bbbk}$ лежат в $\mathbb{K}$, поскольку каждое такое вложение продолжается до вложения $\mathbb{K} \hookrightarrow \overline{\Bbbk}$, образ которого совпадает с $\mathbb{K}$. □

Предостережение 12.1. Башня $\mathbb{F} \supset \mathbb{L} \supset \Bbbk$ нормальных расширений $\mathbb{F} \supset \mathbb{L}$ и $\mathbb{L} \supset \Bbbk$ может не быть нормальным расширением. Например, расширение $\mathbb{Q} \subset \mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q}[x]/(x^4-2)$ раскладывается в башню квадратичных расширений $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$, каждое из которых нормально по упр. 12.14, однако само оно нормальным не является, так как четыре его вложения в алгебраическое замыкание $\overline{\mathbb{Q}} \subset \mathbb{C}$ переводят примитивный элемент $\vartheta = x \pmod{x^4-2}$ поля $\mathbb{Q}[x]/(x^4-2)$ в четыре разных комплексных корня из двойки: $\pm\sqrt[4]{2} \in \mathbb{R}$ и $\pm i\sqrt[4]{2} \notin \mathbb{R}$, и образы этих вложений суть два разных подполя в $\mathbb{C}$ — одно содержится в $\mathbb{R}$, другое нет.

Предложение 12.3
Конечное расширение $\mathbb{K} \supset \Bbbk$ нормально если и только если $\mathbb{K}$ является полем разложения некоторого многочлена[1] $f \in \Bbbk[x]$.

[1] Возможно приводимого над $\Bbbk$.

Доказательство. Пусть нормальное над $\Bbbk$ поле $\mathbb{K} \supset \Bbbk$ порождается как алгебра над $\Bbbk$ элементами $\alpha_1, \dots, \alpha_k$, и пусть $f_i \in \Bbbk[x]$ — минимальный многочлен элемента $\alpha_i$ над полем $\Bbbk$. Тогда многочлен $f = \prod f_i$ полностью раскладывается над $\mathbb{K}$ на линейные множители, и по упр. 12.10 поле $\mathbb{K}$ вкладывается в любое другое поле, над которым $f$ полностью раскладывается на линейные множители. Следовательно, $\mathbb{K}$ является полем разложения многочлена $f$. Наоборот, если $\mathbb{K} \supset \Bbbk$ является полем разложения некоторого многочлена $f \in \Bbbk[x]$, то любое тождественное на подполе $\Bbbk$ вложение $\mathbb{K}$ в фиксированное алгебраическое замыкание $\overline{\Bbbk}$ является изоморфизмом $\mathbb{K}$ на подполе $\Bbbk[\alpha_1, \dots, \alpha_k] \subset \overline{\Bbbk}$, порождённое всеми корнями $\alpha_1, \dots, \alpha_k$ многочлена $f$ в $\overline{\Bbbk}$. Поэтому $\mathbb{K}$ нормально по лем. 12.5 на стр. 177. □

**12.4.1. Композиты.** Зафиксируем алгебраическое замыкание $\overline{\Bbbk}$ поля $\Bbbk$. Для любого набора содержащих $\Bbbk$ и содержащихся в $\overline{\Bbbk}$ полей $\mathbb{K}_1, \dots, \mathbb{K}_m$ наименьшее подполе в $\overline{\Bbbk}$, которое содержит все поля $\mathbb{K}_\nu$, называется *композитом* этих полей и обозначается $\mathbb{K}_1 \dots \mathbb{K}_m$. Иначе композит можно описать как пересечение всех подполей в $\overline{\Bbbk}$, содержащих каждое из полей $\mathbb{K}_i$, или как $\Bbbk$-линейную оболочку всевозможных произведений $\vartheta_1 \dots \vartheta_m$, где $\vartheta_i \in \mathbb{K}_i$ для каждого $i$.

Предложение 12.4

Пусть поля $\mathbb{F}$ и $\mathbb{K}$ содержат $\Bbbk$ и содержатся в $\overline{\Bbbk}$. Если поле $\mathbb{K}$ нормально (соотв. сепарабельно) над $\Bbbk$, то композит $\mathbb{F}\mathbb{K}$ нормален (соотв. сепарабелен) над $\mathbb{F}$.

Доказательство. Поскольку базис поля $\mathbb{K}$ как векторного пространства над $\mathbb{F} \cap \mathbb{K}$ является одновременно и базисом композита $\mathbb{F}\mathbb{K}$ как векторного пространства над $\mathbb{F}$, имеется равенство степеней $[\mathbb{F}\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{F} \cap \mathbb{K}]$. Так как любое тождественное на $\mathbb{F} \cap \mathbb{K}$ вложение $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ продолжается по $\mathbb{F}$-линейности до тождественного на $\mathbb{F}$ вложения $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$, между первыми и вторыми вложениями имеется каноническая биекция. Если $\mathbb{K}$ сепарабельно над $\Bbbk$, то по сл. 12.2 на стр. 176 оба расширения башни $\Bbbk \subset \mathbb{F} \cap \mathbb{K} \subset \mathbb{K}$ сепарабельны, и по предл. 12.1 на стр. 173 имеется $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}]$ тождественных на $\mathbb{F} \cap \mathbb{K}$ вложений $\mathbb{K} \hookrightarrow \overline{\Bbbk}$. Поэтому тождественных на $\mathbb{F}$ вложений $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$ тоже имеется $[\mathbb{K} : \mathbb{F} \cap \mathbb{K}] = [\mathbb{F}\mathbb{K} : \mathbb{F}]$, что по той же предл. 12.1 означает сепарабельность $\mathbb{F}\mathbb{K}$ над $\mathbb{F}$. Если поле $\mathbb{K}$ нормально над $\Bbbk$, то по лем. 12.5 на стр. 177 образы всех вложений $\mathbb{K} \hookrightarrow \overline{\Bbbk}$ совпадают с $\mathbb{K}$. Поэтому образы всех $\mathbb{F}$-линейных вложений $\mathbb{K}\mathbb{F} \hookrightarrow \overline{\Bbbk}$ совпадают с $\mathbb{K}\mathbb{F}$, что по лем. 12.5 означает нормальность $\mathbb{K}\mathbb{F}$ над $\mathbb{F}$. □

Теорема 12.4 (нормальное замыкание)

Для любого конечного сепарабельного расширения $\mathbb{F} \supset \Bbbk$ существует нормальное и сепарабельное над $\Bbbk$ поле $\mathbb{K} \supset \mathbb{F}$, которое вкладывается над $\mathbb{F}$ в любое другое нормальное и сепарабельное над $\Bbbk$ поле $\mathbb{K}' \supset \mathbb{F}$. Все такие поля[1] конечны над $\Bbbk$ и (не канонически) изоморфны друг другу над $\Bbbk$.

Доказательство. Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$ и возьмём в качестве $\mathbb{K}$ композит образов всех $n = \deg \mathbb{F}/\Bbbk$ различных вложений $\mathbb{F} \hookrightarrow \overline{\Bbbk}$. Тогда $\deg \mathbb{K}/\mathbb{F} \leqslant n$, и $\mathbb{F}$ нормально и сепарабельно как над $\mathbb{F}$ так и над $\Bbbk$, а любое вложение $\mathbb{F}$ в любое нормальное сепарабельное расширение $\mathbb{K}' \supset \Bbbk$ продолжается до вложения $\mathbb{K} \hookrightarrow \mathbb{K}'$. □

**12.5. Автоморфизмы полей и соответствие Галуа.** Автоморфизмы поля $\mathbb{K}$, тождественно действующие на его подполе $\Bbbk \subset \mathbb{K}$, называются *автоморфизмами* $\mathbb{K}$ *над* $\Bbbk$. Все такие автоморфизмы образуют группу $\mathrm{Aut}_{\Bbbk}\,\mathbb{K} \overset{\text{def}}{=} \{\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{K} \mid \varphi(t) = t \;\; \forall\, t \in \Bbbk \}$. Так как каждый автоморфизм

[1] Они называются *нормальными замыканиями* сепарабельного расширения $\mathbb{F} \supset \Bbbk$.

поля $\mathbb{K}$ над $\Bbbk$ является продолжением включения $\Bbbk \subset \mathbb{K}$ на расширение $\mathbb{K} \supset \Bbbk$, порядок группы автоморфизмов конечного расширения $\mathbb{K} \supset \Bbbk$ удовлетворяет неравенству $|\operatorname{Aut}_{\Bbbk} \mathbb{K}| \leqslant \deg \mathbb{K}/\Bbbk$ из предл. 12.1 на стр. 173. Конечные расширения, для которых это неравенство превращается в равенство, называются *расширениями Галуа*. Из предл. 12.1 вытекает, что конечное расширение является расширением Галуа если и только если оно нормально и сепарабельно. Группа автоморфизмов расширения Галуа $\mathbb{K} \supset \Bbbk$ называется *группой Галуа* и обозначается

$$\operatorname{Gal} \mathbb{K}/\Bbbk \stackrel{\text{def}}{=} \operatorname{Aut}_{\Bbbk} \mathbb{K}\,.$$

Для любой группы $G$ автоморфизмов поля $\mathbb{K}$ элементы $t \in \mathbb{K}$, неподвижные относительно всех преобразований из $G$, образуют в $\mathbb{K}$ подполе $\mathbb{K}^G \stackrel{\text{def}}{=} \{t \in \mathbb{K} \mid \forall \varphi \in G \;\; \varphi(t) = t\}$, которое называется *полем инвариантов группы $G$*. Отметим, что $\mathbb{K}^G$ содержит простое подполе поля $\mathbb{K}$, изоморфное $\mathbb{Q}$, когда $\operatorname{char}(\Bbbk) = 0$, или $\mathbb{F}_p = \mathbb{Z}/(p)$, когда $\operatorname{char}(\Bbbk) = p > 0$.

Теорема 12.5

Для любой конечной группы $G$ автоморфизмов произвольного поля $\mathbb{K}$ расширение $\mathbb{K} \supset \mathbb{K}^G$ является расширением Галуа степени $|G|$, и $\operatorname{Aut}_{\mathbb{K}^G} \mathbb{K} = G$.

Доказательство. Пусть элементы $\vartheta_1, \dots, \vartheta_m \in \mathbb{K}$ попарно различны и составляют $G$-орбиту элемента $\vartheta = \vartheta_1 \in \mathbb{K}$. Многочлен $f_\vartheta(x) = (x - \vartheta_1) \dots (x - \vartheta_m)$ имеет коэффициенты в $\mathbb{K}^G$ и неприводим над $\mathbb{K}^G$, поскольку группа $G$ переводит в себя множество корней любого многочлена положительной степени из $\mathbb{K}^G[x]$ и не может транзитивно действовать на корнях произведения двух таких многочленов. Тем самым, $f_\vartheta$ является минимальным многочленом элемента $\vartheta$ над полем $\mathbb{K}^G$. Так как $f_\vartheta$ полностью разлагается над $\mathbb{K}$ в произведение попарно различных линейных множителей, расширение $\mathbb{K}^G \subset \mathbb{K}$ алгебраично, нормально и сепарабельно, причём степень над $\mathbb{K}^G$ любого элемента $\vartheta \in \mathbb{K}$ не выше $|G|$. По сл. 12.1 на стр. 172 расширение $\mathbb{K}^G \subset \mathbb{K}$ конечно и $\deg \mathbb{K}/\mathbb{K}^G \leqslant |G|$. С другой стороны, $|G| \leqslant \left|\operatorname{Aut}_{\mathbb{K}^G} \mathbb{K}\right| \leqslant \deg \mathbb{K}/\mathbb{K}^G$. Поэтому все написанные неравенства являются равенствами, и $G = \operatorname{Aut}_{\mathbb{K}^G} \mathbb{K}$. □

Следствие 12.3

Для любых конечного расширения полей $\Bbbk \subset \mathbb{K}$ и подгруппы $G \subset \operatorname{Aut}_{\Bbbk} \mathbb{K}$ равенства $\mathbb{K}^G = \Bbbk$ и $|G| = \deg \mathbb{K}/\Bbbk$ эквивалентны друг другу, и в случае их выполнения $G = \operatorname{Aut}_{\Bbbk} \mathbb{K}$.

Доказательство. По теор. 12.5 в башне $\Bbbk \subset \mathbb{K}^G \subset \mathbb{K}$ степень $\deg \mathbb{K}/\mathbb{K}^G = |G|$, откуда всё и следует. Поучительно, однако, дать другое доказательство, не использующее теорему о примитивном элементе, скрытую в ссылке на сл. 12.1, данной при доказательстве теор. 12.5.

Итак, пусть $|G| = \deg \mathbb{K}/\Bbbk$. Из неравенств $|G| \leqslant \deg \mathbb{K}/\mathbb{K}^G \leqslant \deg \mathbb{K}/\Bbbk$ вытекает, что $\deg \mathbb{K}/\mathbb{K}^G = \deg \mathbb{K}/\Bbbk = \deg \mathbb{K}/\mathbb{K}^G \cdot \deg \mathbb{K}^G/\Bbbk$, откуда $\deg \mathbb{K}^G/\Bbbk = 1$ и $\mathbb{K}^G = \Bbbk$. Наоборот, пусть $\mathbb{K}^G = \Bbbk$. Те же рассуждения, что и в теор. 12.5 показывают, что расширение $\mathbb{K} \supset \Bbbk$ нормально и сепарабельно. Поэтому тождественное вложение $\Bbbk \hookrightarrow \mathbb{K}$ продолжается до автоморфизма поля $\mathbb{K}$ над $\Bbbk$ ровно $\deg \mathbb{K}/\Bbbk$ способами, и $\left|\operatorname{Aut}_{\Bbbk} \mathbb{K}\right| = \deg \mathbb{K}/\Bbbk$. Остаётся показать, что $\operatorname{Aut}_{\Bbbk} \mathbb{K} = G$. Поскольку коэффициенты минимального многочлена $f_\vartheta$ любого элемента $\vartheta \in \mathbb{K}$ инвариантны относительно $\operatorname{Aut}_{\Bbbk} \mathbb{K}$, каждый автоморфизм $\varphi \in \operatorname{Aut}_{\Bbbk} \mathbb{K}$ переводит $\vartheta$ в один из корней многочлена $f_\vartheta$. Так как $f_t$ неприводим, эти корни составляют орбиту группы $G$. Таким образом, для каждого $\vartheta \in \mathbb{K}$ и каждого $\varphi \in \operatorname{Aut}_{\Bbbk} \mathbb{K}$ существует такой элемент $g \in G$, что $g(\vartheta) = \varphi(\vartheta)$. Поэтому для каждого $\varphi \in \operatorname{Aut}_{\Bbbk} \mathbb{K}$ поле $\mathbb{K}$ является объединением по всем $g \in G$ конечного числа подмножеств $V_g = \{\vartheta \in \mathbb{K} \mid g(\vartheta) = \psi(\vartheta)\}$, каждое из которых является подпространством конечномерного векторного пространства $\mathbb{K}$ над полем $\Bbbk$. Если поле $\Bbbk$ бесконечно, то конечномерное пространство над ним не представимо в виде объединения конечного числа собственных подпространств[1], и значит, одно из подпространств $V_g$ совпадает с $\mathbb{K}$, откуда[2] $\varphi = g$. Если поле $\Bbbk$ конечно, то $\mathbb{K}$ тоже конечно и порождается над $\Bbbk$ образующей $\vartheta$ циклической мультипликативной группы $\mathbb{K}^*$. В этом случае $\varphi = g$ для такого $g \in G$, что $\varphi(\vartheta) = g(\vartheta)$. □

Пример 12.6 (поле инвариантов группы треугольника)
Рассмотрим проективную прямую $\mathbb{P}_1 = \mathbb{P}(\Bbbk^2)$ над произвольным полем $\Bbbk$. Группа треугольника $G = S_3$ действует на ней дробно линейными преобразованиями, переставляющими точки $0 = (0 : 1)$, $1 = (1 : 1)$, $\infty = (1 : 0)$. Тождественное преобразование, циклы $\tau = |0, 1, \infty\rangle$, $\tau^{-1} = |\infty, 1, 0\rangle$ и транспозиции $\sigma_0, \sigma_1, \sigma_\infty$, оставляющие на месте точки $0, 1, \infty$ соответственно, преобразуют аффинную координату $t = t_0/t_1$ по формулам:

$$\begin{array}{lll} \mathrm{Id}: t \mapsto t & \tau: t \mapsto 1/(1-t) & \tau^{-1}: t \mapsto (t-1)/t \\ \sigma_0: t \mapsto t/(t-1) & \sigma_1: t \mapsto 1/t & \sigma_\infty: t \mapsto 1-t\,. \end{array} \tag{12-7}$$

Эти шесть замен переменной задают действие группы $G$ на поле $\mathbb{K} = \Bbbk(t)$ рациональных функций по правилу $g: \varphi(t) \mapsto \varphi(g^{-1}(t))$. Поле инвариантов $\mathbb{K}^G$ этого действия состоит из функций $\varphi(t)$, не меняющихся при подстановках (12-7). Согласно теор. 12.5, расширение $\mathbb{K}^G \subset \mathbb{K}$ является расширением Галуа степени 6. Опишем поле $\mathbb{K}^G$ явно. Если рациональная функция $\psi(t) = p(t)/q(t)$ $G$-инвариантна, то любая рациональная функция от $\psi$ тоже $G$-инвариантна. Такие функции образуют подполе $\Bbbk(\psi) \subset \mathbb{K}^G$, и функция $t \in \mathbb{K}$ является корнем многочлена $\psi \cdot q(x) - p(x)$ с коэффициентами в этом подполе. Поэтому $\dim_{\Bbbk(\psi)} \mathbb{K} \leqslant \max(\deg p, \deg q)$. Так как левая часть неравенства делится на $\dim_{\mathbb{K}^G} \mathbb{K} = 6$, мы заключаем, что $\max(\deg p, \deg q) \geqslant 6$, где равенство означает, что $\mathbb{K}^G = \Bbbk(\psi)$. Инвариантную функцию $\psi$ с $\deg p = \deg q = 6$ нетрудно построить из геометрических соображений. Рассмотрим однородный многочлен $f(t_0, t_1)$ без кратных неприводимых множителей, нули которого на $\mathbb{P}_1$ образуют одну $G$-орбиту. Подстановки (12-7) переводят его в многочлен с тем же множеством нулей, т. е. умножают на константы: $f(g^{-1}t) = \lambda(g)\cdot f(t)$, где $\lambda: G \to \Bbbk^*$, $g \mapsto \lambda(g)$, является одномерным характером группы $G$, коих имеется ровно два: тривиальный и знаковый. Поэтому $f$ либо инвариантен относительно всех постановок (12-7), либо сохраняется поворотами и меняет знак при отражениях. Из трёхточечной орбиты $\{0, 1, \infty\}$ таким образом получается знакопеременный многочлен $p = t_0 t_1 (t_0 - t_1)$, квадрат которого $G$-инвариантен, а из двухточечной, образованной собственными векторами поворотов[3] — $G$-инвариантный многочлен $q = t_0^2 - t_0 t_1 + t_1^2$. Минимальный лоранов моном полной степени нуль[4] по $(t_0 : t_1)$, который можно соорудить из $p^2$ и $q$, это

$$\psi(t) = \frac{p^2}{q^3} = \frac{t_0^2 t_1^2 \left(t_0 - t_1\right)^2}{\left(t_0^2 - t_0 t_1 + t_1^2\right)^3} = \frac{t^2 (t-1)^2}{(t^2 - t + 1)^3}$$

так как это отношение многочленов степени $\leqslant 6$, поле инвариантов $\mathbb{K}^G = \Bbbk(\psi)$.

