МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ

Y. Y.

Обрезанная версия 11pt

Дата компиляции:
25 июня 2025 года

Оглавление

Нулевая глава

Предисловие

Общее описание

Этот текст представляет собой набор математических и околоматематических заметок, предназначенный в основном для меня, но, быть может, интересный и для других. Он в крайней степени сырой и постоянно переписывается и дописывается. Содержание, как правило, не выходит за рамки базовых университетских и школьных учебников.

Форматирование

Для вёрстки использовался XeLaTeX. Дизайн приспособлен для отображения на экране, а не печати на бумаге. В частности, несколько гротескный титульный лист нужен для того, чтобы превью на экранах электронных устройств были читаемыми и идентифицируемыми.

Номера страниц в оглавлении кликабельны. Номера страниц в верхних колонтитулах кликабельны и ссылаются на оглавление. Ссылки на бибиографию кликабельны, и библиография снабжена кликабельными обратными ссылками.

В каждом разделе нумерация теорем, лемм и тому подобного начинается заново. Это сделано для того, чтобы разделы можно было с минимумом изменений копировать и вставлять в разные места текста.

Копирайт

следующей ссылке: `https://creativecommons.org/publicdomain/zero/1.0/legalcode.en` (дата обр. 07.01.2025). Вот соответствующие значки: 🄯🄭. Иначе говоря, оно объявляется общественным достоянием.

Обратная связь

Связаться с автором можно по электронной почте `yymath@yandex.ru`.

Буквы в математических формулах

Греческие буквы

Для справки приведём таблицу из греческих букв, используемых в математическом режиме TEX-а. Вместо некоторых прописных греческих букв используются соответствующие латинские.

$$\begin{array}{cccccccc} A\,\alpha & B\,\beta & \Gamma\,\gamma & \Delta\,\delta & E\,\epsilon\,\varepsilon & Z\,\zeta & H\,\eta & \Theta\,\theta\,\vartheta \\ I\,\iota & K\,\kappa & \Lambda\,\lambda & M\,\mu & N\,\nu & \Xi\,\xi & O\,o & \Pi\,\pi\,\varpi \\ P\,\rho\,\varrho & \Sigma\,\sigma\,\varsigma & T\,\tau & \Upsilon\,\upsilon & \Phi\,\phi\,\varphi & X\,\chi & \Psi\,\psi & \Omega\,\omega \end{array}$$

Заметим, что строчная `дзета` (ζ) чем-то похожа на латинскую «z», что позволяет отличать её от `кси` (ξ), а строчная `мю` (μ) — на кириллическую «м», что позволяет отличать её от `эта` (η).

Готические буквы

Для справки приведём таблицу из английских букв, набранных математической фрактурой.

$$\begin{array}{cccccccccccc} \mathfrak{A} & \mathfrak{B} & \mathfrak{C} & \mathfrak{D} & \mathfrak{E} & \mathfrak{F} & \mathfrak{G} & \mathfrak{H} & \mathfrak{I} & \mathfrak{J} & \mathfrak{K} & \mathfrak{L} & \mathfrak{M} \\ \mathfrak{a} & \mathfrak{b} & \mathfrak{c} & \mathfrak{d} & \mathfrak{e} & \mathfrak{f} & \mathfrak{g} & \mathfrak{h} & \mathfrak{i} & \mathfrak{j} & \mathfrak{k} & \mathfrak{l} & \mathfrak{m} \\ \mathfrak{N} & \mathfrak{O} & \mathfrak{P} & \mathfrak{Q} & \mathfrak{R} & \mathfrak{S} & \mathfrak{T} & \mathfrak{U} & \mathfrak{V} & \mathfrak{W} & \mathfrak{X} & \mathfrak{Y} & \mathfrak{Z} \\ \mathfrak{n} & \mathfrak{o} & \mathfrak{p} & \mathfrak{q} & \mathfrak{r} & \mathfrak{s} & \mathfrak{t} & \mathfrak{u} & \mathfrak{v} & \mathfrak{w} & \mathfrak{x} & \mathfrak{y} & \mathfrak{z} \end{array}$$

Обратите внимание на то, что в таблице много пар похожих глифов, например, $\mathfrak{I}$ и $\mathfrak{J}$, $\mathfrak{B}$ и $\mathfrak{P}$, $\mathfrak{r}$ и $\mathfrak{x}$.

Глобальные обозначения, соглашения и определения

Обозначение 1 (Натуральные числа)**.** Вопрос о том, стоит ли начинать натуральные числа с нуля или с единицы, решается радикально: вводятся обозначения $\mathbb{N}_0 \coloneqq \mathbb{N} \cup \{0\} = \mathbb{Z}_{\geqslant 0}$ и $\mathbb{N}_1 \coloneqq \mathbb{N} \setminus \{0\} = \mathbb{Z}_{>0}$, а обозначение $\mathbb{N}$, как правило, не используется. Однако в случае, когда оно используется, $\mathbb{N}$ обозначает $\mathbb{N}_0$, то есть $\{0, 1, 2, 3, 4, \dots\}$, как у Бурбаки.

Замечание 1. Символ $\mathbb{Z}$ происходит от первой буквы немецкого слова «zahlen», означающего «числа».

Обозначение 2 (Включение подмножества)**.** Обозначение $X \subset Y$ означает, что X является подмножеством Y, не обязательно собственным.

Обозначение 3 (Множество конечных подмножеств)**.** Множество конечных подмножеств множества I иногда будет обозначаться символом $\Lambda(I)$.

Соглашение 1 (Отображение)**.** Отображение — это тройка, состоящая из области, кообласти и графика. Графика недостаточно, чтобы задать отображение, необходимо ещё указать кообласть.

Обозначение 4 (Семейство)**.** Символы $(a_i)_{i \in I}$ и $(a_i \mid i \in I)$ обозначают *семейство*, индексированное множеством I, которое теоретико-множественно представляет из себя множество упорядоченных пар (i, a_i), по одной для каждого $i \in I$, то есть график отображения из I, такого что $i \mapsto a_i$ для всех $i \in I$. Если $(X_i)_{i \in I}$ — семейство множеств, то элементы $\prod_{i \in I} X_i$ — это семейства $(a_i)_{i \in I}$, где $a_i \in X_i$ для всех $i \in I$.

Замечание 2. Символ «$\in$» происходит от повёрнутой на 180° кириллической буквы «э», первой буквы слова «это»: «$x \in \mathbb{R}$» — «x — это вещественное число». Шутка. На самом деле это стилизованная греческая буква ϵ, первая буква слова «ἐστί» — «ієстъ»/«єстъ»/«есть».

Соглашение 2 (Кольцо)**.** Будем называть *кольцом* аддитивно записываемую абелеву группу, снабжённую биаддитивной, то есть двусторонне дистрибутивной, внутренней бинарной операцией умножения.

Соглашение 3 (Унитальное кольцо)**.** Кольцо с единицей называется *унитальным* кольцом. Если противное не указано явно, то гомоморфизмы между унитальными кольцами подразумеваются унитальными, то есть переводящими единицу в единицу, и подкольца унитальных колец подразумеваются унитальными с унитальными вложениями.

Обозначение 5 (Единицы мультипликативного моноида)**.** Символ $M^\times$ обозначает группу *единиц*, то есть двусторонне мультипликативно обратимых элементов, мультипликативного моноида M.

Обозначение 6 (Образ в экспоненциальном обозначении)**.** Образ подмножества $X \subset Y$ под действием отображения $y \mapsto y^\lambda : Y \to Z$ или $y \mapsto {}^\lambda y : Y \to Z$ будем обозначать через $X^{:\lambda} := \{x^\lambda \in Z \mid x \in X\}$ или ${}^{\lambda:}X := \{{}^\lambda x \in Z \mid x \in X\}$ соответственно.

Пример 1. Множество квадратов обратимых элементов ассоциативного унитального кольца R обозначается символом $(R^\times)^{:2}$. Если $H \subset G$ — подгруппа группы G, а $g \in G$, то ${}^{g:}H = gHg^{-1}$, где мы используем экспоненциальное обозначение для сопряжения.

Соглашение 4 (Левое и правое)**.** По умолчанию все действия, в частности, модули, считаются «левыми». Морфизмы в категориях компонуются справа налево.

Обозначение 7 (Двойственный модуль)**.** Если M — модуль над ассоциативным унитальным кольцом R, то символ $M^\vee$, как правило, будет обозначать абелеву группу $\mathrm{Hom}_{R\text{-mod}}(M, R)$.

Соглашение 5 (Компактность и хаусдорфовость)**.** Мы не включаем требование хаусдорфовости в определение компактного топологического пространства.

Обозначение 8 (Противоположная категория)**.** Если $\mathcal{C}$ — категория, то противоположная категория обозначается символом $\mathcal{C}^o$, где верхний индекс o — это не цифра 0 и не знак композиции $\circ$, а первая буква английского слова «opposite». Такое же обозначение применяется для колец, групп и тому подобного.

Соглашение 6 (Категория рефлексивного транзитивного отношения)**.** Множество X с рефлексивным транзитивным отношением

$R \subset X \times X$ канонически реализуется как категория с множеством объектов X и множеством морфизмов R. Произвольное множество часто по умолчанию будет считаться реализованным как категория тождественного отношения на нём.

Обозначение 9 (Категория Дельта)**.** Категория непустых конечных ординалов фон Неймана как упорядоченных множеств будет обозначаться символом Δ и называться *категорией Дельта*. Объект в Δ, соответствующий $\{0, 1, \ldots, n\}$, где $n \in \mathbb{N}_0$, обозначается через $[n]$.

Соглашение 7 (Комма-категория)**.** Построенная по паре функторов $\pi : \mathcal{C} \to \mathcal{B} \leftarrow \mathcal{E} : \rho$ «комма-категория» $(\mathcal{C}^{\{0\}} \times \mathcal{E}^{\{1\}}) \times_{\mathcal{B}^{\{0\}} \times \mathcal{B}^{\{1\}}} \mathcal{B}^{[1]}$ будет обозначаться через $\mathcal{C} \,{}^{\pi}\!\int_{\mathcal{B}}^{\rho} \mathcal{E}$ и иногда называться *категорией стрелок*, причём часть индексов у символа `полусвастики` $\int$ может быть опущена.

Замечание 3. Символ $\int$ получен склеиванием символа $\rfloor$ (`\rfloor`) и символа $\lceil$ (`\lceil`).

Замечание 4. Название «комма-категория», очевидно, происходит от английского «comma category». Вот что по поводу этого названия пишет Уильям Ловер:

> The (,) operation then turned out to be fundamental in computing Kan extensions (i.e. adjoints of induced functors). Unfortunately, I did not suggest a name for the operation, so due to the need for reading it somehow or other, it rather distressingly came to be known by the subjective name "comma category", even when it came to be also denoted by a vertical arrow in place of the comma. Originally, it had been common to write (A, B) for the set of maps in a given category $\mathcal{C}$ from an object A to an object B; since objects are just functors from the category 1 to $\mathcal{C}$, the notation was extended to the case where A and B are arbitrary functors whose domain categories are not necessarily 1 and may also be different [6, с. 13].

Тем не менее, название стандартное, и будет использоваться в данном тексте.

Соглашение 8 (Категория объектов над/под данным)**.** Если $\mathcal{C}$ — категория, а $C \in \mathrm{Ob}(\mathcal{C})$ — её объект, то категории $\mathcal{C} \int_{\mathcal{C}} \{C\}$ и $\{C\} \int_{\mathcal{C}} \mathcal{C}$

часто будут обозначаться через $\mathcal{C} \int C$ и $C \int \mathcal{C}$ и называться *категорией объектов над C* и *категорией объектов под C* соответственно.

Соглашение 9 (Категория колец над/под данным кольцом)**.** Исключениями из соглашения 8 являются подкатегории категории колец: для них смысл фраз «категория объектов над данным» и «категория объектов под данным» переставлен. Это сделано для согласованности с переходом к категории аффинных схем для категории коммутативных ассоциативных унитальных колец и согласованности с практикой применения фразы «алгебра над кольцом».

Обозначение 10 (Изоморфность)**.** Выражение типа $A \simeq B$, как правило, означает, что A и B изоморфны, а выражение типа $A \cong B$, как правило, означает, что между A и B есть единственный или однозначно определённый контекстом изоморфизм.

Обозначение 11 (Произведение и копроизведение морфизмов)**.** Морфизм $Y \to X_1 \times X_2$, индуцированный морфизмами $f_1 : Y \to X_1$ и $f_2 : Y \to X_2$, обозначается через $f_1 \barwedge f_2$, а $g_1 \times g_2 : Y_1 \times Y_2 \to X_1 \times X_2$ обозначает морфизм $(g_1 \circ \pi_1) \barwedge (g_2 \circ \pi_2)$, где $g_1 : Y_1 \to X_1$ и $g_2 : Y_2 \to X_2$ — произвольные морфизмы, а π_1 и π_2 — структурные проекции $Y_1 \times Y_2$. С другой стороны, $f_1 \barwedge f_2 = (f_1 \times f_2) \circ \Delta$, где $\Delta \coloneqq \mathrm{Id}_Y \barwedge \mathrm{Id}_Y$. Операции $\barsqcup$ и $\sqcup$ очевидным образом определяются как двойственные к $\barwedge$ и $\times$.

Пример 2. Вот, например, забавный способ изображать квадратную диаграмму: $A \xrightarrow{h \barwedge v} B \times C \rightrightarrows B \sqcup C \xrightarrow{v' \barsqcup h'} D$.

Обозначение 12 ((Ко)ядро и (ко)образ)**.** Ядро морфизма $\varphi : X \to Y$ обозначается $\ker(\varphi) : \mathrm{Ker}(\varphi) \to X$, коядро — $\mathrm{coker}(\varphi) : Y \to \mathrm{Coker}(\varphi)$, образ — $\mathrm{im}(\varphi) : \mathrm{Im}(\varphi) \to Y$, кообраз — $\mathrm{coim}(\varphi) : X \to \mathrm{Coim}(\varphi)$.

Обозначение 13 (Ном-ы и объекты)**.** Пусть $\mathcal{C}$ — категория. Тогда если $X, Y \in \mathrm{Ob}(\mathcal{C})$, то совокупность морфизмов из X в Y в категории $\mathcal{C}$ в общем случае будет обозначаться через $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ или $\mathcal{C}(X, Y)$. Вместо записи $X \in \mathrm{Ob}(\mathcal{C})$ может использоваться запись $X \in \mathcal{C}$.

Соглашение 10 (Посет/чум)**.** Иногда *посетом/чумом* будет называться категория, в которой все уравнители и коуравнители существуют и являются изоморфизмами.

Обозначение 14 (Симметрическая и внешняя степени)**.** Если M — модуль над ассоциативным коммутативным унитальным кольцом A, а I — конечное множество, то I-индексированные внешняя и симметрическая степени M как A-модуля будут обозначаться через $\Lambda^I_A(M)$ и $\mathrm{S}^I_A(M)$ соответственно, или просто через $\Lambda^I(M)$ и $\mathrm{S}^I(M)$.

Обозначение 15 (Функция расстояния)**.** Расстояние между точками x' и x'' в метрическом пространстве X часто будет обозначаться через $\mathrm{d}_X(x', x'')$ или просто через $\mathrm{d}(x', x'')$.

Замечание 5. Буква «d» — это первая буква английского слова «distance».

Обозначение 16 (Матрицы)**.** Пусть I, J и X — три множества. Тогда множество матриц, индексированных $I \times J$, с элементами/записями (англ. entries) из X будет обозначаться через $\mathrm{M}_{I,J}(X)$. Вместо $\mathrm{M}_{I,I}(X)$ может писаться $\mathrm{M}_I(X)$.

Замечание 6. Пара цитат о происхождении термина «матрица»:

> The term “matrix” (Latin for “womb”, “dam” (non-human female animal kept for breeding), “source”, “origin”, “list”, and “register”, are derived from *mater*—mother) was coined by James Joseph Sylvester in 1850, who understood a matrix as an object giving rise to several determinants today called minors, that is to say, determinants of smaller matrices that derive from the original one by removing columns and rows [18].
>
> I have in previous papers defined a “Matrix” as a rectangular array of terms, out of which different systems of determinants may be engendered from the womb of a common parent; these cognate determinants being by no means isolated in their relations to one another, but subject to certain simple laws of mutual dependence and simultaneous deperition [1, с. 247].

Определение 1 (Кольцо диагональных матриц)**.** Пусть R — ассоциативное унитальное кольцо, I — конечное множество, а $(e_{i,j})_{i,j\in I}$ — стандартный базис $\mathrm{M}_I(R)$ как R-модуля. Тогда определим *кольцо диагональных матриц* следующим образом: $\mathrm{D}_I(R) \coloneqq \bigoplus_{i\in I} Re_{i,i} \subset \mathrm{M}_I(R)$.

Определение 2 (Элементарная подгруппа)**.** Пусть R — ассоциативное унитальное кольцо, I — конечное множество, а $(e_{i,j})_{i,j\in I}$ — стандартный базис $\mathrm{M}_I(R)$ как R-модуля. Тогда определим *элементарную подгруппу* $\mathrm{E}_I(R) \subset \mathrm{GL}_I(R)$ как подгруппу, порождённую *элементарными трансвекциями*, то есть элементами вида $t_{j,k}(\lambda) \coloneqq e + \lambda e_{j,k}$, где $e = \sum_{i\in I} e_{i,i}$, $\lambda \in R$, $j, k \in I$ и $j \neq k$.

Определение 3 (Алгебра)**.** Пусть A — коммутативное ассоциативное унитальное кольцо. Тогда *алгеброй над* A или A*-алгеброй* называется кольцо R, снабжённое структурой A-модуля, такой что действия элементов A на аддитивной абелевой группе R коммутируют с эндоморфизмами левого и правого умножения на элементы R.

Наблюдение 1. Пусть A и R — ассоциативные унитальные кольца, причём A коммутативно. Тогда задание на R структуры алгебры над A — это задание гомоморфизма колец $A \to \mathrm{End}_{R\otimes_{\mathbb{Z}} R^o\text{-mod}}(R) \cong \mathrm{Z}(R)$.

Наблюдение 2. Пусть R — модуль над ассоциативным коммутативным унитальным кольцом A. Тогда задание на R структуры алгебры над A — это задание гомоморфизма A-модулей $R \otimes_A R \to R$.

Соглашение 11 (Унитальная алгебра)**.** Соглашение 3 применимо и к алгебрам.

Обозначение 17 (Стандартные категории)**.** Категория множеств обозначается Sets, абелевых групп — Ab, модулей над ассоциативным унитальным кольцом R — R-mod, унитальных колец — Ring, просто колец — Rng, кольцоидов — Rngd, алгебр над коммутативным ассоциативным унитальным кольцом A — A-alg. Если $R \in \mathrm{Ob}(\mathrm{Rng})$, то R-rng $\coloneqq R \int_{\mathrm{Rng}} \mathrm{Rng}$, а если $R \in \mathrm{Ob}(\mathrm{Ring})$, то R-ring $\coloneqq R \int_{\mathrm{Ring}} \mathrm{Ring}$.

Наблюдение 3. Функтор $(\rho : R \to \mathbb{Z}) \mapsto \mathrm{Ker}(\rho) : \mathrm{Ring} \int_{\mathrm{Ring}} \mathbb{Z} \to \mathrm{Rng}$ является эквивалентностью категорий, так как любой такой ρ является левым обратным к каноническому гомоморфизму $\mathbb{Z} \to R$, а потому задаёт изоморфизм $R \cong \mathbb{Z} \oplus \mathrm{Ker}(\rho)$ между R и унитализацией $\mathrm{Ker}(\rho)$.

Обозначение 18 (Класс эквивалентности)**.** Класс эквивалентности элемента x иногда будет обозначаться через $[x]$.

Соглашение 12 (Унитальный многочлен)**.** Многочлены со старшим коэффициентом один мы будем называть *унитальными* многочленами. Иногда их ещё называют *приведёнными* многочленами, но эта практика, на мой вкус, плохо согласована с использованием фразы «неприводимый многочлен» в её обычном значении.[1]

[1]Троица `приведённый`, `неприводимый` и `приводимый` возникает и в теории схем.

Часть I

Не сгруппированные тексты

Глава 1

Почти не подкорректированные старые тексты

1.1. Китайская теорема об остатках

Лемма 1. *Пусть R — ассоциативное унитальное кольцо, $\mathfrak{I},\mathfrak{J}\subset R$ — двусторонние идеалы. Канонический гомоморфизм $R\to R/\mathfrak{I}\times R/\mathfrak{J}$ сюръективен тогда и только тогда, когда $\mathfrak{I}+\mathfrak{J}=R$.*

Доказательство. Следующий короткий комплекс абелевых групп

$$R/(\mathfrak{I}\cap\mathfrak{J})\xrightarrow{x+\mathfrak{I}\cap\mathfrak{J}\mapsto(x+\mathfrak{I},x+\mathfrak{J})}R/\mathfrak{I}\oplus R/\mathfrak{J}\xrightarrow{(x+\mathfrak{I},y+\mathfrak{J})\mapsto x-y+(\mathfrak{I}+\mathfrak{J})}R/(\mathfrak{I}+\mathfrak{J})$$

точен согласно теореме о факторквадрате суммы-пересечения (теорема 11.2.1). Это можно проверить и непосредственно. □

Замечание 1. Идеалы $\mathfrak{I},\mathfrak{J}\subset R$, такие что $\mathfrak{I}+\mathfrak{J}=R$, называются *взаимно простыми*, или *копростыми*, или *комаксимальными*.

Теорема 1. *Пусть R — ассоциативное унитальное кольцо, $(\mathfrak{I}_i)_{i\in I}$ — семейство двусторонних идеалов R, $\operatorname{card}(I)<\infty$. Тогда следующие условия эквивалентны:* (i) *Если $i,j\in I$, $i\neq j$, то канонический гомоморфизм $R\to R/\mathfrak{I}_i\times R/\mathfrak{I}_j$ сюръективен;* (ii) *Канонический гомоморфизм $R\to\prod_{i\in I}R/\mathfrak{I}_i$ сюръективен.*

Доказательство. Очевидно, что (ii) $\implies$ (i). Докажем обратное. Рассмотрим $N \coloneqq \operatorname{Im}(R \to \prod_{i\in I} R/\mathfrak{I}_i)$. Для любых $i, j \in I$, $i \neq j$ мы можем найти $a_{ij} \in N$, такой что i-ая координата a_{ij} равна 1, а j-ая — 0. Тогда $a_i \coloneqq \prod_{j\in I\setminus\{i\}} a_{ij} \in N$ (произведение в произвольном порядке) имеет i-ую координату 1 и остальные координаты 0. Такие a_i порождают $\prod_{i\in I} R/\mathfrak{I}_i$ как R-модуль, поэтому $N = \prod_{i\in I} R/\mathfrak{I}_i$. □

Следствие 1. *В предположениях теоремы 1 следующие условия эквивалентны:* (i) *Если $i, j \in I$, $i \neq j$, то $\mathfrak{I}_i + \mathfrak{I}_j = R$;* (ii) *$R$-кольца $R/\bigcap_{i\in I} \mathfrak{I}_i$ и $\prod_{i\in I} R/\mathfrak{I}_i$ изоморфны.*

Доказательство. Условие (ii) эквивалентно сюръективности канонического гомоморфизма $R \to \prod_{i\in I} R/\mathfrak{I}_i$, что, по теореме 1, эквивалентно сюръективности гомоморфизма $R \to R/\mathfrak{I}_i \times R/\mathfrak{I}_j$ для любых $i, j \in I$, $i \neq j$, что, по лемме 1, эквивалентно условию (i). □

Определение 1. Пусть $(\mathfrak{I}_i)_{i\in I}$ — это семейство подмножеств ассоциативного кольца, где $\operatorname{card}(I) = n < \infty$. *Симметрическое произведение* $\prod^{\mathrm{sym}}_{i\in I} \mathfrak{I}_i$ — это сумма произведений $\mathfrak{I}_{\sigma(1)}\mathfrak{I}_{\sigma(2)} \dots \mathfrak{I}_{\sigma(n)}$ по всем биекциям $\sigma : \{1, 2, \dots, n\} \xrightarrow{\sim} I$, то есть $\prod^{\mathrm{sym}}_{i\in I} \mathfrak{I}_i \coloneqq \sum_{\sigma:\{1,\dots,n\}\xrightarrow{\sim} S} \mathfrak{I}_{\sigma(1)} \dots \mathfrak{I}_{\sigma(n)}$.

Теорема 2. *Пусть R — ассоциативное унитальное кольцо, $(\mathfrak{I}_i)_{i\in I}$ — семейство двусторонних идеалов R,* $\operatorname{card}(I) < \infty$, *причём $\mathfrak{I}_i + \mathfrak{I}_j = R$ при $i, j \in I$, $i \neq j$. Тогда $\prod^{\mathrm{sym}}_{i\in I} \mathfrak{I}_i = \bigcap_{i\in I} \mathfrak{I}_i$.*

Доказательство. Равенство $\prod_{(i,j)\in(I\times I)\setminus\Delta}(\mathfrak{I}_i + \mathfrak{I}_j) = R$ (произведение в произвольном порядке) получается перемножением равенств $\mathfrak{I}_i + \mathfrak{I}_j = R$. Если раскрыть скобки в этом произведении, то в каждый моном не войдёт максимум один из $\mathfrak{I}_i$ (два идеала $\mathfrak{I}_i$ и $\mathfrak{I}_j$ не могут не войти, так как нам нужно забрать что-то из скобки $(\mathfrak{I}_i + \mathfrak{I}_j)$). Отсюда получаем: $\bigcap_{i\in I} \mathfrak{I}_i = (\bigcap_{i\in I} \mathfrak{I}_i) \prod_{(i,j)\in(I\times I)\setminus\Delta}(\mathfrak{I}_i + \mathfrak{I}_j) \subset \prod^{\mathrm{sym}}_{i\in I} \mathfrak{I}_i \subset \bigcap_{i\in I} \mathfrak{I}_i$. □

Пример 1. Пусть M — ненулевой модуль над ассоциативным унитальным кольцом R. Тогда собственный подмодуль $\{(a, b, c) \in M \oplus M \oplus M \mid a + b + c = 0\} \subsetneq M \oplus M \oplus M$ сюръективно проецируется на каждый из трёх подмодулей $M \oplus M \oplus \{0\}, M \oplus \{0\} \oplus M, \{0\} \oplus M \oplus M \subset M \oplus M \oplus M$ — китайская теорема об остатках для семейств не работает для модулей.

1.2. Системы корней классических алгебр Ли

Матричное описание классических алгебр Ли

Пусть V — n-мерное векторное пространство над полем K. Пусть s_{ort} — квадратная перъединичная матрица, задающая невырожденную симметрическую билинейную форму на V. Если n чётно, то определена квадратная матрица $s_{\mathrm{sp}} \coloneqq s_{\mathrm{ort}} s_{\pm}$, где $s_{\pm} \coloneqq \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ — блочная матрица, состоящая из квадратных блоков одинакового размера. Матрица s_{sp} задаёт невырожденную симплектическую билинейную форму на V.

Решения уравнения $s_{\mathrm{ort}} x + x^{\mathrm{t}} s_{\mathrm{ort}} = 0$, то есть $(s_{\mathrm{ort}} x s_{\mathrm{ort}}^{-1})^{\mathrm{t}} = -x$, легко описать, заметив, что сопряжение матрицей s_{ort} заменяет матрицу на «центрально симметричную», что в композиции с транспонированием даёт отражение матрицы относительно побочной диагонали. Отсюда, в частности, становится ясно, что размерность ортогональной алгебры Ли при $\mathrm{char}(K) \neq 2$ равна $(1/2)(n^2 - n)$.

Решения уравнения $(s_{\mathrm{sp}} x s_{\mathrm{sp}}^{-1})^{\mathrm{t}} = -x$ легко описать, заметив, что $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$, а $(s_{\mathrm{sp}} x s_{\mathrm{sp}}^{-1})^{\mathrm{t}} = (s_{\mathrm{ort}}(s_{\pm} x s_{\pm}^{-1}) s_{\mathrm{ort}}^{-1})^{\mathrm{t}}$. Отсюда, в частности, становится ясно, что размерность симплектической алгебры Ли при $\mathrm{char}(K) \neq 2$ равна $(1/2)(n^2 + n)$.

Описание систем корней классических алгебр Ли

Пусть K — поле характеристики 0, I — конечное множество мощности $n \geqslant 2$, $V = K^I$ — векторное пространство над K, $(e_{i,j})_{i,j \in I}$ — стандартный базис в $\mathrm{End}_{K\text{-mod}}(V)$ относительно стандартного базиса в K^I. Пусть $\langle -, - \rangle_{\mathrm{Kil}}$ обозначает форму Киллинга на $\mathfrak{gl}(V)$ или её ограничение на $\mathfrak{sl}(V)$, совпадающее с формой Киллинга на $\mathfrak{sl}(V)$.

Преобразование $[e_{i,i}, -]$ умножает все матричные единицы $e_{i,j}$, где $j \in I \setminus \{i\}$, на 1, матричные единицы $e_{j,i}$, где $j \in I \setminus \{i\}$, — на -1, а остальные матричные единицы — на 0. Отсюда ясно, что $\langle e_{i,i}, e_{j,j} \rangle_{\mathrm{Kil}} = 2n\delta_{i,j} - 2$ для всех $i, j \in I$.

Введём новое скалярное произведение на пространстве диагональных матриц: $\langle e_{i,i}, e_{j,j} \rangle_{\mathrm{Euc}} \coloneqq 2n\delta_{i,j}$, где $i, j \in I$. Тогда для любых $i, j \in I$, таких что $i \neq j$, линейная функция $\langle e_{i,i} - e_{j,j}, - \rangle_{\mathrm{Kil}}$ на пространстве диагональных матриц совпадает с линейной функцией $\langle e_{i,i} - e_{j,j}, - \rangle_{\mathrm{Euc}}$, которая совпадает с корнем, соответствующим собственному вектору $e_{i,j}$,

умноженным на $2n$. В частности, получаем, что $\langle e_{i,i}-e_{j,j}, e_{k,k}-e_{l,l}\rangle_{\mathrm{Kil}} = \langle e_{i,i}-e_{j,j}, e_{k,k}-e_{l,l}\rangle_{\mathrm{Euc}}$ для любых $i,j,k,l \in I$.

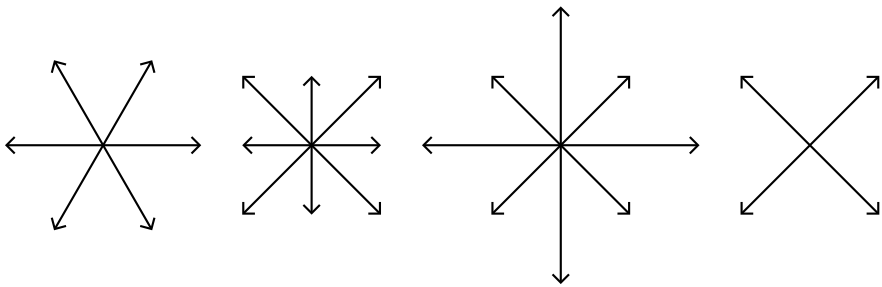


Рис. 1.1. Системы корней A_2, B_2, C_2 и D_2, соответствующие классическим алгебрам Ли $\mathfrak{sl}(3)$, $\mathfrak{o}(5)$, $\mathfrak{sp}(4)$ и $\mathfrak{o}(4)$ соответственно

Аналогичным образом проверяется, что в ортогональной и симплектической алгебрах Ли очевидный базис в пространстве диагональных матриц является ортогональным базисом относительно формы Киллинга, откуда становятся ясными картинки соответствующих систем корней (см. рис. 1.1).

1.3. Определитель и след

Наблюдение 1. Внешние степени задаются соотношениями полилинейности и вырождения. Иллюстрация для второй внешней степени:

$$a \wedge (b+c) = a \wedge b + a \wedge c, \quad (a+b) \wedge c = a \wedge c + b \wedge c, \quad a \wedge a = 0.$$

Это соответствует объёму, так как объём полилинеен и вырождается.

Наблюдение 2. Определитель линейного преобразования g задаётся мультипликативным действием g на старшей внешней степени. Иллюстрация для случая, когда старшая внешняя степень третья:

$$g(a \wedge b \wedge c) = g(a) \wedge g(b) \wedge g(c) = \det(g)(a \wedge b \wedge c).$$

Это соответствует изменению объёма под действием линейного преобразования.

Наблюдение 3. След линейного преобразования d задаётся аддитивным действием d на старшей внешней степени. Иллюстрация для случая, когда старшая внешняя степень третья:

$$d(a \wedge b \wedge c) = d(a) \wedge b \wedge c + a \wedge d(b) \wedge c + a \wedge b \wedge d(c) = \mathrm{tr}(d)(a \wedge b \wedge c).$$

Это соответствует скорости изменения объёма под действием соответствующего линейному преобразованию линейного векторного поля.

Наблюдение 4. Экспонента задаёт связь между определителем и следом:

$$\det(e^x) = e^{\mathrm{tr}(x)}.$$

Это соответствует получению линейного преобразования экспоненцированием линейного векторного поля.

1.4. Дуальность Стоуна

Теорема Стоуна

Введение

Целью этого подраздела является построение контравариантной эквивалентности (то есть дуальности) между категорией пространств Стоуна и категорией булевых колец.

Базовые определения и конструкция функторов

Соглашение 1. В этом разделе все кольца считаются коммутативными, ассоциативными и унитальными.

Определение 1 (Тотально сепарированное пространство)**.** Топологическое пространство T называется *тотально сепарированным* (англ. *totally separated*), если для любых двух различных точек $x, y \in T$ существует непрерывное отображение $f : T \to D$ в дискретное двухточечное топологическое пространство D, такое что $f(x) \neq f(y)$.

Определение 2 (Пространство Стоуна)**.** Топологическое пространство называется *пространством Стоуна*, если оно компактно и тотально сепарированно. Обозначим через Stone категорию пространств Стоуна и непрерывных отображений между ними.

Определение 3 (Булево кольцо)**.** Кольцо называется *булевым кольцом*, если в нём любой элемент является идемпотентом, то есть удовлетворяет уравнению $x^2 = x$. Обозначим через Boole категорию булевых колец и гомоморфизмов между ними.

Определение 4 (Спектр кольца)**.** Для кольца R его *спектр*, обозначаемый $\mathrm{Spec}(R)$, — это множество простых идеалов в R, снабжённое *топологией Зарисского*, заданной базой открытых множеств вида $A_f \coloneqq \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}$, где $f \in R$.

Замечание 1. В обозначениях определения 4 множества A_f, где $f \in R$, образуют базу топологии, так как $A_f \cap A_g = A_{fg}$ для любых $f, g \in R$.

Определение 5 (Кольцо открыто-замкнутых подмножеств топологического пространства)**.** Для топологического пространства T определим $\mathrm{Clop}(T) \in \mathrm{Boole}$ — булево кольцо *открыто-замкнутых* (*clopen*) подмножеств T — как кольцо непрерывных функций $T \to \mathbb{F}_2$, где $\mathbb{F}_2$ взято с дискретной топологией.

Теорема 1 (Компактность спектра)**.** *Для любого кольца R топологическое пространство* $\mathrm{Spec}(R)$ *компактно.*

Доказательство. Очевидно, что замкнутые подмножества спектра R — это множества $V(\mathfrak{I}) \coloneqq \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{I} \subset \mathfrak{p}\}$, соответствующие идеалам $\mathfrak{I} \subset R$. При этом $\bigcap_{i \in I} V(\mathfrak{I}_i) = V(\sum_{i \in I} \mathfrak{I}_i)$, где $(\mathfrak{I}_i)_{i \in I}$ — произвольное семейство идеалов в R, а условие $V(\mathfrak{I}) = \varnothing$ эквивалентно условию $\mathfrak{I} = R$, где $\mathfrak{I}$ — идеал в R. Компактность $\mathrm{Spec}(R)$ эквивалентна следующему утверждению: если $(\mathfrak{I}_i)_{i \in I}$ — произвольное семейство идеалов в R, такое что $\bigcap_{i \in I} V(\mathfrak{I}_i) = \varnothing$ то существует конечное подмножество $F \subset I$, такое что $\bigcap_{i \in F} V(\mathfrak{I}_i) = \varnothing$. Так как условие $\bigcap_{i \in I} V(\mathfrak{I}_i) = \varnothing$ эквивалентно условию $1 \in \sum_{i \in I} \mathfrak{I}_i$, то утверждение очевидно. □

Замечание 2. Для $R \in \mathrm{Boole}$ и $\mathfrak{p} \in \mathrm{Spec}(R)$ кольцо $R/\mathfrak{p}$ изоморфно $\mathbb{F}_2$, так как это целостное булево кольцо. В частности, идеал $\mathfrak{p}$ максимален.

Лемма 1 (Спектр булева кольца)**.** *Если R — булево кольцо, то* $\mathrm{Spec}(R)$ *— пространство Стоуна.*

Доказательство. Если $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(R)$, $\mathfrak{p} \neq \mathfrak{q}$, то существует $f \in \mathfrak{p}$, такое что $f \notin \mathfrak{q}$ (или наоборот). Тогда $\mathrm{Spec}(R) = A_f \sqcup A_g$, где $f + g = 1$, — нужное разложение. □

Определение 6 (Функтор спектра)**.** Гомоморфизм колец $\psi : R_1 \to R_2$ индуцирует непрерывное отображение: $\mathrm{Spec}(R_2) \to \mathrm{Spec}(R_1)$, $\mathfrak{p} \mapsto \psi^{-1}(\mathfrak{p})$. Отсюда получаем функтор $\mathrm{Spec} : \mathrm{Boole} \to \mathrm{Stone}^o$.

Определение 7 (Функтор открыто-замкнутых подмножеств)**.** Непрерывное отображение $\varphi : T_1 \to T_2$ индуцирует гомоморфизм колец: $\mathrm{Clop}(T_2) \to \mathrm{Clop}(T_1)$, $f \mapsto f \circ \varphi$. Отсюда получаем функтор $\mathrm{Clop} : \mathrm{Stone}^o \to \mathrm{Boole}$.

Замечание 3. Для $R \in \mathrm{Boole}$ и $\mathfrak{p} \in \mathrm{Spec}(R)$ уникальный изоморфизм $R/\mathfrak{p} \cong \mathbb{F}_2$ определяет изоморфизм функторов из Boole в категорию множеств: $\mathfrak{p} \mapsto (R \to R/\mathfrak{p} \cong \mathbb{F}_2) : \mathrm{Spec}(R) \leftrightarrow \mathrm{Hom}(R, \mathbb{F}_2) : \mathrm{Ker}(f) \leftarrow\!\shortmid f$.

Замечание 4. Аналогично, функтор $T \mapsto \mathrm{Clop}(T)$ изоморфен функтору, переводящему топологическое пространство T в множество его открыто-замкнутых подмножеств с операциями симметрической разности (сложение) и пересечения (умножение): изоморфизм переводит $f \in \mathrm{Clop}(T)$ в $f^{-1}(1) \subset T$, а открыто-замкнутое $O \subset T$ в его характеристическую функцию $\chi(O) \in \mathrm{Clop}(T)$.

Конструкция естественных изоморфизмов

Определение 8 (Элемент кольца как функция на спектре)**.** Для каждого $R \in \mathrm{Boole}$ определим гомоморфизм $\rho_R : R \to \mathrm{Clop}(\mathrm{Spec}(R))$, где $\rho_R(f) : \mathrm{Spec}(R) \to \mathbb{F}_2$, $\mathfrak{p} \mapsto f \pmod{\mathfrak{p}}$ (непрерывность $\rho_R(f)$ следует из разложения $\mathrm{Spec}(R) = A_f \sqcup A_g$, где $f + g = 1$).

Определение 9 (Точка пространства как идеал кольца функций)**.** Для каждого $T \in \mathrm{Stone}$ определим непрерывное отображение $\theta_T : T \to \mathrm{Spec}(\mathrm{Clop}(T))$, $x \mapsto \mathrm{Ker}(\mathrm{ev}_x)$, где $\mathrm{ev}_x : \mathrm{Clop}(T) \to \mathbb{F}_2$, $f \mapsto f(x)$.

Замечание 5. Изоморфизм $\mathrm{Spec}(R) \cong \mathrm{Hom}(R, \mathbb{F}_2)$, где $R \in \mathrm{Boole}$, переводит отображения ρ_R и θ_T в стандартные отображения в дважды двойственное пространство: $X \to \mathrm{Hom}(\mathrm{Hom}(X, \mathbb{F}_2), \mathbb{F}_2)$, $x \mapsto \mathrm{ev}_x$.