Упражнение 12.15. Убедитесь прямым вычислением, что замены (12-7) не меняют $\psi(t)$.

---

[1] См. упр. 10.12 на стр. 146.

[2] Полезно сопоставить это рассуждение с тем, что использовалось в теор. 12.1 на стр. 172.

[3] Отметим, что сами точки могут быть и не определены над полем $\Bbbk$, но *инвариантный* многочлен, корнями которого они являются, лежит в $\Bbbk[t_0, t_1]$.

[4] А именно, они являются рациональными функциями от $t = t_0/t_1$.

Пример 12.7 (автоморфизмы и вложения конечных полей)
Пусть $q = p^n$, где $p \in \mathbb{N}$ — простое. Поскольку расширение $\mathbb{F}_p \subset \mathbb{F}_q$ нормально и сепарабельно[1], $|\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q| = [\mathbb{F}_q : \mathbb{F}_p] = n$. Итерации $F_p^0 = \mathrm{Id}, F_p, F_p^2, \dots, F_p^{n-1}$ автоморфизма Фробениуса $F_p : \vartheta \mapsto \vartheta^p$ различны, так как равенство $F_p^k = F_p^m$ означает, что все $p^n$ элементов поля $\mathbb{F}_q$ являются корнями многочлена $x^{p^k} - x^{p^m}$, что невозможно при $k, m < n$. Поэтому $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q$ — циклическая группа порядка $n$, порождённая $F_p$. Для каждого $k|n$ подгруппа $G_k \subset \mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_q$, порождённая автоморфизмом $F_p^k$, имеет порядок $n/k$, а её неподвижные точки суть корни многочлена $x^{p^k} - x$. Поэтому $\mathbb{F}_q^{G_k} = \mathbb{F}_{p^k} \subset \mathbb{F}_{p^n}$ является полем разложения многочлена $x^{p^k} - x$, и $G_k \simeq \mathrm{Aut}_{\mathbb{F}_{p^k}} \mathbb{F}_{p^n}$. Любое вложение $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^n}$ является изоморфизмом на подполе $\mathbb{F}_q^{G_k}$, ибо переводит элементы $\mathbb{F}_{p^k}$ в корни многочлена $x^{p^k} - x$. Всего таких вложений имеется $k$, и они образуют одну орбиту группы $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^k}$.

Упражнение 12.16. Покажите, что в $\mathbb{F}_p[x]$ многочлен $x^{p^n} - x$ является произведением всех неприводимых над $\mathbb{F}_p$ приведённых многочленов, степени которых делят $n$.

Теорема 12.6 (соответствие Галуа)
Для любого конечного расширения Галуа $\Bbbk \subset \mathbb{K}$ с группой Галуа $G = \mathrm{Aut}_{\Bbbk} \mathbb{K}$ отображение, сопоставляющее подгруппе $H \subseteq G$ её поле инвариантов $\mathbb{K}^H \subseteq \mathbb{K}$, и отображение, сопоставляющее содержащему $\Bbbk$ подполю $\mathbb{L} \subseteq \mathbb{K}$ подгруппу $\mathrm{Aut}_{\mathbb{L}} \mathbb{K} \subseteq G$, являются взаимно обратными биекциями между множеством подгрупп $H \subseteq G$ и множеством таких полей $\mathbb{L}$, что $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$. При этом нормальные подгруппы $H \trianglelefteq G$ взаимно однозначно соответствуют содержащимся в $\mathbb{K}$ расширениям Галуа $\mathbb{L} \supseteq \Bbbk$, и в этом случае $\mathrm{Gal}\, \mathbb{L}/\Bbbk \simeq G/H$.

Доказательство. Для любого такого поля $\mathbb{L}$, что $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{K}$, расширение $\mathbb{L} \subset \mathbb{K}$ нормально по лем. 12.6 на стр. 177 и сепарабельно по сл. 12.2 на стр. 176. Тем самым, оно является расширением Галуа с группой Галуа $H = \mathrm{Aut}_{\mathbb{L}} \mathbb{K}$, причём $|H| = \deg \mathbb{K}/\mathbb{L}$. Очевидно, что $H$ является подгруппой в $G$. По сл. 12.3 на стр. 179 её поле инвариантов $K^H = \mathbb{L}$. Наоборот, для любой подгруппы $H \subseteq G$ расширение $\mathbb{K}^H \subseteq \mathbb{K}$ является по теор. 12.5 на стр. 179 расширением Галуа с группой Галуа $H$. Это доказывает утверждение о биекции. Для доказательства второго утверждения рассмотрим действие группы $G = \mathrm{Gal}\, \mathbb{K}/\Bbbk$ на содержащихся в $\mathbb{K}$ подполях $\mathbb{L} \supset \Bbbk$. По уже доказанному, централизатор $C_{\mathbb{L}} \overset{\text{def}}{=} \{g \in G \mid g|_{\mathbb{L}} = \mathrm{Id}_{\mathbb{L}}\} = \mathrm{Aut}_{\mathbb{L}} \mathbb{K}$ каждого такого поля $\mathbb{L}$ совпадает с подгруппой $H \subseteq G$, соответствующей по Галуа полю $\mathbb{L}$. Поскольку расширение $\mathbb{K} \supset \Bbbk$ нормально и сепарабельно, любое тождественное на $\Bbbk$ вложение $\varphi : \mathbb{L} \hookrightarrow \mathbb{K}$ продолжается до автоморфизма $g : \mathbb{K} \xrightarrow{\sim} \mathbb{K}$ над $\Bbbk$. Тем самым, $\varphi(\mathbb{L}) = g(\mathbb{L})$ для некоторого $g \in G$, и централизатор поля $\varphi(\mathbb{L})$ в $G$ сопряжён подгруппе $H$: $C_{\varphi(\mathbb{L})} = C_{g(\mathbb{L})} = gC_{\mathbb{L}}g^{-1} = gHg^{-1}$. Согласно лем. 12.6 на стр. 177 и сл. 12.2 на стр. 176 расширение $\mathbb{L} \supset \Bbbk$ всегда сепарабельно, а нормально если и только если $\varphi(\mathbb{L}) = \mathbb{L}$ для всех тождественных на $\Bbbk$ вложений $\varphi : \mathbb{L} \hookrightarrow \mathbb{K}$. Последнее равносильно тому, что все подгруппы, сопряжённые с $H$, совпадают с $H$, т. е. нормальности $H$. В этом случае группа $\mathrm{Gal}\, \mathbb{K}/\Bbbk$ переводит $\mathbb{L}$ в себя, и возникает сюрьективный гомоморфизм $\mathrm{Gal}\, \mathbb{K}/\Bbbk \twoheadrightarrow \mathrm{Gal}\, \mathbb{L}/\Bbbk$ с ядром $\mathrm{Gal}\, \mathbb{K}/\mathbb{L}$. Таким образом, $\mathrm{Gal}\, \mathbb{L}/\Bbbk = (\mathrm{Gal}\, \mathbb{K}/\Bbbk)/(\mathrm{Gal}\, \mathbb{K}/\mathbb{L})$. □

Упражнение 12.17. Убедитесь, что соответствие Галуа оборачивает включения:

$$H \subset K \subset \mathrm{Gal}\, \mathbb{K}/\Bbbk \iff \mathbb{K}^H \supset \mathbb{K}^K \supset \Bbbk$$

[1] См. прим. 12.5 на стр. 175.

и что пересечению подгрупп $H_1 \cap H_2$ отвечает композит $\mathbb{K}_1\mathbb{K}_2$ соответствующих им полей $\mathbb{K}_1 = \mathbb{K}^{H_1}$ и $\mathbb{K}_2 = \mathbb{K}^{H_2}$, а пересечению $\mathbb{K}_1 \cap \mathbb{K}_2$ — наименьшая подгруппа в $G$, содержащая $H_1$ и $H_2$.

## §13. Группы Галуа

**13.1. Построения циркулем и линейкой.** Отождествим ориентированную евклидову плоскость с полем $\mathbb{C}$, указав на ней точки 0 и 1. Традиционный набор школьных задач на построение:

Упражнение 13.1. Даны точки $0,\ 1,\ a,\ b \in \mathbb{C}$. Циркулем и линейкой постройте в $\mathbb{C}$ точки $a \pm b$, $a/b$, $ab$ и $\sqrt{a}$.

показывает, что каждая точка $\zeta$ любого подполя $\mathbb{L} \subset \mathbb{C}$, которое можно получить последовательными квадратичными расширениями поля $\mathbb{Q}$:

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_m = \mathbb{L}\,, \text{ где } \mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big] \text{ и } a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2\,, \tag{13-1}$$

может быть построена циркулем и линейкой. Покажем, что верно и обратное: если число $\zeta \in \mathbb{C}$ строится при помощи циркуля и линейки, отправляясь от заданных точек 0 и 1, то оно лежит в таком подполе $\mathbb{L} \subset \mathbb{C}$, к которому ведёт башня квадратичных расширений вида (13-1), причём все поля $\mathbb{L}_i$ этой башни переводятся в себя комплексным сопряжением $z \mapsto \overline{z}$.

Построение числа $\zeta$ распадается на элементарные шаги, каждый из которых добавляет новую точку $p$, являющуюся пересечением одного из трёх типов: прямых $(ab)$ и $(cd)$, прямой $(ab)$ и проходящей через точку $d$ окружности с центром в $c$ или проходящих через точки $b$ и $d$ окружностей с центрами в точках $a$] и $c$ соответственно. При этом предполагается, что точки $a$, $b$, $c$, $d$ уже построены, а искомая точка пересечения на евклидовой плоскости существует. Положим $\mathbb{L}_1 = \mathbb{Q}\big[\sqrt{-1}\big]$ и допустим по индукции, что $a$, $b$, $c$, $d$ лежат поле $\mathbb{L}_i$ из башни (13-1), причём это поле переводится комплексным сопряжением в себя. Тогда число $(ab) \cap (cd)$ находится по правилу Крамера и тоже лежит в $\mathbb{L}_i$. Для отыскания пары чисел, возникающих при пересечении проходящей через точку $d$ окружности $S$ с центром в точке $c$ с прямой $(ab)$ или с проходящей через $b$ окружностью с центром в $a$ следует подставить в задающее $S$ уравнение $(z-c)(\overline{z}-\overline{c}) = (d-c)(\overline{d}-\overline{c})$ зависящую от параметра $t$ точку $z = a+(b-a)\,t$, которая пробегает прямую $(ab)$ или проходящую через $b$ окружность с центром в $a$, когда $t$ пробегает, соответственно, вещественную прямую $\mathbb{R} \subset \mathbb{C}$ или единичную окружность $\mathrm{U}_1 \subset \mathbb{C}$. Так как в первом случае $\overline{t} = t$, а во втором $\overline{t} = t^{-1}$, мы получим на $t$ квадратное уравнение с коэффициентами из $\mathbb{L}_i$ и вещественным дискриминантом $D \in \mathbb{L}_i \cap \mathbb{R}$.

Упражнение 13.2. Убедитесь в этом, выписав эти уравнения явно в обоих случаях.

Корни этого уравнения лежат либо в поле $\mathbb{L}_i$, либо в квадратичном расширении $\mathbb{L}_{i+1} = \mathbb{L}_i[\sqrt{D}]$, которое переводится комплексным сопряжением в себя. Искомые точки пересечения получаются подстановкой этих корней вместо $t$ в параметрическое представление $a+(b-a)\cdot t$ прямой или окружности, а значит, лежат в $\mathbb{L}_{i+1}$, что воспроизводит предположение индукции.

Предложение 13.1

Конечное расширение Галуа $\mathbb{K} \supset \Bbbk$ тогда и только тогда содержится в поле $\mathbb{L} \supset \Bbbk$, которое можно получить последовательными квадратичными расширениями поля $\Bbbk$:

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_m = \mathbb{L}\,, \text{ где } \mathbb{L}_{i+1} = \mathbb{L}_i\big[\sqrt{a_i}\big] \text{ и } a_i \in \mathbb{L}_i \smallsetminus \mathbb{L}_i^2\,, \tag{13-2}$$

когда $[\mathbb{K} : \Bbbk] = 2^n$ для некоторого $n \in \mathbb{N}$.

Доказательство. Пусть $\mathbb{K}$ содержится в башне (13-2). Из мультипликативности степени вытекает, что $[\mathbb{L} : \Bbbk] = 2^m$, а значит и $[\mathbb{K} : \Bbbk]$, будучи делителем $[\mathbb{L} : \Bbbk]$, тоже является степенью двойки. Наоборот, если $[\mathbb{K} : \Bbbk] = |\mathrm{Gal}\,\mathbb{K}/\Bbbk| = 2^n$, то группа Галуа $G = \mathrm{Gal}\,\mathbb{K}/\Bbbk$ является 2-группой, и её ряд Жордана – Гёльдера[1] $G = G_0 \vartriangleright G_1 \vartriangleright \ldots \vartriangleright G_n = \{e\}$ имеет композиционные факторы $G_i/G_{i+1} \simeq \mathbb{Z}/(2)$ при всех $i$. Соответствие Галуа[2] сопоставляет этой башне подгрупп ведущую от $\Bbbk$ к $\mathbb{K}$ башню квадратичных расширений $\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_n = \mathbb{K}$, в которой $\mathbb{L}_i = \mathbb{K}^{G_i}$. □

Теорема 13.1
Комплексный корень неприводимого многочлена $f(x) \in \mathbb{Q}[x]$ может быть построен циркулем и линейкой исходя из точек $0,\ 1 \in \mathbb{C}$ если и только если степень его поля разложения над $\mathbb{Q}$ является степенью двойки, и в этом случае все корни многочлена $f$ строятся циркулем и линейкой.