Теорема 2 (Теорема Стоуна). *Семейства* $(\rho_R)_{R\in\mathrm{Boole}}$ *и* $(\theta_T)_{T\in\mathrm{Stone}}$, *определённые ранее, задают пару естественных изоморфизмов:*

$$\rho : \mathrm{Id}_{\mathrm{Boole}} \xrightarrow{\sim} \mathrm{Clop}\circ\mathrm{Spec}, \quad \theta : \mathrm{Spec}\circ\mathrm{Clop} \xrightarrow{\sim} \mathrm{Id}_{\mathrm{Stone}^o}.$$

Доказательство (из шести частей).

Общий план. Естественность ρ и θ доказывается прямо. Докажем, что все ρ_R и θ_T — изоморфизмы, доказав биективность всех ρ_R и θ_T и замкнутость всех θ_T.

Инъективность ρ_R. Имеем: $\rho_R(f) = 0 \iff \rho_R(g) = 1$, где $f+g = 1$, то есть g не содержится ни в одном максимальном идеале кольца R, то есть g обратимо, а обратимый идемпотент равен 1. Другое доказательство: R не содержит ненулевых нильпотентов.

Сюръективность ρ_R. Открыто-замкнутое множество $O \subset \mathrm{Spec}(R)$ является объединением открытых множеств вида A_f, так как O открыто, причём конечным объединением, так как O компактно как замкнутое подмножество компактного пространства $\mathrm{Spec}(R)$. Воспользовавшись формулой включений-исключений, получаем желаемое.

Инъективность θ_T. Эквивалентна тотальной сепарированности T.

Сюръективность θ_T. Достаточно доказать, что произвольный идеал $\mathfrak{p} \in \mathrm{Spec}(\mathrm{Clop}(T))$ имеет общий ноль $x \in T$, так как если $\mathfrak{p} \subset \mathrm{Ker}(\mathrm{ev}_x)$, то $\mathfrak{p} = \mathrm{Ker}(\mathrm{ev}_x)$ из-за максимальности. Докажем от противного. Отсутствие общего нуля у $\mathfrak{p}$ означает, что $f \in \mathfrak{p}$ задают покрытие T открыто-замкнутыми множествами. Так как T компактно, то из него можно выбрать конечное подпокрытие, и, воспользовавшись формулой включений-исключений, получить, что $1 \in \mathfrak{p}$ — противоречие.

Замкнутость θ_T. Следует из того, что θ_T — непрерывное отображение из компактного пространства в хаусдорфово. □

Замечание 6. Естественные преобразования ρ и θ удовлетворяют треугольным тождествам (упражнение). То есть мы построили не просто эквивалентность, а *adjoint equivalence*.

Лемма Шуры-Буры

Введение

В этом подразделе будет доказана эквивалентность двух определений пространств Стоуна: как компактных хаусдорфовых вполне несвязных топологических пространств и как компактных тотально сепарированных топологических пространств.

Определения и общие свойства

Определение 10 (Двоеточие)**.** *Двоеточием* называется дискретное топологическое пространство на множестве из двух элементов. Мы будем обозначать двоеточие так: $\{\circ, \bullet\}$.

Определение 11 (Связность)**.** Топологическое пространство X называется *связным*, если любое непрерывное отображение в двоеточие $X \to \{\circ, \bullet\}$ постоянно. Эквивалентно, не существует разложения $X = X_\circ \cup X_\bullet$, где $X_\circ, X_\bullet \neq \varnothing$, $X_\circ \cap X_\bullet = \varnothing$, $X_\circ$ и $X_\bullet$ оба открыты, эквивалентно, замкнуты, в X. То есть X не представляется в виде нетривиальной суммы, в категорном смысле, двух топологических пространств.

Определение 12 (Связные компоненты)**.** Пусть X — топологическое пространство, $x \in X$. Объединение связных подмножеств X, содержащих x, связно, что очевидно из характеризации связности через отображения в двоеточие. Это максимальное связное подмножество X, оно называется *связной компонентой*, или просто *компонентой*, X, содержащей x. Связные компоненты образуют разбиение X.

Определение 13 (Квазикомпоненты)**.** Пусть X — топологическое пространство. Определим разбиение X на *квазикомпоненты* с помощью отношения эквивалентности: $x, y \in X$ лежат в одной квазикомпоненте тогда и только тогда, когда для любого непрерывного отображения $f : X \to \{\circ, \bullet\}$ выполняется равенство $f(x) = f(y)$. То есть квазикомпоненты — это максимальные подмножества $V \subset X$, такие что $f|_V$ постоянно для любого непрерывного $f : X \to \{\circ, \bullet\}$.

Замечание 7. Компоненты содержатся в квазикомпонентах.

Замечание 8. Пусть X — топологическое пространство, V — квазикомпонента X. Тогда V совпадает с пересечением всех открыто-замкнутых подмножеств X, содержащих V. В частности, V замкнуто.

Определение 14 (Вполне несвязность)**.** Топологическое пространство X называется *вполне несвязным* (англ. *totally disconnected*), если все его компоненты связности одноточечные.

Определение 15 (Тотальная сепарированность)**.** Топологическое пространство называется *тотально сепарированным* (англ. *totally separated*), если все его квазикомпоненты одноточечные.

Замечание 9. Тотальная сепарированность влечёт хаусдорфовость.

Случай компактного хаусдорфова пространства

Теорема 3 (Лемма Шуры-Буры)**.** *Если X — компактное хаусдорфово топологическое пространство, то квазикомпоненты X связны.*

Доказательство. Докажем от противного. Пусть C — квазикомпонента. Пусть она не связна. Так как C — замкнутое множество, то это означает, что C представляется в виде дизъюнктного объединения двух непустых замкнутых в X множеств C_x и C_y. Так как компактное хаусдорфово пространство нормально, то C_x и C_y отделяются дизъюнктными открытыми множествами $U_x \supset C_x$ и $U_y \supset C_y$. Множество C, как квазикомпонента, является пересечением некоего семейства открыто-замкнутых множеств $(O_\alpha)_{\alpha\in\Lambda}$: $C = \bigcap_{\alpha\in\Lambda} O_\alpha \subset U$, где $U \coloneqq U_x \cup U_y$. Переходя к дополнениям, получаем покрытие $\bigcup_{\alpha\in\Lambda} O_\alpha^c \supset U^c$. Так как U^c — замкнутое подмножество компактного пространства, то оно компактно, и мы можем выбрать конечное подпокрытие и снова перейти к дополнениям: $C \subset \bigcap_{i\in I} O_i \subset U$, где $I \subset \Lambda$ — конечное подмножество, то есть $O \coloneqq \bigcap_{i\in I} O_i$ открыто-замкнуто. Тогда $U_x \cap O$ и $U_y \cap O$ — два дизъюнктных открыто-замкнутых множества, содержащих C_x и C_y соответственно — противоречие с тем, что C — квазикомпонента. □

Следствие 1. *Для компактных хаусдорфовых топологических пространств компоненты совпадают с квазикомпонентами. В частности, мы получаем эквивалентность двух определений пространств*

Стоуна: как компактных хаусдорфовых вполне несвязных топологических пространств и как компактных тотально сепарированных топологических пространств.

1.5. Векторы Витта и p-адические числа

Соглашения и обозначения

Соглашение 1. В этом разделе $p \in \mathbb{N}_1$ — фиксированное простое число, кольца и алгебры считаются коммутативными, ассоциативными и унитальными.

Обозначение 1. В этом разделе $[n]_0 \coloneqq \{i \in \mathbb{N}_0 \mid 0 \leqslant i < n\}$, где $n \in \mathbb{N}_0$.

Представители Тейхмюллера

Существование и единственность представителей Тейхмюллера

Определение 1 (Представитель Тейхмюллера)**.** Пусть отображение $\pi : R \to \mathbb{Z}/p\mathbb{Z}$, где $R = \mathbb{Z}_p$ или $R = \mathbb{Z}/p^n\mathbb{Z}$, $n \geqslant 1$, — это очевидная редукция, пусть $a \in R$. Если $a^p = a$, то a называется *представителем Тейхмюллера* для $\pi(a) \in \mathbb{Z}/p\mathbb{Z}$.

Лемма 1 (Лемма Гензеля)**.** *Пусть $s \in \mathbb{Z}$ и $f(s) \equiv 0 \pmod{p^n}$, где $f \in \mathbb{Z}[X]$ и $n \geqslant 1$, причём $f'(s) \not\equiv 0 \pmod{p}$. Тогда существует единственное по модулю p^{n+1} число $\tilde{s} \in \mathbb{Z}$, такое что $\tilde{s} \equiv s \pmod{p^n}$ и $f(\tilde{s}) \equiv 0 \pmod{p^{n+1}}$.*

Доказательство. Пусть $\tilde{s} = s + bp^n$, а $f(s) = ap^n$. Тогда

$$\begin{aligned} f(s + bp^n) &\equiv 0 \pmod{p^{n+1}} \\ f(s) + f'(s)bp^n &\equiv 0 \pmod{p^{n+1}} \\ ap^n + f'(s)bp^n &\equiv 0 \pmod{p^{n+1}} \\ (a + f'(s)b)p^n &\equiv 0 \pmod{p^{n+1}} \\ a + f'(s)b &\equiv 0 \pmod{p}. \end{aligned}$$

Если $f'(s) \not\equiv 0 \pmod{p}$, то последнее уравнение однозначным по модулю p образом определяет b, так как $\mathbb{Z}/p\mathbb{Z}$ — поле. □

Следствие 1. *Для любого $\alpha \in \mathbb{Z}/p\mathbb{Z}$ существуют единственные представители Тейхмюллера $\alpha^\tau \in \mathbb{Z}_p$ и $\alpha^{\tau_n} \in \mathbb{Z}/p^n\mathbb{Z}$, где $n \geqslant 1$.*

Доказательство. Возьмём $f(X) = X^p - X$. □

Замечание 1. Существование и единственность представителей Тейхмюллера можно доказать и другим способом.

Для любого $n \geqslant 1$ имеем индуцированный очевидным гомоморфизмом $\rho : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ гомоморфизм $\rho^\times : (\mathbb{Z}/p^n\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, причём $|\mathrm{Ker}(\rho^\times)| = p^{n-1}$, так как $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = p^n - p^{n-1}$ (класс $l \in \mathbb{Z}$ обратим в $\mathbb{Z}/k\mathbb{Z}$ тогда и только тогда, когда l и k взаимно просты).

Пусть $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$, пусть $a_1, a_2 \in \mathbb{Z}/p^n\mathbb{Z}$ и $\rho(a_1) = \rho(a_2) = \alpha$. Тогда $a_1, a_2 \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ и $a_1^{p^{n-1}} = a_2^{p^{n-1}}$, так как $a_1/a_2 \in \mathrm{Ker}(\rho^\times)$. Взяв $a = a_1^{p^{n-1}}$ и $a_2 = a_1^p$, получаем, что $a^p = a$.

Если $a \in \mathbb{Z}/p^n\mathbb{Z}$ и $\rho(a) = 0$, то $a \in p\mathbb{Z}/p^n\mathbb{Z}$, откуда $a^n \in p^n\mathbb{Z}/p^n\mathbb{Z} = 0$.

Разложение в ряды по представителям Тейхмюллера

Наблюдение 1. Очевидно, что для любого $a \in \mathbb{Z}_p$ существует единственное семейство $(\alpha_i)_{i\in\mathbb{N}_0} \in (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}_0}$, такое что $a = \sum_{i=0}^{\infty} \alpha_i^\tau p^i$. Аналогичное разложение $a = \sum_{i=0}^{n} \alpha_i^{\tau_{n+1}} p^i$ есть для $a \in \mathbb{Z}/p^{n+1}\mathbb{Z}$.

Наблюдение 2. Для любого кольца A и любого $a \in A$ выполняются следующие вложения: $p(a+p^nA) \subset pa+p^{n+1}A$, где $n \geqslant 0$, и $(a+p^nA)^p \subset a^p + p^{n+1}A$, где $n \geqslant 1$. Другими словами, если $\tilde{f}(x) = px$ или $\tilde{f}(x) = x^p$, то существует единственное f, такое что следующая диаграмма коммутативна:

$$\begin{array}{ccc} A & \xrightarrow{\ \tilde{f}\ } & A \\ \downarrow & & \downarrow \\ A/p^nA & \xrightarrow{\ f\ } & A/p^{n+1}A. \end{array} \tag{1}$$

Злоупотребляя обозначениями, будем писать $f(x) = px$ и $f(x) = x^p$.

Замечание 2. В верхней строчке диаграммы (1) кольцо A, очевидно, можно заменить на A/p^mA, где $m \geqslant n+1$.

Наблюдение 3. Разложение в ряды по представителям Тейхмюллера можно описать следующей биекцией:

$$(\mathbb{Z}/p\mathbb{Z})^{[n+1]_0} \xrightarrow{\sim} \mathbb{Z}/p^{n+1}\mathbb{Z}, \quad (x_i)_{i\in[n+1]_0} \mapsto \sum_{i=0}^{n} p^i x_i^{p^{n-i}} = \sum_{i=0}^{n} p^i x_i^{\tau_{n+1}}. \quad (2)$$

Это можно увидеть, например, подняв $x_i \in \mathbb{Z}/p\mathbb{Z}$ до $x_i^{\tau_{n+1}} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ и вычислив: $\sum_{i=0}^{n} p^i (x_i^{\tau_{n+1}})^{p^{n-i}} = \sum_{i=0}^{n} p^i x_i^{\tau_{n+1}}$.

Что мы хотим построить

Пусть для каждого кольца R на множестве $R^{\mathbb{N}_0}$ определена согласованная со структурой функтора от R структура кольца $W(R)$, такая что проекции $R^{\mathbb{N}_0} \to R^{[n]_0}$ индуцируют структуры колец $W_n(R)$ на $R^{[n]_0}$ и отображения $W_{n+1}(R) \to R$, $(x_i)_{i\in[n+1]_0} \mapsto \sum_{i=0}^{n} p^i x_i^{p^{n-i}}$ являются гомоморфизмами колец. Тогда биекция (2): $W_{n+1}(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/p^{n+1}\mathbb{Z}$ является гомоморфизмом колец (используем её поднятие до $W_{n+1}(\mathbb{Z}) \to \mathbb{Z}$), откуда получаем изоморфизм колец $W(\mathbb{Z}/p\mathbb{Z}) = \lim_n W_n(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}_p$.

Векторы Витта

Формулировка утверждения

Утверждение 1. *Для каждого кольца R на множестве $\mathbb{W}(R) \coloneqq R^{\mathbb{N}_1}$, называемом* множеством векторов Витта*, существует единственная согласованная со структурой функтора от R структура кольца, такая что для каждого $m \geqslant 1$ отображение $\mathbb{W}(R) \to R$, $(x_n)_{n\in\mathbb{N}_1} \mapsto x^{(m)} \coloneqq \sum_{e|m} e x_e^{m/e}$, называемое m-*ой призрачной/фантомной компонентой*, является гомоморфизмом колец.*

Доказательство единственности

Универсальный случай. Чтобы доказать утверждение 1 вычислим сумму и произведение векторов $(X_i)_{i\in\mathbb{N}_1}, (Y_i)_{i\in\mathbb{N}_1} \in \mathbb{W}\big(\mathbb{Z}\big[X_i, Y_i \,|\, i \in \mathbb{N}_1\big]\big)$. Это задаст сумму и произведение любых $(x_i)_{i\in\mathbb{N}_1}, (y_i)_{i\in\mathbb{N}_1} \in \mathbb{W}(R)$ для любого кольца R применением гомоморфизма $\mathbb{Z}\big[X_i, Y_i \,|\, i \in \mathbb{N}_1\big] \to R$, $X_i \mapsto x_i$, $Y_i \mapsto y_i$ для всех $i \in \mathbb{N}_1$. Для вычисления также будет использоваться вложение $\iota : \mathbb{Z}\big[X_i, Y_i \,|\, i \in \mathbb{N}_1\big] \hookrightarrow \mathbb{Q}\big[X_i, Y_i \,|\, i \in \mathbb{N}_1\big]$.

Единственность и свойства. Применив ι и заметив, что в $\mathbb{Q}$-алгебрах x_n восстанавливается по индукции из $x^{(n)} = \sum_{e|n} e x_e^{n/e}$, сразу получаем единственность сложения и умножения и свойства кольца: для проверки ассоциативности и дистрибутивности используем векторы $(X_i)_{i\in\mathbb{N}_1}, (Y_i)_{i\in\mathbb{N}_1}, (Z_i)_{i\in\mathbb{N}_1} \in \mathbb{W}\big(\mathbb{Z}\big[X_i, Y_i, Z_i \,|\, i \in \mathbb{N}_1\big]\big)$.

Доказательство существования

Формальные ряды. Для произвольного кольца R построим биекцию

$$\mathbb{W}(R) \xrightarrow{\sim} 1 + tR[[t]] \subset R[[t]], \quad (x_n)_{n\in\mathbb{N}_1} \mapsto \prod_{n\geqslant 1}(1 - x_n t^n).$$

Коэффициенты ряда $\prod_{n\geqslant 1}(1-x_n t^n)$ и x_n, где $n \geqslant 1$, восстанавливаются друг из друга по индукции как многочлены с коэффициентами в $\mathbb{Z}$.

Логарифмическое дифференцирование. Выполняется равенство

$$-t\frac{d}{dt}\log\prod_{n\geqslant 1}(1 - X_n t^n) = \sum_{m\geqslant 1} X^{(m)} t^m.$$

Это легко увидеть, зная, что логарифмическая производная геометрической прогрессии равна ей самой:

$$\frac{d}{df}\log\sum_{i=0}^{\infty} f^i = \sum_{i=0}^{\infty} f^i \quad \text{или} \quad f\frac{d}{df}\log\sum_{i=0}^{\infty} f^i = \sum_{i=1}^{\infty} f^i, \tag{3}$$

и взяв $f := X_n t^n$ (тогда $f\frac{d}{df} = \frac{1}{n} t\frac{d}{dt}$).

Замечание 3. Формула (3) является легко запоминаемой формой ряда для логарифма: $\frac{d}{df}\log((1-f)^{-1}) = \sum_{i=0}^{\infty} f^i$, $-\log(1-f) = \sum_{i=1}^{\infty} f^i/i$.

Сложение и умножение. Теперь очевидно, что сложению векторов Витта соответствует умножение соответствующих рядов. Описать умножение векторов Витта тоже не очень трудно:

$$\sum_{\substack{m\geqslant 1\\ e,r|m}} e X_e^{m/e} r Y_r^{m/r} t^m = \sum_{n,e,r\geqslant 1} er\big(X_e^{\operatorname{lcm}(e,r)/e} Y_r^{\operatorname{lcm}(e,r)/r} t^{\operatorname{lcm}(e,r)}\big)^n =$$

$$= -t\frac{d}{dt}\log\prod_{e,r\geqslant 1}\big(1 - X_e^{\operatorname{lcm}(e,r)/e} Y_r^{\operatorname{lcm}(e,r)/r} t^{\operatorname{lcm}(e,r)}\big)^{er/\operatorname{lcm}(e,r)}.$$

Первое равенство — тавтология. Чтобы получить второе равенство, возьмём $f \coloneqq X_e^{\mathrm{lcm}(e,r)/e} Y_r^{\mathrm{lcm}(e,r)/r} t^{\mathrm{lcm}(e,r)}$ (тогда $f\frac{d}{df} = \frac{1}{\mathrm{lcm}(e,r)} t\frac{d}{dt}$) и применим формулу (3).

p-Типические векторы Витта

Определение 2 (p-Типические векторы Витта)**.** Пусть R — кольцо. Из формулы $x^{(n)} = \sum_{e|n} e x_e^{n/e}$ нетрудно убедится, что если применить проекцию забывания всех координат, кроме степеней фиксированного простого: $R^{\{1,2,3,\ldots\}} \to R^{\{p^0,p^1,p^2,\ldots\}}$, то кольцевая структура $\mathbb{W}(R)$ на $R^{\mathbb{N}_1}$ индуцирует кольцевую структуру $W(R)$ на $R^{\{p^0,p^1,p^2,\ldots\}} \leftrightarrow R^{\mathbb{N}_0}$. Кольцо $W(R)$ называется кольцом *p-типических векторов Витта*.

Замечание 4. Операции на $W(R)$ задаются функториальностью по R и условием аддитивности и мультипликативности для любого $k \geqslant 0$ следующих отображений: $W(R) \to R$, $(x_n)_{n\in\mathbb{N}_0} \mapsto x^{(k)_p} \coloneqq \sum_{l=0}^{k} p^l x_l^{p^{k-l}}$.

Замечание 5. Имеем изоморфизм $W(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}_p$, $(x_i)_{i\in\mathbb{N}_0} \mapsto \sum_{i=0}^{\infty} p^i x_i^\tau$.

1.6. Теорема, разложение и кольцо Витта

Теорема Витта

Определение 1 (Ортогональное пространство)**.** Определим *ортогональное пространство* как линейное пространство, снабжённое симметрической билинейной формой.

Определение 2 (Изотропное пространство)**.** Ортогональное пространство, структурная билинейная форма которого нулевая, называется *изотропным пространством*.

Определение 3 (Совершенное спаривание)**.** Назовём спаривание $v \otimes w \mapsto \langle v, w\rangle : P \otimes_K Q \to K$, где P и Q — это векторные пространства над полем K, *совершенным*, если индуцированные отображения $\lambda : P \to Q^\vee$, $v \mapsto \langle v, -\rangle$ и $\rho : Q \to P^\vee$, $w \mapsto \langle -, w\rangle$ биективны.

Наблюдение 1. Отображения λ и ρ из определения 3 выражаются друг через друга с помощью канонических гомоморфизмов $\epsilon_P : P \to (P^\vee)^\vee$ и $\epsilon_Q : Q \to (Q^\vee)^\vee$ следующим образом: $\lambda = \rho^\vee \circ \epsilon_P$ и $\rho = \lambda^\vee \circ \epsilon_Q$.

Определение 4 (Гиперболическое дополнение)**.** Два изотропных подпространства ортогонального пространства называются *гиперболическими дополнениями* друг друга, если ограничение билинейной формы определяет совершенное спаривание между ними.

Наблюдение 2. Пусть V — векторное пространство над полем K, снабжённое сюръективным гомоморфизмом $V \to V^\vee$, а P и Q — его подпространства. Так как отображение ограничения $V^\vee \to P^\vee$ сюръективно, то сквозное отображение $Q \to V \to V^\vee \to P^\vee$ биективно тогда и только тогда, когда Q является дополнением к $P^\perp := \mathrm{Ker}(V \to P^\vee)$ в V.

Теорема 1. *Пусть V — невырожденное конечномерное ортогональное пространство над полем K, где $\mathrm{char}(K) \neq 2$, а $P \subset V$ — его изотропное подпространство. Тогда у P есть гиперболическое дополнение.*

Доказательство. Пусть $Q \subset V$ — произвольное дополнение к $P^\perp$ в V, то есть $V = P^\perp \oplus Q = P \oplus Q^\perp$. Пусть $T : Q \to Q^\perp$, $v \mapsto v^T$ — проекция вдоль P. Определим подпространство $M := \{(1/2)(v + v^T) \in V \mid v \in Q\}$. Тогда M, как и Q, является дополнением к $P^\perp$ в V, потому что для любого $v \in Q$ соответствующий вектор $(1/2)(v + v^T) \in M$ отличается от вектора v на вектор из $P \subset P^\perp$. С другой стороны, пространство M изотропно: для любых векторов $v, w \in Q$ выполняются равенства $\langle v + v^T, w + w^T\rangle = \langle v - v^T, w - w^T\rangle = 0$, так как $\langle v, w^T\rangle = \langle v^T, w\rangle = 0$, а векторы $v - v^T$ и $w - w^T$ лежат в изотропном пространстве P. □

Наблюдение 3. В ортогональном пространстве V дополнения к $V^\perp$, то есть к ядру формы, — это в точности максимальные элементы множества подпространств в V с тривиальным ядром индуцированной формы. Проектирования вдоль $V^\perp$ задают изометрии между ними.

Лемма 1. *Пусть $U' \subset V'$ и $U'' \subset V''$ — две пары вложенных конечномерных ортогональных пространств над полем K, где $\mathrm{char}(K) \neq 2$, причём V' — это минимальное невырожденное подпространство в V', содержащее U', и аналогично для пары $U'' \subset V''$. Тогда любая изометрия $\varphi : U' \xrightarrow{\sim} U''$ продолжается до изометрии $V' \xrightarrow{\sim} V''$.*

Доказательство. Пусть $P' \subset U'$ — это ядро формы на U', и аналогично $P'' = \varphi(P') \subset U''$. Пусть $L' \subset U'$ — это дополнение к P' в U', и аналогично $L'' := \varphi(L') \subset U''$. Пусть $Q' \subset V'$ — это гиперболическое дополнение

к P' в ортогональном дополнении к L' в V', и аналогично для $Q'' \subset V''$. Тогда мы имеем разложения $V' = P' \oplus Q' \oplus L'$ и $V'' = P'' \oplus Q'' \oplus L''$, и утверждение леммы становится очевидным. □

Обозначение 1 (Ортогонал)**.** Если V — ортогональное пространство, а $U \subset V$ — его подпространство, то ортогонал к U в V обозначим через $\perp_V(U) \coloneqq \{v \in V \mid \langle v, u\rangle = 0 \text{ для всех } u \in U\}$.

Теорема 2 (Теорема Витта)**.** *Пусть $U' \subset V'$ и $U'' \subset V''$ — две пары вложенных конечномерных ортогональных пространств над полем K, где $\mathrm{char}(K) \neq 2$, причём V' изометрично V''. Тогда любая изометрия $\varphi : U' \xrightarrow{\sim} U''$ продолжается до изометрии $V' \xrightarrow{\sim} V''$.*

Доказательство (из трёх частей).

Часть 1. Сначала рассмотрим случай одномерных невырожденных U' и U''. Без ограничения общности можно предположить, что $V \coloneqq V' = V''$. Изометрия φ может быть продолжена до автоизометрии пространства $U' + U'' \subset V$, которая может быть продолжена до автоизометрии произвольного минимального невырожденного подпространства $U \subset V$, содержащего $U' + U''$, которая может быть продолжена до автоизометрии V, фиксирующей ортогональное дополнение к U.

Часть 2. Теперь рассмотрим случай произвольных невырожденных U' и U''. Нам нужно доказать, что $\perp_{V'}(U')$ и $\perp_{V''}(U'')$ изометричны. Предположим, что $\dim(U') = \dim(U'') > 1$. Пусть $S' \subset U'$ и $S'' \subset U''$ — изометричные собственные нетривиальные невырожденные подпространства. Тогда, по индукции, $\perp_{U'}(S')$ изометрично $\perp_{U''}(S'')$ и $\perp_{V'}(S')$ изометрично $\perp_{V''}(S'')$, а потому, по индукции, $\perp_{\perp_{V'}(S')}(\perp_{U'}(S')) = \perp_{V'}(U')$ изометрично $\perp_{\perp_{V''}(S'')}(\perp_{U''}(S'')) = \perp_{V''}(U'')$.

Часть 3. Случай произвольных U' и U'' сводится к случаю невырожденных U' и U'' рассмотрением минимального невырожденного подпространства в V', содержащего U', и минимального невырожденного подпространства в V'', содержащего U''. □

Разложение Витта

Определение 5 (Гиперболичность и анизотропность)**.** Ортогональное пространство называется *гиперболическим*, если оно являет-

ся суммой двух изотропных подпространств, являющихся гиперболическими дополнениями друг друга, и *анизотропным*, если в нём нет нетривиальных изотропных подпространств.

Лемма 2. *Пусть V — невырожденное конечномерное ортогональное пространство над полем K, где $\mathrm{char}(K) \neq 2$. Тогда все максимальные изотропные подпространства пространства V изоморфны.*

Доказательство. Следствие теоремы 2 (теоремы Витта). □

Лемма 3. *Пусть V — невырожденное конечномерное ортогональное пространство над полем K, где $\mathrm{char}(K) \neq 2$, а $P, Q, L \subset V$ — его подпространства, причём P и Q — изотропные гиперболические дополнения друг друга, а L — ортогональное дополнение к $P \oplus Q$ в V. Тогда P является максимальным изотропным подпространством пространства V тогда и только тогда, когда пространство L анизотропно.*

Доказательство. Так как $P \oplus L \subset P^\perp$ и $P^\perp \cap Q = 0$, то $P^\perp = P \oplus L$. Все изотропные подпространства пространства V, содержащие P, содержатся в $P^\perp = P \oplus L$. Подпространства пространства $P \oplus L$, содержащие P, очевидным образом взаимно однозначно соответствуют подпространствам пространства L, причём это соответствие сопоставляет изотропным подпространствам изотропные подпространства. □

Теорема 3 (Разложение Витта)**.** *Пусть V — конечномерное ортогональное пространство над полем K, где $\mathrm{char}(K) \neq 2$. Тогда существует тройка $(V_{\mathrm{iso}}, V_{\mathrm{hyp}}, V_{\mathrm{ani}})$ подпространств V, таких что V_{iso} изотропно, V_{hyp} гиперболично, V_{ani} анизотропно, а V является их попарно ортогональной прямой суммой. Группа автоизометрий V транзитивно действует на таких упорядоченных тройках.*

Доказательство. Из наблюдения 3 сразу видно, что V_{iso} определяется однозначно как ядро билинейной формы на V, а $V_{\mathrm{hyp}} \oplus V_{\mathrm{ani}}$ — это одно из его изометричных невырожденных дополнений. Остальное следует из теоремы 1, леммы 2, леммы 3 и теоремы 2 (теоремы Витта). □

Кольцо Витта

Обозначение 2 (Ортогональная прямая сумма)**.** Ортогональную прямую сумму ортогональных пространств V' и V'' над полем K будем обозначать символом $V' \oplus_\perp V''$.

Теорема 4 (Теорема Витта о сокращении)**.** *Пусть K — поле, такое что* $\mathrm{char}(K) \neq 2$*, а V, V' и V'' — три невырожденных конечномерных ортогональных пространства над K. Тогда если $V \oplus_\perp V'$ изометрично $V \oplus_\perp V''$, то V' изометрично V''.*

Доказательство. Следствие теоремы 2 (теоремы Витта). □

Определение 6 (Произведение Кронекера ортогональных пространств)**.** Если V' и V'' — два ортогональных пространства над полем K, то определено ортогональное пространство $V' \otimes_K V''$ с формой $V' \otimes_K V'' \to V'^\vee \otimes_K V''^\vee \to (V' \otimes_K V'')^\vee$, индуцированной формамами $V' \to V'^\vee$ и $V'' \to V''^\vee$ пространств V' и V'' соответственно, называемое *произведением Кронекера* ортогональных пространств V' и V''.

Определение 7 (Кольцо/группа Витта – Гротендика)**.** Пусть K — поле, такое что $\mathrm{char}(K) \neq 2$. Тогда кольцо формальных разностей полукольца классов изометричности невырожденных конечномерных ортогональных пространств над K с операциями ортогональной прямой суммы и произведения Кронекера называется *кольцом Витта – Гротендика* поля K и обозначается $\widehat{\mathrm{W}}(K)$.

Определение 8 (Кольцо/группа Витта)**.** Пусть K — поле, такое что $\mathrm{char}(K) \neq 2$. Тогда фактор $\widehat{\mathrm{W}}(K)$ по идеалу, состоящему из целочисленных кратных класса гиперболической плоскости, называется *кольцом Витта* поля K и обозначается $\mathrm{W}(K)$.

Наблюдение 4. Пусть K — поле, такое что $\mathrm{char}(K) \neq 2$. Тогда для любого невырожденного конечномерного ортогонального пространства над K аддитивное обращение его билинейной формы отвечает аддитивному обращению соответствующего элемента $\mathrm{W}(K)$.

Наблюдение 5. Пусть K — поле, такое что $\mathrm{char}(K) \neq 2$. Тогда элементы $\mathrm{W}(K)$ биективно соответствуют классам изометричности конечномерных анизотропных ортогональных пространств над K.

Пример 1. Кольцо Витта поля $\mathbb{R}$ изоморфно кольцу $\mathbb{Z}$.

1.7. Жорданова нормальная форма

Наблюдение 1. Пусть K — поле, I — конечное множество, Φ — конечное подмножество K, а $(n_\alpha)_{\alpha\in\Phi} \in (\mathbb{N}_1)^{\times\Phi}$. Тогда K-модуль с эндоморфизмом, зануляемым многочленом $\prod_{\alpha\in\Phi}(X-\alpha)^{n_\alpha} \in K[X]$, — это то же самое, что модуль над $K[X]/\prod_{\alpha\in\Phi}(X-\alpha)^{n_\alpha} \cong \prod_{\alpha\in\Phi}(K[X]/(X-\alpha)^{n_\alpha})$, а такой модуль разлагается в индексированную $\alpha \in \Phi$ прямую сумму модулей над $K[X]/(X-\alpha)^{n_\alpha}$. Помимо этого, для каждого $\alpha \in \Phi$ имеем изоморфизм колец $K[X]/(X-\alpha)^{n_\alpha} \xrightarrow{\sim} K[Y]/Y^{n_\alpha}$, $X \mapsto Y+\alpha$.

Теорема 1. *Пусть D — тело, $n \in \mathbb{N}_1$ — натуральное число, а M — $D[X]/X^n$-модуль. Тогда существует семейство $(m_i)_{i\in I} \in \{1,\dots,n\}^{\times I}$, такое что $M \simeq \bigoplus_{i\in I} D[X]/X^{m_i}$, где I — множество.*

Доказательство (из двух частей).

Часть 1. Пусть $x : M \to M$ — это D-гомоморфизм действия X. Сначала докажем, что $D[X]/X^n$-модуль M изоморфен $\bigoplus_{i=1}^n x^{-i}(0)/x^{-i+1}(0)$. Пусть V_n — это дополнение к $x^{-n+1}(0)$ в $x^{-n}(0)$, V_{n-1} — дополнение к $x^{-n+2}(0)$ в $x^{-n+1}(0)$, содержащее $x(V_n)$, V_{n-2} — дополнение к $x^{-n+3}(0)$ в $x^{-n+2}(0)$, содержащее $x(V_{n-1})$, и так далее. Разложение $M = \bigoplus_{i=1}^n V_i$ устанавливает нужный изоморфизм.

Часть 2. Пусть Δ_n — это D-базис V_n, Δ_{n-1} — это D-базис дополнения к $\varphi(V_n)$ в V_{n-1}, Δ_{n-2} — это D-базис дополнения к $\varphi(V_{n-1})$ в V_{n-2} и так далее. Тогда $M = \bigoplus_{k=1}^n \bigoplus_{v\in\Delta_k} \bigoplus_{i=0}^{k-1} D{\cdot}x^i(v)$ — нужное разложение. □

1.8. Изображение конфигурации Дезарга

На рисунке 1.2 изображена конфигурация Дезарга, на которой выделены два взаимно вписанных пятиугольника. Посмотрим, как такую картинку можно нарисовать. Применив растяжения вдоль осей x и y (рис. 1.3), можно считать, что точки A, B и D фиксированы. Тогда выбор точки C задаёт рисунок: проводятся линии CD, $C'D$, CA (до E'), $C'A$ (до E), CB (до F'), $C'B'$ (до F). Точки B, E и F всегда лежат на одной линии, что можно проверить, например, координатным методом.

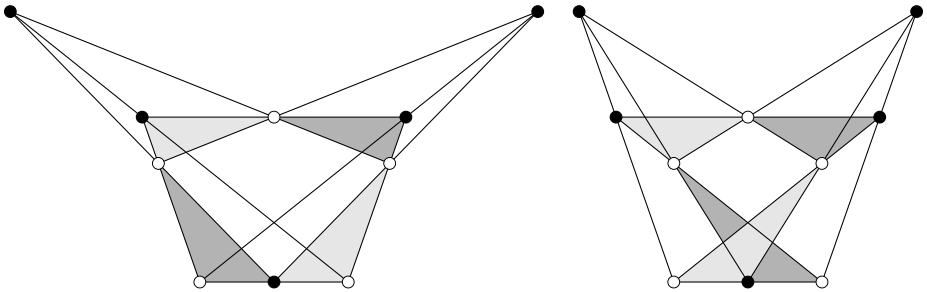


Рис. 1.2. Конфигурация Дезарга — пятиугольники

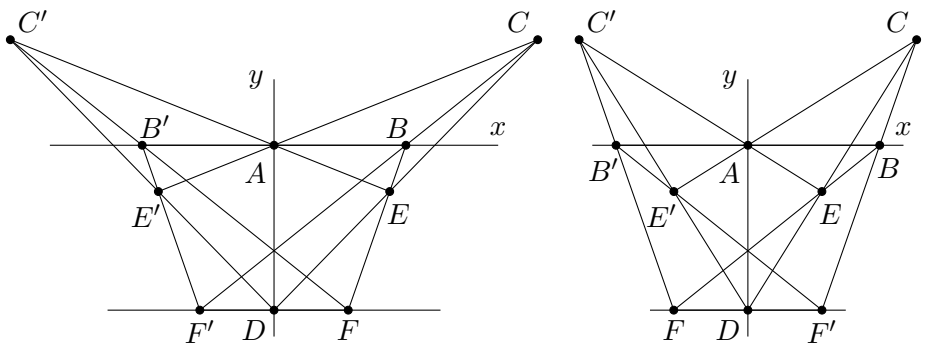


Рис. 1.3. Конфигурация Дезарга — чертежи

1.9. Элемент Казимира

Определение 1 (Элемент Казимира представления)**.** Пусть K — поле, L — конечномерная алгебра Ли над K, а $\rho : L \to \mathrm{End}_{K\text{-mod}}(V)$, где V — конечномерный K-модуль, — представление L, такое что билинейная форма $b : L \otimes_K L \to K$, $x \otimes y \mapsto \mathrm{tr}(\rho(x)\rho(y))$ невырождена. Тогда определена следующая диаграмма:

$$\mathrm{End}_{K\text{-mod}}(L) \xleftarrow[\sim]{\alpha} L \otimes_K L^\vee \xleftarrow[\sim]{\beta} L \otimes_K L \xrightarrow{\gamma} \mathrm{End}_{K\text{-mod}}(V), \qquad (1)$$

где α — стандартное отождествление, изоморфизм β индуцирован изоморфизмом $x \mapsto b(x, -) : L \xrightarrow{\sim} L^\vee$, а отображение γ переводит $x \otimes y$ в $\rho(x)\rho(y)$ для любых $x, y \in L$. Элемент $\Omega_\rho \coloneqq \gamma(\beta^{-1}(\alpha^{-1}(\mathrm{Id}_L)))$ называется *элементом Казимира* представления ρ.

Наблюдение 1 (Инвариантность элемента Казимира)**.** В обозначениях определения 1 отображения α, β и γ являются гомоморфизмами L-модулей, а потому, так как элемент $\mathrm{Id}_L \in \mathrm{End}_{K\text{-mod}}(L)$ является L-инвариантным, то элемент Казимира Ω_ρ тоже является L-инвариантным.

Наблюдение 2 (След элемента Казимира)**.** В обозначениях определения 1 след любого элемента $\mathrm{End}_{K\text{-mod}}(L)$ совпадает со следом его образа в $\mathrm{End}_{K\text{-mod}}(V)$. Это абстрактная тавтология — надо воспользоваться тем, что след элемента $\mathrm{End}_{K\text{-mod}}(L)$ задаётся спариванием в $L \otimes_K L^\vee$. В частности, $\mathrm{tr}(\Omega_\rho) = \dim_K(L)$.

1.10. Целые в квадратичных полях

Теорема 1. *Пусть $d \in \mathbb{Z}$ — бесквадратное целое число, а $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} := \{a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}] \mid a, b \in \mathbb{Q},\ 2a \in \mathbb{Z},\ a^2 - b^2 d \in \mathbb{Z}\}$. Тогда если $d \equiv 2, 3 \pmod 4$, то $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\sqrt{d}]$, а если $d \equiv 1 \pmod 4$, то $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.*

Доказательство. Пусть $a, b \in \mathbb{Q}$ — числа, такие что $2a, a^2 - b^2 d \in \mathbb{Z}$. Так как $a^2 - b^2 d \in \mathbb{Z}$, то $4a^2 - 4b^2 d \in \mathbb{Z}$, откуда, так как $2a \in \mathbb{Z}$, следует, что $4b^2 d \in \mathbb{Z}$, откуда следует, что $2b \in \mathbb{Z}$, так как d бесквадратное. Осталось рассмотреть условие $4(a^2 - b^2 d) = (2a)^2 - (2b)^2 d \equiv 0 \pmod 4$. □

1.11. Категорные треугольные тождества

Пусть $F : \mathcal{C} \rightleftarrows \mathcal{E} : G$ — пара сопряжённых функторов, таких что F — левый сопряжённый, G — правый сопряжённый, а $\eta : \mathrm{Id}_\mathcal{C} \to GF$ и $\varepsilon : FG \to \mathrm{Id}_\mathcal{E}$ — единица и коединица сопряжения. Тогда биекции сопряжения в терминах единиц и коединиц описываются так:

$$(f : X \to G(Y)) \mapsto \varepsilon_Y \circ F(f), \quad (g : F(X) \to Y) \mapsto G(g) \circ \eta_X,$$

где $X \in \mathrm{Ob}(\mathcal{C})$, $Y \in \mathrm{Ob}(\mathcal{E})$, $f \in \mathrm{Ar}(\mathcal{C})$, $g \in \mathrm{Ar}(\mathcal{E})$. Естественность этих отображений эквивалентна естественности ε и η соответственно. На $F(f)$ и $G(g)$ биекции сопряжения действуют так:

$$F(f) \mapsto G(F(f)) \circ \eta_X = \eta_{G(Y)} \circ f, \quad G(g) \mapsto \varepsilon_Y \circ F(G(g)) = g \circ \varepsilon_{F(X)},$$

где равенства являются следствиями естественности единицы и коединицы соответственно. Поэтому, записывая условие взаимной обратности полученных отображений, воспользовавшись естественностью биекций сопряжения, мы получаем два условия:

$$G(\varepsilon_Y) \circ \eta_{G(Y)} \circ f = f, \quad g \circ \varepsilon_{F(X)} \circ F(\eta_X) = g,$$

то есть $G\varepsilon \circ \eta G = \mathrm{Id}_G$ и $\varepsilon F \circ F\eta = \mathrm{Id}_F$. Эти условия типа «композиция единицы и коединицы тождественная» называются *треугольными тождествами*.

Глава 2

Подкорректированные старые тексты

2.1. Структурная теорема для конечно порождённых модулей над областями главных идеалов

Соглашение 1. В этом разделе все кольца считаются коммутативными, ассоциативными и унитальными.

Наблюдение 1. Кольца главных идеалов, очевидно, нётеровы, а каждый конечно порождённый модуль над нётеровым кольцом A является конечно представимым, то есть является коядром гомоморфизма $A^J \to A^I$, задаваемого матрицей из $\mathrm{M}_{I,J}(A)$, где I и J — конечные множества, причём замене базисов в A^J и A^I соответствует её двустороннее домножение на обратимые матрицы:

$$\begin{array}{ccc} A^J & \longrightarrow & A^I \\ \updownarrow & & \updownarrow \\ A^J & \longrightarrow & A^I. \end{array}$$

Лемма 1. *Пусть A — область целостности, $a, b, c \in A$ и $Aa + Ab = Ac \neq 0$, то есть существуют $c_a, a_c, b_c \in A$, такие что $c_a a + c_b b = c \neq 0$, $a_c c = a$, $b_c c = b$. Тогда $\left(\begin{smallmatrix} c_a & c_b \\ -b_c & a_c \end{smallmatrix}\right) \in \mathrm{GL}_2(A)$ и $\left(\begin{smallmatrix} c \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c_a & c_b \\ -b_c & a_c \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$.*

Доказательство. Подставив $a = a_c c$ и $b = b_c c$ в $c = c_a a + c_b b$ и сократив на c, получаем, что $\det(\begin{smallmatrix} c_a & c_b \\ -b_c & a_c \end{smallmatrix}) = c_a a_c + c_b b_c = 1$. □

Теорема 1. *Пусть A — область главных идеалов, $x \in \mathrm{M}_{I,J}(A)$, где I и J — конечные множества. Тогда множество $X \coloneqq \mathrm{GL}_I(A) x \mathrm{GL}_J(A)$ содержит матрицу, у которой в каждой строке и в каждом столбце максимум один ненулевой элемент.*

Набросок доказательства. Можно предположить, что $I, J \neq \varnothing$. По нётеровости A существуют $y = (y_{i,j})_{i\in I, j\in J} \in X$ и $(i_1, j_1) \in I \times J$, такие что идеал Ay_{i_1,j_1} максимален среди идеалов вида $Az_{i',j'}$ для $(z_{i,j})_{i\in I,j\in J} \in X$ и $(i', j') \in I \times J$. Тогда $y_{i_1,j}, y_{i,j_1} \in Ay_{i_1,j_1}$ для всех $i \in I$ и $j \in J$, так как иначе мы могли бы применить лемму 1 и получить противоречие с определением y_{i_1,j_1}. Отсюда следует, что множество $\mathrm{E}_I(A) y \, \mathrm{E}_J(A)$ содержит матрицу вида $(y_{i,j})_{i\in\{i_1\},j\in\{j_1\}} \oplus y'$, где $y' \in \mathrm{M}_{I\setminus\{i_1\},J\setminus\{j_1\}}(A)$, и теорема доказывается по индукции, заменой x на y'. □

Замечание 1. Между прочим, если кольцо A обладает свойством диагонализуемости матриц из формулировки теоремы 1, то A является кольцом главных идеалов, что можно увидеть, рассмотрев случай $|J| = 1$.

Теорема 2 (Примарное разложение)**.** *Пусть A — область главных идеалов, пусть M — конечно порождённый A-модуль. Тогда существует единственное с точностью до переиндексирования конечное семейство примарных идеалов $(\mathfrak{q}_i)_{i\in I}$, такое что $M \cong \bigoplus_{i\in I} A/\mathfrak{q}_i$*

Доказательство (из двух частей).

Доказательство существования. Из наблюдения 1 и теоремы 1 мы получаем разложение M в конечную прямую сумму циклических слагаемых, которые, по китайской теореме об остатках и разложению на простые в областях главных идеалов, разлагаются в конечную прямую сумму примарных циклических слагаемых.

Доказательство единственности. Пусть $M \cong (\bigoplus_{\mathfrak{p}\in\mathcal{P}} \bigoplus_{i=1}^{N_\mathfrak{p}} A/\mathfrak{p}^{n_{\mathfrak{p},i}}) \oplus A^m$, где $\mathcal{P}$ — конечное множество ненулевых простых идеалов, $N_\mathfrak{p} \geqslant 1$ и $n_{\mathfrak{p},1} \geqslant n_{\mathfrak{p},2} \geqslant \cdots \geqslant n_{\mathfrak{p},N_\mathfrak{p}} \geqslant 1$ для всех $\mathfrak{p} \in \mathcal{P}$. Пусть $M_\mathfrak{p} \coloneqq \{x \in M \mid \exists n \geqslant 0 : \mathfrak{p}^n x = 0\}$, где $\mathfrak{p}$ — простой идеал, $M_{\mathrm{free}} \coloneqq M/(\sum_{\mathfrak{p}\text{ prime}} M_\mathfrak{p})$. Тогда $M_\mathfrak{p} \cong \bigoplus_{i=1}^{N_\mathfrak{p}} A/\mathfrak{p}^{n_{\mathfrak{p},i}}$ для $\mathfrak{p} \in \mathcal{P}$, $M_\mathfrak{p} = 0$ для $\mathfrak{p} \notin \mathcal{P}$, $M_{\mathrm{free}} \cong A^m$,

$\dim_{A/\mathfrak{p}}(\mathfrak{p}^{n-1}M_{\mathfrak{p}}/\mathfrak{p}^{n}M_{\mathfrak{p}}) = \max\{k \in \{1,\dots,N_{\mathfrak{p}}\} \mid n_{\mathfrak{p},k} \geqslant n\}$ для $\mathfrak{p} \in \mathcal{P}$ и $1 \leqslant n \leqslant n_{\mathfrak{p},1}$, $\dim_{A/\mathfrak{p}}(M_{\mathrm{free}}/\mathfrak{p}M_{\mathrm{free}}) = m$ для произвольного простого идеала $\mathfrak{p}$. Это доказывает единственность. □

Следствие 1 (Разложение по инвариантным факторам)**.** *Пусть A — область главных идеалов, пусть M — конечно порождённый A-модуль. Тогда существует единственная последовательность собственных идеалов $\mathfrak{d}_1 \supset \mathfrak{d}_2 \supset \cdots \supset \mathfrak{d}_n$, такая что $M \cong \bigoplus_{i=1}^{n} A/\mathfrak{d}_i$.*

Доказательство. По разложению $M \cong (\bigoplus_{\mathfrak{p}\in\mathcal{P}} \bigoplus_{i=1}^{N_{\mathfrak{p}}} A/\mathfrak{p}^{n_{\mathfrak{p},i}}) \oplus A^m$, где $\mathcal{P}$ — конечное множество ненулевых простых идеалов, $N_{\mathfrak{p}} \geqslant 1$ и $n_{\mathfrak{p},1} \geqslant n_{\mathfrak{p},2} \geqslant \cdots \geqslant n_{\mathfrak{p},N_{\mathfrak{p}}} \geqslant 1$ для всех $\mathfrak{p} \in \mathcal{P}$, однозначно строятся/восстанавливаются $\mathfrak{d}_1,\dots,\mathfrak{d}_n$: если $N := \max_{\mathfrak{p}\in\mathcal{P}}(N_{\mathfrak{p}})$, то $n := N+m$, $\mathfrak{d}_i := \mathfrak{b}_{N-i+1}$ для $1 \leqslant i \leqslant N$, где $\mathfrak{b}_i := \prod_{\{\mathfrak{p}\in\mathcal{P} \mid N_{\mathfrak{p}}\geqslant i\}} \mathfrak{p}^{n_{\mathfrak{p},i}}$, и $\mathfrak{d}_i := 0$ для $N+1 \leqslant i \leqslant N+m$. □

2.2. Теорема Гамильтона – Кэли

Формулировка и доказательство

Теорема 1 (Теорема Гамильтона – Кэли)**.** *Если x — эндоморфизм свободного конечно порождённого модуля V над ассоциативным коммутативным унитальным кольцом A, то x является корнем своего характеристического многочлена.*

Доказательство. Эндоморфизм $\varphi \mapsto \varphi x$ превращает $\mathrm{End}_A(V)$-модуль $\mathrm{End}_A(V)$ в модуль над кольцом $\mathrm{End}_A(V)[X] \cong \mathrm{End}_A(V) \otimes_A A[X] \cong \mathrm{End}_{A[X]}(V \otimes_A A[X])$, при этом Id_V зануляется элементом $c := x - X$, а потому и элементом $\mathrm{adj}(c)c = \det(c) \in A[X] \subset \mathrm{End}_{A[X]}(V \otimes_A A[X])$. □

Замечание 1. Приведённое доказательство теоремы Гамильтона – Кэли изложено в статье Алексея Муранова [15].

Наблюдение 1. Пусть A — ассоциативное коммутативное унитальное кольцо, V — конечно порождённый A-модуль, а $\varphi \in \mathrm{End}_{A\text{-mod}}(V)$. По определению V существует сюръективный гомоморфизм $\pi : A^I \to V$, где I — какое-то конечное множество. По проективности A^I существует эндоморфизм $\widetilde{\varphi} \in \mathrm{End}_{A\text{-mod}}(A^I)$, такой что $\varphi \circ \pi = \pi \circ \widetilde{\varphi}$, называемый поднятием φ. Для любого такого $\widetilde{\varphi}$ любой многочлен из $A[X]$, зануляющий $\widetilde{\varphi}$, например, характеристический многочлен $\widetilde{\varphi}$, зануляет и φ.

Дополнение

Теорема 2. *Пусть $\varphi \in \mathrm{End}_{A\text{-mod}}(A^n)$, где $n \in \mathbb{N}_0$, а A — ассоциативное коммутативное унитальное кольцо. Тогда характеристический многочлен φ равен $\sum_{i=0}^{n}(-1)^i \operatorname{tr}(\bigwedge^i \varphi)X^{n-i} \in A[X]$.*

Идея доказательства. Двойной счёт по множеству пар, состоящих из перестановки n-элементного множества и подмножества в множестве её фиксированных точек. □

Наблюдение 2. Пусть $B \coloneqq A[X]/(P(X))$, где A — ассоциативное коммутативное унитальное кольцо, а $P(X) \in A[X]$ — унитальный многочлен. Пусть $x \in B$ — это образ $X \in A[X]$. Очевидно, что множество $\{x^i \in B \mid 0 \leqslant i < \deg(P(X))\}$ является A-базисом B. Идеал многочленов в $A[X]$, зануляющих оператор $x : B \to B$, $f \mapsto xf$, равен $(P(X))$, как сразу видно прямо из определения B. В частности, характеристический многочлен x равен $P(X)$.

Наблюдение 3. Присоединённую матрицу к матрице $(x_{i,j})_{i,j\in I}$ можно определить формулой $(\sum_{\{\sigma\in\mathrm{Aut}(I)|\sigma(j)=i\}} \operatorname{sgn}(\sigma) \prod_{k\in I\setminus\{j\}} x_{k,\sigma(k)})_{i,j\in I}$.

Некоторые следствия

Теорема 3. *Пусть M — конечно порождённый модуль над коммутативным ассоциативным унитальным кольцом A, а ι — ненулевой инъективный эндоморфизм M. Тогда $\mathrm{Ann}_A(\mathrm{Coker}(\iota)) \neq 0$.*

Доказательство. Из теоремы Гамильтона – Кэли следует, что существует унитальный многочлен $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ минимальной степени $n \in \mathbb{N}_1$, такой что $P(\iota) = 0$. Так как на ι можно сокращать слева, то $a_0 \neq 0$. Тогда $a_0 v = -\sum_{i=1}^{n} a_i \iota^i(v) \in \iota(M)$ для любого $v \in M$, то есть $a_0 \in \mathrm{Ann}_A(\mathrm{Coker}(\iota))$. □

Следствие 1. *Пусть A — ненулевое коммутативное ассоциативное унитальное кольцо, а $n, m \in \mathbb{N}_1$ — числа, такие что $n > m$. Тогда не существует инъективного гомоморфизма A-модулей $\iota : A^n \to A^m$.*

Доказательство. Пусть $\iota' : A^m \to A^n$ — какое-то координатное вложение. Тогда $\iota' \circ \iota$ — ненулевой инъективный эндоморфизм A^n, такой что $\mathrm{Ann}_A(\mathrm{Coker}(\iota' \circ \iota)) = 0$, что противоречит теореме 3. □

2.3. Тензорное произведение

Тензорное произведение абелевых групп

Обозначение 1. В этом разделе Hom без индексов обозначает Hom как абелевых групп. То же верно насчёт $\otimes$ и End.

Определение 1 (Тензорное произведение)**.** Определим *тензорное произведение* конечного семейства абелевых групп $(V_i)_{i\in I}$ как абелеву группу $\bigotimes_{i\in I} V_i$, заданную образующими — формальными произведениями $\bigotimes_{i\in I} v_i$, биективными семействам $(v_i)_{i\in I} \in \prod_{i\in I} V_i$, — и соотношениями — $(v'+v'')_{\otimes e} \otimes (\bigotimes_{i\in I\setminus\{e\}} v_i) = v'_{\otimes e} \otimes (\bigotimes_{i\in I\setminus\{e\}} v_i) + v''_{\otimes e} \otimes (\bigotimes_{i\in I\setminus\{e\}} v_i)$, где $e \in I$, $v', v'' \in V_e$, $v_i \in V_i$ для любого $i \in I \setminus \{e\}$.

Замечание 1. Индекс $\otimes e$ в выражении $v'_{\otimes e}$, называемый *позиционным индексом*, указывает на место v' в формальном произведении. Группировка тензорных мономов считается ясной из контекста.

Наблюдение 1. Пусть $(V_i)_{i\in I}$ — пустое семейство абелевых групп, то есть $I = \varnothing$. Тогда $\bigotimes_{i\in I} V_i \cong \mathbb{Z}$.

Наблюдение 2. Пусть $(V_i)_{i\in I}$ — конечное семейство абелевых групп, а $\bigotimes_{i\in I} v_i \in \bigotimes_{i\in I} V_i$. Тогда если $v_e = 0$ для какого-то $e \in I$, то $\bigotimes_{i\in I} v_i = 0$.

Определение 2 (Функториальность $\otimes$)**.** Пусть $(\varphi_i : V_i \to U_i)_{i\in I}$ — конечное семейство гомоморфизмов абелевых групп. Тогда гомоморфизм $\bigotimes_{i\in I} \varphi_i : \bigotimes_{i\in I} V_i \to \bigotimes_{i\in I} U_i$, $\bigotimes_{i\in I} v_i \mapsto \bigotimes_{i\in I} \varphi_i(v_i)$ называется *тензорным произведением* семейства $(\varphi_i)_{i\in I}$.

Утверждение 1 (Сопряжённость $\otimes$ и Hom)**.** *Пусть V, U и M — абелевы группы. Тогда имеем следующий естественный изоморфизм:*

$$\mathrm{Hom}(M\otimes V, U) \underset{((\psi(v))(m)\leftarrow m\otimes v)\leftarrow\psi}{\overset{\varphi\mapsto(v\mapsto(m\mapsto\varphi(m\otimes v)))}{\rightleftarrows}} \mathrm{Hom}(V, \mathrm{Hom}(M, U)). \tag{1}$$

Утверждение 2 (Унитальность $\otimes$)**.** *Пусть V — абелева группа. Тогда имеем естественный изоморфизм $a\otimes v \mapsto av : \mathbb{Z}\otimes V \rightleftarrows V : 1\otimes v \leftarrow\!\shortmid v$.*

Утверждение 3 (Дистрибутивность $\otimes$)**.** *Пусть $\pi : I \to J$ — отображение множеств, J конечно, $(V_i)_{i\in I}$ — семейство абелевых групп.*

Пусть $\mathrm{Sec}(\pi) \coloneqq \{\sigma : J \to I \mid \pi \circ \sigma = \mathrm{Id}_J\}$. *Тогда проекции на слагаемые и вложения слагаемых прямых сумм индуцируют пару взаимно обратных гомоморфизмов:* $\bigotimes_{j\in J} \bigoplus_{i\in\pi^{-1}(j)} V_i \rightleftarrows \bigoplus_{\sigma\in\mathrm{Sec}(\pi)} \bigotimes_{j\in J} V_{\sigma(j)}$.

Утверждение 4 (Точность справа $\otimes$)**.** *Пусть* I *— конечное множество,* $(V_i)_{i\in I}$ *и* $(U_i)_{i\in I}$ *— семейства абелевых групп, причём* U_i *является подгруппой* V_i *для любого* $i \in I$*. Тогда следующая последовательность с очевидным образом определёнными гомоморфизмами точна:*

$$\bigoplus_{e\in I}((U_e)_{\otimes e} \otimes (\bigotimes_{i\in I\setminus\{e\}} V_i)) \to \bigotimes_{i\in I} V_i \to \bigotimes_{i\in I}(V_i/U_i) \to 0.$$

Доказательство. Пусть $\mathcal{U} \subset \bigotimes_{i\in I} V_i$ — это образ первого гомоморфизма. Тогда обратный к гомоморфизму $(\bigotimes_{i\in I} V_i)/\mathcal{U} \to \bigotimes_{i\in I}(V_i/U_i)$ определяется на образующих так: $\bigotimes_{i\in I}(v_i + U_i) \mapsto (\bigotimes_{i\in I} v_i) + \mathcal{U}$. Определение корректно — образ $\bigotimes_{i\in I}(v_i + U_i)$ зависит только от классов $v_i + U_i \in V_i/U_i$, где $i \in I$. □

Пример 1. Пусть R — кольцо, а $\mathfrak{I} \subset R$ — аддитивная подгруппа, такая что $R\mathfrak{I} + \mathfrak{I}R \subset \mathfrak{I}$, то есть двусторонний идеал. Тогда отображение умножения $R \otimes R \to R$ индуцирует отображение $(R/\mathfrak{I}) \otimes (R/\mathfrak{I}) \cong (R \otimes R)/(R \otimes \mathfrak{I} + \mathfrak{I} \otimes R) \to R/\mathfrak{I}$.

Утверждение 5 (Ассоциативность $\otimes$)**.** *Пусть* $\pi : I \to J$ *— отображение конечных множеств,* $(V_i)_{i\in I}$ *— семейство абелевых групп. Тогда имеем следующий изоморфизм:*

$$\bigotimes_{i\in I} V_i \leftrightarrow \bigotimes_{j\in J} \bigotimes_{i\in\pi^{-1}(j)} V_i, \quad \bigotimes_{i\in I} v_i \leftrightarrow \bigotimes_{j\in J} \bigotimes_{i\in\pi^{-1}(j)} v_i. \tag{2}$$

Набросок доказательства. Согласно определению 1 представим каждый из $\bigotimes_{i\in\pi^{-1}(j)} V_i$ как фактор свободной абелевой группы, порождённой формальными тензорными мономами, после чего воспользуемся точностью справа $\bigotimes_{j\in J}(-)$ в смысле утверждения 4, ну и дистрибутивностью $\bigotimes$ относительно $\bigoplus$, то есть утверждением 3. □

Определение 3 (Тензорное произведение колец)**.** Пусть $(R_i)_{i\in I}$ — конечное семейство колец. Определим на абелевой группе $\bigotimes_{i\in I} R_i$ умножение следующим образом:

$$(\bigotimes_{i\in I} R_i) \otimes (\bigotimes_{i\in I} R_i) \xrightarrow{\sim} \bigotimes_{i\in I}(R_i \otimes R_i) \to \bigotimes_{i\in I} R_i,$$
$$(\bigotimes_{i\in I} r'_i) \otimes (\bigotimes_{i\in I} r''_i) \mapsto \bigotimes_{i\in I}(r'_i \otimes r''_i) \mapsto \bigotimes_{i\in I}(r'_i r''_i).$$

Первое отображение — это изоморфизм ассоциативности, а второе — это тензорное произведение отображений умножения в индивидуальных кольцах.

Утверждение 6 (Универсальное свойство тензорного произведения колец)**.** *Пусть $(R_i)_{i\in I}$ — конечное семейство ассоциативных унитальных колец. Тогда кольцо $\bigotimes_{i\in I} R_i$ снабжено семейством гомоморфизмов $\iota_e : R_e \to \bigotimes_{i\in I} R_i$, $r \mapsto r_{\otimes e} \otimes \bigotimes_{i\in I\setminus\{e\}} 1_{\otimes i}$, где $e \in I$, причём образы ι_e и $\iota_{e'}$ при $e \neq e'$ поэлементно коммутируют. Пусть S — ассоциативное унитальное кольцо, а $(\epsilon_e : R_e \to S)_{e\in I}$ — семейство гомоморфизмов, такое что образы ϵ_e и $\epsilon_{e'}$ при $e \neq e'$ поэлементно коммутируют. Тогда существует единственный гомоморфизм $\varphi : \bigotimes_{i\in I} R_i \to S$, такой что $\varphi \circ \iota_e = \epsilon_e$ для любого $e \in I$.*

Тензорное произведение с коэффициентами

Бинарное тензорное произведение с коэффициентами

Определение 4 ((Ко)инварианты Хохшильда)**.** Пусть M — бимодуль над ассоциативным унитальным кольцом R. Определим его *инварианты и коинварианты Хохшильда* следующим образом:

$$\mathrm{HH}^0(R, M) \coloneqq M^{\mathfrak{h}(R)} = \{m \in M \mid rm = mr \text{ для всех } r \in R\},$$
$$\mathrm{HH}_0(R, M) \coloneqq M_{\mathfrak{h}(R)} = M/(rm = mr \mid r \in R,\ m \in M),$$

где факторизация в определении $\mathrm{HH}_0(R, M)$ — это факторизация абелевой группы по соотношениям, а $\mathfrak{h}(R)$ — это кольцо Ли ассоциативного кольца R, действующее на абелевой группе M через композицию гомоморфизма $r \mapsto r \otimes 1 - 1 \otimes r : \mathfrak{h}(R) \to R \otimes R^o$ со структурным гомоморфизмом $R \otimes R^o \to \mathrm{End}(M)$.

Пример 2. Пусть R — ассоциативное унитальное кольцо, $V = {}_R V$ и $U = {}_R U$ — левые R-модули. Тогда $\mathrm{Hom}_R({}_R V, {}_R U) \cong (\mathrm{Hom}(V, U))^{\mathfrak{h}(R)}$.

Определение 5 (Бинарное тензорное произведение с коэффициентами)**.** Пусть R — ассоциативное унитальное кольцо, $V = V_R$ — правый R-модуль, $U = {}_R U$ — левый R-модуль. Определим *тензорное произведение* V и U над R следующим образом: $V_R \otimes_R U \coloneqq (V \otimes U)_{\mathfrak{h}(R)}$.

Наблюдение 3. Пусть S, R и T — ассоциативные унитальные кольца, $M = {}_S M_R$ — S-R-бимодуль, $V = {}_R V$ — левый R-модуль, $U = {}_S U$ — левый S-модуль. Тогда изоморфизм (1) индуцирует изоморфизм

$$\mathrm{Hom}_S({}_S M_R \otimes_{R\,R} V, {}_S U) \cong (\mathrm{Hom}((M \otimes V)_{\mathfrak{h}(R)}, U))^{\mathfrak{h}(S)} \cong$$
$$\cong ((\mathrm{Hom}(M \otimes V, U))^{\mathfrak{h}(R)})^{\mathfrak{h}(S)} \cong ((\mathrm{Hom}(V, \mathrm{Hom}(M, U)))^{\mathfrak{h}(S)})^{\mathfrak{h}(R)} \cong$$
$$\cong (\mathrm{Hom}(V, (\mathrm{Hom}(M, U))^{\mathfrak{h}(S)}))^{\mathfrak{h}(R)} \cong \mathrm{Hom}_R({}_R V, \mathrm{Hom}_S({}_S M_R, {}_S U)).$$

Наблюдение 4 (Функторы замены кольца)**.** Пусть $S \to R$ — гомоморфизм ассоциативных унитальных колец. Такой гомоморфизм индуцирует функтор *ограничения скаляров*: $\mathrm{res}^R_S : R\text{-Mod} \to S\text{-Mod}$, наделяющий R-модуль ${}_R V$ структурой S-модуля с помощью сквозного гомоморфизма $S \to R \to \mathrm{End}(V)$, а также индуцирует на $R = {}_R R_S = {}_S R_R$ структуры R-S-бимодуля и S-R-бимодуля. Естественные изоморфизмы унитальности $\mathrm{Hom}_R({}_R R_S, {}_R V) \leftrightarrow \mathrm{res}^R_S({}_R V) \leftrightarrow {}_S R_R \otimes_{R\,R} V$ переводят изоморфизмы сопряжённости между $\otimes$ и Hom в изоморфизмы следующих сопряжённостей: ${}_R R_S \otimes_S (-) \dashv \mathrm{res}^R_S(-) \dashv \mathrm{Hom}_S({}_S R_R, -)$. Функтор ${}_R R_S \otimes_S (-)$ называется *расширением скаляров*, $\mathrm{Hom}_S({}_S R_R, -)$ — *корасширением скаляров*, а все три вместе — *функторами замены кольца.*

Тензорное произведение с коэффициентами для семейств

Определение 6 (Система коэффициентов)**.** Пусть I — конечное множество. Тогда будем называть *системой коэффициентов* семейство ассоциативных унитальных колец $(R_{i,i'})_{(i,i')\in I^{\times 2}\setminus\Delta}$, такое что $R_{i,i'} = R^o_{i',i}$ для всех $(i, i') \in I^{\times 2} \setminus \Delta$.

Определение 7 (Действие системы коэффициентов)**.** Будем говорить, что на конечном семействе абелевых групп $(V_i)_{i\in I}$ действует система коэффициентов $(R_{i,i'})_{(i,i')\in I^{\times 2}\setminus\Delta}$, если для каждого $i' \in I$ абелева группа $V_{i'}$ снабжена структурой модуля над $\bigotimes_{i\in I\setminus\{i'\}} R_{i,i'}$.

Определение 8 (Тензорное произведение с коэффициентами)**.** Пусть система коэффициентов $(R_{i,i'})_{(i,i')\in I^{\times 2}\setminus\Delta}$ действует на конечном семействе абелевых групп $(V_i)_{i\in I}$. Тогда *тензорное произведение* семейства $(V_i)_{i\in I}$ над $(R_{i,i'})_{(i,i')\in I^{\times 2}\setminus\Delta}$, обозначаемое $\bigotimes_{i\in I}^{R_{i,i'}} V_i$, — это фактор абелевой группы $\bigotimes_{i\in I} V_i$ по соотношениям типа

$$(v_i r_{i,i'})_{\otimes i} \otimes (\bigotimes_{k\in I\setminus\{i\}} v_k) = (r_{i,i'} v_{i'})_{\otimes i'} \otimes (\bigotimes_{k\in I\setminus\{i'\}} v_k),$$

где $(i,i') \in I^{\times 2} \setminus \Delta$, $r_{i,i'} \in R_{i,i'}$, $(v_k)_{k\in I} \in \prod_{k\in I} V_k$.

Утверждение 7 (Ассоциативность). *Пусть $\pi : I \to J$ — отображение конечных множеств. Пусть на семействе абелевых групп $(V_i)_{i\in I}$ действует система коэффициентов $(R_{i,i'})_{(i,i')\in I^{\times 2}\setminus\Delta}$. Тогда изоморфизм ассоциативности* (2) *индуцирует изоморфизм фактор-групп*

$$\bigotimes_{i\in I}^{R_{i,i'}} V_i \leftrightarrow \bigotimes_{j\in J}^{\mathcal{R}_{j,j'}} \bigotimes_{i\in\pi^{-1}(j)}^{R_{i,i'}} V_i, \text{ где } \mathcal{R}_{j,j'} \coloneqq \bigotimes_{(i,i')\in\pi^{-1}(j)\times\pi^{-1}(j')} R_{i,i'}.$$

Набросок доказательства. Утверждение 7 можно получить из утверждения 5 с помощью утверждения 4. □

Замечание 2. Определения 6, 7, 8 и утверждение 7 добавлены с иллюстративными целями, чтобы показать, что определение тензорного произведения не зависит от порядка на множестве индексов.

2.4. Коммутативная локализация

Локализация коммутативного моноида

Определение и задание

Определение 1 (Локализация моноида). Пусть дано отображение множества S в мультипликативный моноид T. Определим *локализацию* T по S, обозначаемую $S^{-1}T$, как начальный объект в категории моноидов под T, в которых образы элементов S обратимы.

Наблюдение 1 (Задание локализации). Ясно, что локализация моноида T по множеству $S \subset T$ может быть задана добавлением к T семейства переменных $(X_s)_{s\in S}$ и факторизацией по семейству соотношений $(X_s s = s X_s = 1)_{s\in S}$.

Определение 2 (Мультипликативное множество). Подмоноид в мультипликативном моноиде иногда называется *мультипликативным множеством*.

Наблюдение 2. Очевидно, что локализация моноида T по множеству S совпадает с локализацией T по свободному моноиду, порождённому S, и совпадает с локализацией T по образу S в T.

Определение 3 (Локализация множества с действием моноида)**.** Пусть T — моноид, $S \subset T$ — мультипликативное множество, а X — T-множество. Определим *локализацию* X по S, обозначаемую $S^{-1}X$, как начальный объект в категории T-множеств Y под X, таких что для любого $s \in S$ отображение $y \mapsto sy : Y \to Y$ биективно.

Обозначение 1. Пусть S — моноид, X — S^o-множество, а Y — S-множество. Тогда $X \star_S Y \coloneqq (X \times Y)/((xs, y) \sim (x, sy))_{s \in S, x \in X, y \in Y}$.

Наблюдение 3. Пусть T — моноид, $S \subset T$ — мультипликативное множество, а X — T-множество. Тогда T-множество $X_S \coloneqq (S^{-1}T) \star_S X$, где $a[(w, x)] \coloneqq [(aw, x)]$ для любых $a \in T$, $w \in S^{-1}T$ и $x \in X$, снабжённое гомоморфизмом $x \mapsto [(1, x)] : X \to X_S$, является локализацией T-множества X по S.

Наблюдение 4. Пусть T — моноид, а $S \subset T$ — мультипликативное множество. Тогда из наблюдения 3 сразу ясно, что локализация T по S как T-множества и локализация T по S как моноида канонически отождествляются.

Явное описание в коммутативном случае

Наблюдение 5. Пусть T — коммутативный моноид, $S \subset T$ — мультипликативное множество, а X — T-множество. Тогда T-множество $X_S \coloneqq (X \times S)/((x, s) \sim (rx, rs))_{x \in X, s, r \in S}$, где $a[(x, s)] \coloneqq [(ax, s)]$ для любых $a \in T$, $x \in X$ и $s \in S$, снабжённое гомоморфизмом $x \mapsto [(x, 1)] : X \to X_S$, является локализацией T-множества X по S.

Обозначение 2. В обозначениях наблюдения 5 класс $[(x, s)] \in X_S$ пары $(x, s) \in X \times S$ будет обозначаться через x/s или $\frac{x}{s}$ и называться *дробью*.

Лемма 1. *Пусть X — множество, а S — коммутативный моноид, действующий на X инъективными эндоморфизмами. Тогда канонический гомоморфизм $X \to S^{-1}X$ инъективен.*

Доказательство. Введём на множестве $X \times S$ отношение $(x_1, s_1) \sim (x_2, s_2) \iff x_1 s_2 = s_1 x_2$. Пусть $(x_1, s_1), (x_2, s_2), (x_3, s_3) \in X \times S$. Тогда условие $(x_1, s_1) \sim (x_2, s_2)$ эквивалентно условию $x_1 s_2 s_3 = s_1 x_2 s_3$, условие $(x_2, s_2) \sim (x_3, s_3)$ — условию $s_1 x_2 s_3 = s_1 s_2 x_3$, а условие $(x_1, s_1) \sim$

(x_3, s_3) — условию $x_1 s_2 s_3 = s_1 s_2 x_3$, откуда ясно, что $\sim$ — это отношение эквивалентности. Сразу видно, что данное отношение эквивалентности порождено соотношениями $(x, s) \sim (rx, rs)$, где $x \in X$, $s, r \in S$. □

Теорема 1. *Пусть S — коммутативный моноид, X — S-множество, а $x, y \in X$ — элементы X. Тогда равенство образов x и y в $S^{-1}X$ эквивалентно существованию $s \in S$, такого что $sx = sy$.*

Доказательство. Действие моноида S на X наследуется множеством $\overline{X} \coloneqq X/(x \sim y \mid \exists s \in S : sx = sy)$, причём элементы S действуют на $\overline{X}$ инъекциями. Очевидно, что локализации X и $\overline{X}$ по S канонически изоморфны. Осталось применить лемму 1. □

Наблюдение 6. Пусть S — коммутативный моноид, а $\iota : X \to Y$ — инъективный гомоморфизм S-множеств. Тогда индуцированный гомоморфизм $S^{-1}\iota : S^{-1}X \to S^{-1}Y$ инъективен.

Определение 4 (Сатурация подмоноида)**.** Пусть T — коммутативный мультипликативный моноид, а $S \subset T$ — его подмоноид. Определим *насыщение* или *сатурацию* S как $S^{\mathrm{sat}} \coloneqq \{a \in T \mid \exists s \in S : a \mid s\}$. Множество S^{sat} мультипликативно. Если $S = S^{\mathrm{sat}}$, то S называется *насыщенным* или *сатурированным* мультипликативным множеством.

Наблюдение 7. Пусть T — коммутативный мультипликативный моноид, а $S \subset T$ — его подмоноид. Тогда $S^{\mathrm{sat}} = \{a \in T \mid a/1 \in (S^{-1}T)^{\times}\}$.

Аддитивная локализация полукольца

Определение

Обозначение 3 (Формальные разности)**.** Если T — аддитивно записываемый коммутативный моноид, а $S \subset T$ — его подмоноид, то элементы локализации T по S, обозначаемой $T - S$, называются *формальными разностями* и записываются в виде $a - s$, где $a \in T$, $s \in S$.

Определение 5 (Аддитивная локализация полукольца)**.** Пусть дано отображение множества S в полукольцо с нулём R. Определим *аддитивную локализацию* R по S, обозначаемую $R - S$, как начальный объект в категории полуколец с нулём под R, в которых образы элементов S аддитивно обратимы.

Определение 6 (Двусторонний полуидеал)**.** Пусть R — полукольцо с нулём. Тогда подмножество $S \subset R$ называется *двусторонним полуидеалом*, если S является аддитивным подмоноидом R и $RS + SR \subset R$.

Наблюдение 8. Ясно, что аддитивная локализация полукольца с нулём R по подмножеству $S \subset R$ совпадает с аддитивной локализацией R по двустороннему полуидеалу в R, порождённому S.

Явное описание

Теорема 2. *Пусть R — полукольцо с нулём, $S \subset R$ — двусторонний полуидеал, а $R - S$ — соответствующая локализация аддитивных моноидов. Тогда на $R - S$ существует единственное дистрибутивное умножение, относительно которого канонический аддитивный сохраняющий ноль гомоморфизм $R \to R - S$ мультипликативен.*

Набросок доказательства. Произведение двух формальных разностей определяется формулой $(a_1 - s_1)(a_2 - s_2) = (a_1a_2 + s_1s_2) - (a_1s_2 + s_1a_2)$. Сразу видно, что это определение корректно. □

Наблюдение 9. В обозначениях теоремы 2 полукольцо с нулём $R - S$ является аддитивной локализацией полукольца с нулём R по S.

Локализация коммутативного кольца

Определение и задание

Определение 7 (Локализация кольца)**.** Пусть дано отображение множества S в ассоциативное унитальное кольцо R. Определим *локализацию* R по S, обозначаемую $S^{-1}R$, как начальный объект в категории ассоциативных унитальных колец над R, в которых образы элементов S мультипликативно обратимы.

Замечание 1. Кольцо $S^{-1}R$ иногда обозначается через R_S или $R[S^{-1}]$. Если $S = R \setminus \mathfrak{p}$ — теоретико-множественное дополнение простого идеала $\mathfrak{p} \subset R$, то вместо R_S часто пишут $R_{\mathfrak{p}}$.

Наблюдение 10 (Задание локализации)**.** Ясно, что локализация ассоциативного унитального кольца R по множеству $S \subset R$ может быть

задана добавлением к R семейства переменных $(X_s)_{s\in S}$ и факторизацией по семейству соотношений $(X_s s = sX_s = 1)_{s\in S}$.

Определение 8 (Локализация модуля)**.** Пусть M — модуль над ассоциативным унитальным кольцом R, а $S \subset R$ — мультипликативное множество. Определим *локализацию* M по S, обозначаемую $S^{-1}M$, как начальный объект в категории R-модулей N под M, таких что для любого $s \in S$ отображение $v \mapsto sv : N \to N$ биективно.

Наблюдение 11. Пусть M — модуль над ассоциативным унитальным кольцом R, а $S \subset R$ — мультипликативное множество. Тогда R-модуль $(S^{-1}R) \otimes_R M$ является локализацией R-модуля M по S.

Наблюдение 12. Пусть R — ассоциативное унитальное кольцо, а $S \subset R$ — мультипликативное множество. Тогда из наблюдения 11 сразу ясно, что локализация R по S как R-модуля и локализация R по S как кольца канонически отождествляются.

Явное описание в коммутативном случае

Теорема 3. *Пусть M — модуль над ассоциативным коммутативным унитальным кольцом A, а $S \subset A$ — мультипликативное множество. Тогда каноническое отображение из локализации M по S как A-множества в локализацию M по S как A-модуля биективно.*

Доказательство. Пусть M_S — это локализация M по S как A-множества. Определим сумму двух элементов M_S формулой $v_1/s_1 + v_2/s_2 = (v_1 s_2 + s_1 v_2)/(s_1 s_2)$. Сразу видно, что это определение корректно и превращает M_S в локализацию M по S как A-модуля. □

Наблюдение 13. Пусть A — ассоциативное коммутативное унитальное кольцо, а $S \subset A$ — мультипликативное множество. Тогда, согласно наблюдению 6, A-модуль $S^{-1}A$ плоский.

Локализация кольца и идеалы

Обозначение 4. Пусть дано отображение множества S в ассоциативное унитальное кольцо R. Двусторонний идеал в $S^{-1}R$, порождённый образом двустороннего идеала $\mathfrak{I} \subset R$, будем обозначать через $S^{-1}\mathfrak{I}$.

Обозначение 5. Если $f : R \to E$ — гомоморфизм ассоциативных унитальных колец, а $\mathfrak{I} \subset E$ — двусторонний идеал, то идеал $f^{-1}(\mathfrak{I})$ иногда будем обозначать через $R \cap \mathfrak{I}$.