Доказательство. Поле разложения $\mathbb{K}$ многочлена $f$ над $\mathbb{Q}$ является расширением Галуа. Если $\deg \mathbb{K}/\mathbb{Q} = 2^m$, то поле $\mathbb{K}$ можно получить из $\mathbb{Q}$ последовательными квадратичными расширениями, как мы видели в доказательстве предл. 13.1 выше. Поэтому все числа из поля $\mathbb{K}$ можно построить циркулем и линейкой. Наоборот, пусть у многочлена $f$ имеется корень $\vartheta \in \mathbb{C}$, который можно построить циркулем и линейкой. Тогда примитивное расширение $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ содержится в некотором расширении $\mathbb{L}$ вида (13-1). Автоморфизм поля $\mathbb{K}$, переводящий корень $\vartheta$ в другой корень $\vartheta'$ многочлена $f$ переводит подполе $\mathbb{Q}[\vartheta] \subset \mathbb{C}$ в подполе $\mathbb{Q}[\vartheta'] \subset \mathbb{C}$. Получающееся таким образом вложение полей $\psi : \mathbb{Q}[\vartheta] \hookrightarrow \mathbb{C}, \vartheta \mapsto \vartheta'$, продолжается до вложения $\overline{\psi} : \mathbb{L} \hookrightarrow \mathbb{C}$, совпадающего с $\psi$ на подполе $\mathbb{Q}[\vartheta] \subset \mathbb{L}$ и переводящего башню (13-1) в башню

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}'_1 \subset \ldots \subset \mathbb{L}'_m = \mathbb{L}' \,, \tag{13-3}$$

в которой $\mathbb{L}'_{i+1} = \mathbb{L}'_i\left[\sqrt{a'_i}\right]$ для некоторого $a'_i = \widetilde{\psi}(a_i) \in \mathbb{L}'_i \smallsetminus \left(\mathbb{L}'_i\right)^2$. Так как $\vartheta' \in \mathbb{L}'$, корень $\vartheta'$ тоже строится циркулем и линейкой. Композит $\mathbb{L}\mathbb{L}'$ содержит оба корня $\vartheta, \vartheta'$ и также является башней квадратичных расширений, поскольку получается последовательным присоединением к $\mathbb{L}$ чисел $a'_1, \ldots, a'_m$, степени которых над соответствующими подполями $\mathbb{L},\ \mathbb{L}\mathbb{L}'_1,\ \ldots\ ,\ \mathbb{L}\mathbb{L}'_{m-1}$ не превышают двойки. Продолжая по индукции, мы построим башню квадратичных раширений, содержащую все корни многочлена $f$, а значит и его поле разложения $\mathbb{K}$. По предл. 13.1 степень $[\mathbb{K} : \mathbb{Q}]$ в этом случае является степенью двойки, что и утверждалось. □

Следствие 13.1
Если число $\zeta \in \mathbb{C}$ строится циркулем и линейкой по данным точкам 0 и 1, то оно алгебраично над $\mathbb{Q}$ и его степень над $\mathbb{Q}$ является степенью двойки.

Доказательство. Примитивное расширение $\mathbb{Q}[\zeta]$ содержится в поле разложения минимального многочлена числа $\zeta$, поэтому степень этого расширения над $\mathbb{Q}$ делит степень поля разложения минимального многочлена. □

Пример 13.1 (трисекция угла, удвоение куба и правильный семиугольник)
Угол $\pi/3$ нельзя разделить на три равные части циркулем и линейкой, поскольку такая возможность влечёт возможность построения циркулем и линейкой числа $\cos(\pi/9)$, имеющего над $\mathbb{Q}$ степень 3.

Упражнение 13.3. Убедитесь, что $\cos(\pi/9)$ является корнем неприводимого над $\mathbb{Q}$ многочлена $8\,x^3 - 6\,x - 1$.

[1] См. Теорему 12.1 на стр. 179 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_12.pdf.

[2] См. теор. 12.6 на стр. 181.

По той же причине циркулем и линейкой нельзя построить сторону куба, объём которого вдвое больше объёма единичного куба: это равносильно построению корня неприводимого над $\mathbb{Q}$ многочлена $x^3 - 2$. Правильный 7-угольник тоже нельзя построить циркулем и линейкой: такое построение позволяло бы построить первообразный корень $\sqrt[7]{1} = e^{2\pi i/7}$, минимальный многочлен которого[1] $\Phi_7(x) = (x^7 - 1)/(x - 1)$ имеет степень 6.

Упражнение 13.4* (построение Гаусса). Постройте правильный 17-угольник циркулем и линейкой.

**13.1.1. Влияние побочных иррациональностей.** Задачу о построении циркулем и линейкой можно расширить, считая что в начале построения даны не только точки 0, 1, но и некоторые другие точки $\zeta_1, \dots, \zeta_n \in \mathbb{C}$. Поскольку все точки поля $\mathbb{F} = \mathbb{Q}(\zeta_1, \dots, \zeta_n) \subset \mathbb{C}$, порождённого этими числами, строятся циркулем и линейкой, можно считать, что изначально заданные точки образуют произвольное[2] подполе $\mathbb{F} \subset \mathbb{C}$. Элементы поля $\mathbb{F}$ называются в этой ситуации *побочными иррациональностями*. Всё сказанное выше сохраняет силу после замены поля $\mathbb{Q}$ полем $\mathbb{F}$. А именно, если даны все точки поля $\mathbb{F}$, то число $\zeta \in \mathbb{C}$ строится циркулем и линейкой если и только если оно содержится в конечной башне последовательных квадратичных расширений поля $\mathbb{F}$, и это равносильно тому, что $\zeta$ алгебраично над $\mathbb{F}$ и степень поля разложения его минимального многочлена над $\mathbb{F}$ является степенью двойки. В частности, для этого необходимо, чтобы степень этого минимального многочлена тоже была степенью двойки.

Упражнение 13.5. Докажите все эти утверждения.

В самом общем виде взятие композита с произвольным полем побочных иррациональностей действует на расширение Галуа следующим образом.

Предложение 13.2 (теорема о побочных иррациональностях)
Пусть поля $\mathbb{F}, \mathbb{K} \supset \Bbbk$ содержатся в некотором общем алгебраически замкнутом поле $\mathbb{L}$ и расширение $\mathbb{K} \supset \Bbbk$ является конечным расширением Галуа. Тогда $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ также является конечным расширением Галуа, и его группа Галуа изоморфна подгруппе $H_{\mathbb{F}\cap\mathbb{K}} \subset \operatorname{Gal} \mathbb{K}/\Bbbk$, отвечающей при соответствии Галуа промежуточному подполю $\Bbbk \subset \mathbb{F} \cap \mathbb{K} \subset \mathbb{K}$.

Доказательство. По предл. 12.3 поле $\mathbb{K}$ является полем разложения некого сепарабельного многочлена $f \in \Bbbk[x]$ и порождается как $\Bbbk$-алгебра его корнями $\vartheta_1, \dots, \vartheta_n \in \mathbb{L}$. Они же порождают $\mathbb{F}\mathbb{K}$ как алгебру над $\mathbb{F}$. По предл. 12.4 расширение $\mathbb{F}\mathbb{K} \supset \mathbb{F}$ нормально и сепарабельно, т. е. является конечным расширением Галуа. Тем самым, $\mathbb{F}\mathbb{K}$ является полем разложения $f$ над $\mathbb{F}$. Автоморфизмы $\mathbb{K}$ над $\Bbbk$ и $\mathbb{F}\mathbb{K}$ над $\mathbb{F}$ оставляют многочлен $f$ на месте и переводят множество его корней в себя, причём каждый автоморфизм однозначно определяется своим действием на корни. Это позволяет рассматривать обе группы $\operatorname{Gal} \mathbb{K} / \Bbbk$ и $\operatorname{Gal} \mathbb{F}\mathbb{K} / \mathbb{F}$ как подгруппы в $S_n$: группа $\operatorname{Gal} \mathbb{K} / \Bbbk$ состоит из всех перестановок корней $\vartheta_1, \dots, \vartheta_n$, которые продолжаются до автоморфизма порождённой ими $\Bbbk$-алгебры $\mathbb{K} = \Bbbk[\vartheta_1, \dots, \vartheta_n]$, а группа $\operatorname{Gal} \mathbb{F}\mathbb{K} / \mathbb{F}$ — из перестановок, продолжающихся до автоморфизма $\mathbb{F}$-алгебры $\mathbb{F}\mathbb{K} = \mathbb{F}[\vartheta_1, \dots, \vartheta_n]$. Так как $\Bbbk \subset \mathbb{F}$, вторая группа содержится в первой и состоит в точности из всех $\mathbb{F}$-линейных преобразований $g : \Bbbk[\vartheta_1, \dots, \vartheta_n] \to \Bbbk[\vartheta_1, \dots, \vartheta_n]$ из группы $\operatorname{Gal} \mathbb{K}/\Bbbk$. Но $\mathbb{F}$-линейность оператора $g$ в точности и означает, что $g$ оставляет на месте подполе $\mathbb{F} \cap \mathbb{K}$. □

[1] Напомню, что круговой многочлен $\Phi_p(x)$ при простом $p$ неприводим по критерию Эйзенштейна.
[2] Не обязательно алгебраическое над $\mathbb{Q}$.

**13.2. Группы многочленов.** Согласно предл. 12.3, поле разложения $\mathbb{L}_f$ любого сепарабельного многочлена $f \in \Bbbk[x]$ является расширением Галуа поля $\Bbbk$. Его группа Галуа над $\Bbbk$ обозначается через $\mathrm{Gal}\, f/\Bbbk$ и называется *группой Галуа многочлена* $f$ над $\Bbbk$. Так как коэффициенты $f$ инвариантны относительно действия группы Галуа, возникает каноническое действие группы $\mathrm{Gal}\, f/\Bbbk$ на корнях $\vartheta_1, \dots, \vartheta_n$ многочлена $f$, и поскольку поле $\mathbb{L}_f$ как алгебра над $\Bbbk$ порождается этими корнями, каждый автоморфизм из группы Галуа однозначно определяется своим действием на корнях, т. е. группа Галуа *канонически вложена* в группу перестановок корней. Перестановка корней лежит в группе Галуа тогда и только тогда, когда она сохраняет все полиномиальные соотношения между корнями. Формализуется это следующим образом.

Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$. Поле разложения $\mathbb{L}_f \subset \overline{\Bbbk}$ является образом гомоморфизма вычисления

$$\mathrm{ev}_{\vartheta_1,\dots,\vartheta_n} : \Bbbk[t_1, \dots, t_n] \to \overline{\Bbbk}, \quad \psi \mapsto \psi(\vartheta_1, \dots, \vartheta_n), \tag{13-4}$$

ядро которого $I_{\Bbbk}(\vartheta) \overset{\text{def}}{=} \ker \mathrm{ev}_{\vartheta_1,\dots,\vartheta_n}$ является идеалом всех полиномиальных соотношений между корнями многочлена $f$, т. е. состоит из всех многочленов $\psi \in \Bbbk[t_1, \dots, t_n]$, равных нулю в точке $\vartheta = (\vartheta_1, \dots, \vartheta_n) \in \mathbb{A}^n\left(\overline{\Bbbk}\right)$. Перестановка переменных $g : t_i \mapsto t_{g(i)}$ корректно факторизуется до эндоморфизма алгебры $\mathbb{L}_f = \Bbbk[t_1, \dots, t_n] / I_{\Bbbk}(\vartheta)$ если и только если она переводит идеал $I_{\Bbbk}(\vartheta)$ себя, т. е. для любого $\psi \in I_{\Bbbk}(\vartheta)$ многочлен $\psi^g(t_1, \dots, t_n) \overset{\text{def}}{=} \psi(t_{\sigma(1)}, \dots, t_{\sigma(n)})$ тоже лежит в $I_{\Bbbk}(\vartheta)$. Тем самым, группа Галуа многочлена $f$ имеет вид

$$\mathrm{Gal}\, f/\Bbbk \simeq \{g \in S_n \mid \forall \psi \in I_{\Bbbk}(\vartheta)\ \psi^g \in I_{\Bbbk}(\vartheta)\} \tag{13-5}$$

Именно так изначально и определял группу многочлена сам Галуа.

Замечание 13.1. Задаваемое формулой (13-5) вложение группы Галуа $\mathrm{Gal}\, f$ в стандартную симметрическую группу $S_n = \mathrm{Aut}\{1, \dots, n\}$ не является каноническим и *зависит* от выбора нумерации корней $\vartheta_i$ многочлена $f$.

Предложение 13.3
Аффинное алгебраическое многообразие $V(I_{\Bbbk}(\vartheta)) \subset \mathbb{A}^n(\overline{\Bbbk})$ представляет собою набор из $m = [\mathbb{L}_f : \Bbbk] = |\mathrm{Gal}\, f/\Bbbk|$ различных точек $(\vartheta_{g(1)}, \dots, \vartheta_{g(n)})$, где $g \in \mathrm{Gal}\, f/\Bbbk$, образующих одну орбиту действия группы $\mathrm{Gal}\, f/\Bbbk \subset S_n$ на пространстве $\mathbb{A}^n$ перестановками координат.

Доказательство. Пусть $f = x^n + a_1 x^{n-1} + \dots + a_{n-1}x + a_n$. По теореме Виета $e_i(\vartheta_1, \dots, \vartheta_n) = (-1)^i a_i$, где $e_i(t_1, \dots, t_n) \in \Bbbk[t_1, \dots, t_n]$ — элементарный симметрический многочлен. Тем самым, $e_i(t_1, \dots, t_n) - (-1)^i a_i \in I_{\Bbbk}(\vartheta)$ для каждого $i$. Если точка $\alpha = (\alpha_1, \dots, \alpha_n) \in V\left(I_{\Bbbk}(\vartheta)\right)$, то $e_i(\alpha_1, \dots, \alpha_n) = (-1)^i a_i$, откуда $(x - \alpha_1) \cdots (x - \alpha_n) = f(x) = (x - \vartheta_1) \cdots (x - \vartheta_n)$, т. е. $(\alpha_1, \dots, \alpha_n) = (\vartheta_{g(1)}, \dots, \vartheta_{g(n)})$ для некоторой перестановки $g \in S_n$. Если $g$ не лежит в группе $\mathrm{Gal}\, f/\Bbbk$, то найдётся такой многочлен $\psi \in I_{\Bbbk}(\vartheta)$, что $\psi^g \notin I_{\Bbbk}(\vartheta)$, и тогда $\psi(\alpha_1, \dots, \alpha_n) = \psi(\vartheta_{g(1)}, \dots, \vartheta_{g(n)}) = \psi^g(\vartheta_1, \dots, \vartheta_n) \neq 0$, что невозможно для точки $\alpha \in V\left(I_{\Bbbk}(\vartheta)\right)$. Мы заключаем, что координаты каждой точки $\alpha \in V\left(I_{\Bbbk}(\vartheta)\right)$ получаются из координат точки $\vartheta$ перестановкой из группы Галуа многочлена $f$. Наоборот, для любой перестановки $g \in \mathrm{Gal}\, f/\Bbbk$ и всех $\psi \in I_{\Bbbk}(\vartheta)$ значение $\psi(\vartheta_{g(1)}, \dots, \vartheta_{g(n)}) = \psi^g(\vartheta_1, \dots, \vartheta_n) = 0$, поскольку $\psi^g \in I_{\Bbbk}(\vartheta)$. Следовательно все точки из $\mathrm{Gal}\, f/\Bbbk$-орбиты точки $\vartheta$ лежат в $V(I_{\Bbbk}(\vartheta))$. □

Упражнение 13.6. Покажите, что сепарабельный многочлен $f \in \Bbbk[x]$ неприводим если и только если группа $\mathrm{Gal}\, f/\Bbbk$ транзитивно действует на его корнях.

**13.2.1. Резольвента Галуа.** Обозначим через $\mathbb{L}_f \supset \Bbbk$ поле разложения многочлена

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \Bbbk[x]\,,$$

а через $\vartheta_1, \dots, \vartheta_n$ — корни $f$ в $\mathbb{L}_f$, и рассмотрим однородную линейную форму

$$\psi = \vartheta_1 t_1 + \dots + \vartheta_n t_n \in \mathbb{L}_f[t_1, \dots, t_n]\,. \tag{13-6}$$

Однородный многочлен $F(t_1, \dots, t_n) = \prod_{\sigma \in S_n} \psi^\sigma = \prod_{\sigma \in S_n} (\vartheta_1 t_{\sigma(1)} + \dots + \vartheta_n t_{\sigma(n)})$ степени $n!$ называется *резольвентой Галуа* многочлена $f$. Группируя вместе сомножители, отвечающие перестановкам $\sigma$ из одного смежного класса подгруппы $G = \operatorname{Gal} f/\Bbbk \subset S_n$, перепишем $F$ в виде

$$F\left(t_1, \dots, t_n\right) = \prod_{h \in S_n/G} F_h\left(t_1, \dots, t_n\right)\,, \tag{13-7}$$

где

$$\begin{aligned} F_h\left(t_1, \dots, t_n\right) &= \prod_{g \in G} \left(\vartheta_1 t_{hg(1)} + \dots + \vartheta_n t_{hg(n)}\right) = \\ &= \prod_{g \in G} \left(\vartheta_{g^{-1}(1)} t_{h(1)} + \dots + \vartheta_{g^{-1}(n)} t_{h(n)}\right) = \prod_{g \in G} g\left(\psi^h\right)\,. \end{aligned} \tag{13-8}$$

В последнем произведении $\psi^h \in \mathbb{L}_f[t_1, \dots, t_n]$ означает линейную форму, полученную из формы $\psi$ перестановкой $h \in S_n$ переменных $t_1, \dots, t_n$, а $g(\psi^h)$ означает результат применения к *коэффициентам* этой формы автоморфизма $g : \mathbb{L}_f \xrightarrow{\sim} \mathbb{L}_f$ из группы Галуа $G = \operatorname{Aut}_{\Bbbk} \mathbb{L}_f$. Так как все линейные формы $g\left(\psi^h\right)$ в произведении (13-8) различны и составляют одну орбиту группы Галуа, каждый многочлен $F_h$ имеет коэффициенты в поле $\Bbbk$ и неприводим над $\Bbbk$. Мы заключаем, что $F \in \Bbbk[t_1, \dots, t_n]$, и формула (13-7) представляет собою разложение многочлена $F$ на неприводимые множители в $\Bbbk[t_1, \dots, t_n]$. Неприводимые многочлены $F_h$ образуют орбиту многочлена $F_e$ при действии симметрической группы $S_n$ на кольце $\Bbbk[t_1, \dots, t_n]$ перестановками переменных, и группа Галуа $G = \operatorname{Gal} f/\Bbbk$ изоморфна стабилизатору многочлена $F_e$ и сопряжена стабилизатору любого из многочленов $F_h$. Суммируем сказанное так:

Предложение 13.4

Перестановки переменных $t_1, \dots, t_n$, переводящие в себя какой-нибудь неприводимый делитель резольвенты Галуа многочлена $f$ в кольце $\Bbbk[t_1, \dots, t_n]$, образуют в $S_n$ подгруппу, изоморфную $\operatorname{Gal} f/\Bbbk$. □

**13.2.2. Редукция коэффициентов.** Пусть теперь поле $\Bbbk = \mathbb{Q}$ и многочлен

$$f = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \mathbb{Z}[x]\,.$$

Обозначим через $\overline{f} = x^n + \overline{a}_1 x^{n-1} + \dots + \overline{a}_{n-1} x + \overline{a}_n \in \mathbb{F}_p[x]$, где $\overline{a}_i = a_i \pmod p$, редукцию $f$ по простому модулю $p \in \mathbb{N}$.