Наблюдение 14 (Локализация коммутирует с факторизацией)**.** Пусть R — ассоциативное унитальное кольцо, $S \subset R$ — множество, а $\mathfrak{I} \subset R$ — двусторонний идеал. Тогда, по универсальным свойствам факторизации и локализации, существует единственный изоморфизм $(S^{-1}R)/(S^{-1}\mathfrak{I}) \cong S^{-1}(R/\mathfrak{I})$ колец над R.

Наблюдение 15. Пусть A — ассоциативное коммутативное унитальное кольцо, $S \subset A$ — мультипликативное множество, а $\mathfrak{a} \subset A$ и $\mathfrak{b} \subset S^{-1}A$ — идеалы. Тогда $S^{-1}\mathfrak{a} = \{a/s \in S^{-1}A \mid a \in \mathfrak{a},\ s \in S\}$, и выполняются следующие равенства:

$$S^{-1}(A \cap \mathfrak{b}) = \mathfrak{b}, \text{ так как } \frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s} \in \mathfrak{b} \Leftrightarrow \frac{a}{1} = \frac{a}{s} \cdot \frac{s}{1} \in \mathfrak{b} \Leftrightarrow a \in A \cap \mathfrak{b};$$

$$\begin{aligned} A \cap (S^{-1}\mathfrak{a}) &= \operatorname{Ker}(A \to S^{-1}A \to (S^{-1}A)/(S^{-1}\mathfrak{a})) = \\ &= \operatorname{Ker}(A \to A/\mathfrak{a} \to S^{-1}(A/\mathfrak{a})) = \{a \in A \mid \exists s \in S : sa \in \mathfrak{a}\}. \end{aligned}$$

Наблюдение 16. Пусть A — ассоциативное коммутативное унитальное кольцо, а $S \subset A$ — мультипликативное множество. Тогда условия $\operatorname{Ker}(A \to S^{-1}A) \neq 0$ и $\operatorname{Ker}(A \to S^{-1}A) = A$ эквивалентны наличию в S делителя нуля из A и нуля из A соответственно. Все делители нуля в A нильпотентны тогда и только тогда, когда для любого мультипликативного множества $S \subset A$ идеал $\operatorname{Ker}(A \to S^{-1}A)$ равен 0 или A.

Теорема 4. *Пусть A — ассоциативное коммутативное унитальное кольцо, а $S \subset A$ — мультипликативное множество. Тогда если в A все делители нуля нильпотентны, то то же верно и для $S^{-1}A$.*

Доказательство. Любая локализация $S^{-1}A$ имеет вид $T^{-1}A$, где $T \subset A$ — мультипликативное множество, такое что $S \subset T$. Пусть T — такое множество, а $\mathfrak{b} := \operatorname{Ker}(S^{-1}A \to T^{-1}A)$. Если $\mathfrak{b} = S^{-1}(A \cap \mathfrak{b}) \neq (0), (1)$, то $\operatorname{Ker}(A \to T^{-1}A) = A \cap \mathfrak{b} \neq (0), (1)$, что противоречит условию. □

Теорема 5. *Пусть A — ассоциативное коммутативное унитальное кольцо, а $S \subset A$ — мультипликативное множество. Тогда если в A все делители нуля равны нулю, то то же верно и для $S^{-1}A$.*

Доказательство. Предположим, что $S^{-1}A \neq 0$, то есть $0 \notin S$. Пусть $T = A \setminus \{0\}$ — мультипликативное множество не делителей нуля в A, а $\mathfrak{b} := \mathrm{Ker}(S^{-1}A \to T^{-1}A)$. Тогда $\mathrm{Ker}(A \to T^{-1}A) = A \cap \mathfrak{b} = 0$, а потому $\mathfrak{b} = S^{-1}(A \cap \mathfrak{b}) = 0$ и $S^{-1}A$ целостно как подкольцо поля $T^{-1}A$. □

Следствие 1. *Пусть A — ассоциативное коммутативное унитальное кольцо, а $S \subset A$ — мультипликативное множество. Тогда соответствие Галуа между идеалами кольца A и идеалами кольца $S^{-1}A$, индуцированное каноническим гомоморфизмом $A \to S^{-1}A$, индуцирует биекцию между простыми/примарными идеалами A, дизъюнктными с S, и простыми/примарными соответственно идеалами $S^{-1}A$.*

Наблюдение 17. Насыщенные мультипликативные множества в ассоциативном коммутативном унитальном кольце — это в точности дополнения объединений семейств простых идеалов.

2.5. Избегание простых (prime avoidance)

Соглашение 1. В этом разделе кольца не подразумеваются унитальными, а простым идеалом называется собственный двусторонний идеал, дополнение которого замкнуто относительно умножения.

Теорема 1. *Пусть G — группа, а $H, K \subsetneq G$ — её собственные подгруппы. Тогда $H \cup K \subsetneq G$.*

Доказательство. Мы можем предположить, что $H \not\subset K$ и $K \not\subset H$, то есть существуют $h \in H \setminus K$ и $k \in K \setminus H$. Тогда $hk \notin H \cup K$. □

Следствие 1. *Пусть G — группа, а $G', H, K \subset G$ — её подгруппы. Если $G' \subset H \cup K$, то $G' \subset H$ или $G' \subset K$.*

Доказательство. Применим теорему 1 к покрытию G' группами $H' := G' \cap H$ и $K' := G' \cap K$. □

Теорема 2. *Пусть $(\mathfrak{I}_i)_{i \in I}$ — конечное семейство двусторонних идеалов ассоциативного кольца R, такое что $R = \bigcup_{i \in I} \mathfrak{I}_i \neq \bigcup_{j \in J} \mathfrak{I}_j$ для любого $J \subsetneq I$. Тогда для любого $i \in I$ идеал $\mathfrak{I}_i$ не простой.*

Доказательство. Для каждого $i \in I$ выберем $a_i \in \mathfrak{I}_i \setminus \bigcup_{j \in I \setminus \{i\}} \mathfrak{I}_j$. Пусть идеал $\mathfrak{I}_e$, где $e \in I$, простой. Выберем биекцию $\rho : \{1, 2, \ldots, n\} \xrightarrow{\sim} I \setminus \{e\}$, где $n \in \mathbb{N}_1$. Тогда $a_e + \prod_{k=1}^{n} a_{\rho(k)} \notin \bigcup_{i \in I} \mathfrak{I}_i = R$ — противоречие. □

Замечание 1. Теорема 2 утверждает, что если ассоциативное кольцо представлено в виде объединения конечного семейства двусторонних идеалов, то из этого семейства можно выкинуть все простые идеалы.

Следствие 2 (Избегание простых)**.** *Пусть R — ассоциативное унитальное кольцо, $S \subset R$ — его подкольцо, а $(\mathfrak{I}_i)_{i \in I}$ — конечное семейство двусторонних идеалов в R, такое что $S \subset \bigcup_{i \in I} \mathfrak{I}_i$. Пусть $I' \coloneqq \{i \in I \mid$ идеал $\mathfrak{I}_i$ простой и $S \not\subset \mathfrak{I}_i\}$. Тогда $S \subset \bigcup_{i \in I \setminus I'} \mathfrak{I}_i$.*

Доказательство. Примерим теорему 2 к семейству $(S \cap \mathfrak{I}_i)_{i \in I}$ двусторонних идеалов кольца S. □

2.6. Собственные отображения

Лемма о трубке

Наблюдение 1 (Лемма о трубке)**.** Пусть $(X_i)_{i \in I}$, $(Y_i)_{i \in I}$, $(U_{i,\alpha})_{i \in I, \alpha \in \Omega}$ — три семейства множеств, такие что $Y_i, U_{i,\alpha} \subset X_i$ для любых $i \in I$ и $\alpha \in \Omega$, причём $\prod_{i \in I} Y_i \subset \bigcup_{\alpha \in \Omega} \prod_{i \in I} U_{i,\alpha}$. Для каждого $i \in I$ определим множество $V_i \coloneqq \bigcap_{\Theta \subset \Omega \mid Y_i \subset \bigcup_{\alpha \in \Theta} U_{i,\alpha}} \bigcup_{\alpha \in \Theta} U_{i,\alpha} = \bigcup_{y_i \in Y_i} \bigcap_{\alpha \in \Omega \mid y_i \in U_{i,\alpha}} U_{i,\alpha} \subset X_i$. Тогда выполняются вложения $\prod_{i \in I} Y_i \subset \prod_{i \in I} V_i \subset \bigcup_{\alpha \in \Omega} \prod_{i \in I} U_{i,\alpha}$.

Определение 1 (Замкнутое отображение)**.** Пусть X и Y — топологические пространства. Тогда отображение $f : X \to Y$ называется *замкнутым*, если для любого замкнутого подмножества $C \subset X$ множество $f(C) \subset Y$ замкнуто.

Наблюдение 2 (Прообраз и образы)**.** Пусть $f : X \to Y$ — отображение множеств. Оно индуцирует тройку отображений между решётками подмножеств: $f_\exists, f_\forall : 2^X \rightleftarrows 2^Y : f^{-1}$, таких что $f_\exists \dashv f^{-1} \dashv f_\forall$. Для $S \subset X$ множество $f_\forall(S)$ будем называть *строгим образом* S.

Наблюдение 3. Отображение замкнуто тогда и только тогда, когда строгие образы открытых множеств открыты.

Теорема 1. *Пусть $K \subset X$ и $K' \subset X'$ — подмножества топологических пространств X и X', такие что $K \times K' \subset X \times X'$ компактно, а O — открытая окрестность $K \times K'$ в $X \times X'$. Тогда существует базовая открытая окрестность $K \times K'$ в $X \times X'$, содержащаяся в O.*

Доказательство. Представим O как объединение семейства базовых открытых подмножеств в $X \times X'$, выберем из этого семейства конечное подпокрытие множества $K \times K'$ и применим к нему наблюдение 1. □

Лемма 1. *Пусть K и X — топологические пространства, причём K компактно. Тогда каноническая проекция $\pi : K \times X \to X$ является замкнутым отображением.*

Доказательство. Пусть $O \subset K \times X$ — открытое множество, а $x \in \pi_\forall(O)$. Применив теорему 1 к $\pi^{-1}(x) \subset O$, получаем базовую открытую окрестность $\pi^{-1}(x) \subset K \times U \subset O$. Тогда U — открытая окрестность точки x, содержащаяся в $\pi_\forall(O)$. Мы доказали, что $\pi_\forall(O)$ открыто. □

Лемма 2. *Пусть X и Y — топологические пространства, причём Y компактно. Пусть $f : X \to Y$ — сюръективное замкнутое отображение с компактными слоями. Тогда X компактно.*

Доказательство. Пусть $\mathcal{U} \subset \mathrm{Open}(X)$ — открытое покрытие X. Для каждого $y \in Y$ выберем конечное подпокрытие $\mathcal{U}_y \subset \mathcal{U}$ слоя $f^{-1}(y)$, после чего выберем из открытого покрытия $(f_\forall(\bigcup_{U \in \mathcal{U}_y} U))_{y \in Y}$ множества Y конечное подпокрытие $(f_\forall(\bigcup_{U \in \mathcal{U}_y} U))_{y \in F}$, где $F \subset Y$. Тогда $\bigcup_{y \in F} \mathcal{U}_y$ — конечное подпокрытие покрытия $\mathcal{U}$. □

Лемма 3. *Пусть K и K' — два компактных топологических пространства. Тогда топологическое пространство $K \times K'$ компактно.*

Доказательство. Согласно лемме 1 проекция $K \times K' \to K'$ является замкнутым отображением с компактными слоями и компактным образом, а потому, согласно лемме 2, пространство $K \times K'$ компактно. □

Лемма 4. *Пусть X — компактное топологическое пространство, а $Y \subset X$ — замкнутое подмножество. Тогда Y компактно.*

Доказательство. Пусть $\mathcal{U} \subset \mathrm{Open}(X)$ — открытое покрытие Y, а $U := X \setminus Y$. Тогда $\mathcal{U} \cup \{U\}$ — открытое покрытие X, и мы можем выбрать конечное подпокрытие $\mathcal{U}' \subset \mathcal{U} \cup \{U\}$. Тогда $\mathcal{U}' \setminus \{U\}$ — конечное подмножество $\mathcal{U}$, покрывающее Y. □

Наблюдение 4. Пусть X и Y — топологические пространства, $S \subset Y$ — подмножество, а $f : X \to Y$ — замкнутое отображение. Тогда отображение $x \mapsto f(x) : f^{-1}(S) \to S$, где топологии на множествах $f^{-1}(S)$ и S индуцированы вложениями $f^{-1}(S) \subset X$ и $S \subset Y$, замкнуто.

Теорема 2. *Пусть X, Y и Z — топологические пространства, а $f : X \to Y$ и $g : Y \to Z$ — два замкнутых отображения с компактными слоями. Тогда $g \circ f : X \to Z$ является замкнутым отображением с компактными слоями.*

Доказательство. Композиция замкнутых отображений, очевидно, замкнута. Нам нужно доказать, что слои $g \circ f$ компактны. Отображение f разлагается в композицию сюръективного замкнутого отображения и вложения замкнутого подмножества, поэтому достаточно доказать теорему для случая, когда f сюръективно, и для случая, когда f — вложение замкнутого подмножества. В первом случае, с учётом наблюдения 4, теорема следует из леммы 2, а во втором — из леммы 4. □

Теорема 3. *Пусть X, X', Y, Y' — топологические пространства, а $f : X \to Y$ и $f' : X' \to Y'$ — два замкнутых отображения с компактными слоями. Тогда $f \times f' : X \times X' \to Y \times Y'$ является замкнутым отображением с компактными слоями.*

Доказательство (из двух частей).

Часть 1. Разложение отображений f и f' в композиции сюръективных отображений и вложений замкнутых подмножеств индуцирует аналогичное разложение их произведения: $X \times X' \to f(X) \times f'(X') \to Y \times Y'$, так что мы можем предположить, что f и f' сюръективны.

Часть 2. Пусть $O \subset X \times X'$ — открытое подмножество, а $(x, x') \in (f \times f')_\forall(O)$. Применив теорему 1 к $(f \times f')^{-1}(x, x') = f^{-1}(x) \times f'^{-1}(x') \subset O$, получаем базовую открытую окрестность $U \times U' \subset O$ множества $f^{-1}(x) \times f'^{-1}(x')$. Тогда $f_\forall(U) \times f'_\forall(U') = (f \times f')_\forall(U \times U') \subset (f \times f')_\forall(O)$

— открытая окрестность точки (x, x'), содержащаяся в $(f \times f')_\forall(O)$. Мы доказали, что множество $(f \times f')_\forall(O)$ открыто. □

Теорема 4. *Если K и K' — дизъюнктные компактные подмножества хаусдорфова топологического пространства X, то у них есть дизъюнктные открытые окрестности.*

Доказательство. Пространство X хаусдорфово тогда и только тогда, когда диагональ $\Delta \subset X \times X$ замкнута. Применим теорему 1 к компактному множеству $K \times K'$ с открытой окрестностью $(X \times X) \setminus \Delta$. □

Замечание 1. Теорема 4 не понадобится в этом разделе.

Собственные отображения

Определение 2 (Собственное отображение)**.** Пусть X и Y — топологические пространства. Отображение $f : X \to Y$ называется *собственным*, если если для любого топологического пространства Z отображение $\mathrm{Id}_Z \times f : Z \times X \to Z \times Y$ замкнуто.

Наблюдение 5. Композиция собственных отображений является собственным отображением.

Наблюдение 6. Пусть X, X', Y, Y' — топологические пространства. Пусть $f : X \to Y$ и $f' : X' \to Y'$ — два собственных отображения. Тогда отображение $f \times f' : X \times X' \to Y \times Y'$ собственно, так как для любого топологического пространства Z отображение $\mathrm{Id}_Z \times f \times f'$ является композицией замкнутых отображений $\mathrm{Id}_Z \times \mathrm{Id}_X \times f'$ и $\mathrm{Id}_Z \times f \times \mathrm{Id}_{Y'}$.

Наблюдение 7. Пусть X и Y — топологические пространства, $S \subset Y$ — подмножество, а $f : X \to Y$ — собственное отображение. Тогда отображение $x \mapsto f(x) : f^{-1}(S) \to S$, где топологии на множествах $f^{-1}(S)$ и S индуцированы вложениями $f^{-1}(S) \subset X$ и $S \subset Y$, собственно.

Определение 3 (Фильтр на множестве)**.** Пусть X — множество. Непустое собственное подмножество множества всех подмножеств в X, замкнутое относительно конечных пересечений и перехода к надмножествам, называется *фильтром* на множестве X.

Определение 4 (Пространство фильтров)**.** Пусть X — множество. Множество всех фильтров на X, которое в этом разделе будет обозначаться $\mathcal{F}(X)$, снабжено топологией, заданной базой открытых множеств $(\{F \in \mathcal{F}(X) \mid S \in F\} \mid S \in 2^X)$.

Наблюдение 8. Пусть X — множество. Тогда каноническое вложение $\iota : X \to \mathcal{F}(X)$, $x \mapsto \{S \in 2^X \mid x \in S\}$ обладает плотным образом.

Определение 5 (Предельные точки фильтра)**.** Пусть X — топологическое пространство, а $F \in \mathcal{F}(X)$. Тогда элементы пересечения замыканий всех элементов F называются *предельными точками* F.

Наблюдение 9. Топологическое пространство X компактно тогда и только тогда, когда у любого фильтра на X есть предельные точки.

Обозначение 1. Символом `pt` обозначается одноточечное топологическое пространство.

Теорема 5. *Пусть X — топологическое пространство. Если отображение $X \to$ `pt` собственно, то есть для любого топологического пространства Z проекция $\pi : Z \times X \to Z$ замкнута, то X компактно.*

Доказательство. Пусть $Z \coloneqq \mathcal{F}(X)$, а $\Gamma \subset Z \times X$ — график канонического вложения $\iota : X \to Z$. С одной стороны, $\overline{\Gamma} \coloneqq \mathrm{Cl}_{Z\times X}(\Gamma)$ состоит из пар $(F, x) \in Z \times X$, таких что x — предельная точка F. С другой стороны, $\pi(\overline{\Gamma}) \supset \pi(\Gamma) = \iota(X)$, а потому, по условию, $\pi(\overline{\Gamma}) = Z$. □

Определение 6 (Слабо собственное отображение)**.** Пусть X и Y — топологические пространства. Тогда отображение $f : X \to Y$ называется *слабо собственным*, если для любого компактного $K \subset Y$ множество $f^{-1}(K) \subset X$ компактно.

Теорема 6 (Характеризации собственности)**.** *Пусть X и Y — топологические пространства, $f : X \to Y$ — отображение. Тогда следующие три условия на f эквивалентны:* (а) *f собственно;* (б) *f замкнуто и слабо собственно;* (в) *f замкнуто с компактными слоями.*

Доказательство. Докажем импликацию (а) $\Longrightarrow$ (б). Пусть $K \subset Y$ — компактное подмножество. Композиция соответствующего ограничения $f^{-1}(K) \to K$ и $K \to \mathtt{pt}$ собственна как композиция двух собственных отображений, поэтому $f^{-1}(K)$ компактно. Импликация (б) $\Longrightarrow$ (в) очевидна, а импликация (в) $\Longrightarrow$ (а) следует из теоремы 3. □

Определение 7 (Универсально замкнутое отображение)**.** Пусть X и Y — топологические пространства. Отображение $f : X \to Y$ называется *универсально замкнутым*, если оно непрерывно, и если для любого непрерывного отображения $Y' \to Y$ индуцированное отображение $X' \coloneqq Y' \times_Y X \to Y'$ замкнуто.

Теорема 7 (Собственность и универсальная замкнутость)**.** *Непрерывное отображение $f : X \to Y$ между топологическими пространствами универсально замкнуто тогда и только тогда, когда оно собственно, то есть для любого топологического пространства Z отображение $\mathrm{Id}_Z \times f : Z \times X \to Z \times Y$ замкнуто.*

Доказательство. Часть «только тогда» следует из того, что отображение $\mathrm{Id}_Z \times f$ является пуллбэком f вдоль проекции $Z \times Y \to Y$. Часть «тогда» следует из того, что любое непрерывное отображение $Z \to Y$ разлагается в композицию гомеоморфизма со своим графиком, вложенным в произведение, и проекции произведения: $Z \to Z \times Y \to Y$. □

Теорема Тихонова

Наблюдение 10. Пусть X и Y — топологические пространства, а $f : X \to Y$ — отображение. Отображение f непрерывно тогда и только тогда, когда $f(\mathrm{Cl}(S)) \subset \mathrm{Cl}(f(S))$ для любого $S \subset X$, и замкнуто тогда и только тогда, когда $f(\mathrm{Cl}(S)) \supset \mathrm{Cl}(f(S))$ для любого $S \subset X$.

Наблюдение 11. Если $(X_i \mid i \in I)$ — семейство топологических пространств, $S \subset \prod_{i\in I} X_i$ — подмножество, а $a \in \prod_{i\in I} X_i$ — элемент, то $a \in \mathrm{Cl}(S)$ тогда и только тогда, когда $\pi^I_F(a) \in \mathrm{Cl}(\pi^I_F(S))$ для любого конечного $F \subset I$, где $\pi^I_F : \prod_{i\in I} X_i \to \prod_{i\in F} X_i$ — стандартная проекция.

Теорема 8 (Относительная теорема Тихонова)**.** *Пусть I — множество, $(X_i)_{i\in I}$ и $(Y_i)_{i\in I}$ — семейства топологических пространств,*

$(f_i : X_i \to Y_i)_{i\in I}$ — семейство собственных отображений. Тогда отображение $\prod_{i\in I} f_i : \prod_{i\in I} X_i \to \prod_{i\in I} Y_i$ собственно.

Доказательство (из четырёх частей).

Часть 1. Зафиксируем обозначения. Пусть Z — топологическое пространство. Пусть $X_J \coloneqq Z \times (\prod_{i\in J} X_i) \times (\prod_{i\in I\setminus J} Y_i)$, где $J \subset I$. Пусть $f_K^J \coloneqq \mathrm{Id}_Z \times (\prod_{i\in K} \mathrm{Id}_{X_i}) \times (\prod_{i\in J\setminus K} f_i) \times (\prod_{i\in I\setminus J} \mathrm{Id}_{Y_i}) : X_J \to X_K$, где $K \subset J \subset I$. Пусть $S = S_I \subset X_I$ — подмножество, а $S_J \coloneqq f_J^I(S_I)$, где $J \subset I$. Согласно наблюдению 10 нам нужно доказать, что любой элемент множества $\mathrm{Cl}(S_\varnothing)$ можно поднять до элемента множества $\mathrm{Cl}(S_I)$.

Часть 2. Построим частично упорядоченное множество $\mathcal{O}$. Элементами $\mathcal{O}$ являются пары (J, a), где $J \subset I$, а $a \in \mathrm{Cl}(S_J)$, причём $(K, b) \preccurlyeq (J, a)$ тогда и только тогда, когда $K \subset J$ и $f_K^J(a) = b$.

Часть 3. Пусть $((K, a_K))_{K\in\mathcal{K}}$, где $\mathcal{K} \subset 2^I$, — цепь в $\mathcal{O}$. Докажем, что она имеет верхнюю грань. Пусть $J \coloneqq \bigcup_{K\in\mathcal{K}} K$. Существует единственный $a_J \in X_J$, такой что $f_K^J(a_J) = a_K$ для любого $K \in \mathcal{K}$. Докажем, что $a_J \in \mathrm{Cl}(S_J)$. По наблюдению 11 нам нужно проверить, что $\pi(a_J) \in \mathrm{Cl}(\pi(S_J))$ для любой проекции на конечное подпроизведение $\pi : X_J \to T$. Такая проекция разлагается в композицию $X_J \to X_K \to T$ для какого-то $K \in \mathcal{K}$, где $X_J \to X_K$ — это f_K^J, а $X_K \to T$ — это проекция на конечное подпроизведение. Поэтому из того, что $a_K \in \mathrm{Cl}(S_K)$ для любого $K \in \mathcal{K}$ следует, что $a_J \in \mathrm{Cl}(S_J)$.

Часть 4. Теперь мы можем применить к $\mathcal{O}$ лемму Цорна. Для любого $(\varnothing, a) \in \mathcal{O}$ существует максимальный элемент $(J, b) \in \mathcal{O}$, больший $(\varnothing, a)$. Предположим, что $J \neq I$. Для любого индекса $e \in I \setminus J$ отображение $f_J^{J\cup\{e\}}$ замкнуто, так как отображение f_e собственно, а потому элемент $b \in \mathrm{Cl}(S_J)$ можно поднять до элемента множества $\mathrm{Cl}(S_{J\cup\{e\}})$ — противоречие. □

Глава 3

Относительно новые тексты

3.1. Теорема Островского

Теорема 1 (Теорема Островского)**.** *Любая нетривиальная мультипликативная норма $\|-\|$ на $\mathbb{Q}$ эквивалентна либо обычному абсолютному значению, либо какой-то из p-адических норм.*

Доказательство (из трёх пунктов).

Общее неравенство. Пусть $m, n \in \mathbb{Z}$, причём $m, n \geqslant 2$. Тогда мы можем записать n-ичное разложение m:

$$m = a_0 + a_1 n + \cdots + a_{\lfloor \frac{\ln(m)}{\ln(n)} \rfloor} n^{\lfloor \frac{\ln(m)}{\ln(n)} \rfloor}.$$

Заметив, что для любого $a \in \mathbb{N}_0$ выполняется неравенство $\|a\| \leqslant a$, получаем:

$$\|m\| \leqslant \|a_0\| + \|a_1\|\|n\| + \cdots + \|a_{\lfloor \frac{\ln(m)}{\ln(n)} \rfloor}\|\|n\|^{\lfloor \frac{\ln(m)}{\ln(n)} \rfloor} \leqslant$$
$$\leqslant n \cdot (1 + \|n\| + \cdots + \|n\|^{\lfloor \frac{\ln(m)}{\ln(n)} \rfloor}).$$

Подставив вместо m элемент m^t, где $t \in \mathbb{N}_1$, возведя в степень $1/t$ и

устремив t к $+\infty$, получаем:

$$\begin{aligned}\|m\| \leqslant \lim_{t\to+\infty}(1+\|n\|+\cdots+\|n\|^{\lfloor t\cdot\frac{\ln(m)}{\ln(n)}\rfloor})^{\frac{1}{t}} =_{\text{при } \|n\|\neq 1}\\ = \lim_{t\to+\infty}\left(\frac{\|n\|^{\lfloor t\cdot\frac{\ln(m)}{\ln(n)}\rfloor+1}-1}{\|n\|-1}\right)^{\frac{1}{t}} = \lim_{t\to+\infty}\left(\frac{\|n\|^{t\cdot\frac{\ln(m)}{\ln(n)}+1\pm 1}-1}{\|n\|-1}\right)^{\frac{1}{t}}.\end{aligned} \tag{1}$$

Неархимедов случай. Пусть существует число $n\in\mathbb{Z}$, такое что $n\geqslant 2$ и $\|n\|\leqslant 1$. Тогда, согласно неравенству (1), для любого $m\in\mathbb{Z}$ выполняется неравенство $\|m\|\leqslant 1$. Пусть $p,l\in\mathbb{N}_1$ — два различных простых числа, таких что $\|p\|,\|l\|\neq 1$. Выберем числа $N,M\in\mathbb{N}_1$, такие что $\|p\|^N,\|l\|^M<1/2$. Тогда норма любого элемента множества $\mathbb{Z}p^N+\mathbb{Z}l^M=\mathbb{Z}$ строго меньше 1, но $\|1\|=1$ — противоречие.

Архимедов случай. Пусть для всех $n\in\mathbb{Z}$, таких что $n\geqslant 2$, выполняется неравенство $\|n\|>1$. Тогда из неравенства (1) получаем, что $\|m\|\leqslant\|n\|^{\frac{\ln(m)}{\ln(n)}}$ для всех $m,n\in\mathbb{Z}$, таких что $m,n\geqslant 2$. По симметрии существует число $c\in\mathbb{R}_{>1}$, такое что $c=\|m\|^{1/\ln(m)}=\|n\|^{1/\ln(n)}$ для всех $m,n\in\mathbb{Z}$, таких что $m,n\geqslant 2$. Отсюда получаем, что $\|n\|=c^{\ln(n)}=e^{\ln(c)\ln(n)}=n^{\ln(c)}$ для всех $n\in\mathbb{Z}$, таких что $n\geqslant 2$. □

3.2. Категории как полугруппы

Мультипликативные полугруппы с нулём

Определение 1 (Бинар)**.** Множество X, снабжённое отображением $(x,y)\mapsto xy : X\times X\to X$ называется *бинаром* в мультипликативной записи или *мультипликативным бинаром.*

Определение 2 (Нулевой элемент)**.** Пусть X — мультипликативный бинар. Тогда элемент $z\in X$ называется *поглощающим элементом* (англ. *absorbing element*), *нулевым элементом* или просто *нулём*, если $xz=z=zx$ для любого $x\in X$.

Теорема 1 (Единственность нуля)**.** *Пусть X — мультипликативный бинар, а $z,z'\in X$ — два нулевых элемента. Тогда $z=z'$.*

Доказательство. Из определения 2 следует, что $z=zz'=z'$. □

Обозначение 1. Нулевой элемент в мультипликативном бинаре часто обозначается символом 0.

Определение 3 (Полугруппа)**.** Мультипликативный бинар X называется мультипликативной *полугруппой*, если для любых $x, y, z \in X$ выполняется равенство $x(yz) = (xy)z$.

Определение категории

Соглашение 1 (Gross)**.** «Groß-полугруппа» — это „полугруппа“, совокупность элементов которой не подразумевается малой, то есть не подразумевается множеством. Записи «groß-отображение», «groß-категория» и «groß-множество» имеют аналогичный смысл.

Замечание 1. Соглашение 1 основано на терминологии из лекций Д. Терешкина по теории категорий в НМУ [19, 23:10].

Определение 4 (Ein)**.** Пусть $\mathcal{C}$ — мультипликативная groß-полугруппа с нулём. Тогда определим groß-множество

$$\mathrm{Ein}(\mathcal{C}) \coloneqq \{e \in \mathcal{C} \setminus \{0\} \mid ex, xe \in \{0, x\} \text{ для любого } x \in \mathcal{C}\}.$$

Замечание 2. Обозначение «Ein» в определении 4 происходит от немецкого слова «einheit». Оно не является общепринятым, но я не знаю общепринятого обозначения.

Определение 5 (Gross-категория)**.** Мультипликативная groß-полугруппа с нулём $\mathcal{C}$ называется *groß-категорией*, если для всех $x, y, z \in \mathcal{C}$ из того, что $xy, yz \neq 0$ следует, что $xyz \neq 0$, и для любого $x \in \mathcal{C} \setminus \{0\}$ существуют $e', e'' \in \mathrm{Ein}(\mathcal{C})$, такие что $e'x, xe'' \neq 0$.

Области и кообласти

Теорема 2 (Единственность (ко)области)**.** *Пусть $\mathcal{C}$ — мультипликативная groß-полугруппа с нулем, $x \in \mathcal{C} \setminus \{0\}$, $e, e' \in \mathrm{Ein}(\mathcal{C})$ и $ex, e'x \neq 0$. Тогда $e = e'$.*

Доказательство. Понятно, что раз $ex, e'x \neq 0$, то $ex = e'x = x$. Тогда $e'ex = e'x = x \neq 0$. Отсюда следует, что $e'e \neq 0$, а из этого, в свою очередь, следует, что $e = e'e = e'$. □

Определение 6 (Отображение (ко)области)**.** Пусть $\mathcal{C}$ — groß-категория. Определим groß-отображения $s, t : \mathcal{C} \setminus \{0\} \rightrightarrows \mathrm{Ein}(\mathcal{C})$ следующими свойствами: $xs(x), t(x)x \neq 0$ для любого $x \in \mathcal{C} \setminus \{0\}$.

Замечание 3. Корректность определения 6 следует из теоремы 2, применённой к $\mathcal{C}$ и $\mathcal{C}^o$, и определения 5.

Замечание 4. Буквы «s» и «t», которыми обозначаются groß-отображения области и кообласти в определении 6, — это первые буквы английских слов «source» и «target».

Теорема 3 ((Ко)области и композиция)**.** *Пусть $\mathcal{C}$ — groß-категория, а $x, y \in \mathcal{C} \setminus \{0\}$. Тогда условие $xy \neq 0$ эквивалентно условию $t(y) = s(x)$, причём если $xy \neq 0$, то $s(xy) = s(y)$ и $t(xy) = t(x)$.*

Доказательство. Если $xy \neq 0$, то $xy = xs(x)y \neq 0$, поэтому $s(x)y \neq 0$, то есть $s(x) = t(y)$. Если $e = s(x) = t(y)$, то $x = xe \neq 0$ и $y = ey \neq 0$, откуда, по определению 5, следует, что $xey \neq 0$, а $xey = xy$. Равенства $s(xy) = s(y)$ и $t(xy) = t(x)$ при $xy \neq 0$ совсем очевидны. □

Наблюдение 1. Пусть $\mathcal{C}$ — groß-категория, а $e \in \mathrm{Ein}(\mathcal{C})$. Тогда выполняются равенства $e = es(e) = s(e)$ и $e = t(e)e = t(e)$.

Общие замечания

Доказанного в этом разделе достаточно, чтобы заметить эквивалентность определения 5 и стандартного определения категории через совокупность объектов и совокупность морфизмов. Вне этого раздела, как правило, будет использоваться стандартное определение категории. Причём, несмотря на то, что определение 5 является, по сути, определением «метакатегории», которая не обязана быть локально малой, обычно в этом тексте будет подразумеваться, что совокупность морфизмов между любыми двумя объектами категории образует множество.

3.3. Разложения Брюа и Гаусса

Стандартные подгруппы в общей линейной группе

Определение 1 (Группа диагональных матриц)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное множество. Тогда *группой*

диагональных матриц порядка I с коэффициентами в R называется группа $\mathrm{T}_I(R) \coloneqq \mathrm{D}_I(R)^\times = \mathrm{D}_I(R) \cap \mathrm{M}_I(R)^\times \subset \mathrm{GL}_I(R)$.

Определение 2 (Группа матриц перестановок)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное множество. Тогда *группой матриц перестановок* порядка I с коэффициентами в R называется группа $\mathrm{W}_I(R) \coloneqq \mathrm{Im}(\sigma \mapsto \sum_{i\in I} e_{\sigma(i),i} : \mathrm{Sym}(I) \to \mathrm{M}_I(R)) \subset \mathrm{GL}_I(R)$.

Определение 3 (Группа мономиальных матриц)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное множество. Тогда *группой мономиальных матриц* порядка I с коэффициентами в R называется группа $\mathrm{N}_I(R) \coloneqq \mathrm{W}_I(R) \ltimes \mathrm{T}_I(R) \subset \mathrm{GL}_I(R)$.

Определение 4 (Кольцо верхних/нижних треугольных матриц)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное линейно упорядоченное множество. Тогда *кольцом верхних треугольных матриц* подрядка I над R называется кольцо $\widehat{\mathrm{B}}_I(R) \coloneqq \{(x_{i,j})_{i,j\in I} \in \mathrm{M}_I(R) \mid x_{i,j} = 0 \text{ при } i > j\} \subset \mathrm{M}_I(R)$, а *кольцом нижних треугольных матриц* подрядка I над R — кольцо $\widehat{\mathrm{B}}_I^-(R) \coloneqq \widehat{\mathrm{B}}_{I^o}(R) \subset \mathrm{M}_I(R)$.

Определение 5 (Группа верхних/нижних треугольных матриц)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное линейно упорядоченное множество. Тогда *группой верхних треугольных матриц* порядка I над R называется группа $\mathrm{B}_I(R) \coloneqq \widehat{\mathrm{B}}_I(R)^\times$, то есть группа обратимых элементов кольца $\widehat{\mathrm{B}}_I(R)$, а *группой нижних треугольных матриц* порядка I над R — группа $\mathrm{B}_I^-(R) \coloneqq \widehat{\mathrm{B}}_I^-(R)^\times$.

Наблюдение 1. Пусть A — ассоциативное коммутативное унитальное кольцо, I — конечное линейно упорядоченное множество, а $x = (x_{i,j})_{i,j\in I} \in \widehat{\mathrm{B}}_I(A) \cap \mathrm{M}_I(A)^\times$ — обратимая верхнетреугольная матрица. Тогда $\det(x) = \prod_{i\in I} x_{i,i} \in A^\times$, а потому $x_{i,i} \in A^\times$ для любого $i \in I$, откуда выводится, что $x^{-1} \in \widehat{\mathrm{B}}_I(A)$. Иначе говоря, $\widehat{\mathrm{B}}_I(A) \cap \mathrm{M}_I(A)^\times = \mathrm{B}_I(A)$.

Пример 1. Пусть I — бесконечное множество. Очевидно, что существует перестановка множества $I \sqcup I$, такая что соответствующая матрица $x \in \mathrm{GL}_2(\mathrm{End}_{\mathbb{Z}\text{-mod}}(\mathbb{Z}^{\oplus I}))$ верхнетреугольна и не диагональна. Тогда матрица x^{-1} нижнетреугольна и не диагональна.

Замечание 1. Я узнал о примере 1 из статьи [4].

Определение 6 (Группа верхних/нижних унитреугольных матриц)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное линейно упорядоченное множество. Тогда *группой верхних унитреугольных матриц* порядка I над R называется группа $\mathrm{U}_I(R) \coloneqq \{((x_{i,j})_{i,j\in I} \in \mathrm{B}_I(R) \mid x_{i,i} = 1 \text{ для всех } i \in I)\}$, а *группой нижних унитреугольных матриц* порядка I над R — группа $\mathrm{U}_I^-(R) \coloneqq \mathrm{U}_{I^o}(R) \subset \mathrm{B}_I^-(R)$.

Наблюдение 2 (Разложение Леви)**.** Пусть R — ассоциативное унитальное кольцо, а I — конечное линейно упорядоченное множество. Тогда $\mathrm{B}_I(R) = \mathrm{T}_I(R) \ltimes \mathrm{U}_I(R)$.

Разложение Брюа

Теорема 1 (Разложение Брюа)**.** *Пусть K — поле, $n \in \mathbb{N}_1$ — натуральное число, $G \coloneqq \mathrm{GL}_n(K)$, $U \coloneqq \mathrm{U}_n(K)$, $N \coloneqq \mathrm{N}_n(K)$. Тогда выполняется равенство $G = UNU$.*

Набросок доказательства. Пусть $x = (x_{i,j})_{i,j=1}^n \in \mathrm{GL}_n(K)$ — невырожденная матрица. Пусть h — это наибольший индекс, такой что $x_{h,1} \neq 0$. Тогда, очевидно, существуют матрицы $u_1, u_2 \in U$, такие что у матрицы $x' = u_1 x u_2$ только один ненулевой элемент в h-ой строке и первом столбце. Осталось по индукции применить разложение Брюа к матрице, полученной из x' вычёркиванием h-ой строки и первого столбца. □

Разложение Гаусса

Теорема 2 (Разложение Гаусса)**.** *Пусть K — поле, $n \in \mathbb{N}_1$ — натуральное число, $G \coloneqq \mathrm{GL}_n(K)$, $U \coloneqq \mathrm{U}_n(K)$, $U^- \coloneqq \mathrm{U}_n^-(K)$, $N \coloneqq \mathrm{N}_n(K)$. Тогда выполняется равенство $G = NU^-U$.*

Набросок доказательства. Пусть $x \in \mathrm{GL}_n(K)$ — невырожденная матрица. Пусть y — матрица, полученная вычёркиванием из x последнего столбца. Тогда какая-то из строчек матрицы y, скажем, i-ая, содержится в линейной оболочке остальных строчек. Вычеркнув i-ую строчку из y мы получим невырожденную квадратную матрицу x', к которой можно применить то же рассуждение, что и к x. Если задуматься, то мы доказали, что существуют матрицы $w \in W \coloneqq \mathrm{W}_n(K)$ и $u^- \in U^-$, такие

что $u^- wx \in B := \mathrm{B}_n(K)$. Иначе говоря, $G = WU^-B$. Осталось, воспользовавшись наблюдением 2, перенести диагональную компоненту B налево: $WU^-B = WU^-TU = WTU^-U = NU^-U$, где $T := \mathrm{T}_n(K)$. □

3.4. Задача Кеплера

Соглашение 1. В этом разделе когда идёт речь о «траекториях» и «орбитах», то имеются в виду траектории и орбиты точки единичной массы, если противное не указано явно.

Теорема 1. *Для любого $\lambda \in \mathbb{C}$ отображение $z \mapsto z^2 : \mathbb{C} \to \mathbb{C}$ переводит эллипсы и ветви гипербол с фокусами $\pm\lambda$ в эллипсы и ветви гипербол соответственно с фокусами 0 и λ^2.*

Доказательство (из трёх частей).

Часть 1. Заметим, что отображение $z \mapsto z + z^{-1} : \mathbb{C} \setminus \{0\} \to \mathbb{C}$, называемое *отображением Жуковского*, переводит окружности с центром в 0 в эллипсы с фокусами ± 2, а лучи, выходящие из 0, в ветви гипербол с фокусами ± 2, в чём легко убедиться, воспользовавшись тригонометрической формой записи комплексных чисел: если $z = r\cos(\omega) + r\sin(\omega)i$, где $\omega \in \mathbb{R}$, $r \in \mathbb{R}_{>0}$, то $z + z^{-1} = (r + r^{-1})\cos(\omega) + (r - r^{-1})\sin(\omega)i$.

Часть 2. Отображение $z \mapsto z^2 : \mathbb{C} \to \mathbb{C}$ переводит эллипсы и ветви гипербол с фокусами ± 2 в эллипсы и ветви гипербол соответственно с фокусами 0 и 4, в чём легко убедиться с помощью первой части доказательства и формулы квадрата суммы: $(z + z^{-1})^2 = (z^2 + z^{-2}) + 2$.

Часть 3. Чтобы завершить доказательство осталось воспользоваться тем, что если $C \subset \mathbb{C}$ и $\alpha \in \mathbb{C}$, то $(\alpha \cdot C)^{:2} = \alpha^2 \cdot C^{:2}$. □

Замечание 1. В контексте теоремы 1 стоит отметить, что для любого непустого $C \subset \mathbb{C}$ выполняется соотношение $\inf_{w \in C^{:2}} |w| = (\inf_{z \in C} |z|)^2$.

Наблюдение 1. Пусть $C \subset \mathbb{C}$ — орбита точки единичной массы в центральном поле с потенциалом $U(r) = \pm r^2/2$, энергией E и кинетическим моментом M. Тогда полуоси коники $C^{:2} \subset \mathbb{C}$ равны $|E|$ и $|M|$.

Наблюдение 2 (Скорость в центральном поле)**.** При движении точки в центральном поле с потенциалом $U(r)$ её скорость, согласно закону сохранения энергии, равна $\sqrt{2(E-U(r))}$, где E — константа, а тангенциальная компонента скорости, согласно закону сохранения кинетического момента, равна M/r, где M — константа.

Наблюдение 3. Для любого $\alpha \in \mathbb{R}\setminus\{0\}$ траектория в центральном поле с потенциалом $U(r)$, энергией E и кинетическим моментом M является также траекторией в центральном поле с потенциалом $\alpha^2 U(r)$, энергией $\alpha^2 E$ и кинетическим моментом αM.

Теорема 2. *Пусть $a, b, c \in \mathbb{Q}^\times$ — числа, такие что $c = a/2 = 2/b$. Тогда многозначная функция $(-)^c$ на $\mathbb{C}^\times$ переводит траектории в центральном поле с потенциалом $U(r) = kr^{a-2}$, энергией E и кинетическим моментом $\pm M$ в траектории в центральном поле с потенциалом $U(r) = -Er^{b-2}$, энергией $-k$ и кинетическим моментом $\pm M$.*

Доказательство. Заметим, что многозначная функция $(-)^c$ на $\mathbb{C}^\times$ переводит в себя множество лучей, исходящих из нуля, и конформна, то есть сохраняет углы, а синус угла наклона вектора скорости к радиус-вектору при движении в центральном поле, согласно наблюдению 2, задаётся формулой $(M/r)/\sqrt{2(E-U(r))}$. Осталось проверить равенство $(M/r)/\sqrt{2(E-kr^{a-2})} = (M/r^c)/\sqrt{2(-k+E(r^c)^{b-2})}$. □

Замечание 2. Числа $a = 4$, $b = 1$ и $c = 2$ подходят условиям теоремы 2.

Наблюдение 4. Для эллиптической или гиперболической орбиты точки единичной массы в центральном поле с потенциалом $U(r) = \pm r^{-1}$ согласно теореме 2 и наблюдениям 1 и 3 выполняются следующие соотношения: $2a = |E|^{-1}$ и $p = M^2$, где E — энергия, M — кинетический момент, a — большая полуось, а p — фокальный параметр.

Теорема 3. *Пусть точка единичной массы движется в центральном поле с потенциалом $U(r) = -r^{-1}$ по эллиптической орбите с большой полуосью a. Тогда период её обращения равен $2\pi a^{3/2}$.*

Доказательство. Пусть b — малая полуось эллиптической орбиты, M — кинетический момент точки, а T — период обращения. Тогда, согласно второму закону Кеплера, то есть закону сохранения кинетического

момента, $T = \pi ab/(|M|/2)$. С другой стороны, $|M| = a^{-1/2}b$ согласно наблюдению 4. Поэтому $T = \pi ab/(a^{-1/2}b/2) = 2\pi a^{3/2}$. □

Замечание 3. Почти весь материал этого раздела взят из книг В. И. Арнольда [3, с. 42], [8, с. 29] и [2, с. 75].

3.5. Алгоритм RSA

Теорема 1. *Пусть $n \in \mathbb{N}_1$ — бесквадратное число, $\lambda(n)$ — экспонента группы $(\mathbb{Z}/n\mathbb{Z})^\times$, а $s \in \mathbb{N}_0$ — число, такое что $s \equiv 1 \pmod{\lambda(n)}$. Тогда $x^s = x$ для любого $x \in \mathbb{Z}/n\mathbb{Z}$.*

Доказательство. Практически очевидно из канонического изоморфизма $\mathbb{Z}/n\mathbb{Z} \cong \prod_{p\in\mathcal{P}} \mathbb{Z}/p\mathbb{Z}$, где $\mathcal{P}$ — множество простых делителей n. □

Замечание 1. Если, в обозначениях теоремы 1, выбрать числа $e, d \in \mathbb{N}_0$, взаимно обратные по модулю $\lambda(n)$, то соответствующие отображения $x \mapsto x^e : \mathbb{Z}/n\mathbb{Z} \rightleftarrows \mathbb{Z}/n\mathbb{Z} : x^d \hookleftarrow x$ будут взаимно обратными биекциями, причём по n и e в общем случае довольно трудно вычислить класс $[d] \in \mathbb{Z}/\lambda(n)\mathbb{Z}$. Это обстоятельство лежит в основе *алгоритма RSA*: первое отображение зашифровывает сообщения, а второе их расшифровывает.

Часть II

Сгруппированные тексты

Глава 4

Теория множеств

4.1. Диагональный аргумент Кантора

Обозначение 1 (Множество подмножеств)**.** Множество подмножеств множества X, иногда называемое *булеаном* X, будем обозначать символом 2^X — так же, как множество отображений из X в $2 = \{0, 1\}$.

Теорема 1 (Теорема Кантора)**.** *Если X — множество, а $\varphi : X \to 2^X$ — отображение, то φ не сюръективно.*

Доказательство. Пусть $C \coloneqq \{x \in X \mid x \notin \varphi(x)\}$. Тогда если $c \in X$ и $\varphi(c) = C$, то утверждение «$c \in C$» эквивалентно утверждению «$c \notin C$» — противоречие. □

Замечание 1. В обозначениях формулировки и доказательства теоремы 1 характеристическая функция $X \to \{0, 1\}$ подмножества $X \setminus C \subset X$ разлагается в композицию диагонального отображения $X \to X \times X$ и отображения $X \times X \to \{0, 1\}$, соответствующего $\varphi : X \to 2^X$, поэтому рассуждение из приведённого доказательства теоремы 1 часто называют *диагональным аргументом Кантора.*

Наблюдение 1 (Парадокс Рассела)**.** Предположим, что существует множество всех множеств, которое мы обозначим буквой X. Тогда отображение $x \mapsto x \cap X : X \to 2^X$ сюръективно, так как обратно слева вложению $x \mapsto x : 2^X \to X$, что противоречит теореме Кантора.

Наблюдение 2 (Несчётность множества вещественных чисел)**.** По теореме Кантора множество вещественных чисел из интервала $[0, 1]$, у которых существует троичное разложение, в котором не участвует цифра 1, биективное $2^{\mathbb{N}_1}$ и называемое *множеством Кантора*, несчётно. Как следствие, множество вещественных чисел несчётно.

4.2. Теорема Кантора – Бернштейна – Шрёдера

Теорема 1 (Теорема Кантора – Бернштейна – Шрёдера)**.** *Пусть* $\iota : X \to X$ *— вложение множества* X *в себя, а* $Y \subset X$ *— подмножество* X*, такое что* $\iota(X) \subset Y$*. Тогда существует биекция* $\rho : X \xrightarrow{\sim} Y$*.*

Доказательство. Для любого $i \in \mathbb{N}_1$ множества $X \setminus Y$ и $\iota^i(X \setminus Y) \subset Y$ дизъюнктны, а потому, по инъективности ι, для любых $i, j \in \mathbb{N}_0$, таких что $i < j$, множества $\iota^i(X \setminus Y)$ и $\iota^j(X \setminus Y)$ тоже дизъюнктны. Пусть $Z \coloneqq \bigsqcup_{i=0}^{\infty} \iota^i(X \setminus Y) \subset X$. Ясно, что $X = Z \sqcup (X \setminus Z)$ и $Y = \iota(Z) \sqcup (X \setminus Z)$. Определим биекцию $(\rho : X \xrightarrow{\sim} Y) \coloneqq (x \mapsto \iota(x) : Z \xrightarrow{\sim} \iota(Z)) \sqcup (\mathrm{Id}_{X \setminus Z})$. □

Замечание 1. Теорему 1 можно переформулировать следующим образом: «Если два множества вкладываются друг в друга, то они равномощны».

4.3. Лемма Цорна

Определение 1 (Замкнутое влево подмножество)**.** Подмножество Y частично упорядоченного множества X называется *замкнутым влево*, если $\bigcup_{y \in Y} X_{\leqslant y} \subset Y$. Множество замкнутых влево подмножеств частично упорядоченного множества X будет обозначаться через $[1]^X$.

Определение 2 (Последующие элементы)**.** Пусть X — частично упорядоченное множество, а $x \in X$ — его элемент. Тогда минимальные элементы $X_{>x}$ будут называться последующими к x элементами.

Определение 3 (Фундированность)**.** Частично упорядоченное множество X называется *фундированным*, если в множестве $[1]^X$ у любого не максимального элемента есть последующий.

Определение 4 (Ординал)**.** Фундированное линейно упорядоченное множество называется *ординалом.*

Определение 5 (Подординал)**.** Ординал B называется *подординалом* ординала A, что записывается $B \preccurlyeq A$, если B является замкнутым влево подмножеством A с индуцированным порядком.

Определение 6 (Отображение последования)**.** Пусть A — ординал. Тогда *отображение последования* $r_A : [1]^A \setminus \{A\} \to [1]^A$ переводит любой не максимальный элемент $[1]^A$ в последующий элемент $[1]^A$.

Лемма 1 (Лемма о сравнении)**.** *Пусть A и B — два ординала, такие что отображения последования r_A и r_B принимают одинаковые значения на пересечении их областей определения. Тогда какой-то из ординалов A и B является подординалом другого.*

Доказательство. Пусть C — это объединение общих подординалов A и B, которое является наибольшим общим подординалом A и B. Если $C \neq A$ и $C \neq B$, то определён ординал $r_A(C) = r_B(C)$, который строго больше C и является подординалом A и B — противоречие. □

Теорема 1 (Лемма Куратовского – Цорна)**.** *Пусть U — частично упорядоченное множество, а M — множество цепей в U, являющихся ординалами, упорядоченное отношением «быть подординалом». Тогда, в предположении аксиомы выбора, в M есть максимальный элемент.*

Доказательство. Предположим, что это не так. Тогда для каждого $A \in M$, существует $A' \in M$, такой что A — максимальный собственный подординал в A'. Воспользовавшись аксиомой выбора, выберем отображение $r_U : M \to M$, сопоставляющее каждому $A \in M$ такой A'. Пусть $L \coloneqq \{A \in M \mid r_A(B) = r_U(B) \text{ для всех } B \prec A\}$. Тогда, воспользовавшись леммой о сравнении, легко увидеть, что $\bigcup_{A \in L} A \in L$. Но $\bigcup_{A \in L} A \prec r_U(\bigcup_{A \in L} A) \in L$ — противоречие. □

Наблюдение 1 (Принцип максимума Хаусдорфа)**.** Теорема 1 допускает следующую эквивалентную переформулировку, которую называют *принципом максимума Хаусдорфа*: «В любом частично упорядоченном множестве существует максимальная по включению цепь».

Замечание 1. Ещё одна стандартная переформулировка теоремы 1 звучит так: «Частично упорядоченное множество, в котором любая цепь имеет верхнюю грань, содержит максимальный элемент».

Пример 1. Частично упорядоченное множество счётных подмножеств несчётного множества удовлетворяет условию наличия верхних граней у счётных цепей, но не содержит максимальных элементов.

Глава 5

Вещественные числа

5.1. Сечения Дедекинда

Пара слов о целых и рациональных числах

Кольцо целых чисел, обозначаемое $\mathbb{Z}$, — это кольцо формальных разностей, то есть кольцо Гротендика, полукольца $\mathbb{N}_0$. Поле рациональных чисел, обозначаемое $\mathbb{Q}$, — это поле частных кольца $\mathbb{Z}$. Структура поля на $\mathbb{Q}$ единственным образом продолжается до структуры линейно упорядоченного поля.

Дедекиндовы пары и леммы об обратимости

Обозначение 1. Пусть X — частично упорядоченное множество, а $y \in X$ — его элемент. Тогда $X_{\leqslant y} \coloneqq \{x \in X \mid x \leqslant y\}$, $X_{\geqslant y} \coloneqq \{x \in X \mid x \geqslant y\}$, $X_{<y} \coloneqq \{x \in X \mid x < y\}$, $X_{>y} \coloneqq \{x \in X \mid x > y\}$.

Определение 1 (Левые и правые сечения Дедекинда)**.** Назовём подмножество Y линейно упорядоченного множества X *левым/правым сечением Дедекинда*, если $Y \neq \varnothing, X$ и для любого $y \in Y$ выполняется строгое включение $X_{\leqslant y} \subsetneq Y$ или, соответственно, $X_{\geqslant y} \subsetneq Y$.

Определение 2 (Дедекиндовы дополнения и пары)**.** Пусть X — это $\mathbb{Q}$ или $\mathbb{Q}_{>0}$. Левое сечение Дедекинда $L \subset X$ и правое сечение Дедекинда $R \subset X$ называются *дедекиндовыми дополнениями* друг друга,

а пара (L, R) — *дедекиндовой парой*, если $L \cap R = \varnothing$, и для любого рационального $\varepsilon > 0$ существуют $l \in L$ и $r \in R$, такие что $r - l \leqslant \varepsilon$.

Наблюдение 1. Пусть X — это $\mathbb{Q}$ или $\mathbb{Q}_{>0}$. Дизъюнктные левое сечение Дедекинда $L \subset X$ и правое сечение Дедекинда $R \subset X$ являются дедекиндовыми дополнениями друг друга тогда и только тогда, когда для любого рационального $\varepsilon > 0$ открытая ε-окрестность множества L имеет непустое пересечение с R, то есть $\{x \in X \mid \exists l \in L : |x-l| < \varepsilon\} \cap R \neq \varnothing$, или, эквивалентно, открытая ε-окрестность множества R имеет непустое пересечение с L, то есть $L \cap \{x \in X \mid \exists r \in R : |x - r| < \varepsilon\} \neq \varnothing$. Эти условия эквивалентны тому, что L — максимальное по включению левое сечение Дедекинда, дизъюнктное с R, а R — максимальное по включению правое сечение Дедекинда, дизъюнктное с L. Отсюда следует, что у любого левого/правого сечения Дедекинда в X существует единственное дедекиндово дополнение.

Определение 3 («Поэлементное» сложение, умножение и обращение подмножеств)**.** Для подмножеств $M, M', M'' \subset \mathbb{Q}$, в частности, левых или правых сечений Дедекинда, определим множества $-M := \{-x \in \mathbb{Q} \mid x \in M\}$, $M' + M'' := \{x' + x'' \in \mathbb{Q} \mid x' \in M',\ x'' \in M''\}$ и $M' \cdot M'' := \{x' \cdot x'' \in \mathbb{Q} \mid x' \in M',\ x'' \in M''\}$. Если $M \subset \mathbb{Q}^\times$, то определим множество $M^{:(-1)} := \{x^{-1} \in \mathbb{Q} \mid x \in M\}$.

Определение 4 (Сложение дедекиндовых пар в $\mathbb{Q}$)**.** Пусть (L', R') и (L'', R'') — дедекиндовы пары в $\mathbb{Q}$. Определим их сумму как дедекиндову пару $(L' + L'', R' + R'')$.

Наблюдение 2. Дедекиндовы пары в $\mathbb{Q}$ образуют абелеву группу относительно сложения. Нулём в этой группе является пара $(\mathbb{Q}_{<0}, \mathbb{Q}_{>0})$, а аддитивно обратной к паре (L, R) является пара $(-R, -L)$.

Лемма 1. *Пусть (L, R) — дедекиндова пара в $\mathbb{Q}_{>0}$. Тогда $(R^{:(-1)}, L^{:(-1)})$ — это дедекиндова пара в $\mathbb{Q}_{>0}$.*

Набросок доказательства. Заметим, что существует $C \in \mathbb{Q}_{>0}$, такое что если $l \in L$ и $r \in R$ достаточно близки, то $C \leqslant l \leqslant r$, после чего воспользуемся тождеством $1/l - 1/r = (r - l)/(lr)$. □

Лемма 2. *Пусть (L', R') и (L'', R'') — дедекиндовы пары в $\mathbb{Q}_{>0}$. Тогда $(L' \cdot L'', R' \cdot R'')$ — это дедекиндова пара в $\mathbb{Q}_{>0}$.*

Набросок доказательства. Заметим, что существует $C' \in \mathbb{Q}_{>0}$, такое что если $l' \in L'$ и $r' \in R'$ достаточно близки, то $l' \leqslant r' \leqslant C'$, и аналогично для пары (L'', R''), после чего воспользуемся тождеством $r'r'' - l'l'' = r'(r'' - l'') + (r' - l')l''$. □

Определение 5 (Умножение дедекиндовых пар в $\mathbb{Q}_{>0}$)**.** Пусть (L', R') и (L'', R'') — дедекиндовы пары в $\mathbb{Q}_{>0}$. Определим их произведение как дедекиндову пару $(L' \cdot L'', R' \cdot R'')$.

Наблюдение 3. Дедекиндовы пары в $\mathbb{Q}_{>0}$ образуют коммутативную группу относительно умножения. Единицей в этой группе является пара $(\{x \in \mathbb{Q}_{>0} \mid x < 1\}, \{x \in \mathbb{Q}_{>0} \mid 1 < x\})$, а мультипликативно обратной к паре (L, R) является пара $(R^{:(-1)}, L^{:(-1)})$.

Конструкция поля дедекиндовых сечений

Определение 6 (Сечение Дедекинда)**.** Правые сечения Дедекинда в $\mathbb{Q}$ будем называть просто *сечениями Дедекинда*.

Определение 7 (Отношение порядка на сечениях Дедекинда)**.** Стандартным порядком на множестве сечений Дедекинда будем считать порядок, противоположный порядку, заданному вложенностью сечений друг в друга как множеств.

Наблюдение 4. Порядок на множестве сечений Дедекинда линейный и ограниченно полный: инфимумам соответствуют объединения.

Определение 8 (Сложение сечений Дедекинда)**.** Суммой сечений Дедекинда R' и R'' назовём сечение Дедекинда $R' + R''$.

Наблюдение 5. Сечения Дедекинда образуют упорядоченную аддитивную абелеву группу. Аддитивная обратимость любого сечения Дедекинда следует из наблюдения 2.

Определение 9 (Умножение неотрицательных сечений Дедекинда)**.** Пусть R' и R'' — неотрицательные, то есть такие, что $R' \geqslant 0$ и $R'' \geqslant 0$, сечения Дедекинда. Определим их произведение как неотрицательное сечение Дедекинда $R' \cdot R''$.

Наблюдение 6. Множество неотрицательных сечений Дедекинда образует полукольцо с нулём. Если мы отождествим множество всех сечений Дедекинда с кольцом Гротендика, то есть кольцом формальных разностей, этого полукольца, то увидим, что операция умножения неотрицательных сечений Дедекинда однозначно двусторонне дистрибутивно продолжается на множество всех сечений Дедекинда, превращая его в упорядоченное кольцо.

Наблюдение 7. По наблюдению 3 строго положительные, то есть строго большие нуля, сечения Дедекинда мультипликативно обратимы, откуда следует, что кольцо сечений Дедекинда является полем. Часто оно отождествляется с полем *вещественных чисел*, также называемых *действительными числами*, и обозначается символом $\mathbb{R}$.

Единственность полного по Дедекинду линейно упорядоченного поля

Наблюдение 8. Любое линейно упорядоченное поле имеет характеристику ноль.

Определение 10 (Архимедово поле)**.** Линейно упорядоченное поле $\mathcal{R}$ называется *архимедовым*, если множество $\mathbb{Z} \subset \mathcal{R}$ не ограничено в $\mathcal{R}$.

Наблюдение 9. Пусть $\mathcal{R}$ — архимедово линейно упорядоченное поле. Тогда для любого $a \in \mathcal{R}^\times$ множество $a\mathbb{Z} \subset \mathcal{R}$ не ограничено.

Теорема 1. *Пусть $\mathcal{R}$ — архимедово линейно упорядоченное поле. Тогда для любых $a, b \in \mathcal{R}$, таких что $a < b$, существует рациональное число $r \in \mathbb{Q}$, такое что $a < r < b$.*

Доказательство. По наблюдению 9 существует число $m \in \mathbb{N}_1$, такое что $m(b-a) > 1$. Пусть $n \in \mathbb{Z}$ — минимальный элемент $\mathbb{Z}$, такой что $ma < n$. Тогда $ma < n < mb$ и $a < n/m < b$. □

Определение 11 (Полнота по Дедекинду)**.** Линейно упорядоченное поле называется *полным по Дедекинду*, если оно является ограниченно полным как частично упорядоченное множество, то есть содержит супремумы ограниченных сверху подмножеств или, эквивалентно, содержит инфимумы ограниченных снизу подмножеств.

Теорема 2. *Пусть $\mathcal{R}$ — полное по Дедекинду линейно упорядоченное поле. Тогда $\mathcal{R}$ архимедово.*

Доказательство. Пусть $s \in \mathcal{R}$ — супремум $\mathbb{Z} \subset \mathcal{R}$. Так как $s - 1 < s$, то существует число $n \in \mathbb{Z}$, такое что $s - 1 < n$, откуда следует, что $s < n + 1$ — противоречие. □

Теорема 3. *Пусть $\mathcal{R}$ — произвольное полное по Дедекинду линейно упорядоченное поле, а $\mathcal{D}$ — поле сечений Дедекинда. Тогда существует единственный изоморфизм $\mathcal{R} \xrightarrow{\sim} \mathcal{D}$ линейно упорядоченных полей.*

Набросок доказательства. Во-первых, воспользовавшись теоремами 1 и 2, легко убедиться, что $\mathbb{Q} \cap \mathcal{R}_{>a} \in \mathcal{D}$ для любого $a \in \mathcal{R}$, а отображение $a \mapsto \mathbb{Q} \cap \mathcal{R}_{>a} : \mathcal{R} \to \mathcal{D}$ биективно и является сохраняющим порядок кольцевым гомоморфизмом. Во-вторых, у поля $\mathcal{R}$ нет сохраняющих порядок нетривиальных автоморфизмов, так как их нет у $\mathbb{Q}$. □

Замечание 1. Отметим, что любой автоморфизм поля $\mathbb{R}$ сохраняет порядок, так как переводит квадраты в квадраты.

5.2. Компактность и связность отрезка

Определение 1 (Интервал)**.** Назовём подмножество $I \subset X$ частично упорядоченного множества X *интервалом*, если для любых $x, y \in I$ и $z \in X$, таких что $x \leqslant z \leqslant y$, выполняется включение $z \in I$.

Теорема 1 (Компактность и связность отрезка)**.** *Пусть $\mathcal{U} \subset \mathrm{Open}([0,1])$ — множество открытых подмножеств отрезка $[0,1] \subset \mathbb{R}$, такое что $\bigcup_{U \in \mathcal{U}} U$ замкнуто в $[0,1]$ и не пусто. Тогда $[0,1]$ является конечным объединением элементов $\mathcal{U}$.*

Доказательство. Для произвольного подмножества $X \subset [0,1]$ обозначим через $\mathcal{I}_X$ множество открытых в $[0,1]$ интервалов, содержащихся в конечных объединениях элементов $\mathcal{U}$ и содержащих X.

По условию существует непустой $I \in \mathcal{I}_\varnothing$. Пусть $I_{\max}$ — это объединение элементов $\mathcal{I}_I$, $C_{\inf} \coloneqq \inf(I_{\max})$, $C_{\sup} \coloneqq \sup(I_{\max})$. Тогда $C_{\inf}, C_{\sup} \in \mathrm{Cl}(I_{\max}) \subset \mathrm{Cl}(\bigcup_{U \in \mathcal{U}} U) = \bigcup_{U \in \mathcal{U}} U$, поэтому существуют $I_{\inf} \in \mathcal{I}_{\{C_{\inf}\}}$ и $I_{\sup} \in \mathcal{I}_{\{C_{\sup}\}}$. Так как $I_{\inf} \cap I_{\max} \neq \varnothing$ и $I_{\sup} \cap I_{\max} \neq \varnothing$, то существуют

$I_{\text{left}}, I_{\text{right}} \in \mathcal{I}_I$, такие что $I_{\text{inf}} \cap I_{\text{left}} \neq \varnothing$ и $I_{\text{sup}} \cap I_{\text{right}} \neq \varnothing$. Тогда $I_{\text{big}} := I_{\text{inf}} \cup I_{\text{left}} \cup I_{\text{right}} \cup I_{\text{sup}} \in \mathcal{I}_I$. Если $C_{\text{inf}} \neq 0$ или $C_{\text{sup}} \neq 1$, то $I_{\text{big}} \not\subset I_{\max}$, что противоречит определению $I_{\max}$. Поэтому $I_{\text{big}} = I_{\max} = [0, 1]$. □

Замечание 1. Очевидно, что теорема 1 допускает следующую эквивалентную переформулировку: единичный вещественный отрезок компактен и связен.

Глава 6

Базовые свойства метрических пространств

6.1. Лемма Лебега о покрытии

Теорема 1 (Лемма Лебега о покрытии)**.** *Если M — компактное метрическое пространство, а $\mathcal{U} \subset \mathrm{Open}(M)$ — его открытое покрытие, то существует число $R \in \mathbb{R}_{>0}$ такое что любой открытый шар в M радиуса меньше R содержится в каком-то элементе $\mathcal{U}$.*

Доказательство. Рассмотрим функцию $f : M \to \mathbb{R}$, сопоставляющую точке $x \in M$ супремум радиусов открытых шаров с центром в x, содержащихся в каком-то элементе $\mathcal{U}$. Так как функция f непрерывна, а пространство M компактно, то в какой-то точке M функция f принимает своё наименьшее значение, которое не может быть нулевым. □

Теорема 2 (Теорема Кантора – Гейне)**.** *Пусть $\varphi : M \to M'$ — непрерывное отображение из компактного метрического пространства M в метрическое пространство M'. Тогда φ равномерно непрерывно.*

Первое доказательство. Рассмотрим покрытие пространства M прообразами всех открытых шаров в M' и применим к нему лемму Лебега о покрытии (теорему 1). □

Второе доказательство. Для любого числа $\varepsilon \in \mathbb{R}_{>0}$ множество $X \coloneqq \{(x, y) \in M \times M \mid \mathrm{d}_{M'}(\varphi(x), \varphi(y)) \geqslant \varepsilon\} = (\mathrm{d}_{M'} \circ (\varphi \times \varphi))^{-1}([\varepsilon, \infty))$ ком-

пактно как замкнутое подмножество компактного пространства $M \times M$, а потому непрерывная функция $\mathrm{d}_M|_X$ принимает на X своё наименьшее значение, которое не может быть нулевым. □

6.2. Полные метрические пространства

Наблюдение 1. Пусть X — метрическое пространство, $(a_i)_{i\in I}$ и $(b_j)_{j\in J}$ — две сходящиеся последовательности в X. Тогда выполняется равенство $\mathrm{d}(\lim(a_i \mid i \in I), \lim(b_j \mid j \in J)) = \lim(\mathrm{d}(a_i, b_j) \mid (i,j) \in I \times J)$.

Теорема 1 (Характеризации метрической полноты)**.** *Пусть X — метрическое пространство. Тогда следующие условия эквивалентны:*

а) *Любая последовательность Коши в X сходится;*

б) *Для любой пары (Y, Y') из метрического пространства Y и его плотного подмножества $Y' \subset Y$ любое равномерно непрерывное отображение $f' : Y' \to X$ продолжается до непрерывного отображения $f : Y \to X$.*

Доказательство (из двух частей).

Часть (а) $\Rightarrow$ (б). Пусть $y \in Y$. Выберем сходящуюся к y в Y последовательность $s : I \to Y'$. Заметим, что s является последовательностью Коши, а потому $f' \circ s$ — тоже. Определим $f(y)$ как предел $f' \circ s$. Пусть $r : J \to Y'$ — другая сходящаяся к y в Y последовательность. Тогда $s \sqcup r : I \sqcup J \to Y'$ — последовательность Коши, а потому $f' \circ (s \sqcup r)$ — тоже, а потому пределы $f' \circ s$ и $f' \circ r$ равны и отображение f определено корректно. Непрерывность f следует из наблюдения 1.

Часть (б) $\Rightarrow$ (а). Обозначим образ вложения $n \mapsto 2^{-n} : \mathbb{N}_0 \to [0,1]$ через N', а замыкание N' в $[0,1]$ — через N. Тогда последовательности $\mathbb{N}_0 \to X$ естественно биективны отображениям $N' \to X$, а пределы последовательностей задаются непрерывными продолжениями этих отображений на N. Осталось заметить, что последовательность $\mathbb{N}_0 \to X$ является последовательностью Коши тогда и только тогда, когда соответствующее отображение $N' \to X$ равномерно непрерывно. □

Определение 1 (Полное метрическое пространство)**.** Метрическое пространство X называется *метрически полным* или просто *полным*, если оно удовлетворяет эквивалентным условиям теоремы 1.

Определение 2 (Пополнение метрического пространства)**.** *Пополнением* метрического пространства X называется полное метрическое пространство Y, снабжённое изометрическим вложением $X \to Y$ с плотным образом.

Замечание 1. Из теоремы 1 следует, что между любыми двумя пополнениями метрического пространства X существует единственная изометрия, тождественная на X.

Определение 3 (Вложение Куратовского)**.** Пусть X — метрическое пространство, а F — пространство непрерывных функций из X в $\mathbb{R}$ с sup-расстоянием. Тогда *вложением Куратовского* называется изометрическое вложение

$$x \mapsto \mathrm{d}_X(x, -) : X \to \{f \in F \mid \mathrm{d}_F(f, \mathrm{d}_X(y, -)) < \infty \text{ для всех } y \in X\}.$$

Наблюдение 2. Замыкание образа вложения Куратовского метрического пространства является его метрическим пополнением.

6.3. Теорема Банаха о фиксированной точке

Определение 1 (Растяжение и липшицевость)**.** Пусть X и Y — метрические пространства, а $\varphi : X \to Y$ — отображение. Инфимум $\lambda \in \mathbb{R}$, таких что $\mathrm{d}_Y(\varphi(x'), \varphi(x'')) \leqslant \lambda \cdot \mathrm{d}_X(x', x'')$ для всех $x', x'' \in X$, называется *растяжением* или *липшицевой нормой* φ. Если липшицева норма φ не равна $+\infty$, то φ называется *липшицевым*.

Определение 2 (Равномерно сжимающее отображение)**.** Отображение между метрическими пространствами называется *равномерно сжимающим*, если его растяжение строго меньше единицы.

Теорема 1 (Теорема Банаха о фиксированной точке)**.** *Пусть X — полное метрическое пространство, а $\varphi : X \to X$ — равномерно сжимающее отображение. Тогда у φ существует единственная фиксированная точка.*

Доказательство. Единственность очевидна — остальные точки обязаны приближаться к фиксированной. Теперь докажем существование. Обозначим растяжение φ через λ и выберем произвольную точку $x \in X$. Из неравенств $\mathrm{d}(\varphi^{\circ(n+1)}(x), \varphi^{\circ(n+2)}(x)) \leqslant \lambda \cdot \mathrm{d}(\varphi^{\circ n}(x), \varphi^{\circ(n+1)}(x))$, где $n \in \mathbb{N}_0$, следует, что расстояния между членами последовательности $(\varphi^{\circ n}(x))_{n=0}^{\infty}$ не больше расстояний между соответствующими членами последовательности $(c \cdot s_n)_{n=0}^{\infty}$, где $c \coloneqq \mathrm{d}(x, \varphi(x))$, $s_n \coloneqq \sum_{i=1}^{n} \lambda^{i-1}$. Так как последовательность $(s_n)_{n=0}^{\infty}$ сходится, то она является последовательностью Коши, откуда следует, что последовательность $(\varphi^{\circ n}(x))_{n=0}^{\infty}$ является последовательностью Коши, и, как следствие, сходится. Предел и будет фиксированной точкой, так как из непрерывности φ следует, что $\varphi(\lim_{n\to\infty} \varphi^{\circ n}(x)) = \lim_{n\to\infty} \varphi(\varphi^{\circ n}(x)) = \lim_{n\to\infty} \varphi^{\circ n}(x)$. □

Глава 7

Дифференциальное исчисление

7.1. Теорема о среднем значении

Теорема 1 (Теорема Ролля о среднем)**.** *Пусть* $f : [0,1] \to \mathbb{R}$ *— непрерывная функция, дифференцируемая на интервале* $(0,1)$*. Тогда если* $f(0) = f(1)$*, то существует точка* $x \in (0,1)$*, такая что* $f'(x) = 0$*.*

Набросок доказательства. Случай постоянной f тривиален, рассмотрим случай не постоянной f. Так как отрезок $[0,1]$ компактен, то на нём существует точка, в которой f принимает наибольшее значение, и точка, в которой f принимает наименьшее значение. Так как f не постоянна, то по крайней мере одна из этих точек лежит в интервале $(0,1)$. Нетрудно убедиться, что её можно взять в качестве x. □

Теорема 2 (Теорема Коши о среднем)**.** *Пусть* $\gamma : [0,1] \to \mathbb{R}^2$ *— непрерывное отображение, дифференцируемое на интервале* $(0,1)$*, такое что* $\gamma'(t) \neq 0$ *для любого* $t \in (0,1)$*. Тогда существует точка* $x \in (0,1)$*, такая что вектор* $\gamma(1) - \gamma(0)$ *является кратным* $\gamma'(x)$*.*

Доказательство. Применим теорему Ролля о среднем (теорема 1) к композиции отображения γ с ортогональной проекцией $\mathbb{R}^2$ на прямую, ортогональную вектору $\gamma(1) - \gamma(0)$. □

Теорема 3 (Теорема Лагранжа о среднем). *Пусть $f : [0,1] \to \mathbb{R}$ — непрерывная функция, дифференцируемая на интервале $(0,1)$. Тогда существует точка $x \in (0,1)$, такая что $f'(x) = f(1) - f(0)$.*

Доказательство. Применим теорему Коши о среднем (теорема 2) к отображению $t \mapsto (t, f(t)) : [0,1] \to \mathbb{R}^2$. □

Теорема 4 (Многомерная теорема Лагранжа). *Пусть E — евклидово пространство, а $\gamma : [0,1] \to E$ — непрерывное отображение, дифференцируемое на интервале $(0,1)$, такое что $u := \gamma(1) - \gamma(0) \neq 0$. Тогда существует точка $x \in (0,1)$, такая что $|u| = \gamma'(x) \cdot \frac{u}{|u|} \leqslant |\gamma'(x)|$.*

Доказательство. Применим классическую теорему Лагранжа о среднем (теорема 3) к функции $t \mapsto (\gamma(t) - \gamma(0)) \cdot \frac{u}{|u|} : [0,1] \to \mathbb{R}$. □

7.2. Теорема об обратной функции

Теорема 1. *Пусть E — это евклидово пространство, а $\varphi : E \to E$ — дифференцируемое отображение, такое что $\varphi(0) = 0$, отображение $D(\varphi)_0$ биективно, а отображение $x \mapsto D(\varphi)_x : E \to \mathrm{Hom}_{\mathbb{R}\text{-mod}}(E,E)$ непрерывно в нуле. Тогда существует открытая окрестность нуля $U \subset E$, такая что $\varphi(U)$ открыто, а $x \mapsto \varphi(x) : U \to \varphi(U)$ биективно.*

Доказательство. Во-первых, заметим, что для любого $y \in E$ множество $\varphi^{-1}(y)$ совпадает с множеством фиксированных точек отображения $T_{-y} \circ \hat{\varphi} : E \to E$, где $T_{-y} : E \to E$, $x \mapsto x - y$, а $\hat{\varphi} := \varphi + \mathrm{Id}_E$.

Во-вторых, заметим, что без потери общности можно предположить, что $D(\varphi)_0 = -\mathrm{Id}$, то есть $D(\hat{\varphi})_0 = 0$, заменив φ на композицию φ и линейного автоморфизма E.

Теперь зафиксируем два числа $\varepsilon, \rho \in \mathbb{R}_{>0}$, таких что $\varepsilon + \rho = 1$. Так как отображение $x \mapsto D(\hat{\varphi})_x \mapsto \|D(\hat{\varphi})_x\| : E \to \mathrm{Hom}_{\mathbb{R}\text{-mod}}(E,E) \to \mathbb{R}$ непрерывно в нуле и $\|D(\hat{\varphi})_0\| = \|0\| = 0$, то существует $R \in \mathbb{R}_{>0}$, такое что $\|D(\hat{\varphi})_x\| \leqslant \varepsilon$ для любого $x \in \overline{B}_R(0)$.

Согласно многомерной теореме Лагранжа (теорема 7.1.4) растяжение отображения $\hat{\varphi}|_{\overline{B}_R(0)}$ не превосходит ε. В частности, $\hat{\varphi}(\overline{B}_R(0)) \subset \overline{B}_{\varepsilon R}(0)$ и $T_{-y}(\hat{\varphi}(\overline{B}_R(0))) \subset B_R(0)$ для всех $y \in B_{\rho R}(x)$.

Зафиксируем произвольный $y \in B_{\rho R}(x)$ и применим теорему Банаха о фиксированной точке к отображению $x \mapsto T_{-y}(\hat{\varphi}(x)) : \overline{B}_R(0) \to \overline{B}_R(0)$.

Мы получим, что существует единственная точка $x \in \overline{B}_R(0)$ такая что $\varphi(x) = y$, причём $x = T_{-y}(\hat{\varphi}(x)) \in B_R(0)$.

Множество $U \coloneqq B_R(0) \cap \varphi^{-1}(B_{\rho R}(0))$, для которого $\varphi(U) = B_{\rho R}(0)$, удовлетворяет условию теоремы. □

7.3. Равенство смешанных производных

Теорема 1 (Равенство смешанных производных). *Пусть $U = U' \times U'' \subset \mathbb{R}^2$ — открытая окрестность нуля, а $f : U \to \mathbb{R}$ — функция, такая что $f(0) = 0$, смешанная производная $\partial_2\partial_1 f$ существует во всех точках U и непрерывна в нуле. Пусть $g : U \to \mathbb{R}$, $(x_1, x_2) \mapsto f(x_1, x_2) - (f(x_1, 0) + f(0, x_2))$. Тогда $\partial_2\partial_1 f(0) = \lim_{x_1,x_2\to 0}(g(x_1, x_2)/(x_1x_2))$.*

Доказательство. Зафиксируем точку $(x_1, x_2) \in U$. Применив теорему Лагранжа о среднем к функции $\alpha \mapsto g(\alpha x_1, x_2) : [0, 1] \to \mathbb{R}$, получаем, что $g(x_1, x_2) = x_1\partial_1 g(\alpha_1 x_1, x_2)$ для какого-то $\alpha_1 \in (0, 1)$. Применив теорему Лагранжа о среднем к функции $\alpha \mapsto x_1\partial_1 g(\alpha_1 x_1, \alpha x_2) : [0, 1] \to \mathbb{R}$, получаем, что $g(x_1, x_2) = x_1x_2\partial_2\partial_1 g(\alpha_1 x_1, \alpha_2 x_2)$ для какого-то $\alpha_2 \in (0, 1)$. Заметив, что $\partial_2\partial_1 g = \partial_2\partial_1 f$ как функции на U, и устремив x_1 и x_2 к нулю, получаем, что $\partial_2\partial_1 f(0) = \lim_{x_1,x_2\to 0}(g(x_1, x_2)/(x_1x_2))$. □

7.4. Лемма Адамара

Обозначение 1. Пусть $r \geqslant i \geqslant 0$ — целые числа. Символом C_r^i будем обозначать биноминальный коэффициент, равный $r!/(i!(r - i)!)$.