Теорема 13.2

Если многочлен $\overline{f} \in \mathbb{F}_p[x]$ сепарабелен, то имеется вложение групп $\operatorname{Gal} \overline{f}/\mathbb{F}_p \hookrightarrow \operatorname{Gal} f/\mathbb{Q}$.

Доказательство. Корни $\vartheta_1, \dots, \vartheta_n$ многочлена $f$ в его поле разложения $\mathbb{L}_f$ целы над $\mathbb{Z}$. Поэтому коэффициенты формы $\psi = \vartheta_1 t_1 + \dots + \vartheta_n t_n$ из (13-6), а с ними и коэффициенты всех многочленов $F_h$ из разложения (13-7), лежат в кольце целых $\mathcal{O} \subset \mathbb{L}_f$. Так как коэффициенты каждого многочлена $F_h$ инвариантны относительно $\operatorname{Gal}\mathbb{L}_f/\mathbb{Q}$, они лежат в $\mathbb{Q}\cap\mathcal{O}=\mathbb{Z}$, т. е. разложение (13-7) имеет место в $\mathbb{Z}[t_1,\dots,t_n]$. Приводя его по модулю $p$, получаем в $\mathbb{F}_p[t_1,\dots,t_n]$ равенство

$$\overline{F}(t_1,\dots,t_n)=\prod_{h\in S_n/G}\overline{F}_h(t_1,\dots,t_n) \tag{13-9}$$

Обозначим через $\overline{\vartheta}_i=\vartheta_i\ (\mathrm{mod}\ p)$ классы корней $\vartheta_i$ в $\mathbb{F}_p$-алгебре $A\overset{\text{def}}{=}\mathcal{O}/(p)$. В $A[t]$ многочлен $\overline{f}(x)=\prod(x-\overline{\vartheta}_i)$ полностью раскладывается на линейные множители, и все они различны в силу сепарабельности $\overline{f}$ над $\mathbb{F}_p$.

Упражнение 13.7. Убедитесь, что $\mathbb{F}_p$-подалгебра в $A$, порождённая $\overline{\vartheta}_1,\dots,\overline{\vartheta}_n$, является полем разложения многочлена $\overline{f}$ над $\mathbb{F}_p$.

Стало быть, многочлен $\overline{F}\in\mathbb{F}_p[t_1,\dots,t_n]$ является резольвентой Галуа многочлена $\overline{f}\in\mathbb{F}_p[x]$ над $\mathbb{F}_p$. По предл. 13.4 группу Галуа $\operatorname{Gal}\overline{f}/\mathbb{F}_p$ можно вложить в группу перестановок переменных $t_i$, как стабилизатор какого-нибудь неприводимого делителя многочлена $\overline{F}$ в $\mathbb{F}_p[t_1,\dots,t_n]$. Зафиксируем такой делитель $P$, и пусть он приходит из разложения на неприводимые множители над полем $\mathbb{F}_p$ редукции $\overline{F}_h$ неприводимого делителя $F_h$ многочлена $F$ в кольце $\mathbb{Z}[t_1,\dots,t_n]$. Отождествим $\operatorname{Gal}f/\mathbb{Q}$ с группой перестановок переменных, переводящих $F_h$ в себя. Поскольку каждая не лежащая в $\operatorname{Gal}f/\mathbb{Q}$ перестановка из $S_n$ переводит $F_h$ в другой неприводимый множитель $F_{h'}\neq F_h$ многочлена $F$, она не может оставлять на месте многочлен $P$, являющийся делителем $\overline{F}_h$. Следовательно $\operatorname{Gal}\overline{f}/\mathbb{F}_p\subset\operatorname{Gal}f/\mathbb{Q}$. □

Следствие 13.2
Пусть редукция по модулю $p$ неприводимого приведённого многочлена $f\in\mathbb{Z}[x]$ распадается в произведение неприводимых над $\mathbb{F}_p$ многочленов $q_1,\dots,q_m$ степеней $\lambda_1\geqslant\dots\geqslant\lambda_m$. Тогда группа Галуа $\operatorname{Gal}f/\mathbb{Q}$ содержит перестановку циклового типа $\lambda$.

Доказательство. Поле разложения многочлена $\overline{f}$ над $\mathbb{F}_p$ конечно, и его группа Галуа над $\mathbb{F}_p$ циклическая[1]. Так как она транзитивно действует на корнях каждого из неприводимых многочленов $q_i$, образующий элемент группы $\operatorname{Gal}\overline{f}/\mathbb{F}_p$ осуществляет перестановку корней многочлена $\overline{f}$ циклового типа $\lambda$. По теор. 13.2 эта перестановка содержится и в $\operatorname{Gal}f/\mathbb{Q}$. □

Пример 13.2 (многочлен с группой $S_5$)
Вычислим группу Галуа многочлена $f(x)=x^5-x-1$ над $\mathbb{Q}$. Для этого разложим его на неприводимые множители над $\mathbb{F}_2$ и над $\mathbb{F}_3$. В нетривиальном разложении степень одного из неприводимых множителей $\leqslant 2$, и произведение всех неприводимых приведённых многочленов степеней 1 и 2 в $\mathbb{F}_p[x]$ равно[2] $x^{p^2}-x$. При помощи алгоритма Евклида убеждаемся, что над $\mathbb{F}_2$

$$\text{нод}(x^5-x-1,\ x^4-x)=x^2+x+1$$

и разложение на неприводимые имеет вид $\overline{f}=(x^2+x+1)(x^3+x^2+1)$, тогда как над полем $\mathbb{F}_3$ $\text{нод}(x^5-x-1,\ x^9-x)=1$, и значит, $\overline{f}$ неприводим. По сл. 13.2 группа $\operatorname{Gal}f/\mathbb{Q}$ содержит цикл длины 5 и перестановку циклового типа $(3,2)$. Возводя последнюю в куб, заключаем, что группа Галуа содержит транспозицию. Так как цикл максимальной длины и транспозиция порождают

[1] См. прим. 12.7 на стр. 181.
[2] См. упр. 12.16 на стр. 181.

всю симметрическую группу, $\mathrm{Gal}\, f\,/\,\mathbb{Q} \simeq S_5$. Из теор. 13.5, которую мы докажем на стр. 192 ниже, вытекает, что корни многочлена $x^5 - x - 1$ не выражаются через рациональные числа при помощи четырёх арифметических операций и извлечения корней произвольных степеней.

**13.3. Группы круговых полей.** Расширение $\mathbb{Q}[\zeta_n] \supset \mathbb{Q}$, порождённое как алгебра над $\mathbb{Q}$ примитивным корнем $n$-той степени из единицы $\zeta_n \overset{\text{def}}{=} e^{2\pi i/n} \in \mathbb{C}$, называется $n$-тым *круговым*[1] полем. Это поле содержит циклическую мультипликативную группу $\boldsymbol{\mu}_n \subset \mathbb{Q}[\zeta_n]$ корней $n$-той степени из единицы и является полем разложения сепарабельного многочлена $x^n - 1$. Поэтому круговое поле является расширением Галуа поля $\mathbb{Q}$, а каждый автоморфизм $\sigma \in \mathrm{Gal}\,\mathbb{Q}[\zeta_n]/\mathbb{Q}$ переводит образующую $\zeta_n$ группы $\boldsymbol{\mu}_n$ в образующую группы $\boldsymbol{\mu}_n$, т. е. действует по правилу $\sigma : \zeta_n \mapsto \zeta_n^{m(\sigma)}$, где $m(\sigma) \in (\mathbb{Z}/(n))^*$ обратим в кольце вычетов $\mathbb{Z}/(n)$. Это задаёт гомоморфное вложение группы Галуа кругового поля в мультипликативную группу обратимых элементов кольца вычетов:

$$\mathrm{Gal}\,\mathbb{Q}[\zeta_n]/\mathbb{Q} \hookrightarrow \left(\mathbb{Z}/(n)\right)^*, \quad \sigma \mapsto m(\sigma)\,. \tag{13-10}$$

Поскольку множество $R_n \overset{\text{def}}{=} \{\zeta_n^m \mid \text{нод}(n,m) = 1\} \subset \boldsymbol{\mu}_n$ всех первообразных корней степени $n$ из единицы переводится группой $\mathrm{Gal}\,\mathbb{Q}[\zeta_n]/\mathbb{Q}$ в себя, *$n$-тый круговой многочлен*

$$\Phi_n(x) \overset{\text{def}}{=} \prod_{\xi \in R_n} (x - \xi)$$

инвариантен относительно группы Галуа, и значит, лежит в $\mathbb{Q}[x]$. Будучи полиномами от корней многочлена $x^n - 1$, все коэффициенты многочлена $\Phi_n(x)$ целы над $\mathbb{Z}$, и тем самым $\Phi_n(x) \in \mathbb{Z}[x]$. Так, $\Phi_2(x) = x + 1$, $\Phi_3(x) = (x - \omega)(x - \omega^2) = x^2 + x + 1$, $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$, $\Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$, $\Phi_6(x) = (z - \zeta_6)(x - \zeta_6^{-1}) = x^2 - x + 1$ и т. д. Круговое поле $\mathbb{Q}[\zeta_n]$ является полем разложения кругового многочлена $\Phi_n$ и $\mathrm{Gal}\,\mathbb{Q}[\zeta_n]/\mathbb{Q} = \mathrm{Gal}\,\Phi_n/\mathbb{Q}$.

**13.3.1. Элементы Фробениуса.** При простом $p \nmid n$ многочлен $x^n - 1$ сепарабелен над $\mathbb{F}_p$. Редукция $\overline{\Phi}_n$ многочлена $\Phi_n$ по модулю $p$ тоже сепарабельна над $\mathbb{F}_p$, т. к. $\overline{\Phi}_n$ делит $x^n - 1$. Поэтому сопоставление $\xi \mapsto \overline{\xi} = \xi \,(\mathrm{mod}\ p) \in \mathcal{O}\,/\,(p)$ задаёт биекцию между множеством $R_n \subset \mathcal{O} \subset \mathbb{Q}[\zeta_n] \subset \mathbb{C}$ комплексных первообразных корней и множеством корней многочлена $\overline{\Phi}_n$ в его поле разложения над $\mathbb{F}_p$, которое порождается этими корнями как алгебра над $\mathbb{F}_p$ и является конечным расширением Галуа поля $\mathbb{F}_p$ с циклической группой Галуа, порождённой автоморфизмом Фробениуса[2] $\overline{\xi} \mapsto \overline{\xi}^p$. По теор. 13.2 в группе Галуа $\mathrm{Gal}\,\Phi_n/\mathbb{Q}$ имеется такая перестановка комплексных первообразных корней $\sigma \in \mathrm{Aut}\,R_n$, что $\overline{\sigma(\xi)} = \overline{\xi}^p$. Мы заключаем, что автоморфизм мультипликативной группы $\boldsymbol{\mu}_n \subset \mathbb{Q}[\zeta_n]$, заданный правилом

$$F_p : \boldsymbol{\mu}_n \xrightarrow{\sim} \boldsymbol{\mu}_n\,, \quad \xi \mapsto \xi^p\,, \tag{13-11}$$

продолжается до автоморфизма кругового поля $\mathbb{Q}[\zeta_n]$ над $\mathbb{Q}$. Он называется *$p$-элементом Фробениуса* в группе Галуа кругового поля. Таким образом, для всех простых $p \nmid n$ автоморфизмы Фробениуса из групп $\mathrm{Gal}\,\overline{\Phi}_n/\mathbb{F}_p$ *канонически* вложены в группу $\mathrm{Gal}\,\Phi_n/\mathbb{Q}$.

Применяя к корню $\zeta_n \in R_n$ автоморфизмы $F_p$ со всевозможными простыми $p \nmid n$, а также их итерации, можно получить все первообразные корни: любой из них имеет вид $\zeta_n^m$ для некоторого $m = p_1^{m_1} \cdots p_k^{m_k}$, взаимно простого с $n$, и равен $F_{p_1}^{m_1} \cdots F_{p_k}^{m_k} \zeta_n$. Мы заключаем, что группа Галуа кругового многочлена транзитивно действует на его корнях.

[1] Или *циклотомическим*.

[2] См. прим. 12.7 на стр. 181 и доказательство сл. 13.2 на стр. 188.

Предложение 13.5
Многочлен $\Phi_n$ неприводим над $\mathbb{Q}$ и является минимальным многочленом первообразного корня $\zeta_n$ над $\mathbb{Q}$, а вложение (13-10) является изоморфизмом групп, т. е. $\operatorname{Gal}\Phi_n \simeq (\mathbb{Z}/(n))^*$. В частности, $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$, где $\varphi$ — функция Эйлера.

Доказательство. Если бы многочлен $\Phi_n$ был приводим над $\mathbb{Q}$, его группа Галуа переводила бы множество корней каждого неприводимого множителя в себя и не могла бы транзитивно действовать на корнях многочлена $\Phi_n$. Из транзитивности действия группы $\operatorname{Gal}\Phi_n$ на корнях вытекает неравенство $|\operatorname{Gal}\Phi_n| \geqslant \deg\Phi_n = \varphi(n) = |(\mathbb{Z}/(n))^*|$, гарантирующее сюрьективность вложения (13-10). □

Пример 13.3 (Гауссова сумма)
При простом $p > 2$ любая мультипликативная подгруппа $H \subset \mathbb{F}_p^*$ индекса 2 содержит все ненулевые квадраты поля $\mathbb{F}_p$, поскольку в $\mathbb{F}_p^*/H \simeq \mathbb{Z}/(2)$ выполняется равенство $\xi^2 H = \xi H \cdot \xi H = H$. Это означает, что мультипликативная подгруппа индекса индекса 2 в $\mathbb{F}_p^*$ единственна и совпадает с группой ненулевых квадратов. Мы заключаем, что группа Галуа кругового поля $\mathbb{Q}[\zeta_p]$, порождённого корнем $\zeta_p = e^{2\pi i/p}$, тоже содержит ровно одну подгруппу индекса 2, и изоморфизм $m : \operatorname{Gal}\Phi_p \xrightarrow{\sim} \mathbb{F}_p^*$ из форм. (13-10) на стр. 189 отождествляет эту подгруппу с группой ненулевых квадратов в $\mathbb{F}_p^*$. Согласно соответствию Галуа, круговое поле $\mathbb{Q}[\zeta_p]$ содержит ровно одно квадратичное расширение $\mathbb{K} \supset \mathbb{Q}$, и оно порождается над $\mathbb{Q}$ числом[1]

$$\vartheta = \sum_{\substack{\sigma\in\operatorname{Gal}\Phi_p:\\ m(\sigma)\in\mathbb{F}_p^{*\,2}}} \sigma(\zeta_p) - \sum_{\substack{\sigma\in\operatorname{Gal}\Phi_p:\\ m(\sigma)\notin\mathbb{F}_p^{*\,2}}} \sigma(\zeta_p) = \sum_{m=1}^{p-1} \left[\frac{m}{p}\right]\cdot\zeta_p^m\,, \tag{13-12}$$

которое инвариантно относительно подгруппы $\mathbb{F}_p^{*\,2} \subset \operatorname{Gal}\Phi_p$ и меняет знак под действием всех остальных автоморфизмов кругового поля.

Упражнение 13.8. Покажите, что $\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{Q}[\zeta_p]$ для всех простых $p > 2$, и явно выразите этот квадратный корень через корни $p$-той степени из единицы. Правая часть (13-12) называется *Гауссовой суммой*.

**13.4. Циклические расширения.** Элемент $\zeta$ произвольного поля $\Bbbk$ называется *примитивным* или *первообразным* корнем степени $m$ из единицы, если $\zeta^m = 1$ и $\zeta^i \neq 1$ при всех $0 < i < m$. Если поле $\Bbbk$ содержит такой корень $\zeta$, то циклическая мультипликативная группа корней уравнения $x^m = 1$ в поле $\Bbbk$ имеет порядок $m$ и порождается элементом $\zeta$, а множество образующих этой группы есть множество всех примитивных корней из единицы степени $m$. В частности, многочлен $x^m - 1$ в этом случае сепарабелен. Поэтому $m$ не делится на $\operatorname{char}(\Bbbk)$, и все многочлены $x^d - a \in \Bbbk[x]$ степени $d|m$ тоже сепарабельны. Мы продолжим обозначать циклическую мультипликативную группу корней $m$-той степени из единицы через $\boldsymbol{\mu}_m \subset \Bbbk^*$, и обозначим через $\Bbbk^{*s}$ мультипликативную группу $s$-тых степеней ненулевых элементов поля $\Bbbk$.