Наблюдение 1. Пусть $r \in \mathbb{N}_1$. В результате разложения выражения $(1 - 1)^r$ по биному Ньютона получается формула $\sum_{i=0}^{r}(-1)^i C_r^i = 0$.

Лемма 1. *Пусть $f : \mathbb{R} \to \mathbb{R}$ — функция класса C^r, где $r \in \mathbb{N}_1$, такая что $f(0) = 0$. Пусть $g : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, $x \mapsto f(x)/x$, а $t \in \mathbb{R} \setminus \{0\}$. Тогда существуют вещественные числа $\alpha_i \in (0, 1)$, где $1 \leqslant i \leqslant r$, такие что $g^{(r-1)}(t) = \frac{1}{r}\sum_{i=1}^{r}(-1)^{i-1}C_r^i f^{(r)}(\alpha_i t)$. Помимо этого, если f класса C^{r+1}, то существуют вещественные числа $\beta_i \in (0, 1)$, где $1 \leqslant i \leqslant r$, такие что $g^{(r-1)}(t) = \frac{1}{r}f^{(r)}(0) + \frac{1}{r(r+1)}\sum_{i=1}^{r}(-1)^{i-1}C_{r+1}^{i+1}f^{(r+1)}(\beta_i t)t$.*

Доказательство. Применяя правило Лейбница, получаем следующее равенство: $g^{(r-1)}(t) = \sum_{i=1}^{r} C_{r-1}^{i-1}(-1)^{i-1}(i-1)!t^{-i}f^{(r-i)}(t)$. По теореме Тейлора для каждого $1 \leqslant i \leqslant r$ существует вещественное число $\alpha_i \in (0,1)$, такое что $f^{(r-i)}(t) = (\sum_{j=0}^{i-1} \frac{1}{j!}f^{(r-i+j)}(0)t^j) + \frac{1}{i!}f^{(r)}(\alpha_i t)t^i$. Подставив это выражение в выражение для $g^{(r-1)}(t)$ и произведя необходимые сокращения, получаем первую формулу.

Вторая формула аналогичным образом получается подстановкой выражения $f^{(r-i)}(t) = (\sum_{j=0}^{i} \frac{1}{j!}f^{(r-i+j)}(0)t^j) + \frac{1}{(i+1)!}f^{(r+1)}(\beta_i t)t^{i+1}$, где $\beta_i \in (0,1)$ для каждого $1 \leqslant i \leqslant r$, в выражение для $g^{(r-1)}(t)$. □

Замечание 1. По первой формуле леммы 1 сразу вычисляется предел $\lim_{t\to 0} g^{(r-1)}(t) = \frac{1}{r}\sum_{i=1}^{r}(-1)^{i-1}C_r^i f^{(r)}(0) = \frac{1}{r}f^{(r)}(0)$, а по второй — предел $\lim_{t\to 0}((g^{(r-1)}(t) - \frac{1}{r}f^{(r)}(0))/t) = \frac{1}{r(r+1)}\sum_{i=1}^{r}(-1)^{i-1}C_{r+1}^{i+1}f^{(r+1)}(0) = \frac{1}{r(r+1)}(C_{r+1}^1 - C_{r+1}^0)f^{(r+1)}(0) = \frac{1}{r+1}f^{(r+1)}(0)$.

Теорема 1 (Лемма Адамара)**.** *Пусть $f : \mathbb{R}^n \to \mathbb{R}$ — функция класса C^r, где $r \in \mathbb{N}_1$, а $l : \mathbb{R}^n \to \mathbb{R}$ — ненулевая линейная функция, такая что $\{x \in \mathbb{R}^n \mid l(x) = 0\} \subset \{x \in \mathbb{R}^n \mid f(x) = 0\}$. Тогда существует единственная функция $g : \mathbb{R}^n \to \mathbb{R}$ класса C^{r-1}, такая что $f = g \cdot l$.*

Набросок доказательства. Мы можем предположить, что в $\mathbb{R}^n$ выбраны координаты, а l — это отображение $(x_i)_{i=1}^n \mapsto x_1 : \mathbb{R}^n \to \mathbb{R}$.

Сначала рассмотрим случай $r = 1$. Пусть $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, причём $x_1 \neq 0$. Тогда $f(x_1, x_2, \ldots, x_n)/x_1 = \partial_1 f(\alpha x_1, x_2, \ldots, x_n)$ для какого-то $\alpha \in (0,1)$. Это показывает, что функция $\mathbb{R}^n \to \mathbb{R}$, которая переводит $x \in \mathbb{R}^n$ в $f(x)/l(x)$ при $l(x) \neq 0$, и в $\partial_1 f(x)$ при $l(x) = 0$, является непрерывной и подходит в качестве g. Единственность g очевидна.

Теперь рассмотрим случай $r \geqslant 2$. Пусть $(k_i)_{i=1}^n$ — семейство элементов $\mathbb{N}_0$, такое что $\sum_{i=1}^n k_i \leqslant r-1$. Нам нужно доказать, что функция $\partial_1^{k_1}\cdots\partial_n^{k_n} g : \mathbb{R}^n \to \mathbb{R}$ существует и непрерывна. Очевидная непосредственная проверка показывает, что функция $\hat{g} \coloneqq \partial_2^{k_2}\cdots\partial_n^{k_n} g : \mathbb{R}^n \to \mathbb{R}$ существует и является в точности единственной непрерывной функцией на $\mathbb{R}^n$, удовлетворяющей равенству $\hat{f} = \hat{g} \cdot l$, где $\hat{f} \coloneqq \partial_2^{k_2}\cdots\partial_n^{k_n} f$.

Доказательство существования и непрерывности функции $\partial_1^{k_1}\hat{g}$ получается последовательным применением двух формул леммы 1 к ограничениям $\hat{f}$ на слои проекции $(x_i)_{i=1}^n \mapsto (x_i)_{i=2}^n : \mathbb{R}^n \to \mathbb{R}^{n-1}$. □

Следствие 1. *Пусть $f : \mathbb{R}^n \to \mathbb{R}$ — функция класса C^r, где $r \in \mathbb{N}_1 \cup \{\infty\}$, такая что $f(0) = 0$. Пусть $l_i : \mathbb{R}^n \to \mathbb{R}$, где $1 \leqslant i \leqslant n$, — стандартные координатные функции. Тогда существуют функции $g_i : \mathbb{R}^n \to \mathbb{R}$ класса C^{r-1}, где $1 \leqslant i \leqslant n$, такие что $f = \sum_{i=1}^n g_i \cdot l_i$.*

Доказательство. Докажем теорему индукцией по n. Введём обозначение $H \coloneqq \{x \in \mathbb{R}^n \mid l_n(x) = 0\}$. По предположению индукции ограничение $f|_H : H \to \mathbb{R}$ представляется в виде $\sum_{i=1}^{n-1} \hat{g}_i \cdot \hat{l}_i$, где $\hat{g}_i$ имеют класс C^{r-1}, а $\hat{l}_i$ — это стандартные координатные функции. Для каждого $1 \leqslant i \leqslant n-1$ возьмём $g_i \coloneqq \hat{g}_i \circ \pi$, где $\pi : \mathbb{R}^n \to H$ — стандартная проекция. По теореме 1 функция $f - (f|_H \circ \pi) = f - \sum_{i=1}^{n-1} g_i \cdot l_i$ представляется в виде $g_n \cdot l_n$, где g_n имеет класс C^{r-1}. □

Замечание 2. Часто леммой Адамара называется следствие 1, а не теорема 1.

7.5. Лемма Морса

Теорема 1. *Пусть $(A, \mathfrak{m}, k)$ — ассоциативное коммутативное унитальное локальное кольцо, такое что $2 \in A^\times$, а M — конечно порождённый A-модуль, снабжённый формой $b : \mathrm{S}^2_A(M) \to A$ такой что индуцированная форма $\overline{b} : \mathrm{S}^2_k(\overline{M}) \to k$, где $\overline{M} \coloneqq M/\mathfrak{m}M$, невырождена. Тогда модуль M свободен, а форма b невырождена и диагонализуема.*

Доказательство. Докажем теорему индукцией по $m \coloneqq \dim_k(\overline{M})$. Если $m = 0$, то $M = 0$ по лемме Накаямы. Теперь рассмотрим случай $m \geqslant 1$. Пусть $\overline{v} \in \overline{M}$ — вектор, такой что $\overline{b}(\overline{v}, \overline{v}) \in k^\times$, а $v \in M$ — его поднятие. Тогда $b(v, v) \in A^\times$, откуда, в частности, следует, что A-гомоморфизм $\alpha \mapsto \alpha v : A \to Av$ биективен, так как его ядро лежит в ядре индуцированной на A формы, которое тривиально. Так как индуцированные формы на Av и $k\overline{v}$ невырождены, то $M = Av \oplus (Av)^\perp$ и $\overline{M} = k\overline{v} \oplus (k\overline{v})^\perp$, причём отображение редукции $M \to \overline{M}$ переводит $(Av)^\perp$ в $(k\overline{v})^\perp$ сюръективно, что позволяет завершить доказательство по индукции. □

Следствие 1. *Если в условиях теоремы 1 кольцо A — это кольцо ростков в точке 0 функций класса C^r, где $r \in \mathbb{N}_0 \cup \{\infty\}$, из $\mathbb{R}^n$ в $\mathbb{R}$, то форма b приводится к диагональному виду с ± 1 на диагонали.*

Доказательство. Это следствие того, что группа $A^\times/(A^\times)^{:2}$ состоит из двух элементов — классов $\pm 1 \in A^\times$. □

Замечание 1. Очевидно, что при условиях следствия 1 «сигнатура» b в понятном смысле определена однозначно и совпадает с сигнатурой $\overline{b}$.

Теорема 2 (Лемма Морса)**.** *Пусть f — росток в точке 0 функции класса C^{r+2}, где $r \in \mathbb{N}_1 \cup \{\infty\}$, из $\mathbb{R}^n$ в $\mathbb{R}$, такой что $f(0) = 0$, $(\partial_i f(0))_{i=1}^n = 0$, а матрица $(\partial_i\partial_j f(0))_{i,j=1}^n$ невырождена. Пусть вещественная квадратичная форма, заданная матрицей $(\partial_i\partial_j f(0))_{i,j=1}^n$, эквивалентна квадратичной форме $\sum_{i=1}^n a_i X_i^2$, где $a_i \in \{\pm 1\}$ для всех $1 \leqslant i \leqslant n$. Тогда существует семейство $(u_i)_{i=1}^n$ ростков в точке 0 функций класса C^r из $\mathbb{R}^n$ в $\mathbb{R}$, таких что $u_i(0) = 0$ для всех $1 \leqslant i \leqslant n$, матрица $(\partial_i u_j(0))_{i,j=1}^n$ невырождена, а $f = \sum_{i=1}^n a_i u_i^2$.*

Доказательство. Применив лемму Адамара к f, получаем разложение $f = \sum_{i=1}^n g_i l_i$, где l_i обозначает росток i-ой координатной функции, а g_i для $1 \leqslant i \leqslant n$ — это ростки функций класса C^{r+1}. Прямое вычисление по правилу Лейбница показывает, что для любого $1 \leqslant i \leqslant n$ выполняется равенство $\partial_i f(0) = g_i(0)$. Применив лемму Адамара к функциям g_i, где $1 \leqslant i \leqslant n$, получаем разложение $f = \sum_{i,j=1}^n h_{i,j} l_i l_j$, где $h_{i,j}$ для $1 \leqslant i, j \leqslant n$ — это ростки функций класса C^r. Заменив $h_{i,j}$ на $(h_{i,j} + h_{j,i})/2$ для каждой пары $1 \leqslant i, j \leqslant n$, можно предположить, что $h_{i,j} = h_{j,i}$ для любых $1 \leqslant i, j \leqslant n$. Прямое вычисление по правилу Лейбница показывает, что для любых $1 \leqslant i, j \leqslant n$ выполняется равенство $\partial_i\partial_j f(0) = 2 \cdot h_{i,j}(0)$, в частности, матрица $(h_{i,j}(0))_{i,j=1}^n$ невырождена.

Пусть A — это кольцо ростков в точке 0 функций класса C^r из $\mathbb{R}^n$ в $\mathbb{R}$. Тогда по следствию 1 существует матрица $(s_{i,j})_{i,j=1}^n \in \mathrm{GL}_n(A)$ такая что $\sum_{i=1}^n a_i(\sum_{j=1}^n s_{i,j}X_j)^2 = \sum_{i,j=1}^n h_{i,j}X_iX_j$. Для каждого $1 \leqslant i \leqslant n$ возьмём $u_i := \sum_{j=1}^n s_{i,j} l_j$. Прямое вычисление по правилу Лейбница показывает, что для любых $1 \leqslant i, j \leqslant n$ выполняется равенство $\partial_i u_j(0) = s_{j,i}(0)$, в частности, матрица $(\partial_i u_j(0))_{i,j=1}^n$ невырождена. □

Глава 8

Группы перестановок

8.1. Группы и их действия

Теорема об орбитах и стабилизаторах

Определение 1 (Транзитивность)**.** Действие группы на множестве называется *транзитивным действием* или *орбитой*, если фактор множества по этому действию одноточечный.

Наблюдение 1 (Разложение на орбиты)**.** Множество, снабжённое действием группы, однозначно представляется в виде дизъюнктного объединения орбит этой группы.

Теорема 1 (Теорема об орбитах и стабилизаторах)**.** *Пусть G — группа, $\mathcal{S}$ — частично упорядоченное множество подгрупп группы G, а $\mathcal{O}$ — категория пунктированных орбит группы G. Тогда стандартные функторы $G/(-) : \mathcal{S} \rightleftarrows \mathcal{O} : \mathrm{Stab}$ — функторы множества правых смежных классов и стабилизатора отмеченной точки — являются квазиобратными эквивалентностями категорий.*

Доказательство. Единственная относительно нетривиальная часть доказательства — это построение естественного изоморфизма $(G/(-)) \circ \mathrm{Stab} \xrightarrow{\sim} \mathrm{Id}$, с необходимостью единственного. Пусть X — G-орбита с отмеченной точкой $x \in X$, а $H \coloneqq \mathrm{Stab}_G(x)$. Для любого $g \in G$ отобразим смежный класс $gH \in G/H$ в точку $gHx = gx \in X$. Корректность определения этого отображения и его G-эквивариантность очевидны. $\square$

Следствие 1. *Пусть G — группа, а $H \subset G$ — её подгруппа. Тогда действие G на G/H левым умножением примитивно тогда и только тогда, когда H — максимальная собственная подгруппа в G.*

Замечание 1. В обозначениях теоремы 1 группа G действует на $\mathcal{O}$ эндофункторами замены точки и действует на $\mathcal{S}$ сопряжением. Функтор Stab является G-эквивариантным относительно этих действий.

Замечание 2. Группа автоморфизмов плоскости, скажем, аффинных или метрических, — это прекрасный пример для иллюстрации базовых понятий теории групп.

Приложения теоремы об орбитах и стабилизаторах

Наблюдение 2 (Разложение группы на двойные смежные классы)**.** Пусть G — группа, а $K, H \subset G$ — её подгруппы. Рассмотрев действие группы $K \times H^o$ на множестве G двусторонним умножением, получаем разложение G на двойные смежные классы KgH, где $g \in G$.

Наблюдение 3 (Формула Фробениуса для индекса)**.** В условиях наблюдения 2 каждый KgH является дизъюнктным объединением $|K : K \cap gHg^{-1}|$ элементов G/H, поскольку KgH — это объединение элементов орбиты точки $gH \in G/H$ под действием K на G/H левым умножением, при этом $\mathrm{Stab}_K(gH) = K \cap \mathrm{Stab}_G(gH) = K \cap gHg^{-1}$.

Следствие 2 (Формула произведения)**.** *В условиях наблюдения 2, если K и H конечны, то $|KH| = |H||K : K \cap H| = |H||K|/|K \cap H|$.*

Теорема 2. *Пусть G — группа, а $H, K \subset G$ — её подгруппы. Тогда выполняется неравенство $|G : H \cap K| \leqslant |G : H||G : K|$.*

Доказательство. Стабилизатор точки $(H, K) \in (G/H) \times (G/K)$ относительно очевидного действия G на $(G/H) \times (G/K)$ левым умножением равен $H \cap K$, при этом $|(G/H) \times (G/K)| = |G : H||G : K|$. □

Теорема 3. *Пусть G — конечная группа, а $H \subset G$ — её подгруппа, такая что простые делители порядка H не меньше индекса H. Тогда H нормальна.*

Доказательство. Подгруппа H нормальна тогда и только тогда, когда все орбиты действия H левым умножением на правых смежных классах G по H одноточечные. Теперь воспользуемся тем, что сумма порядков орбит, одна из которых одноточечная, равна индексу H, а порядок каждой орбиты делит порядок H. □

Теорема 4 (Теоремы Силова)**.**

а) *В конечной группе порядка $p^n m$, где m не делится на простое p, существует подгруппа порядка p^n, называемая силовской p-подгруппой.*

б) *Все подгруппы порядка p^k для какого-то k, называемые p-подгруппами, лежат в силовских p-подгруппах, которые все сопряжены.*

в) *Если n_p — количество силовских p-подгрупп, то $n_p \equiv 1 \pmod p$.*

Доказательство.

а) В нашей группе количество подмножеств мощности p^n не делится на p: $(1+x)^{p^n m} \equiv (1+x^{p^n})^m \equiv 1 + mx^{p^n} + \ldots \pmod p$. Группа действует умножением на множестве таких подмножеств, причём порядок по крайней мере одной орбиты не делится на p. Стабилизатор точки из этой орбиты имеет порядок p^n.

б) Если мы посмотрим на действие произвольной p-подгруппы на этой орбите, то порядок какой-то из её орбит не будет делится на p, то есть она будет одноточечной.

в) Рассмотрим действие силовской p-подгруппы P сопряжением на множестве силовских p-подгрупп. У неё только одна одноточечная орбита: сама P, так как если P фиксирует другую силовскую p-подгруппу H, то PH — p-подгруппа, строго большая P, что невозможно. □

Лемма 1. *Пусть I — конечное множество, а $\lambda \in \mathbb{Q}$. Тогда у уравнения $\sum_{i\in I} 1/X_i = \lambda$ конечное число нулей в $\mathbb{N}_1^I$.*

Доказательство. Случаи $I = \varnothing$ или $\lambda \leqslant 0$ очевидны. Пусть $I \neq \varnothing$, $\lambda > 0$, а $(x_i)_{i\in I} \in \mathbb{N}_1^I$ — ноль уравнения. Минимальный из x_i не может быть строго больше $|I|/|\lambda|$. Подстановка целых чисел из интервала

$(0, |I|/|\lambda|]$ в уравнение $\sum_{i\in I} 1/X_i = \lambda$ вместо одной из переменных даёт конечное число уравнений того же типа на остальные переменные, и лемма доказывается индукцией по $|I|$. □

Теорема 5 (Теорема Э. Ландау)**.** *Порядок конечной группы с фиксированным числом классов сопряжённости элементов ограничен.*

Доказательство. Порядок группы равен сумме порядков классов сопряжённости, при этом класс сопряжённости единицы одноточечный. Поделив соответствующее уравнение на порядок группы, мы выразим число один в виде суммы обратных к натуральным числам, одно из которых равно порядку группы. Теперь воспользуемся леммой 1. □

Теорема 6 («Лемма Бернсайда»)**.** *Пусть G — конечная группа, транзитивно действующая на множестве X. Тогда среднее число фиксированных точек элементов G равно единице: $\frac{1}{|G|}\sum_{g\in G}|X^g| = 1$.*

Доказательство. Множество $\{(g, x) \in G \times X \mid gx = x\}$, очевидно, биективно и $\bigsqcup_{g\in G}\{x \in X \mid gx = x\}$, и $\bigsqcup_{x\in X}\{g \in G \mid gx = x\}$, а второе из этих множеств равномощно G. □

Следствие 3 (Теорема Жордана)**.** *Пусть G — группа, транзитивно и нетривиально действующая на конечном множестве X. Тогда существует $g \in G$, который не фиксирует ни одной точки X.*

Доказательство. Пусть G' — это образ G в конечной группе $\mathrm{Sym}(X)$. Так как $1 \in G'$ фиксирует $|X| \geqslant 2$ точек X, то, согласно «лемме Бернсайда», существует $g' \in G'$, который не фиксирует ни одной точки X. Возьмём в качестве $g \in G$ любой прообраз g'. □

Замечание 3. Теорему Жордана можно количественно усилить, см. теорему 5 в статье [5].

Замечание 4. Теорему Жордана можно переформулировать так: вложение собственной подгруппы конечного индекса не может быть сюръективным на классах сопряжённости.

Замечание 5. Не биективное вложение бесконечных множеств $J \to I$ индуцирует не биективное вложение групп финитарных перестановок $\mathrm{FSym}(J) \to \mathrm{FSym}(I)$, которое биективно на классах сопряжённости.

8.2. Простота больших знакопеременных групп

Наблюдение 1. Если умножить перестановку на транспозицию, соединяющую элементы разных циклов, то эти циклы сольются, а если на соединяющую элементы одного цикла, то этот цикл разложится на два. Это рассуждение сразу даёт разложение перестановки в произведение транспозиций, определение знака и его корректность.

Наблюдение 2. Ограничим действие конечной нетривиальной симметрической группы на себе сопряжением до действия знакопеременной группы. Тогда орбиты перестановок, у которых в цикленном разложении присутствует цикл чётной длины или два цикла одинаковой нечётной длины, не изменятся, так как их стабилизаторы содержат нечётные перестановки, а орбиты перестановок, состоящих из циклов попарно различной нечётной длины, распадутся на две равномощные.

Лемма 1. *Группа* $\mathrm{Alt}(5)$ *проста.*

Доказательство. В $\mathrm{Alt}(5)$ содержатся перестановки цикленных типов (5), $(3,1,1)$, $(2,2,1)$, $(1,1,1,1,1)$. Соответствующие классы сопряжённости имеют порядки 12, 12, 20, 15, 1. Никакая нетривиальная сумма записей этого списка, включающая 1, не делит $|\mathrm{Alt}(5)| = 60$. □

Наблюдение 3 (Группа вращений додекаэдра)**.** Пусть G — это группа вращений додекаэдра. Визуально очевидно, что порядки классов сопряжённости в G равны 12, 12, 20, 15, 1. Отсюда следует, что группа G простая, откуда, в свою очередь, следует, что гомоморфизм $G \to \mathrm{Sym}(5)$ действия G на своих силовских 2-подгруппах инъективен. Его образ имеет индекс 2, а потому совпадает с $\mathrm{Alt}(5) \subset \mathrm{Sym}(5)$.

Теорема 1. *Группа* $G \coloneqq \mathrm{Alt}(\Omega)$*, где* $5 \leqslant |\Omega| < \infty$*, проста.*

Доказательство. Докажем теорему индукцией по $|\Omega|$. Случай $|\Omega| = 5$ — это лемма 1. Пусть $|\Omega| \geqslant 6$, а $\sigma \in G \setminus \{1\}$. Нам нужно доказать, что сопряжённые к σ в G порождают G. Так как центр G тривиален и G порождена 3-циклами, то существует 3-цикл $\tau \in G$, такой что $\gamma \coloneqq [\sigma, \tau] = \sigma(\tau\sigma^{-1}\tau^{-1}) \neq 1$. Заметим, что γ является произведением 3-циклов $\tau' \coloneqq \sigma\tau\sigma^{-1}$ и τ^{-1}. Если τ' и τ^{-1} не независимы, то γ лежит в стабилизаторе точки из Ω, и мы победили. Если τ' и τ^{-1} независимы,

то, согласно наблюдению 2, перестановка $\gamma' \coloneqq \tau'\tau$ сопряжена γ в G. Тогда $\gamma\gamma' = \tau'\tau^{-1}\tau'\tau = (\tau')^2$ — 3-цикл, и мы снова победили. □

8.3. Автоморфизмы симметрических групп

Автоморфизмы группы $\mathrm{Sym}(\Omega)$ при $|\Omega| \neq 6$

Определение 1 (Симметрическая группа)**.** Пусть Ω — множество. Тогда группа автоморфизмов Ω как множества называется *симметрической группой* и обозначается через $\mathrm{Sym}(\Omega)$.

Определение 2 (Группа финитарных перестановок)**.** Пусть Ω — множество. Тогда подгруппа в группе $\mathrm{Sym}(\Omega)$, которая состоит из всех перестановок $\sigma \in \mathrm{Sym}(\Omega)$, таких что множество фиксированых точек σ имеет конечное дополнение, обозначается через $\mathrm{FSym}(\Omega)$ и называется группой *финитарных перестановок*.

Обозначение 1. Если $n \in \mathbb{N}_0$, то $\mathrm{Sym}(n) \coloneqq \mathrm{Sym}(\{1, 2, \ldots, n\})$.

Соглашение 1 (Инволюция)**.** В этом разделе *инволюцией* называется нетривиальная перестановка, которая обратна сама себе.

Соглашение 2 (Звезда)**.** В этом подразделе *звездой* называется произвольное множество попарно не коммутирующих транспозиций в какой-то фиксированной симметрической группе.

Наблюдение 1. Если $k \geqslant 2$ и $k \neq 3$, то у элементов k-элементной звезды всегда есть ровно одна общая подвижная точка (см. рис. 8.2а).

Наблюдение 2. Максимальные звёзды в $\mathrm{Sym}(4)$ делятся на две орбиты относительно действия $\mathrm{Sym}(4)$, индуцированного сопряжением. Звёзды из одной орбиты порождают $\mathrm{Sym}(4)$, а из другой — нет.

Теорема 1. *Если автоморфизм $\Phi' \in \mathrm{Aut}(\mathrm{FSym}(\Omega))$, где Ω — произвольное множество, переводит транспозиции в транспозиции, то Φ' индуцирован каким-то элементом $\varphi \in \mathrm{Sym}(\Omega)$.*

Доказательство. Пусть $|\Omega| \geqslant 3$. Тогда Φ' задаёт перестановку $\varphi \in \mathrm{Sym}(\Omega)$ через действие Φ' на порождающих звёздах, эквивариантно биективных элементам Ω. При этом, так как транспозиции — это в точности пересечения пар различных порождающих звёзд, то Φ' и φ одинаково действуют на транспозиции, а потому и на все элементы $\mathrm{FSym}(\Omega)$. Случаи $|\Omega| = 0, 1, 2$ разбираются отдельно. □

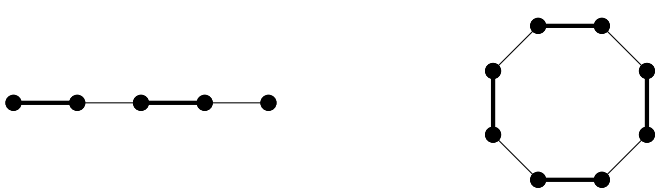
Наблюдение 3. Пусть Ω — множество, такое что $|\Omega| \neq 2$. Тогда централизатор $\mathrm{FSym}(\Omega)$ в $\mathrm{Sym}(\Omega)$ тривиален.

Лемма 1. *Если Ω — множество, а $\Psi \in \mathrm{Aut}(\mathrm{Sym}(\Omega))$ — автоморфизм, продолжающий автоморфизм $\Psi' \coloneqq \mathrm{Id} \in \mathrm{Aut}(\mathrm{FSym}(\Omega))$, то $\Psi = \mathrm{Id}$.*

Доказательство. Можно предположить, что $|\Omega| \neq 2$. Тогда, согласно наблюдению 3, имеем вложение $\iota : \mathrm{Sym}(\Omega) \to \mathrm{Aut}(\mathrm{FSym}(\Omega))$, $\sigma \mapsto {}^{\sigma}(-)$, такое что $\iota(\Psi(\sigma)) = \Psi' \circ \iota(\sigma) \circ \Psi'^{-1} = \iota(\sigma)$ для любого $\sigma \in \mathrm{Sym}(\Omega)$. □

Теорема 2. *Если автоморфизм $\Phi \in \mathrm{Aut}(\mathrm{Sym}(\Omega))$, где Ω — произвольное множество, переводит транспозиции в транспозиции, то Φ индуцирован каким-то элементом $\varphi \in \mathrm{Sym}(\Omega)$.*

Доказательство. Следует из теоремы 1 и леммы 1, так как, очевидно, $\Phi(\mathrm{FSym}(\Omega)) = \mathrm{FSym}(\Omega)$. □



a. С фиксированными точками b. Без фиксированных точек

Рис. 8.1. Примеры пар сопряжённых инволюций

Теорема 3. *Пусть Ω — множество, такое что $|\Omega| \neq 6$. Тогда любой автоморфизм группы $\mathrm{Sym}(\Omega)$ является внутренним автоморфизмом.*

Доказательство. Согласно теореме 2 достаточно доказать, что любой автоморфизм группы $\mathrm{Sym}(\Omega)$ переводит транспозиции в транспозиции.

Если Ω конечно, то в классе сопряжённости инволюций, элементы которого имеют фиксированные точки, есть пара элементов, расположенных как на рис. 8.1a, а в классе, элементы которого не имеют фиксированных точек, — как на рис. 8.1b. Отсюда ясно, что если $|\Omega| \neq 4, 6$, то в любом классе инволюций, кроме класса транспозиций, есть пара элементов, порядок произведения которых строго больше 3. А в $\mathrm{Sym}(4)$ все инволюции без фиксированных точек попарно коммутируют, в отличие от транспозиций. □

Автоморфизмы группы Sym(6)

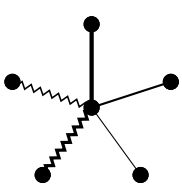
Соглашение 3 (Длинная инволюция)**.** В этом подразделе *длинной инволюцией* называется инволюция без фиксированных точек.

Соглашение 4 (Пятёрка)**.** В этом подразделе пятёрки попарно не коммутирующих длинных инволюций в $\mathrm{Sym}(6)$ называются просто *пятёрками.*

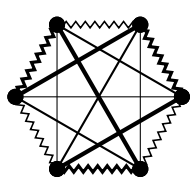
Наблюдение 4. Длинные инволюции в $\mathrm{Sym}(6)$ коммутируют тогда и только тогда, когда у них есть общий цикл.

Наблюдение 5. Группа $\mathrm{Sym}(6)$ транзитивно действует на множестве упорядоченных пар не коммутирующих длинных инволюций в $\mathrm{Sym}(6)$.

Наблюдение 6. Любая пара не коммутирующих длинных инволюций в $\mathrm{Sym}(6)$ однозначно достраивается до пятёрки (см. рис. 8.2b).



a. Цикленного типа $(2, 1^{,4})$



b. Цикленного типа $(2^{,3})$

Рис. 8.2. Пятёрки попарно не коммутирующих инволюций в $\mathrm{Sym}(6)$

Лемма 2. *Группа элементов* $\mathrm{Sym}(6)$*, переводящих фиксированную пятёрку в себя, имеет порядок* 120 *и реализует в точности все перестановки элементов пятёрки.*

Доказательство. Согласно наблюдению 5 любую упорядоченную пару различных элементов пятёрки можно перевести в любую другую упорядоченную пару различных элементов пятёрки действием элемента Sym(6), при этом, согласно наблюдению 6, пятёрка автоматически перейдёт в себя. Стабилизатор в Sym(6) упорядоченной пары элементов пятёрки имеет порядок 6 и реализует в точности все перестановки оставшихся трёх элементов пятёрки (см. рис. 8.2b). □

Наблюдение 7. Согласно наблюдениям 5 и 6 группа Sym(6) транзитивно действует на пятёрках. С учётом леммы 2 количество пятёрок равно 6.

Наблюдение 8. Канонический гомоморфизм из Sym(6) в группу перестановок шести пятёрок инъективен, так как в Sym(6) нет нетривиальной нормальной подгруппы индекса, кратного шести.

Замечание 1. Проверить, что в Sym(6) нет нетривиальной нормальной подгруппы индекса, кратного шести, можно посмотрев на список 1, 15, 15, 40, 40, 45, 90, 90, 120, 120, 144 порядков классов сопряжённости в Sym(6) и заметив, что включающая 1 нетривиальная сумма записей списка не может принадлежать списку 120, 60, 40, 30, ... делителей числа $|\mathrm{Sym}(6)|/6$.

Наблюдение 9. Действие транспозиции из Sym(6) на пятёрку никогда не переводит её в себя (см. рис. 8.2b), а потому транспозиции переходят в перестановки шести пятёрок, не имеющие фиксированной точки.

Теорема 4. *Группа внешних автоморфизмов группы* Sym(6) *имеет порядок* 2.

Доказательство. Мы уже построили нетривиальный элемент в группе внешних автоморфизмов Sym(6). Осталось заметить, что любой внешний автоморфизм Sym(6) обязан переводить инволюции цикленного типа $(2,1^4)$ в инволюции цикленного типа (2^3), и наоборот, откуда, согласно теореме 2, следует, что произведение любых двух внешних автоморфизмов Sym(6) является внутренним автоморфизмом Sym(6). □

Наблюдение 10. Пятёрки попарно не коммутирующих инволюций без фиксированных точек на множестве пятёрок попарно не коммутирую-

щих инволюций без фиксированных точек на шестиэлементном множестве эквивариантно биективны элементам исходного множества.

Глава 9

Модули над некоммутативными кольцами

9.1. Разложения и идемпотенты

Наблюдение 1. Пусть $R \cong \bigoplus_{i\in I} R_i$, где $|I| < \infty$, — ассоциативное унитальное кольцо, разложенное в конечное произведение колец, а M — R-модуль. Тогда $M \cong R \otimes_R M \cong (\bigoplus_{i\in I} R_i) \otimes_R M \cong \bigoplus_{i\in I}(R_i \otimes_R M)$. Так как для любого $i \in I$ образ $R_i \otimes_R M$ в M равен $R_i M$, то $M \cong \bigoplus_{i\in I} R_i M$. Иначе говоря, модуль над конечным произведением колец является прямой суммой образов действий координатных единиц.

Наблюдение 2. Унитальное кольцо $\mathbb{Z}^{\times I}$, где I — конечное множество, можно задать образующими e_i, где $i \in I$, соответствующими координатным единицам, и соотношениями $e_i^2 = e_i$ для любого $i \in I$, $e_i e_j = 0$ для любых $i, j \in I$, таких что $i \neq j$, и $\sum_{i\in I} e_i = 1$. При этом один из e_i и последнее соотношение можно убрать. В частности, существует очевидный изоморфизм $\mathbb{Z}[X]/(X^2 - X) \xrightarrow{\sim} \mathbb{Z} \times \mathbb{Z}$, $X \mapsto (1, 0)$.

Пример 1. Пусть M — модуль над ассоциативным унитальным кольцом R, а $x : M \to M$ — его идемпотентный эндоморфизм. Тогда, согласно наблюдению 2, x индуцирует на M структуру модуля над кольцом

$(\mathbb{Z}\times\mathbb{Z})\otimes_{\mathbb{Z}} R\cong R\times R$, а потому, согласно наблюдению 1, и разложение M в прямую сумму двух R-подмодулей.

Пример 2. Пусть R — ассоциативное унитальное кольцо, рассматриваемое как бимодуль над собой, а $x\in \mathrm{End}_{R\otimes_{\mathbb{Z}}R^o\text{-mod}}(R)\cong \mathrm{Z}(R)$ — его идемпотентный эндоморфизм. Тогда, согласно примеру 1, x индуцирует разложение R в прямую сумму двух двусторонних идеалов.

Наблюдение 3. Пусть R — ассоциативное унитальное кольцо, M — R-модуль, I и J — конечные множества, а $E:=\mathrm{End}_{R\text{-mod}}(M)$. Тогда пара гомоморфизмов колец $\mathbb{Z}^I\to E$ и $\mathbb{Z}^J\to E$, образы которых поэлементно коммутируют, соответствующих разложениям $M=\bigoplus_{i\in I}V_i$ и $M=\bigoplus_{j\in J}U_j$, индуцирует гомоморфизм колец $\mathbb{Z}^I\otimes_{\mathbb{Z}}\mathbb{Z}^J\cong\mathbb{Z}^{I\times J}\to E$, соответствующий разложению $M=\bigoplus_{i\in I,j\in J}(V_i\cap U_j)$.

Следствие 1. *Если M — модуль над ассоциативным унитальным кольцом R, такой что кольцо $\mathrm{End}_{R\text{-mod}}(M)$ коммутативно, то разложение M в конечную внутреннюю прямую сумму неразложимых подмодулей определено однозначно, если существует.*

Следствие 2. *Разложение ассоциативного унитального кольца в конечную внутреннюю прямую сумму неразложимых двусторонних идеалов определено однозначно, если существует.*

9.2. Модули над кольцом матриц

Эквивалентность категорий

Теорема 1. *Пусть R — ассоциативное унитальное кольцо, а I, J и K — три конечных непустых множества. Тогда гомоморфизм $\rho_{I,J,K}:\mathrm{M}_{I,J}(R)\otimes_{\mathrm{M}_J(R)}\mathrm{M}_{J,K}(R)\to\mathrm{M}_{I,K}(R)$, $x\otimes y\mapsto xy$ биективен.*

Доказательство. Стандартные разложения $\mathrm{M}_{I,J}(R)\cong\bigoplus_{i\in I}\mathrm{M}_{\{i\},J}(R)$, $\mathrm{M}_{J,K}(R)\cong\bigoplus_{k\in K}\mathrm{M}_{J,\{k\}}(R)$ и $\mathrm{M}_{I,K}(R)\cong\bigoplus_{i\in I,k\in K}\mathrm{M}_{\{i\},\{k\}}(R)$ индуцируют разложение $\rho_{I,J,K}=\bigoplus_{i\in I,k\in K}\rho_{\{i\},J,\{k\}}$. Гомоморфизм $\rho_{J,J,J}$ биективен, а потому $\rho_{\mathtt{pt},J,\mathtt{pt}}$ — тоже, а потому $\rho_{I,J,K}$ — тоже. □

Наблюдение 1. Пусть R — ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда из теоремы 1 ясно, что функторы

$V \mapsto \mathrm{M}_{I,\mathtt{pt}}(R) \otimes_R V : R\text{-mod} \rightleftarrows \mathrm{M}_I(R)\text{-mod} : \mathrm{M}_{\mathtt{pt},I}(R) \otimes_{\mathrm{M}_I(R)} U \leftarrow\!\shortmid U$ задают эквивалентность категорий R-mod и $\mathrm{M}_I(R)$-mod.

Наблюдение 2. Пусть R — ассоциативное унитальное кольцо, I — конечное непустое множество, U — $\mathrm{M}_I(R)$-модуль, а $(e_{i,j})_{i,j\in I}$ — стандартный базис $\mathrm{M}_I(R)$ как R-модуля. Тогда подкольцо $\bigoplus_{i\in I} Re_{i,i} \subset \mathrm{M}_I(R)$ задаёт разложение $U = \bigoplus_{i\in I} e_{i,i}U$, причём для любых $i, j \in I$ действие $e_{i,j}$ изоморфно переводит $e_{j,j}U$ в $e_{i,i}U$. Это ещё один способ увидеть эквивалентность категорий R-mod и $\mathrm{M}_I(R)$-mod.