---

[1] Напомню, что *символ Лежандра – Якоби* $\left[\frac{m}{p}\right] \overset{\text{def}}{=} \begin{cases} 0 & \text{если } m \pmod p = 0 \\ 1 & \text{если } m \pmod p \in \mathbb{F}_p^2 \smallsetminus 0 \\ -1 & \text{если } m \pmod p \notin \mathbb{F}_p^2. \end{cases}$

Теорема 13.3
Если в поле $\Bbbk$ есть примитивный корень степени $m$ из единицы и $a \in \Bbbk^*$, то разложение двучлена $f(x) = x^m - a$ на неприводимые множители в $\Bbbk[x]$ всегда имеет вид $f = g_1 \dots g_k$ с $g_i(x) = x^n - b_i$, где $b_i \in \Bbbk^*$ и $n = m/k$. Такое разложение возникает если и только если группа $\operatorname{Gal} f/\Bbbk$ циклическая порядка $n$, и в этом случае $a \in {\Bbbk^*}^k$. В частности, неприводимость $f$ равносильна равенству $|\operatorname{Gal} f/\Bbbk| = m$, а также тому, что $\Bbbk$-алгебра $\Bbbk[x]/(f)$ является полем разложения многочлена $f$.

Доказательство. Фиксируем алгебраическое замыкание $\overline{\Bbbk}$ и какой-нибудь корень $\alpha \in \overline{\Bbbk}$ двучлена $f$. Корни $f$ в $\overline{\Bbbk}$ находится в биекции с корнями из единицы и имеют вид $\xi\alpha$, где $\xi$ пробегает $\boldsymbol{\mu}_m$. Если $g \in \operatorname{Gal} f/\Bbbk$ переводит $\alpha$ в $g(\alpha) = \zeta_g\alpha$, то $g$ действует и на остальные корни $f$ умножением на $\zeta_g$, ибо $g(\xi\alpha) = \xi g(\alpha) = \xi\zeta_g\alpha = \zeta_g\xi\alpha$. Поэтому отображение

$$\operatorname{Gal} f/\Bbbk \hookrightarrow \boldsymbol{\mu}_m\,, \quad g \mapsto \zeta_g = g(\alpha)/\alpha\,, \tag{13-13}$$

является инъективным гомоморфизмом групп. Обозначим через $G \subset \boldsymbol{\mu}_m$ его образ. Так как группа $\boldsymbol{\mu}_m$ циклическая, $G \simeq \operatorname{Gal} f/\Bbbk$ является циклической группой порядка $n|m$ и порождается некоторым примитивным корнем $\zeta$ степени $n$ из единицы. Смежные классы $G\xi \subset \boldsymbol{\mu}_m$ подгруппы $G$ биективно соответствуют орбитам действия группы Галуа на корнях $f$, и каждой такой орбите отвечает неприводимый множитель $f_\xi(x) \overset{\text{def}}{=} \prod_{\nu=0}^{n-1}\left(x - \zeta^\nu\xi\alpha\right)$ двучлена $f$ в $\Bbbk[x]$.

Упражнение 13.9. Покажите, что $f_\xi(x) = x^n - \xi^n\alpha^n$.

Так как $f_\xi \in \Bbbk[x]$, все элементы $b_\xi = \xi^n\alpha^n$ и, в частности, $c = \alpha^n$ лежат в $\Bbbk$. Таким образом, разложение $f$ на неприводимые множители в $\Bbbk[x]$ имеет вид $x^m - a = \prod_{\xi\in\boldsymbol{\mu}_m/G}\left(x^n - b_\xi\right)$, а свободный член $a = \alpha^m = c^k \in {\Bbbk^*}^k$, где $k = m/n$. Неприводимость $f$ означает равенство $n = m$, и в этом случае вложение (13-13) является изоморфизмом, а алгебра $\Bbbk[x]/(f)$ — полем, содержащим вместе с $\alpha = x \pmod f$ и все остальные $m$ корней $\xi\alpha$ двучлена $f$. □

Упражнение 13.10. В условиях теор. 13.3 покажите, что совпадение в $\overline{\Bbbk}$ полей разложения двучленов $x^m - a$ и $x^m - b$ равносильно равенству $a = b^r c^m$ для неких $c \in \Bbbk$ и целого $r$, взаимно простого с $m$.

Определение 13.1
Расширение Галуа $\mathbb{K} \supset \Bbbk$ называется *циклическим степени* $m$, если $\operatorname{Gal} \mathbb{K}/\Bbbk$ является циклической группой $m$-того порядка.

Теорема 13.4
Всякое циклическое расширение степени $m$ любого поля $\Bbbk$, содержащего первообразный корень $m$-той степени из единицы, является полем разложения неприводимого двучлена $x^m - a$ с $a \in \Bbbk$.

Доказательство. Пусть группа Галуа $G = \operatorname{Gal} \mathbb{K}/\Bbbk$ циклического расширения $\mathbb{K} \supset \Bbbk$ порождена автоморфизмом $\sigma \in \operatorname{Aut}_{\Bbbk} \mathbb{K}$ порядка $m$. Фиксируем какой-нибудь первообразный корень $m$-той степени из единицы $\zeta \in \Bbbk$ и рассмотрим $\Bbbk$-линейный эндоморфизм поля $\mathbb{K}$

$$L_{\zeta,\sigma} \overset{\text{def}}{=} \sum_{i=0}^{p-1}\zeta^i\sigma^i : \ \vartheta \mapsto \sum_{i=0}^{p-1}\zeta^i\sigma^i(\vartheta)\,.$$

Поскольку автоморфизмы $\sigma^0 = \mathrm{Id}$, $\sigma$, $\sigma^2$, … , $\sigma^{m-1}$ являются различными мультипликативными характерами[1] абелевой группы $\mathbb{K}^*$ над полем $\mathbb{K}$, они линейно независимы в пространстве функций[2] $\mathbb{K}^* \to \mathbb{K}$. Поэтому эндоморфизм $L_{\zeta,\sigma}$ ненулевой.

Упражнение 13.11. Убедитесь, что $\sigma L_{\zeta,\sigma} = \zeta^{-1} L_{\zeta,\sigma}$.

Равенство $\left(\sigma - \zeta^{-1}\right) L_{\zeta,\sigma} = 0$ означает, что образ оператора $L_{\zeta,\sigma}$ состоит из собственных векторов оператора $\sigma$ с собственным значением $\zeta^{-1}$. Тем самым, в $\mathbb{K}$ имеется такое ненулевое $\alpha$, что $\sigma(\alpha) = \zeta^{-1}\alpha$. Галуа-орбита числа $\alpha$ состоит из $m$ различных чисел $\sigma^i(\alpha) = \zeta^{-i}\alpha$, $0 \leqslant i \leqslant m-1$, являющихся корнями двучлена $f(x) = x^m - \alpha^m$, свободный член которого $a = \alpha^m$ лежит в $\Bbbk$, так как он инвариантен относительно группы Галуа: $\sigma(\alpha^m) = \sigma(\alpha)^m = \zeta^{-m}\alpha^m = \alpha^m$. Поскольку корни $f$ образуют одну орбиту группы Галуа, двучлен $f$ неприводим, а так как все корни лежат в $\Bbbk[\alpha]$, примитивное расширение $\Bbbk[\alpha]$ является полем разложения $f$. Поскольку $\Bbbk[\alpha] \subset \mathbb{K}$ и степень обоих полей над $\Bbbk$ равна $m$, они совпадают друг с другом. □

Упражнение 13.12* (изоморфизм Куммера). Для каждого элемента $a \in \Bbbk^* / \Bbbk^{*m}$ зафиксируем некоторый корень $\alpha = \sqrt[m]{a} \in \overline{\Bbbk}$ и сопоставим каждому автоморфизму $\sigma \in \mathrm{Gal}\,\overline{\Bbbk}/\Bbbk$ корень из единицы $\zeta_\sigma = \sigma(\alpha)/\alpha \in \boldsymbol{\mu}_m$. Покажите, что таким образом корректно задаётся изоморфизм групп $\Bbbk^*/\Bbbk^{*m} \xrightarrow{\sim} \mathrm{Hom}(\mathrm{Gal}\,\overline{\Bbbk}/\Bbbk, \boldsymbol{\mu}_m)$.

**13.5. Разрешимые расширения.** Конечная группа $G$ называется *разрешимой*, если все её композиционные факторы Жордана – Гёльдера[3] суть простые циклические группы. Расширение Галуа $\mathbb{K} \supset \Bbbk$ поля $\Bbbk$ характеристики нуль называется *разрешимым*, если разрешима его группа Галуа $\mathrm{Gal}\,\mathbb{K}/\Bbbk$. Из установленных во втором семестре первого курса свойств композиционных рядов вытекает, что разрешимость группы $G$ равносильна существованию убывающей фильтрации $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ подгруппами $G_{i+1} \lhd G_i$ с абелевыми факторами $G_i/G_{i+1}$.

Упражнение 13.13. Убедитесь, что любая подгруппа и любая фактор группа разрешимой группы $G$ разрешимы, и наоборот, разрешимость нормальной подгруппы $H \lhd G$ и фактора $G/H$ влекут разрешимость $G$.

Теорема 13.5

Пусть[4] $\mathrm{char}(\Bbbk) = 0$ и один из корней неприводимого многочлена $f \in \Bbbk[x]$ выражается через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечений корней произвольных степеней. Тогда группа $\mathrm{Gal}\,f/\Bbbk$ разрешима, и все корни $f$ выражаются в радикалах через элементы поля $\Bbbk$.

Доказательство. Зафиксируем алгебраическое замыкание $\overline{\Bbbk} \supset \Bbbk$. Если корень $\alpha \in \overline{\Bbbk}$ многочлена $f$ выражается в радикалах, то он лежит в подполе $\mathbb{L} \subset \overline{\Bbbk}$, к которому ведёт башня примитивных расширений

$$\Bbbk = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_m = \mathbb{L} \tag{13-14}$$

вида $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$, где $a_i \in \mathbb{L}_i$. Для доказательства теоремы достаточно вложить поле $\mathbb{L}$ в поле $\mathbb{L}' \supset \Bbbk$, являющееся расширением Галуа с разрешимой группой $\mathrm{Gal}\,\mathbb{L}'/\Bbbk$. Тогда

[1] См. n° 5.4.1 на стр. 72.

[2] См. цитированный выше n° 5.4.1 на стр. 72, в частности упр. 5.21.

[3] См. n° 12.2 на стр. 178 лекции http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_12.pdf.

[4] Требование $\mathrm{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\mathrm{char}(\Bbbk)$ не делила ни один из показателей радикалов, участвующих в формуле для вычисления корня. Приводимое доказательство в этом случае тоже работает.

поле разложения $\mathbb{K}$ многочлена $f$ будет нормальным над $\Bbbk$ подполем в $\mathbb{L}'$, и его группа Галуа $\mathrm{Gal}\,\mathbb{K}\,/\,\Bbbk = (\mathrm{Gal}\,\mathbb{L}'\,/\,\Bbbk)\,/\,(\mathrm{Gal}\,\mathbb{L}'\,/\,\mathbb{K})$, будучи фактором разрешимой группы, тоже будет разрешима. Для построения $\mathbb{L}'$ расширим башню (13-14) до башни $\Bbbk \subset \mathbb{L}'_0 \subset \mathbb{L}'_1 \subset \ldots \subset \mathbb{L}'_m = \mathbb{L}'$, в которой $\mathbb{L}_i \subset \mathbb{L}'_i$ и все $\mathbb{L}'_i$ являются расширениями Галуа поля $\Bbbk$. В качестве $\mathbb{L}'_0$ возьмём поле разложения многочлена $x^N - 1$ с таким $N$, чтобы в $\mathbb{L}'_0$ содержались первообразные корни из единицы всех степеней $k_i$, являющихся показателями радикалов в формуле для $\alpha$. Далее действуем по индукции: если $\mathbb{L}'_i$ уже построено, то в качестве $\mathbb{L}'_{i+1}$ возьмём поле разложения многочлена $\prod_{\sigma\in\mathrm{Gal}\,\mathbb{L}'_i/\Bbbk}(x^{k_i} - \sigma(a_i))$ над полем $\mathbb{L}'_i$. Так как коэффициенты этого многочлена инвариантны относительно группы $\mathrm{Gal}\,\mathbb{L}'_i/\Bbbk$, они лежат в $\Bbbk$, и $\mathbb{L}'_{i+1} \supset \Bbbk$ является расширением Галуа, содержащим поле $\mathbb{L}_{i+1} = \mathbb{L}_i[x]/(x^{k_i} - a_i)$. Поле $\mathbb{L}'_{i+1}$ получается из поля $\mathbb{L}'_i$ цепочкой последовательных переходов к полям разложения двучленов вида $x^n - a$ с $a \in \mathbb{L}'_i$. По теор. 13.3 все такие переходы являются расширениями Галуа с циклическими группами Галуа. Согласно предл. 13.5 и предл. 12.4 первый шаг нашего построения — переход от $\Bbbk$ к $\mathbb{L}'_0$ — также является расширением Галуа с абелевой группой Галуа. Таким образом, поле $\mathbb{L}'$ можно получить из $\Bbbk$ последовательными абелевым расширением Галуа, и его группа $\mathrm{Gal}\,\mathbb{L}'\,/\,\Bbbk$ разрешима. □

Пример 13.4 (общее уравнение степени $n$ и теорема Абеля)
Зафиксируем произвольное поле $\mathbb{F}$. Многочлен

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{F}(a_1, \ldots, a_n)[x]\,, \tag{13-15}$$

рассматриваемый над полем $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$ рациональных функций от $n$ алгебраически независимых переменных $a_1, \ldots, a_n$ с коэффициентами в $\mathbb{F}$, называется *общим*, поскольку придавая его коэффициентам конкретные значения из поля $\mathbb{F}$, можно получить любой «конкретный» многочлен $f \in \mathbb{F}[x]$. В частности, если имеется формула, выражающая корни общего многочлена (13-15) через элементы поля $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$ в радикалах[1], то она позволяет единообразно решить в радикалах все уравнения $n$-той степени с коэффициентами из $\mathbb{F}$. Из прим. 13.2 на стр. 188 следует, что над полем $\mathbb{F} = \mathbb{Q}$ такой формулы нет. Чтобы проанализировать наличие такой формулы над произвольным полем $\mathbb{F}$, вычислим группу $\mathrm{Gal}\,f/\Bbbk$. Обозначим через $t_1, \ldots, t_n$ корни $f$ в его поле разложения $\mathbb{K} \supset \Bbbk$. Поскольку $\mathbb{K}$ алгебраично над $\Bbbk$, его базис трансцендентности над $\mathbb{F}$ согласно сл. 9.6 можно выбрать из элементов $t_1, \ldots, t_n$, порождающих $\mathbb{K}$ как $\mathbb{F}$-алгебру[2]. Так как $\mathrm{tr\,deg}_{\mathbb{F}}\,\mathbb{K} \geqslant n$, базисом трансцендентности $\mathbb{K}$ над $\mathbb{F}$ является весь набор $t_1, \ldots, t_n$. В частности, $t_1, \ldots, t_n$ алгебраически независимы над $\mathbb{F}$ и различны, многочлен $f$ сепарабелен, а $\mathbb{K} = \mathbb{F}(t_1, \ldots, t_n)$ является расширением Галуа поля $\Bbbk = \mathbb{F}(a_1, \ldots, a_n)$. Поскольку любая перестановка независимых переменных продолжается до автоморфизма поля рациональных функций, группа $\mathrm{Gal}\,\mathbb{K}\,/\,\Bbbk = S_n$, степень $[\mathbb{K} : \Bbbk] = n!$ и поле инвариантов $\mathbb{F}(t_1, \ldots, t_n)^{S_n} = \mathbb{F}(a_1, \ldots, a_n)$. Так как подгруппа $A_n \lhd S_n$ проста, группа $S_n$ не разрешима, а значит, общее уравнение степени $n \geqslant 5$ не разрешимо в радикалах ни над каким полем $\mathbb{F}$. Этот результат известен как *теорема Абеля*[3].

Упражнение 13.14. Покажите, что поле инвариантов $\mathbb{K}^{A_n}$ подгруппы $A_n \lhd S_n$ является квадратичным расширением поля $\Bbbk$ элементом $\sqrt{D(f)} = \prod_{1\leqslant i<j\leqslant n}(t_i - t_j)$.

---

[1] Как это делает, например, школьная формула $x_\pm = (p \pm \sqrt{p^2 - 4q})\,/\,2$ для решения «общего» квадратного уравнения $x^2 + px + q = 0$.

[2] По теореме Виета $a_i$ являются полиномами от $t_i$.

[3] Сам Абель доказал эту теорему для поля $\mathbb{F} = \mathbb{C}$ с привлечением комплексного анализа.

Замечание 13.2. Отсутствие «общей» формулы для решения в радикалах полиномиального уравнения $n$-той степени не запрещает существования специальных «конкетных» уравнений, корни которых можно выразить в радикалах через коэффициенты уравнения.

Теорема 13.6
Пусть[1] $\mathrm{char}(\Bbbk) = 0$ и $f \in \Bbbk[x]$ приведён и неприводим. Если группа $\mathrm{Gal}\, f / \Bbbk$ разрешима, то все корни многочлена $f$ выражаются через элементы поля $\Bbbk$ посредством четырёх арифметических действий и извлечения корней.