Некоторые централизаторы в кольце матриц

Следствие 1. *Пусть R — ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда очевидное вложение кольца R^o в $\mathrm{End}_S(R^I)$, где $S \coloneqq \mathrm{End}_{R\text{-mod}}(R^I)$, биективно.*

Доказательство. Заметим, что $\mathrm{End}_R(R) \cong R^o$, и применим эквивалентность из наблюдений 1 и 2. □

Следствие 2. *Пусть R — ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда очевидное вложение кольца R в $\mathrm{Z}_{\mathrm{M}_I(R)}(\mathrm{M}_I(\mathbb{Z}))$ биективно.*

Доказательство. Пусть $S \coloneqq R^o$. Согласно следствию 1 централизатор $\mathrm{M}_I(S)$ в $E \coloneqq \mathrm{End}_{\mathbb{Z}\text{-mod}}(S^I)$ равен R. С другой стороны, он равен централизатору $\mathrm{M}_I(\mathbb{Z})$ в $\mathrm{Z}_E(S) \cong \mathrm{M}_I(R)$. Иначе говоря, следствие 2 — это переформулировка следствия 1. □

Следствие 3. *Пусть R — ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда $\mathrm{Z}(\mathrm{M}_I(R)) \cong \mathrm{Z}(R)$, $\mathrm{Z}_{\mathrm{M}_I(R)}(\mathrm{E}_I(\mathbb{Z})) \cong R$. Если $\mathrm{card}(I) > 1$, то $\mathrm{Z}(\mathrm{GL}_I(R)) \cong \mathrm{Z}(R)^\times$, а $\mathrm{Z}(\mathrm{GL}_1(R)) \cong \mathrm{Z}(R^\times)$.*

Доказательство. Равенство $\mathrm{Z}(\mathrm{M}_I(R)) = \mathrm{Z}(R)$ очевидным образом следует из следствия 2. Централизатор $\mathrm{E}_I(\mathbb{Z})$ в $\mathrm{M}_I(R)$ совпадает с централизатором $\mathbb{Z}$-подалгебры в $\mathrm{M}_I(R)$, порождённой образом $\mathrm{E}_I(\mathbb{Z})$, которая равна образу $\mathrm{M}_I(\mathbb{Z})$. Равенство $\mathrm{Z}(\mathrm{GL}_1(R)) = \mathrm{Z}(R^\times)$ — тавтология, а если $\mathrm{card}(I) > 1$, то $\mathrm{Z}(\mathrm{GL}_I(R)) = \mathrm{Z}_{\mathrm{M}_I(R)}(\mathbb{Z}\langle x \,|\, x \in \mathrm{GL}_I(R)\rangle)^\times = \mathrm{Z}_{\mathrm{M}_I(R)}(\mathbb{Z}\langle x \,|\, x \in \mathrm{E}_I(R)\rangle)^\times = \mathrm{Z}_{\mathrm{M}_I(R)}(\mathrm{M}_I(R))^\times = \mathrm{Z}(R)^\times$. □

Замечание 1. Для любого ассоциативного унитального кольца R выполняется вложение $\mathrm{Z}(R)^\times = R^\times \cap \mathrm{Z}(R) \subset \mathrm{Z}(R^\times)$.

Пример 1. Пусть $R \coloneqq \mathbb{C}[\rtimes X]$ — это фактор копроизведения ассоциативных унитальных колец $\mathbb{C}$ и $\mathbb{Z}[X]$ по соотношениям $Xa = \bar{a}X$, где $a \in \mathbb{C}$. Тогда $\mathrm{Z}(R)^\times = \mathbb{R}^\times \subsetneq \mathrm{Z}(R^\times) = \mathbb{C}^\times$.

Замечание 2. Я узнал о примере 1 из ответа [9] на «Mathematics Stack Exchange».

Наблюдение 3. Пусть R — ассоциативное унитальное кольцо, I — конечное множество, а $S \coloneqq R^{\times I}$. Тогда $\mathrm{End}_{S^o\text{-mod}}(S) \cong S$, а потому $\mathrm{Z}_{\mathrm{M}_I(R)}(\mathrm{D}_I(\mathbb{Z})) = \mathrm{D}_I(R)$.

Идеалы в кольце матриц

Следствие 4. *Пусть R — ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда любой левый идеал в $\mathrm{M}_I(R) \cong R^I \otimes_R R^I$ имеет вид $R^I \otimes_R U$, где $U \subset R^I$ — R-подмодуль.*

Доказательство. Заметим, что эквивалентность категорий переводит подобъекты в подобъекты, и воспользуемся наблюдением 1 или 2. □

Следствие 5. *Пусть R — ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда любой двусторонний идеал в $\mathrm{M}_I(R)$ имеет вид $\mathrm{M}_I(\mathfrak{I})$, где $\mathfrak{I} \subset R$ — двусторонний идеал в R.*

Доказательство. Пусть $S \coloneqq R \otimes_{\mathbb{Z}} R^o$ и $T \coloneqq \mathrm{M}_I(R) \otimes_{\mathbb{Z}} \mathrm{M}_I(R)^o \cong \mathrm{M}_{I\times I}(S)$. Заметим, что эквивалентность из наблюдений 1 и 2 переводит S-модуль R в T-модуль $S^{I\times I} \otimes_S R \cong R^{I\times I} \cong \mathrm{M}_I(R)$. □

Замечание 3. Следствия 4 и 5 можно получить и напрямую, элементарными методами.

Следствие 6. *Пусть R — простое ассоциативное унитальное кольцо, а I — конечное непустое множество. Тогда кольцо $\mathrm{M}_I(R)$ простое.*

9.3. Нётеровы и артиновы модули

Основные определения и теорема Гильберта о базисе

Соглашение 1 (О градуировках и фильтрациях)**.** В этом разделе градуировки и фильтрации абелевых групп — это $\mathbb{N}_0$-градуировки и исчерпывающие $\mathbb{N}_0$-фильтрации соответственно.

Наблюдение 1. Для любого частично упорядоченного множества Θ следующие два условия эквивалентны: а) Все возрастающие последовательности элементов Θ стабилизируются; б) В любом непустом подмножестве Θ существует максимальный элемент.

Определение 1 (Нётеров/артинов модуль)**.** Модуль M над ассоциативным унитальным кольцом R называется *нётеровым/артиновым*, если множество подмодулей M удовлетворяет условию стабилизации возрастающих/убывающих соответственно цепочек.

Наблюдение 2. Модуль M над ассоциативным унитальным кольцом R нётеров тогда и только тогда, когда любой подмодуль M конечно порождён.

Наблюдение 3. Пусть M — абелева группа с фильтрацией $(M_i)_{i=0}^{\infty}$, а $N \subsetneq M$ — её собственная подгруппа с индуцированной фильтрацией $(N_i)_{i=0}^{\infty} \coloneqq (N \cap M_i)_{i=0}^{\infty}$. Тогда индуцированное вложение $\mathrm{gr}(N) = \bigoplus_{i=0}^{\infty} N_i/N_{i-1} \to \mathrm{gr}(M) = \bigoplus_{i=0}^{\infty} M_i/M_{i-1}$ не биективно.

Определение 2. Будем называть градуированный модуль M над градуированным ассоциативным унитальным кольцом R *градуированно-нётеровым/градуированно-артиновым*, если частично упорядоченное множество градуированных подмодулей M удовлетворяет условию стабилизации возрастающих/убывающих соответственно цепочек.

Теорема 1. *Пусть R — градуированное ассоциативное унитальное кольцо, а M — фильтрованный R-модуль, такой что присоединённый градуированный R-модуль $\mathrm{gr}(M)$ градуированно-нётеров/градуированно-артинов. Тогда R-модуль M нётеров/артинов соответственно.*

Доказательство. Если $N \subset N' \subset N'' \subset N''' \subset \cdots$ — строго возрастающая цепочка подмодулей M с индуцированными фильтрациями, то,

согласно наблюдению 3, индуцированная цепочка $\mathrm{gr}(N) \to \mathrm{gr}(N') \to \mathrm{gr}(N'') \to \mathrm{gr}(N''') \to \cdots$ градуированных подмодулей $\mathrm{gr}(M)$ тоже строго возрастающая, и аналогично для убывающих цепочек. □

Теорема 2. *Пусть M — градуированный модуль над градуированным ассоциативным унитальным кольцом R. Тогда R-модуль M нётеров/артинов тогда и только тогда, когда R-модуль M градуированно-нётеров/градуированно-артинов соответственно.*

Доказательство. Часть «только тогда» очевидна, докажем часть «тогда». Градуировка на M индуцирует фильтрацию на M, такую что присоединённый градуированный R-модуль $\mathrm{gr}(M)$ градуированно изоморфен M. Осталось применить теорему 1. □

Наблюдение 4. Пусть Θ — частично упорядоченное множество, удовлетворяющее условию стабилизации возрастающих цепочек. Тогда частично упорядоченное множество монотонных отображений $\mathbb{N}_0 \to \Theta$ тоже удовлетворяет условию стабилизации возрастающих цепочек.

Теорема 3 (Теорема Гильберта о базисе)**.** *Пусть R — ассоциативное унитальное нётерово слева кольцо. Тогда кольцо $R[X]$ тоже нётерово слева.*

Доказательство. На кольце $R[X]$ имеется стандартная градуировка, такая что градуированные левые идеалы в $R[X]$ имеют вид $\bigoplus_{i=0}^{\infty} \mathfrak{I}_i X^i$, где $\mathfrak{I}_0 \subset \mathfrak{I}_1 \subset \mathfrak{I}_2 \subset \cdots$ — цепочка левых идеалов в R. Осталось воспользоваться теоремой 2 и наблюдением 4. □

Теорема 4. *Пусть M — модуль над ассоциативным унитальным кольцом R, а N — подмодуль в M. Тогда если модули N и M/N артиновы/нётеровы, то модуль M артинов/нётеров соответственно.*

Доказательство. Рассмотрим R как градуированное кольцо, полностью сидящее в градуировке ноль, а M — как модуль с фильтрацией $N \subset M$, после чего применим теорему 1. □

Прямые суммы и условия конечности

Теорема 5. *Пусть M — модуль над ассоциативным унитальным кольцом R, а $\varphi \in \mathrm{End}_{R\text{-mod}}(M)$. Тогда если M артинов/нётеров, а φ инъективен/сюръективен соответственно, то φ биективен.*

Доказательство. Если φ инъективен, но не биективен, то $\mathrm{Im}(\varphi) \supsetneq \mathrm{Im}(\varphi^2) \supsetneq \mathrm{Im}(\varphi^3) \supsetneq \cdots$ — бесконечная строго убывающая последовательность подмодулей в M, а если φ сюръективен, но не биективен, то $\mathrm{Ker}(\varphi) \subsetneq \mathrm{Ker}(\varphi^2) \subsetneq \mathrm{Ker}(\varphi^3) \subsetneq \cdots$ — бесконечная строго возрастающая последовательность подмодулей в M. □

Замечание 1. Теорема 5 утверждает, что артинов модуль не может быть изоморфен своему собственному подмодулю, а нётеров — своему фактормодулю по нетривиальной подгруппе.

Следствие 1. *Пусть M — ненулевой артинов или нётеров модуль над ассоциативным унитальным кольцом R, а I и J — множества, хотя бы одно из которых конечно. Тогда если R-модули $M^{\oplus I}$ и $M^{\oplus J}$ изоморфны, то множества I и J равномощны.*

Пример 1. Пусть I — бесконечное множество, R — ассоциативное унитальное кольцо, $V \coloneqq R^{\oplus I}$, а $E \coloneqq \mathrm{End}_{R^o\text{-mod}}(V)$. Тогда левый E-модуль E изоморфен $V^{\times I}$, а потому левые E-модули E и $E^{\oplus 2}$ изоморфны.

Наблюдение 5. Пусть $(M_i)_{i\in I}$ — семейство ненулевых конечно порождённых модулей над ассоциативным унитальным кольцом R. Пусть κ — наименьшая мощность множества образующих R-модуля $\bigoplus_{i\in I} M_i$. Тогда если I бесконечно, то $\kappa = \mathrm{card}(I)$, а если I конечно, то κ — тоже.

Следствие 2. *Пусть $(M_i)_{i\in I}$ и $(N_j)_{j\in J}$ — два семейства ненулевых конечно порождённых модулей над ассоциативным унитальным кольцом R, причём множества I и J не равномощны и хотя бы одно из них бесконечно. Тогда R-модули $\bigoplus_{i\in I} M_i$ и $\bigoplus_{j\in J} N_j$ не изоморфны.*

Вопрос 1. Пусть M — ненулевой артинов модуль над ассоциативным унитальным кольцом R, а I и J — два не равномощных бесконечных множества. Верно ли, что R-модули $M^{\oplus I}$ и $M^{\oplus J}$ не изоморфны?

Длина модуля и теорема Жордана – Гёльдера

Определение 3 (Композиционный ряд модуля)**.** Пусть M — модуль над ассоциативным унитальным кольцом R. Тогда конечная последовательность $0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$ подмодулей M, такая что для любого $i = 1, \ldots, n$ присоединённый R-модуль M_i/M_{i-1}

прост, называется *композиционным рядом* модуля M, а число $n \in \mathbb{N}_0$ называется *длиной* этого композиционного ряда.

Определение 4 (Композиционная длина модуля)**.** Пусть M — модуль над ассоциативным унитальным кольцом R. Тогда *композиционная длина* или просто *длина* M, обозначаемая $l(M)$, определяется как минимальная длина композиционного ряда M, если у M существует композиционный ряд, и ∞ в противном случае.

Теорема 6. *Модуль M над ассоциативным унитальным кольцом R является модулем конечной длины тогда и только тогда, когда он одновременно нётеров и артинов.*

Доказательство. Часть «только тогда» очевидна, докажем часть «тогда». Если $M \neq 0$, то, по нётеровости M, в M существует максимальный собственный подмодуль $M' \subsetneq M$. Если $M' \neq 0$, то, по нётеровости M', в M' существует максимальный собственный подмодуль $M'' \subsetneq M'$. Так как M артинов, то продолжая таким образом, мы за конечное число шагов дойдём до нулевого модуля и получим композиционный ряд. □

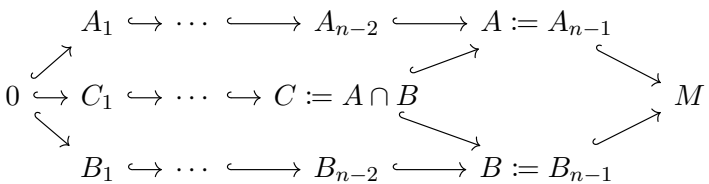
Теорема 7. *Пусть M — модуль над ассоциативным унитальным кольцом R. Тогда длина M совпадает с супремумом длин конечных строго возрастающих цепочек подмодулей в M.*

Доказательство (из двух частей).

Часть 1. Заметим, что достаточно доказать, что если $l(M) < \infty$, а $N \subsetneq M$ — собственный подмодуль, то $l(N) < l(M)$, потому что из этого утверждения выводится, что длины конечных строго возрастающих цепочек подмодулей не превосходят длины модуля.

Часть 2. Пусть $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$, где $n \in \mathbb{N}_0$, — композиционный ряд. Тогда на N индуцирована фильтрация $(N_i)_{i=0}^n := (N \cap M_i)_{i=0}^n$, причём индуцированное вложение $\mathrm{gr}(N) \to \mathrm{gr}(M)$ не биективно по наблюдению 3, но биективно на ненулевых градуированных компонентах по лемме Шура. Это значит, что если выкинуть из фильтрации $(N_i)_{i=0}^n$ повторяющиеся элементы, которые там обязательно есть, то получится композиционный ряд для N. □

Теорема 8 (Теорема Жордана–Гёльдера)**.** *Пусть M — модуль над ассоциативным унитальным кольцом R, а $(A_i)_{i=0}^n$ и $(B_i)_{i=0}^n$, где $n \in \mathbb{N}_0$, — два композиционных ряда для M. Тогда набор классов изоморфизма присоединённых факторов фильтрации $(A_i)_{i=0}^n$ совпадает с соответствующим набором для $(B_i)_{i=0}^n$.*



(1)

Доказательство. Докажем теорему индукцией по $l(M)$. Введём обозначения $A \coloneqq A_{n-1}$, $B \coloneqq B_{n-1}$ и $C \coloneqq A \cap B$. Если $A = B$, то достаточно применить индукционное предположение к $A = B$. Пусть $A \neq B$. Тогда $A \neq C \neq B$ и канонические вложения $A/C \to M/B$ и $B/C \to M/A$ биективны по лемме Шура. Осталось выбрать произвольный композиционный ряд $(C_i)_{i=0}^{n-2}$ для C, посмотреть на диаграмму (1) и применить индукционное предположение к A и B. □

9.4. Полупростые модули

Простые модули и лемма Шура

Определение 1 (Простой модуль)**.** Модуль над ассоциативным унитальным кольцом называется *простым*, если у него ровно один собственный подмодуль — нулевой.

Лемма 1 (Лемма Шура)**.** *Ненулевой гомоморфизм из простого модуля инъективен, ненулевой гомоморфизм в простой модуль сюръективен. Как следствие, ненулевой гомоморфизм из простого модуля в простой модуль является изоморфизмом.*

Доказательство. Следует из рассмотрения ядра и образа гомоморфизма соответственно. □

Следствие 1. *Кольцо эндоморфизмов простого модуля является телом.*

Определение и основные свойства полупростоты

Определение 2 (Полупростой модуль)**.** Пусть M — модуль над ассоциативным унитальным кольцом R. Тогда M называется *полупростым*, если у любого подмодуля в M есть дополнение в M.

Теорема 1 (Полупростота подфакторов)**.** *Пусть M — полупростой модуль над ассоциативным унитальным кольцом R. Тогда подмодули и фактормодули M являются полупростыми модулями.*

Доказательство (из двух частей).

Полупростота подмодулей. Пусть $\iota_N^M : N \to M$ и $\iota_L^N : L \to N$ — инъективные гомоморфизмы. Так как модуль M полупрост, то у $\iota_N^M \circ \iota_L^N$ есть левый обратный, а потому у ι_L^N — тоже.

Полупростота фактормодулей. Пусть $\pi_M^U : M \to U$ и $\pi_U^V : U \to V$ — сюръективные гомоморфизмы. Так как модуль M полупрост, то у $\pi_U^V \circ \pi_M^U$ есть правый обратный, а потому у π_U^V — тоже. □

Лемма 2. *Пусть M — ненулевой полупростой модуль над ассоциативным унитальным кольцом R. Тогда в M есть простой подмодуль.*

Доказательство. Так как $M \neq 0$, то M содержит ненулевой циклический подмодуль $C \subset M$, который полупрост по теореме 1. В ненулевых циклических модулях есть максимальные собственные подмодули по теореме о существовании максимальных идеалов. Дополнение в C к максимальному собственному подмодулю в C и будет минимальным ненулевым, то есть простым, подмодулем в $C \subset M$. □

Теорема 2 (Критерий полупростоты)**.** *Модуль M над ассоциативным унитальным кольцом R полупрост тогда и только тогда, когда является прямой суммой семейства простых модулей.*

Доказательство (из двух частей).

Часть «тогда». Пусть $M = \bigoplus_{i \in I} M_i$ — прямая сумма простых модулей, а $N \subset M$ — подмодуль в M. Воспользовавшись леммой Цорна, рассмотрим максимальное подмножество $J \subset I$, такое что $N \cap \bigoplus_{j \in J} M_j = 0$. Пусть $e \in I$. Если $M_e \not\subset N \oplus (\bigoplus_{j \in J} M_j)$, то $M_e \cap (N \oplus (\bigoplus_{j \in J} M_j)) = 0$, так как это подмодуль в M_e, откуда $e \in J$ — противоречие.

Часть «только тогда». Пусть модуль M полупрост, а $(M_i)_{i\in I}$ — семейство всех простых подмодулей в M. Воспользовавшись леммой Цорна, рассмотрим максимальное подмножество $J \subset I$, для которого сумма $\sum_{j\in J} M_j$ прямая. Если дополнение к $\sum_{j\in J} M_j$ в M ненулевое, то в нём, согласно лемме 2, есть простой подмодуль — противоречие. □

Наблюдение 1. Пусть M — модуль над ассоциативным унитальным кольцом R, а $(M_i)_{i\in I}$ — семейство простых подмодулей в M, такое что $M = \sum_{i\in I} M_i$. Тогда, согласно теореме 1, модуль M полупрост как гомоморфный образ полупростого, согласно теореме 2, модуля $\bigoplus_{i\in I} M_i$.

Разложение на изотипические компоненты

Определение 3 (Изотипические компоненты)**.** Пусть R — ассоциативное унитальное кольцо, M — полупростой R-модуль, а N — простой R-модуль. Тогда сумма всех подмодулей в M, изоморфных N, называется *N-изотипической компонентой* модуля M.

Определение 4 (Изотипический модуль)**.** Полупростой модуль M над ассоциативным унитальным кольцом R называется *изотипическим*, если у него ровно одна ненулевая изотипическая компонента.

Теорема 3 (Разложение на изотипические компоненты)**.** *Если M — полупростой модуль над ассоциативным унитальным кольцом R, то M является прямой суммой своих изотипических компонент.*

Доказательство. Пусть $M = \bigoplus_{i\in I} M_i$ — разложение M в прямую сумму простых подмодулей, а $N \subset M$ — произвольный простой подмодуль в M. Тогда, согласно лемме Шура, ограничение стандартной проекции $\pi_e : \bigoplus_{i\in I} M_i \to M_e$, где $e \in I$, на N равно нулю, если $N \not\simeq M_e$. Иначе говоря, $N \subset \bigoplus_{\{i\in I | M_i \simeq N\}} M_i \subset \bigoplus_{i\in I} M_i$. □

Наблюдение 2. Пусть N — простой модуль над ассоциативным унитальным кольцом R. Тогда гомоморфизмы полупростых R-модулей переводят N-изотипические компоненты в N-изотипические компоненты.

Полупростота и условия конечности

Наблюдение 3. Для полупростых модулей свойства артиновости, нётеровости и конечной порождённости совпадают. В частности, ассоциативное унитальное кольцо, полупростое как левый модуль над собой, артиново и нётерово как левый модуль над собой.

Теорема 4. *Пусть N — простой модуль над ассоциативным унитальным кольцом R, а I и J — два не равномощных множества. Тогда модули $N^{\oplus I}$ и $N^{\oplus J}$ не изоморфны.*

Доказательство. Если I или J бесконечно, то утверждение теоремы следует из рассмотрения минимальных мощностей порождающих множеств (следствие 9.3.2), а если I и J конечны — то из нётеровости или артиновости N (следствие 9.3.1), либо, в качестве альтернативы, можно воспользоваться теоремой Крулля – Шмидта (теорема 9.6.1). □

Простые кольца и полупростота

Определение 5 (Цоколь модуля)**.** Пусть M — модуль над ассоциативным унитальным кольцом R. Тогда сумма всех простых подмодулей в M называется *цоколем* M.

Теорема 5. *Пусть M — модуль над ассоциативным унитальным кольцом R, такой что у M нетривиальный цоколь и M прост как модуль над $R \otimes_{\mathbb{Z}} E$, где $E \coloneqq \mathrm{End}_{R\text{-mod}}(M)$. Тогда M — изотипический полупростой R-модуль.*

Доказательство. Цоколь и его изотипические компоненты являются $(R \otimes_{\mathbb{Z}} E)$-подмодулями в M. □

Замечание 1. Обратное к теореме 5 тоже верно: изотипический полупростой модуль M над ассоциативным унитальным кольцом R является простым модулем над $R \otimes_{\mathbb{Z}} E$, где $E \coloneqq \mathrm{End}_{R\text{-mod}}(M)$.

Следствие 2. *Пусть R — простое ассоциативное унитальное кольцо, в котором существует минимальный ненулевой левый идеал. Тогда кольцо R полупросто как левый модуль над собой.*

Доказательство. Кольцо R просто тогда и только тогда, когда оно просто как модуль над $R \otimes_{\mathbb{Z}} R^o$, а $R^o \cong \mathrm{End}_{R\text{-mod}}(R)$. Осталось воспользоваться теоремой 5. □

Пример 1. Пусть $R \coloneqq \mathbb{Q}\langle X, \partial_X\rangle \subset \mathrm{End}_{\mathbb{Q}\text{-mod}}(\mathbb{Q}[X])$ — алгебра Вейля. Тогда $[\partial_X, X] = 1$ и $R = \bigoplus_{n,m\in\mathbb{N}_0} \mathbb{Q} \cdot X^n \partial_X^m$ — разложение на собственные подпространства с различными собственными значениями для операторов $(X*) \circ [\partial_X, -]$ и $(*\partial_X) \circ [-, X]$. Кольцо R простое, так как из любого ненулевого элемента R несколько раз применив операторы $[X, -]$ и $[\partial_X, -]$ можно получить ненулевой элемент $\mathbb{Q}$. Так как $R \supsetneq R\partial_X \supsetneq R\partial_X^2 \supsetneq \cdots$ и $R \supsetneq XR \supsetneq X^2R \supsetneq \cdots$ — бесконечные строго убывающие последовательности левых/правых соответственно идеалов в R, то кольцо R не артиново слева/справа.

Теорема Джекобсона о плотности

Наблюдение 4 (Теорема Джекобсона о плотности)**.** Пусть R — ассоциативное унитальное кольцо, N — простой R-модуль, а I — множество. Тогда для любого собственного подмодуля $L \subset N^{\oplus I}$ существует ненулевой R-гомоморфизм $\varphi : N^{\oplus I} \to N$, такой что $\varphi(L) = 0$.

Замечание 2. Классическая теорема Джекобсона о плотности — это наблюдение 4, применённое к случаю циклического L и конечного I.

Центральные простые алгебры

Тензорное произведение простых алгебр

Теорема 6. *Пусть N — простой модуль над ассоциативным унитальным кольцом R, а $D \coloneqq \mathrm{End}_{R\text{-mod}}(N)^o$. Тогда функтор $N \otimes_D (-) : D\text{-mod} \to R\text{-mod}$ строгий и полный, а его существенный образ замкнут относительно перехода к подмодулям и фактормодулям.*

Доказательство. То, что функтор строгий и полный, следует из того, что все модули над D свободные, а R-модуль N конечно порождён — морфизмы в D-mod и его существенном образе, то есть категории R-модулей, изоморфных прямым суммам N, задаются столбцово-финитарными матрицами с элементами в D^o. □

Следствие 3. *Пусть N — простой модуль над ассоциативным унитальным кольцом R, а V — модуль над телом $D := \mathrm{End}_{R\text{-mod}}(N)^o$. Тогда любой R-подмодуль в $N \otimes_D V$ имеет вид $N \otimes_D U$, где $U \subset V$ — D-подмодуль.*

Теорема 7. *Пусть k — поле, R — центральная простая ассоциативная унитальная алгебра над k, а R' — простая ассоциативная унитальная алгебра над k. Тогда кольцо $R \otimes_k R'$ простое.*

Доказательство. Введём обозначения $S := R \otimes_{\mathbb{Z}} R^o$ и $S' := R' \otimes_{\mathbb{Z}} (R')^o$. Тогда R является простым S-модулем и $\mathrm{End}_{S\text{-mod}}(R) \cong \mathrm{Z}(R) \cong k$. Согласно следствию 3 произвольный S-подмодуль $M \subset R \otimes_k R'$ имеет вид $R \otimes_k U$ для какого-то k-подмодуля $U \subset R'$. Если M является ещё и S'-подмодулем, то $U \subset R'$ — тоже S'-подмодуль. Так как R' — простой S'-модуль, то M либо тривиальный, либо несобственный. □

Пример 2. Пусть K — поле, $k \subsetneq K$ — его собственное подполе, а R и R' — две простые ассоциативные унитальные алгебры над K. Тогда очевидный сюръективный гомоморфизм $R \otimes_k R' \to R \otimes_K R'$ имеет нетривиальное ядро. Это показывает, что тензорное произведение двух простых алгебр над полем не обязано быть простой алгеброй.

Теорема 8. *Пусть R и R' — ассоциативные унитальные алгебры над ассоциативным коммутативным унитальным кольцом A, причём R' свободен как A-модуль. Тогда если кольцо $R \otimes_A R'$ простое, то кольцо R тоже простое.*

Доказательство. Пусть $\mathfrak{I} \subset R$ — нетривиальный собственный двусторонний идеал. Тогда $\mathfrak{I} \otimes_A R' \subset R \otimes_A R'$ — тоже нетривиальный собственный двусторонний идеал. □

Централизаторы в тензорном произведении алгебр

Теорема 9. *Пусть R и R' — ассоциативные унитальные алгебры над ассоциативным коммутативным унитальным кольцом A, а $S \subset R$ — A-подалгебра, причём R' свободна как A-модуль. Тогда $\mathrm{Z}_{R \otimes_A R'}(S)$ совпадает с $\mathrm{Z}_R(S) \otimes_A R'$.*

Доказательство. Заметим, что $\mathrm{Z}_R(S)$ совпадает с инвариантами действия S как алгебры Ли на R коммутированием, $\mathrm{Z}_{R\otimes_A R'}(S)$ совпадает с инвариантами индуцированного действия S как алгебры Ли на $R\otimes_A R'$, а функтор $(-)\otimes_A A^{\oplus I}\cong(-)^{\oplus I}$, где I — множество, сохраняет инварианты действий. □

Следствие 4. *Пусть R и R' — ассоциативные унитальные алгебры над полем k, а $S\subset R$ и $S'\subset R'$ — их k-подалгебры. Тогда $\mathrm{Z}_{R\otimes_k R'}(S\otimes_k S')$ совпадает с $\mathrm{Z}_R(S)\otimes_k \mathrm{Z}_{R'}(S')$.*

Пример 3. Пусть $R\coloneqq\mathbb{Z}\langle X,Y\rangle/([X,Y]-1)$ — алгебра Вейля. Тогда очевидный гомоморфизм $\mathrm{Z}(R)\otimes_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z})\to\mathrm{Z}(R\otimes_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}))$, где p — простое число, не сюръективен.

Группа Брауэра поля

Обозначение 1 (ЦПА)**.** Сокращение «ЦПА» означает «центральная простая ассоциативная унитальная алгебра».

Теорема 10. *Пусть R — конечномерная ЦПА над полем k. Тогда стандартный гомоморфизм $R\otimes_k R^o\to\mathrm{End}_{k\text{-mod}}(R)$ биективен.*

Доказательство. Гомоморфизм инъективен, так как кольцо $R\otimes_k R^o$ простое, и сюръективен по соображениям размерности. □

Определение 6 (Группа Брауэра поля)**.** Пусть k — поле. Тогда моноид, заданный образующими — классами изоморфизма конечномерных ЦПА над k — и соотношениями — $[R\otimes_k R']=[R][R']$ для любых конечномерных ЦПА R и R' над k и $[\mathrm{M}_n(k)]=1$ для любого $n\in\mathbb{N}_1$ — называется *группой Брауэра* поля k и обозначается $\mathrm{Br}(k)$.

Замечание 3. Группа Брауэра названа так в честь Ричарда/Рихарда Дагоберта Брауэра (Richard Dagobert Brauer) (10.02.1901–17.04.1977).

Теорема Артина – Веддербёрна

Теорема 11. *Унитальное ассоциативное кольцо, полупростое как левый модуль над собой, изоморфно конечному произведению колец типа $\mathrm{M}_n(D)$, где D — тело, а $n\in\mathbb{N}_1$. И наоборот, кольца $\mathrm{M}_n(D)$ полупросты как левые модули над собой.*

Доказательство. Пусть унитальное ассоциативное кольцо A полупросто как левый A-модуль: $A \cong \bigoplus_{i\in I} M_i^{\oplus S_i}$, где I конечно, все S_i конечные непустые, модули M_i простые, $M_i \not\cong M_j$ при $i \neq j$. В прямой сумме конечное число слагаемых, так как A-модуль A конечно порождён единицей, а нетривиальная бесконечная прямая сумма — нет. Тогда $A \cong \mathrm{End}_{A\text{-mod}}(A)^o \cong (\prod_{i\in I} \mathrm{M}_{S_i}(D_i))^o \cong \prod_{i\in I} \mathrm{M}_{S_i}(D_i^o)$, где $D_i := \mathrm{End}_{A\text{-mod}}(M_i)$, по лемме Шура. Обратно, если S — конечное множество, а D — тело, то $\mathrm{M}_S(D) \cong \bigoplus_{s\in S} \mathrm{M}_{S,\{s\}}(D)$ — разложение в прямую сумму изоморфных простых $\mathrm{M}_S(D)$-подмодулей. □

Наблюдение 5. Пусть D — тело, а $n \in \mathbb{N}_1$. Тогда композиционная длина $\mathrm{M}_n(D)$ как левого модуля над собой равна n, а кольцо эндоморфизмов любого простого $\mathrm{M}_n(D)$-модуля изоморфно D^o.

Наблюдение 6. Согласно следствию 9.1.2 и наблюдению 5, с учётом простоты кольца матриц над телом, разложение теоремы 11 определено однозначно в понятном смысле.

Теорема Нётер – Сколема

Теорема 12 (Теорема Нётер – Сколема)**.** *Пусть R и S — две конечномерные простые ассоциативные унитальные алгебры над полем k, причём k-алгебра R центральна. Тогда для любых двух гомоморфизмов k-алгебр $f, g : S \to R$ существует внутренний автоморфизм $h : R \xrightarrow{\sim} R$, такой что $h \circ f = g$.*

Доказательство. Пусть ${}_fR$ — это R, рассмотренная как модуль над $S \otimes_k R^o$ путём ограничения скаляров вдоль $f \otimes \mathrm{Id} : S \otimes_k R^o \to R \otimes_k R^o$, а ${}_gR$ — вдоль $g \otimes \mathrm{Id} : S \otimes_k R^o \to R \otimes_k R^o$.

Тогда $\mathrm{Hom}_{S\otimes_k R^o\text{-mod}}({}_fR, {}_gR)$, вложенное в $\mathrm{Hom}_{R^o\text{-mod}}({}_fR, {}_gR) \cong R$, отождествляется с $\{a \in R \mid af(s) = g(s)a$ для всех $s \in S\}$. В частности, $\mathrm{Iso}_{S\otimes_k R^o\text{-mod}}({}_fR, {}_gR) \cong \{a \in R^\times \mid af(s)a^{-1} = g(s)$ для всех $s \in S\}$.

Осталось заметить, что так как конечномерная k-алгебра $S \otimes_k R^o$ простая по теореме 7, то все $S \otimes_k R^o$-модули одинаковой k-размерности изоморфны, а $\dim_k({}_fR) = \dim_k(R) = \dim_k({}_gR)$. □

9.5. Радикал Джекобсона

Определение и эквивалентные характеризации

Определение 1 (Аннулятор модуля)**.** Пусть R — ассоциативное унитальное кольцо, а M — R-модуль. Ядро структурного гомоморфизма $R \to \mathrm{End}_{\mathbb{Z}\text{-mod}}(M)$ называется *аннулятором* M в R и обозначается $\mathrm{Ann}_R(M)$.

Определение 2 (Радикал Джекобсона кольца)**.** Пусть R — ассоциативное унитальное кольцо. Пересечение аннуляторов простых R-модулей называется *радикалом Джекобсона* кольца R.

Определение 3 (Аннулятор элемента)**.** Пусть R — ассоциативное унитальное кольцо, M — R-модуль, а $x \in M$ — элемент M. Ядро гомоморфизма $a \mapsto ax : R \to Rx \subset M$ модулей над R называется *аннулятором* x в R и обозначается $\mathrm{Ann}_R(x)$.

Теорема 1 (Характеризации радикала Джекобсона)**.** *Пусть* $\mathfrak{J}$ — *радикал Джекобсона ассоциативного унитального кольца* R*. Тогда* $\mathfrak{J}$ *можно охарактеризовать следующими эквивалентными способами:*

а) $\mathfrak{J}$ *совпадает с пересечением всех максимальных левых идеалов* R*;*

б) $\mathfrak{J}$ *совпадает с множеством всех* $x \in R$*, таких что для любого* $a \in R$ *элемент* $1 - ax \in R$ *обратим слева;*

в) $\mathfrak{J}$ *совпадает с множеством всех* $x \in R$*, таких что для любого* $a \in R$ *элемент* $1 - ax \in R$ *двусторонне обратим;*

г) $\mathfrak{J}$ *совпадает с множеством всех* $x \in R$*, таких что для любых* $a, b \in R$ *элемент* $1 - axb \in R$ *двусторонне обратим;*

д) $\mathfrak{J}$ *как множество совпадает с радикалом Джекобсона кольца* R^o*.*

Доказательство.

а) Пересечение аннуляторов простых R-модулей совпадает с пересечением аннуляторов ненулевых элементов простых R-модулей, а это в точности максимальные левые идеалы R.

б) Пусть $x \in R$. Тогда условие «$x \notin \mathfrak{J}$» эквивалентно условию «существует максимальный левый идеал $\mathfrak{m} \subset R$, такой что $x \notin \mathfrak{m}$», которое эквивалентно условию «существует максимальный левый идеал $\mathfrak{m} \subset R$, такой что образ x в $R/\mathfrak{m}$ не равен нулю», которое эквивалентно условию «существует максимальный левый идеал $\mathfrak{m} \subset R$, такой что существует $a \in R$, такой что $ax \equiv 1 \pmod{\mathfrak{m}}$», которое эквивалентно отрицанию условия из пункта (б).

в) Условие из пункта (в), очевидно, сильнее условия из пункта (б). Докажем обратное. Пусть $x \in \mathfrak{J}$. Левые обратные к элементам множества $1 + Rx \subset R$ фиксируют класс $1 + Rx \in R/(Rx)$, а потому и сами ему принадлежат, а потому обратимы слева. Отсюда следует, что элементы множества $1 + Rx$ двусторонне обратимы.

г) С одной стороны, условие из пункта (г), очевидно, сильнее условия из пункта (в), так как можно взять $b = 1$. С другой стороны, $\mathfrak{J}$ является двусторонним идеалом, поэтому если $x \in \mathfrak{J}$, то $xb \in \mathfrak{J}$ для любого $b \in R$, откуда следует условие из пункта (г).

д) Пункт (д) является прямым следствием характеризации (г). □

Лемма Накаямы

Общая формулировка и доказательство

Теорема 2 (Лемма Накаямы)**.** *Пусть M — ненулевой конечно порождённый модуль над ассоциативным унитальным кольцом R, а $\mathfrak{J}$ — радикал Джекобсона кольца R. Тогда $\mathfrak{J}M \neq M$.*

Доказательство. У M есть ненулевой циклический фактор-модуль, например, фактор M по подмодулю, порождённому максимальным собственным подмножеством минимального порождающего M множества, а у ненулевого циклического фактор-модуля есть простой фактор-модуль, который зануляется радикалом Джекобсона. □

Лемма Накаямы для коммутативных колец

Теорема 3. *Пусть M — конечно порождённый модуль над ассоциативным коммутативным унитальным кольцом A, а $\mathfrak{a}$ — идеал в A, такой что $\mathfrak{a}M = M$. Тогда существует $x \in 1 + \mathfrak{a}$, такой что $xM = 0$.*

Доказательство. Пусть $S \coloneqq 1 + \mathfrak{a} \subset A$. Так как идеал $\mathfrak{a}_S \coloneqq \mathfrak{a}A_S \subset A_S$ содержится в радикале Джекобсона кольца A_S, и выполняется равенство $\mathfrak{a}_S M_S = M_S$, то $M_S = 0$, что в предположении конечной порождённости M эквивалентно существованию $x \in S$, такого что $xM = 0$. □

Замечание 1. Если в условиях теоремы 3 взять в качестве $\mathfrak{a}$ радикал Джекобсона кольца A, то элемент x будет обратимым, и из равенства $xM = 0$ будет следовать равенство $M = 0$. Таким образом, теорему 3 можно воспринимать как эквивалентную переформулировку леммы Накаямы для коммутативных колец.

Следствие 1. *Пусть M — конечно порождённый модуль над ассоциативным коммутативным унитальным кольцом A. Тогда любой сюръективный A-эндоморфизм $\varphi : M \to M$ является изоморфизмом.*

Доказательство. Эндоморфизм φ задаёт на M структуру $A[X]$-модуля, такого что $XM = M$. Тогда, по теореме 3, существует $P(X) \in A[X]$, такой что $(1 - P(X)X)M = 0$, то есть $\mathrm{Id}_M = P(\varphi) \circ \varphi = \varphi \circ P(\varphi)$. □

Следствие 2. *Пусть A — ненулевое коммутативное ассоциативное унитальное кольцо, а $\varphi : A^{\oplus n} \to A^{\oplus m}$, где $n, m \in \mathbb{N}_0$, — сюръективный гомоморфизм A-модулей. Тогда $n \geqslant m$.*

Доказательство. Пусть $n < m$. Тогда композиция φ и произвольной координатной проекции с нетривиальным ядром $\pi : A^{\oplus m} \to A^{\oplus n}$ является не биективным, но сюръективным эндоморфизмом $A^{\oplus n}$, что противоречит следствию 1. □

Радикал Джекобсона и полупростота

Наблюдение 1. В артиновом модуле пересечение любого семейства подмодулей совпадает с пересечением какого-то конечного подсемейства этого семейства.

Наблюдение 2. Для полупростого модуля над ассоциативным унитальным кольцом артиновость эквивалентна нётеровости, которая эквивалентна конечной порождённости.