Доказательство. Обозначим через $\mathbb{K} \supset \Bbbk$ поле разложения многочлена $f$, а через $\mathbb{L} \supset \Bbbk$ результат присоединения к $\Bbbk$ первообразного корня степени $n = |\,\mathrm{Gal}\,\mathbb{K}/\Bbbk|$ из единицы. Все элементы поля $\mathbb{L}$ выражаются в радикалах через элементы поля $\Bbbk$. По предл. 13.2 расширение $\mathbb{L}\mathbb{K} \supset \mathbb{L}$ является расширением Галуа, и его группа Галуа $G$ является подгруппой разрешимой группы $\mathrm{Gal}\,\mathbb{K} / \Bbbk$. Поэтому $G$ тоже разрешима и имеет фильтрацию $G = G_0 \supset G_1 \supset \ldots \supset G_m = \{e\}$ с простыми циклическими факторами $G_i / G_{i+1} \simeq \mathbb{Z}/(p_i)$. Тем самым, поле $\mathbb{L}\mathbb{K}$ получается из $\mathbb{L}$ последовательными циклическими расширениями Галуа. По теор. 13.4 каждое такое расширение получается присоединением радикала. Следовательно, все элементы поля $\mathbb{L}\mathbb{K}$ выражаются в радикалах через элементы поля $\Bbbk$. □

[1] Требование $\mathrm{char}(\Bbbk) = 0$ можно ослабить до требования, чтобы $\mathrm{char}(\Bbbk)$ не совпадала с порядком никакого композиционного фактора Жордана – Гёльдера группы Галуа многочлена $f$. Приводимое доказательство в этом случае тоже работает.

## Ответы и указания к некоторым упражнениям

Упр. 1.2. В силу биективности отображения Сегре, соотношения инцидентности между прямыми на квадрике Сегре такие же, как между координатными прямыми на $\mathbb{P}_1 \times \mathbb{P}_1$. Так как всякая проходящая через заданную точку $p$ прямая, целиком лежащая на квадрике Сегре $S$, лежит в пересечении $S \cap T_pS$ этой квадрики с её касательной плоскостью в точке $p$, и плоская коника $S \cap T_pS$ уже полностью исчерпывается парой пересекающихся в точке $p$ прямых из разных семейств, никаких других прямых на квадрике Сегре нет.

Упр. 1.3. Для любого $\mathbb{Z}$-билинейного отображения $\varphi : \mathbb{Z}\times A \to W$ равенство $\varphi = F \circ \tau$ выполняется для единственного $\mathbb{Z}$-линейного отображения $F : A \to W$, $a \mapsto \varphi(1, a)$.

Упр. 1.4. Ср. с упр. 1.3.

Упр. 2.1. То, что $SV$ и $\iota$ однозначно определяются своим универсальным свойством, доказывается дословно также, как в лем. 1.1 на стр. 6.

Упр. 2.2. Выберем базис $E$ в $U \cap W$, дополним его множествами $E'$ и $E''$ до базисов в $U$ и $W$ соответственно, и зафиксируем в $V$ базис вида $E \sqcup E' \sqcup E'' \sqcup E'''$. Пространство $U^{\otimes n} \cap W^{\otimes n}$ состоит из линейных комбинаций тензорных мономов, составленных из базисных векторов, лежащих в $E$, и стало быть, совпадает с $(U \cap W)^{\otimes n}$.

Упр. 2.3. Для любых $x, y \in I$ произведение $(a + x)(b + y) = ab + (ay + xb + xy) \cong ab \pmod{I}$. Обратите внимание, что для только левых или только правых идеалов это может быть неверно.

Упр. 2.4. Каждое линейное отображение $f : V \to A$ в коммутативную $K$-алгебру $A$ однозначно поднимается по универсальному свойству тензорной алгебры до гомоморфизма алгебр $\tilde{f} : TV \to A$ по формуле $\tilde{f}(v_1 \otimes \cdots \otimes v_n) = f(v_1)\cdots f(v_n)$. Так как в коммутативной алгебре $f(u)f(w) = f(w)f(u)$ для всех $u, w \in V$, гомоморфизм $\tilde{f}$ аннулирует все разности $u \otimes w - w \otimes u$ и пропускается через факторизацию $TV \twoheadrightarrow T/\mathcal{I}_{\mathrm{sym}} \simeq SV$. Это доказывает выполнение универсального свойства. То, что $SV$ и $\iota$ однозначно им определяются, устанавливается дословно так же, как в лем. 1.1 на стр. 6.

Упр. 2.5. Дословно те же аргументы, что и для тензорного произведения, см. лем. 1.1 на стр. 6.

Упр. 2.6. Ответ: $\binom{n+d-1}{d-1}$. Это число решений уравнения $m_1 + \cdots + m_d = n$ в неотрицательных целых числах $m_1, \dots, m_d$.

Упр. 2.7. Модифицируйте решение упр. 2.4.

Упр. 2.8. Форма $\alpha$ меняет знак при транспозиции любых двух аргументов, поскольку

$$0 = \alpha(\dots, (v + w), \dots, (v + w), \dots) = \alpha(\dots, v, \dots, w, \dots) + \alpha(\dots, w, \dots, v, \dots).$$

Упр. 2.9. Дословно те же аргументы, что и в лем. 1.1 на стр. 6.

Упр. 2.10. Отправляя линейную форму $\xi : \Lambda^n V \to \Bbbk$ в её композицию с антикоммутативным умножением $\alpha_n : V \times \cdots \times V \to \Lambda^n V$, мы получаем линейное отображение $(\Lambda^n V)^* \to \mathrm{Alt}^n(V, \Bbbk)$, являющееся изоморфизмом в силу универсального свойства $\alpha_n$.

Упр. 2.11. Фиксируем в $U$ базис $e_1, \dots, e_m$. Если $\omega \notin \Lambda^m U$, то в $\omega$ есть моном $e_I$, не содержащий какого-нибудь базисного вектора, скажем, $e_j$. Тогда $e_j \wedge \omega \neq 0$, ибо содержит ненулевой моном $e_{j\sqcup I}$. Наоборот, если $\omega \in \Lambda^m U$, то $\omega = \lambda \cdot e_1 \wedge \ldots \wedge e_m$, и $e_i \wedge \omega = 0$ для всех $i$, а значит, $u \wedge \omega = 0$ для всех $u \in U$.

Упр. 2.12. Стабилизатор каждого монома из обиты $E_{\boldsymbol{m}}$ в группе $S_n$ состоит из $m_1!\, m_2!\, \cdots\, m_k!$ независимых перестановок одинаковых тензорных сомножителей между собою. Остаётся применить формулу для длины орбиты.

Упр. 2.14. Используйте те же аргументы, что и в примере 1.2 из части I.

Упр. 2.16. Так как утверждение линейно по $v$, $f$, $g$, его достаточно проверить для $v = e_i$, $f = x_1^{m_1} \dots x_d^{m_d}$, $g = x_1^{k_1} \dots x_d^{k_d}$.

Упр. 2.21. Аналогично упр. 2.16.

Упр. 2.22. Сначала убедитесь, что $\Lambda^n U \cap \Lambda^n W = \Lambda^n (U \cap W)$ в $\Lambda^n V$ для любых подпространств $U, W \subset V$.

Упр. 2.25. Каждый моном $e_i \wedge e_j$ поляризуется в билинейную форму

$$\frac{1}{2}(e_i \otimes e_j - e_j \otimes e_i) \colon V^* \times V^* \to \Bbbk\,, \quad (x_k, x_m) \mapsto \begin{cases} 1/2 & \text{при } k = i, m = j \\ -1/2 & \text{при } k = j, m = i \\ 0 & \text{в остальных случаях} \end{cases}$$

поэтому каждая пара слагаемых $a_{ij}\left(e_i \wedge e_j - e_i \wedge e_j\right)$, где $i < j$, поляризуется в квадратичную форму, матрица Грама которой имеет $a_{ij}$ и $-a_{ij}$, соответственно, в клетках $(i, j)$ и $(j, i)$, и нули в остальных местах.

Упр. 2.26. Пусть $U_1 \neq U_2$. Выберем базис в $U_1 \cap U_2$, дополним его до базисов в $U_1$, $U_2$, и включим все эти векторы в некоторый базис пространства $V$. Тогда $\Lambda^k U_1$ и $\Lambda^k U_2$ будут порождаться различными базисными мономами пространства $\Lambda^k V$.

Упр. 2.27. По условию, $\boldsymbol{w} = \boldsymbol{e} \cdot X_{\boldsymbol{w}}^t$, $\boldsymbol{u} = \boldsymbol{e} \cdot X_{\boldsymbol{u}}^t$, $\boldsymbol{w} = u \cdot C_{\boldsymbol{uw}}$, где $\boldsymbol{e}$, $\boldsymbol{u}$, $\boldsymbol{w}$ суть строки из базисных векторов в $V$ и $U$. Следовательно, $X_{\boldsymbol{w}}^t = X_{\boldsymbol{u}}^t C_{\boldsymbol{uw}}$.

Упр. 2.28. См. http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/lec_08.pdf, раздел 8.4.2 на стр. 118.

Упр. 3.3. Поскольку $\Delta_\delta$ обращается в нуль при подстановке $x_i = x_j$, он делится в кольце $\mathbb{Z}[x_1, \dots, x_n]$ на $(x_i - x_j)$. Так как каждая из разностей $(x_i - x_j)$ неприводима, $f$ делится на $\prod_{i<j}(x_i - x_j)$. Сравнивая лексикографически старшие мономы в этом произведении и в $\Delta_\delta$, заключаем, что частное равно 1.

Упр. 3.4. Разложим перестановку $g$ циклового типа $\lambda$ в произведение независимых циклов и запишем их по строкам диаграммы так, чтобы действие перестановки $g$ циклически сдвигало все элементы вдоль строк на единицу влево. Сопряжение перестановки $g$ перестановкой $h$ состоит в замене содержимого клеток диаграммы по правилу $i \mapsto h(i)$. Стабилизатор $g$ состоит из всех перестановок, независимо циклически сдвигающих номера вдоль строк и переставляющих строки одинаковой длины между собою как единое целое.

Упр. 3.5. В правом нижнем углу матрицы $\left(h_{\lambda_i + j - i}\right)$, начиная с позиции $(m+1, m+1)$, где $m$ — высота диаграммы $\lambda$, будет стоять верхняя унитреугольная матрица, левее которой все элементы в строках будут нулевые.

Упр. 4.1. Устойчивое паросочетание между $i$-м и $(i+1)$-м столбцом устанавливается так: последовательно перебираем шарики в $(i+1)$-ом столбце двигаясь снизу вверх и назначаем очередному шарику $\boldsymbol{ш}$ партнёром самый верхний шар $i$-го столбца, лежащий строго ниже $\boldsymbol{ш}$ и ещё не назначенный никому партнёром, а если таких шаров нет, объявляем $\boldsymbol{ш}$ свободным. После того, как все шары $(i+1)$-го столбца разделены на свободные и имеющие партнёров, все шары $i$-го столбца, не являющиеся ничьими партнёрами, тоже объявляются свободными. Операция $L_i$ перемещает на одну клетку влево самый верхний свободный шар $(i+1)$-го столбца или ничего не делает, если свободных шаров в $(i+1)$-ом столбце нет. Операция $R_i$ перемещает на одну клетку вправо самый нижний свободный шар $i$-го столбца или ничего не делает, если в $i$-ом столбце нет свободных шаров.

Упр. 4.3. Диаграммы $\ydiagram{4,1,1}$ и $\ydiagram{3,3}$ несравнимы по отношению $\trianglerighteq$.

Упр. 4.4. $s_{(1)} \cdot s_{(1,1)} = s_{(2,1)} + s_{(1,1,1)} = s_{(1,1)} \cdot s_{(1)}$

Упр. 4.5. Для вычисления $s_\lambda \cdot e_k$ к диаграмме $\lambda$ надо дописать $k$ клеток и заполнить их без повторений числами от 1 до $k$. Попадание двух таких клеток в одну строку противоречит либо табличному ограничению, либо ограничению Яманучи. Для вычисления $s_\lambda \cdot h_k$ к диаграмме $\lambda$ надо дописать $k$ клеток, заполненных единицами. Попадание двух таких клеток в один столбец противоречит табличному ограничению.

Упр. 5.1. Для всех $w \in W$ и $u \in U$ вектор $f(w+u) = fw + fu$ лежит в том же классе, что и $fw$, поскольку $fu \in U$.

Упр. 5.3. При $m \geqslant 2$ классы многочленов, делящихся на $p$, составляют нетривиальный подмодуль в $\Bbbk[t]/\left(p^m\right)$. При $m = 1$ фактор кольцо $\Bbbk[t]/(p)$ является полем, т. е. для любого ненулевого класса $[g] \in \Bbbk[t]/(p)$ существует такой многочлен $h \in \Bbbk[t]$, что $h \cdot [g] = [1]$. Поэтому любой класс $[f] \in \Bbbk[t]/(p)$ получается из класса $[g]$ применением оператора $h(t) \cdot f(t)$.

Упр. 5.4. Диагональный оператор с собственными числами $\lambda_1, \dots, \lambda_n$ аннулируется многочленом $\prod(t-\lambda_i)$. Наоборот, поскольку многочлен, аннулирующий модуль (5-2), делится на максимальную степень каждого элементарного делителя, все элементарные делители имеют вид $t-\lambda$ и входят в разложение (5-2) только в первых степенях, что и означает диагонализуемость оператора умножения на $t$.

Упр. 5.5. Верхней гранью цепи из $\mathcal{S}'$ является объединение всех модулей цепи.

Упр. 5.6. Пусть $w = u + v$. Тогда $fw = fu + fv$ и $fv \in V$. Поэтому $\pi(fw) = fu = f\pi(w)$.

Упр. 5.7. Пусть $\pi(S) \neq 0$ для простого подмодуля $U \subset W$. Поскольку $f\pi(s) = \pi(fs) \in \pi(S)$ для всех $f \in R$ и $s \in S$, подпространство $\pi(S)$ является $R$-подмодулем. Для любого $R$-подмодуля $M \subset \pi(S)$ пересечение
$$S \cap \pi^{-1}(M) = \{s \in S \mid \pi(s) \in M\}$$
является $R$-подмодулем в $S$: если $\pi(s) \in M$, то $\pi(fs) = f\pi(s) \in M$ для всех $f \in R$ и $s \in S$. Так как в $S$ нет нетривиальных собственных подмодулей, их нет и в $\pi(S)$.

Упр. 5.8. Верхней гранью цепи из $\mathcal{S}$ является объединение или, что то же самое, прямая сумма всех модулей цепи.

Упр. 5.9. (а) и (б) проверяются непосредственно; (в) проверяется так: если $\varphi(v) = 0$, то $\varphi(fv) = f\varphi(v) = f(0) = 0$ для всех $f \in R$, а если $v = \varphi(u)$, то $fv = f\varphi(u) = \varphi(fu)$ для всех $g \in R$; (г) фактически было доказано в упр. 5.7.

Упр. 5.12. $\varphi\psi = \sum_{\alpha,\beta} \iota_\alpha \varphi_{\alpha\beta} \pi_\beta \circ \sum_{\mu,\nu} \iota_\mu \varphi_{\mu\nu} \pi_\nu = \sum_{\alpha,\nu} \iota_\alpha p_{\alpha\nu} \pi_\nu$, where $p_{\alpha\nu} = \sum_\eta \varphi_{\alpha\eta}\psi_{\eta\nu}$, because
$$\pi_\beta \iota_\mu = \begin{cases} \mathrm{Id}_{V_\eta} & \text{for } \beta = \mu = \eta \\ 0 & \text{otherwise} \end{cases}$$

Упр. 5.13. Из равенства $\mathrm{Ass}(R) = \mathrm{End}(V)$ вытекает, что $A_R$ действует транзитивно на ненулевых векторах пространства $V$, т. е. $A_R$-орбита любого ненулевого вектора совпадает со всем пространством $V$.

Упр. 5.17. Поскольку правило $g : \varphi \mapsto g\varphi g^{-1}$ линейно по $\varphi$, его достаточно проверять только на разложимых $\varphi = \xi \otimes w$ с $\xi \in U^*$, $w \in W$. По определению

$$\varrho^* \otimes \lambda(g) : \xi \otimes w \mapsto \varrho(g^{-1})^* \xi \otimes \lambda(g) w = (\xi \circ g^{-1}) \otimes (gw) .$$

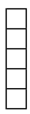
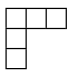
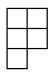
Этот оператор переводит $u \in U$ в $\xi(g^{-1}u) \cdot gw = g\left(\xi(g^{-1}u) \cdot w\right) = g \circ (\xi \otimes w) \circ g^{-1}(u)$.

Упр. 5.21. Пусть множество различных гомоморфизмов $\psi_\nu : G \to \Bbbk^*$ линейно зависимо. Рассмотрим линейную зависимость $\lambda_1\psi_1 + \dots + \lambda_n\psi_n = 0$ с минимально возможным числом слагаемых и какой-нибудь элемент $h \in G$, на котором $\psi_1(h) \neq \psi_2(h)$. Поскольку для каждого $g \in G$ выполняется равенство $\sum_i \lambda_i \psi_i(h)\psi_i(g) = \sum_i \lambda_i \psi_i(hg) = 0$, имеется ещё одно линейное соотношение между функциями $\psi_i$ с коэффициентами $\lambda_i\,\psi_i(h)$. Деля все коэффициенты на $\psi_1(h)$ и вычитая из первой зависимости, получаем линейную зависимость между $\psi_i$ с нулевым коэффициентом при $\psi_1$ и ненулевым коэффициентом при $\psi_2$. Она нетривиальна и содержит меньше слагаемых. Противоречие.

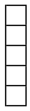
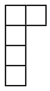
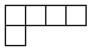
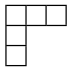
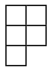
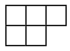
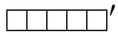
Упр. 5.31. Достаточно показать, что никакая ненулевая линейная форма $\varphi \in \mathrm{Sym}^n(W)^*$ не зануляется на всех тензорах $w^{\otimes n}$. Зафиксируем в $W$ базис $e_1, \dots, e_d$. Пусть $w = \sum x_i e_i$, а $\varphi$ переводит стандартный базисный вектор $e_{[m_1 \dots m_d]} \in \mathrm{Sym}^n(W)$ в число $a_{m_1 \dots m_d} \in \Bbbk$. Тогда $\varphi\left(w^{\otimes n}\right) = \sum_{m_1 \dots m_d} a_{m_1 \dots m_d} x_1^{m_1} x_2^{m_2} \dots x_d^{m_d}$. Над бесконечным полем $\Bbbk$ такой многочлен тогда и только тогда является тождественно нулевой функцией от $x_1, \dots, x_n$, когда все его коэффициенты $a_{m_1 \dots m_d} = 0$.

Упр. 5.32. Пусть все тензоры вида $w^{\otimes n}$ с $F(w) \neq 0$ лежат в гиперплоскости $\mathrm{Ann}\,\psi$, где $\psi$ — линейная форма на $\mathrm{Sym}^n(W)$. Функция $G(w) = \psi(w^{\otimes})$ является однородным многочленом степени $n$ на $W$. По условию, многочлен $F \cdot G$ является тождественно нулевой функцией на $W$. Поэтому это нулевой многочлен, и так как $F \neq 0$, то $G = 0$, т. е. $\psi(w^{\otimes}) \equiv 0$ и *все* тензоры $w^{\otimes} \in \mathrm{Ann}\,\psi$, что противоречит принципу Аронгольда из упр. 5.31.

Упр. 6.7. Группа $A_5$ имеет два трёхмерных неприводимых представления вращениями икосаэдра (отличающиеся на композицию с внешним автоморфизмом $A_5$, который задаётся сопряжением любой транспозицией внутри $S_5$) и четырёхмерное представление вращениями симплекса. Полная таблица неприводимые характеров $A_5$ такова:

| классы |  |  |  | (12345) | (21345) |
|---|---|---|---|---|---|
| число элементов | 1 | 20 | 15 | 12 | 12 |
| значения характеров: | | | | | |
| тривиальный | 1 | 1 | 1 | 1 | 1 |
| икосаэдр-1 | 3 | 0 | $-1$ | $\frac{1+\sqrt{5}}{2}$ | $\frac{1-\sqrt{5}}{2}$ |
| икосаэдр-2 | 3 | 0 | $-1$ | $\frac{1-\sqrt{5}}{2}$ | $\frac{1+\sqrt{5}}{2}$ |
| симплициальный | 4 | 1 | 0 | $-1$ | $-1$ |
| пятимерный | 5 | $-1$ | 1 | 0 | 0 |

Группа $S_5$ имеет знаковое одномерное представление sgn и симплициальное представление $\varDelta$. Представления $\operatorname{sgn}\otimes\varDelta$ и $\Lambda^2\varDelta$ тоже неприводимы, а $S^2\varDelta = \operatorname{sgn}\oplus\varDelta\oplus\zeta$, где $\zeta$ — неприводимое пятимерное представление, которое геометрически описывается как действие $S_5 \simeq \mathrm{PGL}_2(\mathbb{F}_5)$ на пространстве функций на $\mathbb{P}_1(\mathbb{F}_5)$ с нулевой суммой значений. Изоморфизм $\mathrm{PGL}_2(\mathbb{F}_5) \xrightarrow{\sim} S_5$ задаётся действием группы $\mathrm{PGL}_2(\mathbb{F}_5)$ сопряжениями на множестве нелинейных[1] инволюций без неподвижных точек на $\mathbb{P}_1(\mathbb{F}_5)$. Ответ:

| классы |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| число элементов | 1 | 10 | 30 | 20 | 15 | 20 | 24 |
| значения характеров: | | | | | | | |
| тривиальный | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| знаковый $\alpha$ | 1 | $-1$ | $-1$ | 1 | 1 | $-1$ | 1 |
| симплициальный $\vartheta$ | 4 | 2 | 0 | 1 | 0 | $-1$ | $-1$ |
| четырёхмерный $\vartheta\otimes\alpha$ | 4 | $-2$ | 0 | 1 | 0 | 1 | $-1$ |
| шестимерный $\Lambda^2\vartheta$ | 6 | 0 | 0 | 0 | $-2$ | 0 | 1 |
| пятимерный $\zeta\subset S^2\vartheta$ | 5 | 1 | $-1$ | $-1$ | 1 | 1 | 0 |
| пятимерный $\zeta\otimes\alpha$ | 5 | $-1$ | 1 | $-1$ | 1 | $-1$ | 0 |

Упр. 6.8. Выберите в $U\otimes W$ базис, согласованный с этим прямым разложением и рассмотрите соответствующий ему базис из мономов $m$-й степени.

Упр. 6.10. Каноническое отображение $B$-модулей $B\otimes_A A \to B$, ассоциированное с вложением $A$-модулей $A \hookrightarrow B$, является изоморфизмом для любого расширения $A\subset B$ ассоциативных алгебр с единицами.

Упр. 6.14. Зафиксируем систему представителей $\{g_1,\dots,g_r\}$ смежных классов $G/H$. Тогда $G = g_1H\sqcup\ldots\sqcup g_rH = Hg_1^{-1}\sqcup\ldots\sqcup Hg_r^{-1}$, и каждый $H$-инвариантный оператор $\varphi:\ \Bbbk[G]\to V$ однозначно задаётся указанием $s$ векторов $v_\nu = \varphi\left(g_\nu^{-1}\right)\in V$ ибо действует на остальные базисные векторы по правилу $\varphi\left(hg_\nu^{-1}\right) = hv_\nu$. Поэтому

$$\dim\operatorname{Hom}_H(\Bbbk[G],V) = [G:H]\cdot\dim V = \dim\Bbbk[G]\otimes_{\Bbbk[H]}V\,.$$

Преобразование Фурье от $H$-инвариантного оператора $\varphi:\ g_\nu^{-1}\mapsto v_\nu$ равно

$$\frac{1}{|G|}\sum_{g\in G} g^{-1}\otimes_{\Bbbk[H]}\varphi(g) = \frac{1}{|G|}\sum_{\nu}\sum_{h\in H} g_\nu h^{-1}\otimes_{\Bbbk[H]}\varphi\left(hg_\nu^{-1}\right) = \frac{|H|}{|G|}\sum_\nu g_\nu v_\nu \in \bigoplus_\nu g_\nu V$$

и зануляется только когда все $v_\nu = 0$.

Упр. 7.4. Будем писать $T\succ_a U$, если $T\succ U$, и наибольшее из чисел, стоящих в заполнениях $T$ и $U$ в разных клетках, равно $a$. Если $T\succ_a U$ и $U\succ_b W$, то $T\succ_a W$ при $a\geqslant b$ и $T\succ_b W$ при $a\leqslant b$.

Упр. 7.5. Для всех $q\in R_T$ и $p\in C_U$ выполнено строгое неравенство $pU\succ qT$. По лем. 7.1 существует транспозиция $\tau\in R_U\cap C_T$, и вычисление (7-13) показывает, что $c_T\{U\} = 0$.

[1] Т. е. не лежащих в $\mathrm{PGL}_2(\mathbb{F}_5)$. На шеститочечном множестве $\mathbb{P}_1 = \mathbb{P}(\mathbb{F}_5^2)$ имеется 15 инволюций без неподвижных точек, и ровно 10 из них лежат в $\mathrm{PGL}_2(\mathbb{F}_5)$. Последние находятся в биекции с такими точками плоскости $\mathbb{P}_2 = \mathbb{P}(S^2\mathbb{F}_5^2)$, которые не являются произведениями $ab$ точек $a,b\in\mathbb{P}_1 = \mathbb{P}(\mathbb{F}_5^2)$. Ср. с примером 18.5 на стр. 233 лекции http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2021/lec_18.pdf.

Упр. 7.8. Вычисление аналогично вычислению определителя Вандермонда: в кольце многочленов $\mathbb{Z}[\eta_1, \dots, \eta_n]$ определитель делится на каждую из разностей $\eta_i - \eta_j$, а значит, и на $\prod_{i<j}(\eta_i - \eta_j)$. Сравнение лексикографически старших мономов показывает, что частное равно 1.

Упр. 7.9. Индукцией по количеству столбцов покажите, что произведение длин крюков любой диаграммы $\lambda$ равно $\prod_i \eta_i!/\prod_{i<j}(\eta_i - \eta_j)$, где $\eta = \lambda + \delta$, и воспользуйтесь формулой Фробениуса. Индуктивный переход основан на том, что длина крюка $i$-той сверху клетки первого столбца равна $\eta_i - n + \ell$, где $\ell$ — число строк в диаграмме.

Упр. 8.1. Транзитивность очевидна, рефлексивность — взять $\xi = \mathrm{Id}$, кососимметричность: в силу возможности сокращать слева (соотв. справа), равенства $\varphi = \psi\xi = \varphi\xi'\xi$ (соотв. $\varphi = \xi\psi = = \xi\xi'\psi$) влекут $\xi'\xi = \mathrm{Id}$ (соотв. $\xi\xi' = \mathrm{Id}$), а равенства $\psi = \varphi\xi' = \psi\xi\xi'$ (соотв. $\psi = \varphi\xi' = \psi\xi\xi'$) влекут $\xi\xi' = \mathrm{Id}$ (соотв. $\xi\xi' = \mathrm{Id}$)

Упр. 8.6. Типичный ответ: «$\ln|x| + C$, где $C$ — произвольная константа» *неверен*[1]. На самом деле деле $C$ является сечением *постоянного пучка* $\mathbb{R}^{\sim}$ над несвязным открытым множеством $\mathbb{R} \smallsetminus 0$.

Упр. 8.12. Элементу $a \in F(A)$ отвечает естественное преобразование $f_X : \mathrm{Hom}(A, X) \to F(X)$, посылающее стрелку $\varphi : A \to X$ в значение отображения $F(\varphi) : F(A) \to F(X)$ на элементе $a$. Обратное отображение сопоставляет естественному преобразованию $f_*$ значение отображения $f_A : h^A(A) \to F(A)$ на элементе $\mathrm{Id}_A \in h^A(A)$. Проверяется это с помощью построенной по произвольной стрелке $\varphi : A \to X$ диаграммы

$$\begin{tikzcd} h^A(A) = \mathrm{Hom}(A, A) \arrow[r, "h^A(\varphi)"] \arrow[d, "f_A"'] & \mathrm{Hom}(A, X) = h^A(X) \arrow[d, "f_X"] \\ F(A) \arrow[r, "F(\varphi)"] & F(X)\,, \end{tikzcd} \tag{13-16}$$

верхняя строка которой переводит $\mathrm{Id}_A$ в $\varphi$, так что $f_X(\varphi) = F(\varphi)\big(f_A(\mathrm{Id}_A)\big)$.

Упр. 8.22. Отображения $\mathrm{Hom}_{\mathcal{M}od\text{-}B}(B, Y) \to Y$, $\varphi \mapsto \varphi(1)$, и $Y \to \mathrm{Hom}_{\mathcal{M}od\text{-}B}(B, Y)$, переводящее элемент $y \in Y$ в умножение $\varphi : b \mapsto yb$, взаимно обратны и $A$-линейны справа.

Упр. 8.24. Отображения $x \otimes_B b \mapsto xb$ и $x \mapsto x \otimes \otimes_B 1$ являются взаимно обратными $A$-линейными справа изоморфизмами между $X \otimes_B B$ и $X$.

Упр. 8.26. См. упр. 6.14 на стр. 93 и предшествующее ему обсуждение.

Упр. 8.27. Непрерывному отображению $f : |X| \to Y$ из $\mathrm{Hom}_{\mathcal{T}op}(|X|, Y)$ биективно соответствует естественное по $[n] \in \mathrm{Ob}\,\Delta$ преобразование $f_n : X_n \to \mathrm{Hom}_{\mathcal{T}op}(\Delta^n, Y)$ из $\mathrm{Hom}_{p\mathcal{S}h}(X, S(Y))$, сопоставляющее точке $x \in X_n$ композицию $f \circ \iota|_{x \times \Delta^n} : \Delta^n \to |X| \to Y$, где $\iota|_{x \times \Delta^n} : \Delta^n \to |X|$ это ограничение отображения факторизации[2] $\iota : \bigsqcup_{n \geqslant 0} X_n \times \Delta^n \to |X|$ на правильный симплекс $\{x\} \times \Delta^n \subset X_n \times \Delta^n$ (убедитесь, что $f_n$ функториально зависит от комбинаторного симплекса $[n]$). Обратная биекция сопоставляет естественному по $[n] \in \mathrm{Ob}\,\Delta$ набору отображений $f_n : X_n \to \mathrm{Hom}_{\mathcal{T}op}(\Delta^n, Y)$ отображение $|X| \to Y$, переводящее класс точки $(x, s) \in X_n \times \Delta^n$ по модулю соотношений $(X(\varphi)x, s) = (x, \varphi s)$ в значение непрерывного отображения $f_n(x) : \Delta^n \to Y$ в точке $s \in \Delta^n$ (убедитесь, что это значение не зависит от выбора представителя $(x, s)$ в его классе эквивалентности). Естественное преобразование $t_Y : |S(Y)| \to Y$ переводит класс пары

$$(g : \Delta^n \to Y, t \in \Delta^n) \in S_n(Y) \times \Delta^n = \mathrm{Hom}_{\mathcal{T}op}(\Delta^n, Y) \times \Delta^n\,,$$

[1] И в былые годы абитуриентам мехмата случалось получать за такой ответ двойку на устном вступительном экзамене по математике.

[2] Непрерывного в силу определения фактор топологии.

представляющей точку из фактор пространства $|S(Y)|$, геометрической реализации симплициального множества $S(Y)$, в точку $g(t) \in Y$ (убедитесь, что отображение $t_Y$ корректно определено, непрерывно и функториально по топологическому пространству $Y$). Действие естественного преобразования $s_X : X \to S(|X|)$ над комбинаторным симплексом $[n] \in \mathrm{Ob}\,\Delta$ переводит точку $x \in X_n$ в сингулярный симплекс $\iota|_{x \times \Delta^n} : \Delta^n \to |X|$ топологического пространства $|X|$ (убедитесь, что он функториален по $[n] \in \mathrm{Ob}\,\Delta$ и предпучку $F \in \mathrm{Ob}\,\mathcal{F}un(\Delta^{\mathrm{opp}}, \mathcal{S}et)$).

Упр. 9.1. Будучи подмодулем в поле, модуль $\mathcal{O}_K$ не имеет кручения и, стало быть, свободен. Его ранг не выше $d$, поскольку любые $d + 1$ векторов из $\mathcal{O}_K$ линейно зависимы над $\mathbb{Q}$, а значит, и над $\mathbb{Z}$. С другой стороны, подходящие натуральные кратности любых $d$ базисных векторов пространства $K$ дают линейно независимую над $\mathbb{Q}$ систему векторов в $\mathcal{O}_K$. Поэтому ранг $\mathcal{O}_K$ не меньше $d$. Всякий базис модуля $\mathcal{O}_K$ над $\mathbb{Z}$ одновременно является базисом $K$ над $\mathbb{Q}$, и в таком базисе оператор умножения на любой элемент $\zeta \in \mathcal{O}_K$ записывается целочисленной матрицей, ибо умножение на $\zeta$ переводит $\mathcal{O}_K$ в себя.

Упр. 9.2. Если $\mathbb{Q}[\sqrt{d_1}] \simeq \mathbb{Q}[\sqrt{d_2}]$, то $d_2 = (a + b\sqrt{d_1})^2 = a^2 + d_1 b^2 + 2ab\sqrt{d_1}$ для некоторых $a, b \in \mathbb{Q}$, откуда $ab = 0$ и $a^2 + d_1 b^2 = d_2$, что возможно только при $a = 0$, $b = 1$, $d_1 = d_2$.

Упр. 10.1. Если $a^n = 0$ и $b^m = 0$, то $(a + b)^{m+n-1} = 0$ и $(ca)^n = 0$ для всех $c$.

Упр. 10.5. Поскольку формула для произведения разложимых тензоров билинейна, она корректно распространяется по линейности на неразложимые тензоры. Универсальные отображения $A \xrightarrow{\alpha} A \otimes B \xleftarrow{\beta} B$ действуют по правилам $\alpha(a) = a \otimes 1$ и $\beta(b) = 1 \otimes b$. Их универсальные свойства вытекают из универсальных свойств тензорного произведения: если заданы гомоморфизмы алгебр с единицами $\varphi : A \to C$ и $\psi : B \to C$, то отображение $A \times B \to C$, $(a, b) \mapsto \varphi(a) \cdot \psi(b)$, билинейно, а значит, однозначно пропускается через тензорное произведение $A \otimes B$.

Упр. 10.6. Первые три равенства и включения $V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ) \subset V(I) \cup V(J)$ очевидны из определений.

Упр. 10.7. Если $V(f) = X$, то $f \in I(X)$, и значит, $f = 0$ в $\Bbbk[X] = \Bbbk[x_1, \dots, x_n]/I(X)$. Если $V(f) = \varnothing$, то множество нулей идеала $J \subset \Bbbk[x_1, \dots, x_n]$, порождённого идеалом $I(X)$ и многочленом $f$ пусто, и из слабой теоремы о нулях вытекает, что $1 \equiv sf \pmod{I(X)}$ для некоторого $s \in \Bbbk[x_1, \dots, x_n]$, т. е. $f$ обратим в $\Bbbk[X]$.

Упр. 10.8. $Y = (Y \cap Z) \cup \overline{Y \smallsetminus Z}$, где по условию $Y \cap Z \neq Y$.

Упр. 10.9. Иначе $X = (X \smallsetminus U) \cup V(f - g)$.

Упр. 10.12. Если $V = \cup W_i$ и $\xi_i \in V^*$ — такие ненулевые линейные формы, что $W_i \subseteq \mathrm{Ann}\,\xi_i$, то ненулевой многочлен $f = \prod \xi_i$ тождественно зануляется на $\mathbb{A}(V)$.

Упр. 10.13. Используйте покрытие $U = \bigcup \mathcal{D}(x_i)$ и предл. 10.4.

Упр. 10.14. Каждое пересечение $I \cap I(X_i)$ является собственным векторным подпространством в $I$, поскольку включение $I \subset I(X_\nu)$ означало бы, что $X_\nu \subset \bigcup_{i \neq j}(X_i \cap X_j)$, а это в силу непроводимости $X_\nu$ влечёт включение $X_\nu \subset X_i \cap X_j$ для некоторых $i \neq j$, что невозможно, т. к. ни одна из неприводимых компонент не содержится в другой. Если все неделители нуля в $I$ лежат в собственном подространстве, то $I$ оказывается объединением конечного числа собственных подпространств.

Упр. 10.15. Элемент прямого произведения не делит нуль если и только если каждая из его компонент не делит нуль: $S^{-1}_{K_1 \times \ldots \times K_k} = S^{-1}_{K_1} \times S^{-1}_{K_2} \times \cdots \times S^{-1}_{K_k}$.

Упр. 10.17. Пусть $A = \Bbbk[X]$, $B = \Bbbk[Y]$. Вложение $\varphi^* : B \hookrightarrow A$ задаёт на $A$ структуру конечно порождённой $B$-алгебры, т. е. представляет $A$ в виде $A \simeq B[x_1, \dots, x_m]/J$, что и утверждается.

Упр. 11.1. Если $x_i x_j \neq 0$, то $t_{j,\nu} = x_\nu / x_j = \left(x_\nu : x_i\right) / \left(x_j : x_i\right) = t_{i,\nu} / t_{i,j}$ (при $\nu = i$ надо считать $t_{i,i} = 1$). Поэтому $\varphi^*_{ji} : t_{j,\nu} \mapsto t_{i,\nu} / t_{i,j}$. Обратный к $\varphi^*_{ji}$ гомоморфизм $\Bbbk\left[\mathcal{D}\left(t_{i,j}\right)\right] \to \Bbbk\left[\mathcal{D}\left(t_{j,i}\right)\right]$ действует по той же формуле $t^{(i)}_j \mapsto 1/t^{(j)}_i$, $t_{i,\nu} \mapsto t_{j,\nu}/t_{j,i}$.

Упр. 11.2. В каждом таком $W$ имеется единственный базис $w_1, \dots, w_k$, проектирующийся в стандартный базис $e_{i_1}, \dots, e_{i_k}$ координатной $k$-плоскости. Матрица $z$, по строкам которой стоят координаты векторов $w_i$ в стандартном базисе пространства $\Bbbk^m$, имеет $s_I(z) = E$. В $\mathrm{GL}_k$-орбите каждой матрицы $x \operatorname{im} U_I$ также имеется единственная матрица $z$ с $s_I(z) = E$ — именно, $z = s_I(x)^{-1} \cdot x$.

Упр. 11.3. Элементы $k \times m$-матрицы $s_J^{-1}\left(\varphi_I(t)\right) \cdot \varphi_I(t)$ являются рациональными функциями от элементов матрицы $t$ со знаменателями $\det s_J\left(\varphi_I(t)\right)$ и, стало быть, регулярны в $\mathcal{D}\left(\det s_J\left(\varphi_I(t)\right)\right)$. Поэтому отображение $\varphi_{JI}$, переводящее эту матрицу в её $k \times (m-k)$-подматрицу, образованную столбцами с не лежащими в $J$ номерами, регулярно. Обратное отображение задаётся той же формулой: $t \mapsto s_{\hat{I}}\left(s_I^{-1}\left(\varphi_J(t)\right) \cdot \varphi_J(t)\right)$ (удостоверьтесь в этом!).

Упр. 11.4. Это следует из определения локальной регулярной функции и зам. 10.2. на стр. 146.

Упр. 11.5. Отображение $\varkappa$ можно задать формулой $(x_0 : x_1 : x_2) \mapsto (x_1 x_2 : x_0 x_2 : x_0 x_1)$, из которой видно, что оно не определено только в точках $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$ и образ $\varkappa$ тоже равен дополнению до этих трёх точек.

Упр. 11.6. В обозначениях из прим. 11.1 на стр. 151 пересечение множества нулей однородного многочлена $\overline{f}(x_0, x_1, \dots, x_n)$ со стандартной картой $U_i \subset \mathbb{P}_n$ задаётся в аффинных координатах $t_i$ карты $U_i$ полиномиальным уравнением $\overline{f}(t_{i,0}, \dots, t_{i,i-1}, 1, t_{i,i+1}, \dots, t_{i,n}) = 0$.

Упр. 11.14. Пусть $X_1, X_2 \subset X$ — два замкнутых неприводимых подмножества и $U \subset X$ — открытое множество, такое что оба пересечения $X_1 \cap U$, $X_2 \cap U$ непусты. Тогда $X_1 = X_2 \iff X_1 \cap U = X_2 \cap U$, поскольку $X_i = \overline{X_i \cap U}$.

Упр. 11.15. Докажите, что произведение конечных сюрьекций $X \to \mathbb{A}^n$, $Y \to \mathbb{A}^m$ является конечной сюрьекцией $X \times Y \to \mathbb{A}^n \times \mathbb{A}^m$.

Упр. 11.16. Выберите в $H$ какой-нибудь базис, запишите координаты векторов этого базиса и координаты точки $p$ по строкам $(n-d+1) \times (n+1)$-матрицы. Условие $p \in H$ означает, что ранг этой матрицы равен $n-d$. Зануление всех миноров порядка $n-d+1$ является системой билинейных уравнений на плюккеровы координаты[1] подпространства $H$ и однородные координаты точки $p$.

Упр. 11.18. $\Gamma$ задаётся однородными по всем $f_i$ и $p$ уравнениями $f_0(p) = f_1(p) = \ldots = f_n(p) = 0$.

Упр. 11.19. Возьмите $n+1$ гиперплоскостей, пересекающихся в одной точке, и возведите задающие их линейные формы в подходящие степени.

Упр. 11.21. Вложим $\mathrm{Gr}(2,4)$ в $\mathbb{P}_5 = \mathbb{P}(\Lambda^2 V)$ по Плюккеру. Прямая $(ab)$ лежит на поверхности $V(f)$ если и только если многочлен $f$ тождественно зануляется на линейной оболочке векторов $a$ и $b$, которая является образом свёртки $V^* \to V$ с бивектором $a \wedge b$. Убедитесь, что условие тождественного по $\xi \in V^*$ зануления функции $\xi \mapsto f(\xi \llcorner (a \wedge b))$ записывается системой однородных полиномиальных уравнений на коэффициенты $f$ и плюккеровы координаты бивектора $a \wedge b$.

Упр. 12.2. В силу конечности $\mathbb{F}$ гомоморфизм колец $\mathbb{Z} \to \mathbb{F}$, переводящий $1 \in \mathbb{Z}$ в $1 \in \mathbb{F}$, имеет ненулевое ядро $(p) \subset \mathbb{Z}$, и его образ изоморфен $\mathbb{Z}/(p) \subset \mathbb{F}$. Поскольку в нём нет делителей нуля, число $p$ простое, и образ — поле $\mathbb{F}_p$ совпадающее с простым подполем в $\mathbb{F}$.

[1]Напомню, что плюккеровыми координатами подпространства являются старшие миноры матрицы, составленной из координат какого-нибудь базиса в этом подпространстве.

Упр. 12.6. Если $f(x) = (x - \alpha) \cdot g(x)$, то по правилу Лейбница $f'(x) = g(x) + (x - \alpha) \cdot g'(x)$, откуда $g(\alpha) = f'(\alpha) = 0$.

Упр. 12.7. Поскольку $\deg f \geqslant 2$, производная $f' \neq 0$ и $\deg f' < \deg f$. Так как $f$ не имеет отличных от константы делителей, степень которых меньше $\deg f$, нод$(f, f') = 1$.

Упр. 12.11. Это вытекает из лем. 12.4.

Упр. 12.16. Корни многочлена $x^{p^n} - x$ распадаются на орбиты группы $G = \operatorname{Aut} \mathbb{F}_{p^n} \simeq \mathbb{Z}/(n)$. Длина $m$ каждой орбиты $\alpha_1, \dots, \alpha_m$ делит $n$, а произведение $\prod(x - \alpha_i)$ по всем элементам $G$-орбиты является неприводимым приведённым многочленом с коэффициентами из $\mathbb{F}_p = \mathbb{F}_{p^n}^G$. Поскольку многочлен $x^{p^n} - x$ сепарабелен, его разложение на простые множители в $\mathbb{F}_p[x]$ имеет вид произведения попарно различных приведённых неприводимых многочленов, степени которых делят $n$. С другой стороны, неприводимый приведённый многочлен $g \in \mathbb{F}_p[x]$ степени $m$ делит $x^{p^n} - x$ тогда и только тогда, когда он имеет корень в поле разложения $\mathbb{F}_{p^n}$ многочлена $x^{p^n} - x$. Это равносильно наличию вложения $\mathbb{F}_p[x]/(g) = \mathbb{F}_{p^m}$ в $\mathbb{F}_{p^n}$, т. е. тому, что $m|n$.

Упр. 13.1. Поскольку четыре арифметических действия над комплексными числами и извлечение из них квадратных корней полностью сводятся к этим пяти операциям над вещественными и мнимыми частями, можно предполагать числа $a$ и $b$ вещественными. В этом случае $a \pm b$ строятся непосредственно, $a/b$ и $ab$ — при помощи подобия или теоремы Фалеса (для этого и требуется отрезок длины 1), а $\sqrt{a} = \sqrt{1 \cdot a}$ — при помощи теоремы о среднем геометрическом в прямоугольном треугольнике (для этого и также требуется отрезок длины 1).

Упр. 13.2. При пересечении окружности и прямой получается вещественный трёхчлен

$$(b-a)(\overline{b}-\overline{a})\,t^2 + \big((b-a)(\overline{a}-\overline{c}) + (a-c)(\overline{b}-\overline{a})\big)\,t + (b-a)(\overline{b}-\overline{a}) - (d-c)(\overline{d}-\overline{c}),$$

при пересечении двух окружностей — трёхчлен $\alpha t^2 + \beta t + \overline{\alpha} = 0$, у которого $\alpha = (b-a)(\overline{a}-\overline{c})$, а $\beta = (b-a)(\overline{b}-\overline{a}) + (a-c)(\overline{a}-\overline{c}) - (d-c)(\overline{d}-\overline{c}) \in \mathbb{R}$.

Упр. 13.3. Воспользуйтесь равенством $\cos(3\varphi) = 4\cos\varphi - 3\cos^2\varphi$ при $\varphi = \pi/9$ и убедитесь, что у многочлена $8\,x^3 - 6\,x - 1$ нет рациональных корней.

Упр. 13.6. Пусть корни $\{\vartheta_1, \dots, \vartheta_k\} \subset \{\vartheta_1, \dots, \vartheta_n\}$ образуют орбиту группы Галуа. Тогда коэффициенты многочлена $g(x) = (x - \vartheta_1) \dots (x - \vartheta_k)$ инвариантны относительно действия группы Галуа, и значит, $g \in \Bbbk[x]$. Таким образом, многочлен $f$ является произведением многочленов $g$, отвечающих орбитам действия группы Галуа $\operatorname{Gal} f/\Bbbk$ на корнях $f$. С другой стороны, группа Галуа переводит в себя множество корней любого многочлена с коэффициентами из $\Bbbk$ и, тем самым, не может транзитивно действовать на корнях приводимого в $\Bbbk[x]$ многочлена $f$.

Упр. 13.7. Поле разложения $\mathbb{L}_{\overline{f}}$ многочлена $\overline{f}$ над $\mathbb{F}_p$ является башней примитивных расширений $\mathbb{F}_p = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \dots \subset \mathbb{L}_m = \mathbb{L}_{\overline{f}}$, на каждом этаже которой происходит присоединение одного из корней $\vartheta$ многочлена $\overline{f}$. Так как $\overline{f}$ полностью распадается в $A[t]$ в произведение различных линейных множителей, тавтологическое вложение $\mathbb{F}_p \hookrightarrow A$ продолжается вдоль башни до гомоморфизма $\mathbb{F}_p$-алгебр $\mathbb{L}_{\overline{f}} \to A$, который инъективен, ибо $\mathbb{L}_{\overline{f}}$ — поле, и имеет образом $\mathbb{F}_p$-подалгебру, порождённую корнями многочлена $\overline{f}$ в $A$.

Упр. 13.8. Подставляя $t = 1$ в $1 + t + \dots + t^{p-1} = \Phi_p(t) = \prod_{k=1}^{p-1}(t - \zeta^k)$, где $\zeta = e^{2\pi i/p}$, получаем

$$p = \prod_{k=1}^{(p-1)/2} (1-\zeta^k)(1-\zeta^{-k}) = \prod_{k=1}^{(p-1)/2} (-\zeta^{-k}) \cdot (1-\zeta^k)^2 = (-1)^{(p-1)/2}\alpha^2\beta^2\,,$$

где $\beta = \prod_{k=1}^{(p-1)/2}(1-\zeta^k)$, а $\alpha = \zeta^m$ с $2m \equiv -\sum_{k=1}^{(p-1)/2} k = (1-p^2)/8 \pmod{p}$.

Упр. 13.9. Поскольку $\prod_{\nu=0}^{n-1}\left(x-\zeta^\nu\right) = x^n - 1$, значения элементарных симметрических многочленов $e_i(\zeta^0, \zeta^1, \dots, \zeta^{n-1}) = 0$ при $1 \leqslant i \leqslant n-1$. Поэтому все коэффициенты многочлена $f_\xi$, кроме старшего, равного 1, и свободного члена, равного $-\xi^n\alpha^n$, нулевые: $e_i(\zeta^0\xi\alpha, \zeta^1\xi\alpha, \dots, \zeta^{n-1}\xi\alpha) = \xi^i\alpha^i e_i(\zeta^0, \zeta^1, \dots, \zeta^{n-1}) = 0$.

Упр. 13.13. Пересекая с подгруппой $H \subset G$ цепочку $G = G_0 \supset G_1 \supset \dots \supset G_m = \{e\}$, в которой $G_{i+1} \lhd G_i$ и факторы $G_i/G_{i+1}$ абелевы, получим цепочку $H = G_0 \cap H \supseteq G_1 \cap H \supseteq \dots \supseteq G_m \cap H = H$ с факторами $(G_i \cap H)/(G_{i+1} \cap H) \simeq ((G_i \cap H)\, G_{i+1})/G_{i+1} \subset G_i/G_{i+1}$. Будучи подгруппами абелевых факторов $G_{i+1} / G_i$, они тоже абелевы. Умножая цепочку $G = G_0 \supset G_1 \supset \dots \supset G_m = \{e\}$ на подгруппу $N \lhd G$ получаем цепочку $G = G_0N \supset G_1N \supset \dots \supset G_mN = N$, факторы которой по $N$ дают ведущую от $G/N$ к $e = N/N$ цепочку подгрупп с факторами $(G_iN/N)/(G_{i+1}N/N) \simeq G_i/(G_{i+1}(N \cap G_i)) \simeq (G_i/G_{i+1})/((G_i \cap N)/G_{i+1})$. Будучи факторами абелевых групп $G_i/G_{i+1}$, они абелевы. Цепочки $H = H_0 \supset H_1 \supset \dots \supset H_m = \{e\}$ и $G/H = Q_0 \supset Q_1 \supset \dots \supset Q_k = \{e\}$ для $H \lhd G$ и $G/H$ собираются в $G = Q_0' \supset Q_1' \supset \dots \supset Q_k' = H \supset H_1 \supset \dots \supset H_m = \{e\}$, где $Q_i'$ обозначают полные прообразы подгрупп $Q_i \subset G/H$ при гомоморфизме факторизации $G \twoheadrightarrow G/H$.