Определение 4 (Радикал Джекобсона модуля)**.** Пусть M — модуль над ассоциативным унитальным кольцом R. Пересечение максимальных собственных подмодулей в M называется *радикалом Джекобсона* или просто *радикалом* модуля M.

Наблюдение 3. Пусть M — полупростой модуль над ассоциативным унитальным кольцом R, а $\mathfrak{J}_M$ — радикал Джекобсона M. Тогда, так как M является прямой суммой простых модулей, то $\mathfrak{J}_M = 0$.

Теорема 4. *Пусть M — артинов модуль над ассоциативным унитальным кольцом R, такой что $\mathfrak{J}_M = 0$, где $\mathfrak{J}_M$ — это радикал Джекобсона M. Тогда M полупрост.*

Доказательство. Согласно наблюдению 1 существует конечное семейство $(M_i)_{i\in I}$ максимальных собственных подмодулей M, такое что $\mathfrak{J}_M = \bigcap_{i\in I} M_i$. Тогда канонический гомоморфизм $M \to \prod_{i\in I}(M/M_i)$ в полупростой модуль $\prod_{i\in I}(M/M_i) \cong \bigoplus_{i\in I}(M/M_i)$ инъективен и M полупрост, так как подмодуль полупростого модуля полупрост. □

Следствие 3 (Критерий полупростоты кольца)**.** *Ассоциативное унитальное кольцо полупросто тогда и только тогда, когда оно артиново слева и его радикал Джекобсона равен нулю.*

Доказательство. Заметим, что полупростое кольцо автоматически артиново слева по наблюдению 2, так как оно является циклическим модулем над собой, после чего воспользуемся наблюдением 3 и теоремой 4. □

Радикал Джекобсона и артиновы кольца

Теорема Акидзуки – Хопкинса – Левицкого

Определение 5 (Аннулятор идеала)**.** Пусть R — ассоциативное унитальное кольцо, $\mathfrak{a}$ — правый идеал в R, а M — R-модуль. Тогда *аннулятором* $\mathfrak{a}$ в M, обозначаемым $\mathrm{Ann}_M(\mathfrak{a})$, называется R-подмодуль $\{m \in M \mid am = 0 \text{ для всех } a \in \mathfrak{a}\}$ модуля M.

Лемма 1. *Пусть R — ассоциативное унитальное кольцо, $\mathfrak{a}$ — правый идеал в R, $\mathfrak{J}$ — радикал Джекобсона R, а M — артинов R-модуль. Тогда если $\mathrm{Ann}_M(\mathfrak{a}) \subsetneq M$, то $\mathrm{Ann}_M(\mathfrak{a}) \subsetneq \mathrm{Ann}_M(\mathfrak{a}\mathfrak{J})$.*

Доказательство. Пусть $N \subset M$ — минимальный подмодуль M, строго содержащий $\operatorname{Ann}_M(\mathfrak{a})$. Тогда $\mathfrak{J}N \subset \operatorname{Ann}_M(\mathfrak{a})$, то есть $\mathfrak{a}\mathfrak{J}N = 0$, так как $N/\operatorname{Ann}_M(\mathfrak{a})$ — простой R-модуль. □

Лемма 2. *Пусть R — ассоциативное унитальное артиново слева кольцо, а $\mathfrak{J}$ — радикал Джекобсона R. Тогда $\mathfrak{J}$ нильпотентен, то есть $\mathfrak{J}^n = 0$ для какого-то $n \in \mathbb{N}_1$.*

Доказательство. Так как R артиново слева, то ряд $\mathfrak{J} \supset \mathfrak{J}^2 \supset \mathfrak{J}^3 \supset \cdots$ стабилизируется на некотором $\mathfrak{J}^n$, где $n \in \mathbb{N}_1$. По лемме 1 идеал $\mathfrak{J}^n$ зануляет все артиновы R-модули, в частности, само R, откуда следует, что $\mathfrak{J}^n = 0$. □

Теорема 5 (Теорема Акидзуки – Хопкинса – Левицкого)**.** *Пусть R — ассоциативное унитальное артиново слева кольцо, а M — R-модуль. Тогда M нётеров тогда и только тогда, когда M артинов.*

Доказательство. Пусть $\mathfrak{J} \subset R$ — радикал Джекобсона R. По лемме 2 существует $n \in \mathbb{N}_1$, такое что $\mathfrak{J}^n = 0$. Тогда нётеровость/артиновость M эквивалентна нётеровости/артиновости каждого из присоединённых факторов фильтрации $M = \mathfrak{J}^0M \supset \mathfrak{J}^1M \supset \mathfrak{J}^2M \supset \cdots \supset \mathfrak{J}^nM = 0$, а эти факторы являются модулями над полупростым кольцом $R/\mathfrak{J}$, для которого нётеровость и артиновость модулей эквивалентна. □

Следствие 4. *Пусть R — ассоциативное унитальное артиново слева кольцо. Тогда R нётерово слева.*

Характеризация коммутативных артиновых колец

Теорема 6. *Ассоциативное коммутативное унитальное кольцо артиново тогда и только тогда, когда оно нётерово и нульмерно по Круллю.*

Доказательство (из двух частей).

Часть «только тогда». Пусть A — артиново ассоциативное коммутативное унитальное кольцо, а $\mathfrak{J}$ — радикал Джекобсона A. Согласно наблюдению 1 существует конечное множество $\mathcal{M}$ максимальных идеалов в A, такое что $\mathfrak{J} = \bigcap_{\mathfrak{m}\in\mathcal{M}} \mathfrak{m}$. Из леммы 2 и китайской теоремы об остатках следует, что $\mathfrak{J}^n = \prod_{\mathfrak{m}\in\mathcal{M}} \mathfrak{m}^n = 0$ для некоего $n \in \mathbb{N}_1$, и канонический

гомоморфизм $A \to \prod_{\mathfrak{m}\in\mathcal{M}} A/\mathfrak{m}^n$ биективен. Для любого $\mathfrak{m} \in \mathcal{M}$ в кольце $A/\mathfrak{m}^n$ один простой идеал — образ $\mathfrak{m}$. Факторы конечной фильтрации A-модуля $A/\mathfrak{m}^n$ образами степеней $\mathfrak{m}$ — это векторные пространства над полем $A/\mathfrak{m}$, для которых артиновость совпадает с нётеровостью. Учитывая, что артиновость и нётеровость стабильны относительно перехода к расширениями, подмодулям и фактормодулям, получаем, что артиновы кольца нульмерны и нётеровы.

Часть «тогда». В нётеровом ассоциативном коммутативном унитальном кольце нильрадикал нильпотентен и является конечным пересечением простых идеалов в соответствии с разложением на неприводимые компоненты, что в нульмерном случае позволяет применить рассуждение, аналогичное рассуждению из первой части доказательства. □

Наблюдение 4. Пусть A — ассоциативное коммутативное унитальное артиново кольцо. Тогда топологическое пространство $\mathrm{Spec}(A)$ дискретно, а потому $A \cong \prod_{\mathfrak{p}\in\mathrm{Spec}(A)} A_{\mathfrak{p}}$.

Наблюдение 5. Ассоциативные коммутативные унитальные локальные кольца, очевидно, не разлагаются в нетривиальное произведение колец. Поэтому разложение ассоциативного коммутативного унитального артинова кольца A в конечное произведение локальных колец является разложением на неразложимые, и, согласно следствию 9.1.2, его слагаемые однозначно определены как идеалы в A.

9.6. Теорема Крулля – Шмидта для модулей

Наблюдение 1. Пусть ψ — эндоморфизм абелевой группы V. Тогда утверждение $\mathrm{Ker}(\psi) \cap \mathrm{Im}(\psi) = 0$ эквивалентно утверждению $\mathrm{Ker}(\psi) = \mathrm{Ker}(\psi^{\circ 2})$, а утверждение $\mathrm{Ker}(\psi) + \mathrm{Im}(\psi) = V$ эквивалентно утверждению $\mathrm{Im}(\psi) = \mathrm{Im}(\psi^{\circ 2})$.

Лемма 1 (Лемма Фиттинга)**.** *Пусть M — нётеров и артинов модуль над ассоциативным унитальным кольцом R, а $\varphi \in \mathrm{End}_{R\text{-mod}}(M)$. Тогда существует $n \in \mathbb{N}_1$, такое что $M = \mathrm{Ker}(\varphi^{\circ n}) \oplus \mathrm{Im}(\varphi^{\circ n})$. В частности, если модуль M неразложим, то эндоморфизм φ либо является изоморфизмом, либо нильпотентен.*

Доказательство. Заметим, что так как модуль M нётеров и артинов, то ряды $\operatorname{Ker}(\varphi) \subset \operatorname{Ker}(\varphi^{\circ 2}) \subset \cdots$ и $\operatorname{Im}(\varphi) \supset \operatorname{Im}(\varphi^{\circ 2}) \supset \cdots$ стабилизируются, после чего применим наблюдение 1. □

Замечание 1. Если M — модуль над ассоциативным унитальным кольцом R, такой что все его эндоморфизмы либо нильпотентны, либо являются изоморфизмами, то M неразложим, так как у него не может быть нетривиального идемпотентного эндоморфизма.

Лемма 2. *Если все элементы ассоциативного унитального кольца R, которые не являются двусторонне обратимыми, являются нильпотентными, то они все лежат в радикале Джекобсона R. В частности, в этом случае суммы нильпотентов из R нильпотентны.*

Доказательство. Пусть $x \in R$ — нильпотент, а $a \in R$ — произвольный элемент. Так как x не обратим слева, то ax — тоже, откуда следует, что ax — нильпотент, откуда следует, что $1 - ax$ двусторонне обратим. □

Теорема 1 (Теорема Крулля–Шмидта)**.** *Пусть M — нётеров и артинов модуль над ассоциативным унитальным кольцом R, а $(V_i)_{i\in I}$ и $(U_j)_{j\in J}$ — два конечных семейства неразложимых подмодулей модуля M, такие что $M = \bigoplus_{i\in I} V_i = \bigoplus_{j\in J} U_j$. Тогда для любого $e \in I$ существует $r \in J$, такой что $M = V_e \oplus (\bigoplus_{j\in J\setminus\{r\}} U_j) = U_r \oplus (\bigoplus_{i\in I\setminus\{e\}} V_i)$.*

Доказательство. Для любых $e \in I$ и $r \in J$ через $\rho_{r,e} : V_e \to U_r$ обозначим отображение, проецирующее V_e в U_r вдоль $\bigoplus_{j\in J\setminus\{r\}} U_j$, а через $\pi_{e,r} : U_r \to V_e$ — отображение, проецирующее U_r в V_e вдоль $\bigoplus_{i\in I\setminus\{e\}} V_i$. Для произвольного $e \in I$ выполняется равенство $\operatorname{Id}_{V_e} = \sum_{j\in J} \pi_{e,j} \circ \rho_{j,e}$, из которого, согласно леммам 1 и 2, следует, что для какого-то $r \in J$ эндоморфизм $\pi_{e,r} \circ \rho_{r,e}$ является изоморфизмом, откуда, с учётом неразложимости U_r, следует, что отображения $\rho_{r,e}$ и $\pi_{e,r}$ являются изоморфизмами, а это утверждение эквивалентно утверждению, которое требуется доказать. □

Замечание 2. Помимо Вольфганга Крулля (1899–1971) и Отто Шмидта (1891–1956) в формулировке и доказательстве теоремы Крулля – Шмидта и её вариантов участвовали много математиков, в частности, Джозеф Веддербёрн (1882–1948) и Роберт Ремак (1888–1942).

Замечание 3. Между прочим, заметим, что доказательство теоремы 1 становится особенно простым, если предположить, что модуль M полупрост — отпадает необходимость в леммах 1 и 2.

Глава 10

Некоторые некоммутативные тождества

10.1. Тождества с сопряжением и мультипликативными коммутаторами

Данный подраздел представляет собой небольшую «шпаргалку», содержащую стандартные тождества с сопряжением и мультипликативными коммутаторами и их выводы. Мы используем правонормированные коммутаторы. В тождествах с левонормированными коммутаторами надо использовать сопряжение слева, а не справа, а также группировать кратные коммутаторы влево: [[,],], а не вправо: [, [,]].

$$a^b := b^{-1}ab,\ [a,b] := a^{-1}b^{-1}ab,\ ab = ba^b,\ a[a,b] = a^b,\ ba[a,b] = ab,$$
$$a^{bc} = (a^b)^c,\ (ab)^c = a^c b^c,\ [a,b]^{-1} = [b,a],\ [a,b]^g = [a^g, b^g].$$

$$a[a,bc] = a^{bc} = (a^b)^c = (a[a,b])^c = a^c[a,b]^c = a[a,c][a,b]^c \implies$$
$$\implies [a,bc] = [a,c][a,b]^c.$$

Обращением получаем: $[bc,a] = [b,a]^c[c,a]$.

Подставив $b = c^{-1}$, получаем: $[c,a] = [a,c^{-1}]^c$.

$$a(bc)[bc,a] = (bc)a \text{ (цикл } (a,b,c)) \implies$$
$$\implies abc[bc,a][ca,b][ab,c] = abc \implies [bc,a][ca,b][ab,c] = 1.$$

$$a^b[a^b,[b,c]] = (a^b)^{[b,c]} = a^{b[b,c]} = a^{b^c},$$
$$X := [a^b,[b,c]] = [a^b,[c,b^{-1}]^b] = [a,[c,b^{-1}]]^b,$$
$$bca^bX = bca^{b^c} = cb^ca^{b^c} = cab^c \text{ (цикл } (a,b,c))$$
$$\Downarrow$$
$$[a^b,[b,c]][b^c,[c,a]][c^a,[a,b]] = 1 \text{ (тождество Холла)},$$
$$[a,[c,b^{-1}]]^b[b,[a,c^{-1}]]^c[c,[b,a^{-1}]]^a = 1 \text{ (тождество Холла – Витта)}.$$

10.2. Тождества в алгебрах Ли и Йордана

Обозначение 1. Пусть R — кольцо. Введём обозначения $a* : R \to R$, $x \mapsto ax$ и $*a : R \to R$, $x \mapsto xa$, где $a \in R$.

Наблюдение 1. Пусть R — кольцо. Заметим, что $d \in \mathrm{End}_{\mathbb{Z}\text{-mod}}(R)$ является дифференцированием R тогда и только тогда, когда диаграмма (1), где mult — это отображение умножения в R, коммутативна.

$$\begin{array}{ccc} R \otimes_{\mathbb{Z}} R & \xrightarrow{\text{mult}} & R \\ {\scriptstyle d\otimes 1+1\otimes d}\downarrow & & \downarrow{\scriptstyle d} \\ R \otimes_{\mathbb{Z}} R & \xrightarrow{\text{mult}} & R \end{array} \tag{1}$$

Введём обозначения $\lambda(a) := a \otimes 1$ и $\rho(a) := 1 \otimes a$, где $a \in \mathrm{End}_{\mathbb{Z}\text{-mod}}(R)$. Тогда (2) — это, по сути, проверка того, что коммутатор дифференцирований является дифференцированием.

$$[\lambda(a)+\rho(a), \lambda(b)+\rho(b)] = [\lambda(a),\lambda(b)]+[\rho(a),\rho(b)] = \lambda([a,b])+\rho([a,b]) \tag{2}$$

Наблюдение 2. Пусть R — ассоциативное кольцо. Введём обозначения $\lambda(a) := a*$ и $\rho(a) := *(-a)$, где $a \in R$. Тогда (2) — это проверка того, что коммутатор в R удовлетворяет тождеству Якоби – Лейбница.

Наблюдение 3. Пусть R — ассоциативное кольцо. Тогда антикоммутатор в R, то есть йорданово умножение $(a,b) \mapsto a \circ b := ab+ba : R \times R \to R$,

удовлетворяет йорданову тождеству, потому что если $a \in R$ и $b \in R$ коммутируют, то $a*+*a$ и $b*+*b$ тоже коммутируют.

Наблюдение 4. Пусть R — кольцо. То, что $d \in \mathrm{End}_{\mathbb{Z}\text{-mod}}(R)$ является дифференцированием R, эквивалентно тому, что $[d, a*] = (da)*$ для любого $a \in R$.

Замечание 1. Например, в алгебре Вейля, то есть алгебре дифференциальных операторов с полиномиальными коэффициентами, выполняется соотношение $[\partial/\partial x, x] = 1$, невозможное для конечных матриц в характеристике 0, в чём можно убедиться, взяв след.

Наблюдение 5. Обычно $e^{a\otimes 1+1\otimes a} = e^a \otimes e^a$ и $e^{a*-*a} = e^a * \circ * e^{-a}$, когда эти выражения имеют смысл.

Наблюдение 6. Форма Киллинга — это след произведения. Взяв след от тождества $[a, bc] = [a, b]c + b[a, c]$, получаем её инвариантность.

Наблюдение 7. Если (3, слева) — коммутативная диаграмма модулей над ассоциативным коммутативным унитальным кольцом A, то (3, справа) — тоже.

$$\begin{array}{ccc} V & \xrightarrow{d'} & V \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ V & \xrightarrow{d} & V \end{array} \qquad\qquad \begin{array}{ccc} V \otimes_A V & \xrightarrow{d'\otimes 1+1\otimes d'} & V \otimes_A V \\ {\scriptstyle g\otimes g}\downarrow & & \downarrow{\scriptstyle g\otimes g} \\ V \otimes_A V & \xrightarrow{d\otimes 1+1\otimes d} & V \otimes_A V \end{array} \tag{3}$$

Наблюдение 8. Пусть R — алгебра над ассоциативным коммутативным унитальным кольцом A, отображение $d : R \to R$ — дифференцирование R над A, а a и b — элементы A. Тогда мы имеем коммутативную диаграмму (4), где mult — это отображение умножения в R, которая делает очевидной формулу (5), где $x, y \in R$, а $n \in \mathbb{N}_0$.

$$\begin{array}{ccc} R \otimes_A R & \xrightarrow{(d-a)\otimes 1+1\otimes(d-b)} & R \otimes_A R \\ {\scriptstyle \mathrm{mult}}\downarrow & & \downarrow{\scriptstyle \mathrm{mult}} \\ R & \xrightarrow{d-(a+b)} & R \end{array} \tag{4}$$

$$(d-(a+b))^n(xy) = \sum_{i=0}^{n} \binom{n}{i} ((d-a)^{n-i}(x))((d-b)^i(y)) \tag{5}$$

Наблюдение 9. Пусть $A \coloneqq K[X]/(X^p - 1)$, где K — поле характеристики $p \neq 0$, а $x \in A$ — образ $X \in K[X]$. Тогда у нас есть два K-линейных отображения: $x : A \to A$, $f \mapsto xf$ и $\partial/\partial x : A \to A$, $f \mapsto \partial f/\partial x$. Так как $[\partial/\partial x, x] = 1$, то $[x\partial/\partial x, x] = [x, x]\partial/\partial x + x[\partial/\partial x, x] = x$, поэтому x и $x\partial/\partial x$ порождают двумерную разрешимую подалгебру Ли в $\mathrm{End}_{K\text{-mod}}(A)$. Множество $\{x^n \mid 0 \leqslant n < p\} \subset A$ — является собственным базисом для $x\partial/\partial x$ с попарно различными собственными значениями, но в нём нет собственных векторов для $x : A \to A$. Следовательно, у эндоморфизмов x и $x\partial/\partial x$ нет общего собственного вектора.

Наблюдение 10. Пусть $R \coloneqq \mathbb{Q}\langle X, Y\rangle/(P \in \mathbb{Q}\langle X, Y\rangle \mid \deg(P) \geqslant 3)$ — алгебра усечённых многочленов от двух не коммутирующих переменных, а $x, y \in R$ — образы $X, Y \in \mathbb{Q}\langle X, Y\rangle$. Тогда, в понятном смысле, выполняются равенства $e^x e^y = e^{x+y+(1/2)(xy-yx)}$ и $e^x e^y e^{-x} e^{-y} = e^{xy-yx}$.

Замечание 2. Первая формула наблюдения 10 — это усечённая форма формулы Бейкера – Кэмпбелла – Хаусдорфа – Дынкина, полная версия которой формулируется и доказывается в разделе 10.3.

Следствие 1. *Пусть R — ассоциативное унитальное кольцо, а $x, y \in R$ — его элементы, такие что $x^2 = y^2 = xyx = yxy = 0$. Тогда, в понятном смысле, выполняется равенство $e^x e^y e^{-x} e^{-y} = e^{xy-yx}$.*

Пример 1. Пусть R — ассоциативное унитальное кольцо, $a_1, a_2 \in R$, а $\varepsilon_1, \varepsilon_2 \in R[E_1, E_2]/(E_1^2, E_2^2)$ — образы E_1 и E_2 соответственно. Тогда $e^{x_1} e^{x_2} e^{-x_1} e^{-x_2} = e^{x_1 x_2 - x_2 x_1}$, где $x_1 \coloneqq a_1\varepsilon_1$, $x_2 \coloneqq a_2\varepsilon_2$.

Пример 2. Пусть R — ассоциативное унитальное кольцо, I — конечное множество, $u_1, u_2 \in \mathrm{M}_{\mathtt{pt},I}(R)$ — две строки, а $v_1, v_2 \in \mathrm{M}_{I,\mathtt{pt}}(R)$ — два столбца, причём $u_1 v_1 = u_2 v_2 = u_1 v_2 = 0$. Тогда $e^{x_1} e^{x_2} e^{-x_1} e^{-x_2} = e^{x_1 x_2 - x_2 x_1}$, где $x_1 \coloneqq v_1 u_1$, $x_2 \coloneqq v_2 u_2$.

Замечание 3. Формула из примера 2 называется коммутационной формулой для трансвекций.

Наблюдение 11. Пусть V — конечномерное векторное пространство над полем K. Пусть $s : V \xrightarrow{\sim} V^\vee$ — невырожденная билинейная форма, $x : V \to V$ — линейное отображение, $x^\vee : V^\vee \to V^\vee$ — двойственное отображение. Форма s ли-инвариантна относительно x тогда и только

тогда, когда $sx + x^\vee s = 0$, то есть $sxs^{-1} = -x^\vee$. Взяв след, получаем равенство $\operatorname{tr}(x) = \operatorname{tr}(sxs^{-1}) = \operatorname{tr}(-x^\vee) = -\operatorname{tr}(x)$, то есть $2\operatorname{tr}(x) = 0$.

Наблюдение 12. Пусть $p \in \mathbb{N}_1$ — простое число, а $X, Y \in \mathbb{F}_p[X, Y]$ — коммутирующие переменные. Тогда $(X-Y)(X-Y)^{p-1} = (X-Y)^p = X^p - Y^p = (X-Y)(X^{p-1} + X^{p-2}Y + \cdots + XY^{p-2} + Y^{p-1})$, откуда следует, что $(X-Y)^{p-1} = X^{p-1} + X^{p-2}Y + \cdots + XY^{p-2} + Y^{p-1}$.

Наблюдение 13. Пусть $p \in \mathbb{N}_1$ — простое число, R — ассоциативная унитальная $\mathbb{F}_p$-алгебра, x — элемент R, а $D : R \to R$ — дифференцирование кольца R. Тогда, применив наблюдение 12, получаем формулу $\operatorname{ad}(x)^{p-1}(D(x)) = (x * - * x)^{p-1}(D(x)) = D(x^p)$, где $\operatorname{ad}(x) = [x, -]$.

Наблюдение 14. Пусть $p \in \mathbb{N}_1$ — простое число, а $X, Y, T \in \mathbb{F}_p\langle X, Y\rangle[T]$ — переменные. Тогда, продифференцировав тождество (6) по T, согласно наблюдению 13, получаем тождество (7).

$$(XT + Y)^p = X^pT^p + s_{p-1}(X, Y)T^{p-1} + \cdots + s_1(X, Y)T + Y^p \tag{6}$$

$$\underbrace{[XT + Y, [XT + Y, [XT + Y, \ldots, [XT + Y}_{p-1}, X]]] \ldots] = \\ = (p-1)s_{p-1}(X, Y)T^{p-2} + \cdots + 2s_2(X, Y)T + s_1(X, Y) \tag{7}$$

10.3. Формула Бейкера – Кэмпбелла – Хаусдорфа – Дынкина

Предисловие

Практически весь материал этого раздела позаимствован из раздела 6 текста [12], который содержит несколько доказательств теоремы Бейкера – Кэмпбелла – Хаусдорфа и её уточнений. Я узнал об этом тексте из учебника по алгебрам Ли и группам Ли П. Этингофа [17, Remark 14.8].

Критерии Фридрихса и Дынкина – Шпехта – Уивера

Определение 1. Пусть K — поле, а $\mathcal{X}$ — множество. Определим K-линейные отображения $D, R : K\langle\mathcal{X}\rangle \rightrightarrows K\langle\mathcal{X}\rangle$ на мономах следующим

образом: $D(X_1 \cdots X_n) = nX_1 \cdots X_n$ для любых $X_1, \ldots, X_n \in \mathcal{X}$, где $n \geqslant 0$, $R(1) = 0$, $R(X) = X$ для любого $X \in \mathcal{X}$, $R(X_1 \cdots X_n) = [X_1, [X_2, \ldots, [X_{n-1}, X_n]] \ldots]$ для любых $X_1, \ldots, X_n \in \mathcal{X}$, где $n \geqslant 2$.

Лемма 1. *Пусть K — поле, $\mathcal{X}$ — множество, а $(K\langle\mathcal{X}\rangle, \mu, \eta, \delta, \varepsilon, S)$ — это $K\langle\mathcal{X}\rangle$ со стандартной структурой алгебры Хопфа. Тогда*

$$\mu \circ (D \otimes S) \circ \delta = R. \tag{1}$$

Доказательство. Достаточно проверить формулу (1) на мономах. Равенство $(\mu \circ (D \otimes S) \circ \delta)(1) = R(1)$ проверяется непосредственно. Пусть $X_1, \ldots, X_n \in \mathcal{X}$, где $n \geqslant 1$. Тогда

$$(\mu \circ (D \otimes S) \circ \delta)(X_1 \cdots X_n) =$$

$$= \sum_{(c_1,\ldots,c_n)\in\{0,1\}^n} (-1)^{\sum_{i=1}^n (1-c_i)} \Big(\sum_{i=1}^n c_i\Big) X_1^{c_1} \cdots X_n^{c_n} X_n^{1-c_n} \cdots X_1^{1-c_1} =$$

$$= \sum_{(c_1,\ldots,c_n)\in\{0,1\}^n} (-1)^{\sum_{i=1}^n (1-c_i)} \Big(\sum_{i=1}^n c_i\Big) X_1^{c_1} \cdots X_{n-1}^{c_{n-1}} X_n X_{n-1}^{1-c_{n-1}} \cdots X_1^{1-c_1} =$$

$$= \sum_{(c_1,\ldots,c_{n-1})\in\{0,1\}^{n-1}} (-1)^{\sum_{i=1}^{n-1} (1-c_i)} X_1^{c_1} \cdots X_{n-1}^{c_{n-1}} X_n X_{n-1}^{1-c_{n-1}} \cdots X_1^{1-c_1} =$$

$$= R(X_1 \cdots X_n). \qquad \square$$

Теорема 1 (Критерии Фридрихса и Дынкина – Шпехта – Уивера)**.** *Пусть K — поле, характеристика которого равна нулю, $\mathcal{X}$ — множество, $(K\langle\mathcal{X}\rangle, \mu, \eta, \delta, \varepsilon, S)$ — это $K\langle\mathcal{X}\rangle$ со стандартной структурой алгебры Хопфа, а f — элемент $K\langle\mathcal{X}\rangle$. Тогда следующие условия эквивалентны:*

а) *Многочлен f является K-линейной комбинацией кратных коммутаторов элементов $\mathcal{X}$;*

б) *Выполняется равенство $\delta(f) = f \otimes 1 + 1 \otimes f$ (критерий Фридрихса);*

в) *Выполняются равенства $\varepsilon(f) = 0$ и $R(f) = D(f)$ (критерий Дынкина – Шпехта – Уивера).*

Доказательство. Импликация (в) $\Longrightarrow$ (а) очевидна, а импликация (а) $\Longrightarrow$ (б) следует из классической формулы $[g\otimes 1+1\otimes g, h\otimes 1+1\otimes h] = [g,h]\otimes 1 + 1\otimes [g,h]$, где $g,h\in K\langle\mathcal{X}\rangle$, — множество $\{d\in K\langle\mathcal{X}\rangle \mid \delta(d) = d\otimes 1 + 1\otimes d\}$ является подалгеброй Ли в $K\langle\mathcal{X}\rangle$. Осталось доказать импликацию (б) $\Longrightarrow$ (в). Пусть f удовлетворяет условию (б). Применяя отображение $\varepsilon\otimes \mathrm{Id}$ к обеим сторонам равенства $\delta(f) = f\otimes 1 + 1\otimes f$ получаем равенство $f = \varepsilon(f)1 + \varepsilon(1)f = \varepsilon(f) + f$, откуда следует, что $\varepsilon(f) = 0$. Подставив выражение $\delta(f) = f\otimes 1 + 1\otimes f$ в формулу (1), получаем, что $D(f) = D(f)S(1) + D(1)S(F) = R(f)$. □

Теорема Бейкера – Кэмпбелла – Хаусдорфа

Определение 2 (Ряд Бейкера – Кэмпбелла – Хаусдорфа)**.** Следующий формальный ряд называется *рядом Бейкера – Кэмпбелла – Хаусдорфа*:

$$\log(e^X e^Y) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k}\Big(\sum_{m,n=0}^{\infty}\frac{X^m Y^n}{m!n!} - 1\Big)^k = \\ = \sum_{k=1}^{\infty}\sum_{m_1+n_1>0}\cdots\sum_{m_k+n_k>0}\frac{(-1)^{k-1}}{k}\frac{X^{m_1}Y^{n_1}\cdots X^{m_k}Y^{n_k}}{m_1!n_1!\cdots m_k!n_k!}\in\mathbb{Q}\langle\langle X,Y\rangle\rangle. \tag{2}$$

Теорема 2 (Теорема Бейкера – Кэмпбелла – Хаусдорфа)**.** *Все однородные компоненты ряда Бейкера – Кэмпбелла – Хаусдорфа, то есть ряда* $\log(e^X e^Y)\in\mathbb{Q}\langle\langle X,Y\rangle\rangle$*, представляются в виде* $\mathbb{Q}$*-линейных комбинаций кратных коммутаторов переменных* X *и* Y*.*

Набросок доказательства. Гомоморфизм $\delta : \mathbb{Q}\langle X,Y\rangle \to \mathbb{Q}\langle X,Y\rangle^{\otimes_{\mathbb{Q}}2} \cong \mathbb{Q}\langle X_1,Y_1\rangle\langle X_2,Y_2\rangle$, переводящий X в $X\otimes 1 + 1\otimes X$, а Y в $Y\otimes 1 + 1\otimes Y$, имеет единственное продолжение до непрерывного в стандартной топологии на формальных рядах отображения $\delta : \mathbb{Q}\langle\langle X,Y\rangle\rangle \to \mathbb{Q}\langle\langle X_1,Y_1\rangle\rangle\langle\langle X_2,Y_2\rangle\rangle \cong \prod_{m,n=0}^{\infty}(\mathbb{Q}\langle X,Y\rangle_m \otimes_{\mathbb{Q}} \mathbb{Q}\langle X,Y\rangle_n) \supset \mathbb{Q}\langle\langle X,Y\rangle\rangle^{\otimes_{\mathbb{Q}}2}$. Осталось заметить, что экспонента задаёт биекцию между элементами $f\in\mathbb{Q}\langle\langle X,Y\rangle\rangle$ с постоянным членом 0, удовлетворяющими условию $\delta(f) = f\otimes 1 + 1\otimes f$, и элементами $g\in\mathbb{Q}\langle\langle X,Y\rangle\rangle$ с постоянным членом 1, удовлетворяющими условию $\delta(g) = g\otimes g$, а потом использовать теорему 1, а точнее, критерий Фридрихса. □

Формула Дынкина для ряда БКХ

Определение 3 (Идемпотент Дынкина)**.** Пусть K — поле характеристики ноль, а $\mathcal{X}$ — конечное множество. Тогда *идемпотентом Дынкина* называется K-линейное и непрерывное в стандартной топологии на $K\langle\langle\mathcal{X}\rangle\rangle$ отображение $P : K\langle\langle\mathcal{X}\rangle\rangle \to K\langle\langle\mathcal{X}\rangle\rangle$, такое что $P(X_1 \cdots X_n) = \frac{1}{n}R(X_1 \cdots X_n)$ для любых $X_1, \ldots, X_n \in \mathcal{X}$, где $n \geqslant 1$, а $P(1) = 0$.

Наблюдение 1. Пусть K — поле характеристики ноль, а $\mathcal{X}$ — конечное множество. Тогда идемпотент Дынкина $P : K\langle\langle\mathcal{X}\rangle\rangle \to K\langle\langle\mathcal{X}\rangle\rangle$ идемпотентен, то есть $P \circ P = P$, а образ P совпадает с рядами, все однородные компоненты которых представляются в виде K-линейных комбинаций кратных коммутаторов элементов $\mathcal{X}$.

Теорема 3 (Формула Дынкина)**.** *В кольце* $\mathbb{Q}\langle\langle X, Y\rangle\rangle$ *выполняется следующее соотношение, которое называется* формулой Дынкина для ряда Бейкера – Кэмпбелла – Хаусдорфа*, или же* формулой Бейкера – Кэмпбелла – Хаусдорфа – Дынкина*:*

$$\log(e^X e^Y) = \sum_{k=1}^{\infty} \sum_{m_1+n_1>0} \cdots \sum_{m_k+n_k>0} \frac{(-1)^{k-1}}{k \sum_{i=1}^{k}(m_i+n_i) \prod_{j=1}^{k} m_j! n_j!} \times$$
$$\times [\underbrace{X, [X, \ldots, [X}_{m_1}, [\underbrace{Y, [Y, \ldots, [Y}_{n_1}, \ldots, [\underbrace{X, [X, \ldots, [X}_{m_k}, [\underbrace{Y, [Y, \ldots, Y}_{n_k}]] \ldots]]. \tag{3}$$

Доказательство. Применим идемпотент Дынкина к формуле (2). □

Глава 11

Леммы из гомологической алгебры

11.1. Лемма о четырёх гомоморфизмах

Теорема 1 (4-Лемма)**.** *Пусть R — ассоциативное унитальное кольцо,* (1) *— коммутативный квадрат R-модулей, а $\rho : \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\alpha')$ и $\rho' : \mathrm{Coker}(\alpha) \to \mathrm{Coker}(\alpha')$ — индуцированные гомоморфизмы. Тогда одновременная сюръективность ρ и инъективность ρ' эквивалентна точности тотального комплекса* (2) *квадрата* (1) *в среднем члене.*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\beta'} \\ C & \xrightarrow{\alpha'} & D \end{array} \qquad (1) \qquad\qquad 0 \to A \xrightarrow{\alpha \bar{\times} \beta} B \oplus C \xrightarrow{(-\beta') \bar{\square} \alpha'} D \to 0 \qquad (2)$$

Доказательство. Пусть $\iota : C \to B \oplus C$ и $\pi : B \oplus C \to B$ — стандартные вложение и проекция, а $\mathfrak{B} \subset \mathfrak{Z} \subset B \oplus C$ — границы и циклы комплекса (2) в среднем члене. Тогда условие сюръективности ρ эквивалентно условию $\iota^{-1}(\mathfrak{B}) = \iota^{-1}(\mathfrak{Z})$, а инъективности ρ' — условию $\pi(\mathfrak{B}) = \pi(\mathfrak{Z})$. Эти два условия вместе эквивалентны условию $\mathfrak{B} = \mathfrak{Z}$. □

Наблюдение 1. В обозначениях теоремы 1 инъективность ρ эквивалентна точности (2) в A, а сюръективность ρ' — точности (2) в D.

Наблюдение 2. В обозначениях теоремы 1 декартовость/кодекартовость квадрата (1) эквивалентны точности слева/справа соответственно его тотального комплекса (2).

11.2. Квадрат суммы-пересечения

Теорема 1 (Квадрат суммы-пересечения). *Пусть $M, N \subset U$ — модули над ассоциативным унитальным кольцом R. Тогда имеем два следующих бидекартовых коммутативных квадрата, называемых «квадрат суммы-пересечения» и «факторквадрат суммы-пересечения»:*

$$\begin{array}{ccc} M\cap N & \hookrightarrow & M \\ \downarrow & & \downarrow \\ N & \hookrightarrow & M+N, \end{array} \qquad \begin{array}{ccc} U/(M\cap N) & \twoheadrightarrow & U/M \\ \downarrow & & \downarrow \\ U/N & \twoheadrightarrow & U/(M+N). \end{array}$$

Доказательство. Бидекартовость первого квадрата очевидна, например, пара элементов $m \in M$ и $n \in N$, имеющих одинаковый образ в $M+N$, является образом элемента из $M \cap N$, что доказывает точность тотального комплекса $0 \to M \cap N \to M \oplus N \to M + N \to 0$ в среднем члене. Второй квадрат является фактором U, то есть бидекартового квадрата, составленного из четырёх копий U и тождественных морфизмов, по первому квадрату. Осталось перейти к соответствующим тотальным комплексам и заметить, что фактор точного комплекса по точному подкомплексу точен. □

Следствие 1 (Изоморфизм суммы-пересечения). *В обозначениях теоремы 1 квадрат суммы-пересечения индуцирует следующий изоморфизм между коядрами: $M/(M \cap N) \xrightarrow{\sim} (M+N)/N$.*

11.3. Критерий Бэра инъективности модуля

Теорема 1 (Критерий Бэра). *Модуль Q над ассоциативным унитальным кольцом R является инъективным тогда и только тогда, когда для любого левого идеала $\mathfrak{I} \subset R$ любой гомоморфизм R-модулей $\mathfrak{I} \to Q$ продолжается до гомоморфизма R-модулей $R \to Q$.*

Доказательство. Часть «только тогда» напрямую следует из определения инъективности. Докажем часть «тогда». Пусть M — R-модуль. Пусть $\mathcal{S}$ — это множество гомоморфизмов из подмодулей модуля M в Q, упорядоченных так, что быть меньше значит быть ограничением. К $\mathcal{S}$ можно применить лемму Цорна, и получить, что каждый элемент $\mathcal{S}$ мажорируется максимальным. Пусть $f : N \to Q$, где $N \subset M$, — максимальный элемент $\mathcal{S}$. Пусть $N \neq M$. Пусть C — циклический подмодуль в M, порождённый некоторым $a \in M \setminus N$. По теореме о квадрате суммы-пересечения (теорема 11.2.1) сумма двух подмодулей является их абстрактной амальгамированной суммой над их пересечением, поэтому чтобы продолжить $f : N \to Q$ до гомоморфизма $N + C \to Q$, и, тем самым, прийти к противоречию, нам нужно найти гомоморфизм $C \to Q$, совпадающий с f на $N \cap C$. То есть нам достаточно доказать, что гомоморфизмы в Q продолжаются с подмодулей циклических модулей на сами циклические модули. Так как циклические модули изоморфны фактормодулям R, то нам достаточно доказать, что гомоморфизмы в Q продолжаются с подмодулей R на само R. □

Глава 12

Теория полей

12.1. Теория Галуа

Предисловие

Большинство материала этого раздела основано на курсе по теории Галуа М. Вербицкого [10]. Помимо этого использовался учебник Джеймса Милна [14].

Диагонализуемые алгебры и расширения Галуа

Определение 1 (Диагонализуемая алгебра)**.** Конечномерная ассоциативная коммутативная унитальная алгебра A над полем k называется *диагонализуемой* над полем K/k, если K-алгебра $K \otimes_k A$ изоморфна K-алгебре $K^{\times I}$ для какого-то конечного множества I.

Замечание 1. В ситуации определения 1 изоморфизм $K \otimes_k A \xrightarrow{\sim} K^{\times I}$ называется *диагонализацией*.

Определение 2 (Расширение Галуа)**.** Конечное расширение полей K/k называется *расширением Галуа*, если k-алгебра K диагонализуема над K.

Определение 3 (Группа Галуа)**.** Пусть K/k — конечное расширение Галуа. Тогда его *группой Галуа* называется группа $\mathrm{Aut}_{k\text{-ring}}(K)$.

Скрученное групповое кольцо

Определение 4 (Скрученное групповое кольцо)**.** Пусть R — ассоциативное унитальное кольцо, G — группа, а $\rho : G \to \mathrm{Aut}_{\mathrm{Ring}}(R)$, $g \mapsto (\lambda \mapsto {}^g\lambda)$ — действие G на R. Определим *скрученное групповое кольцо* $R[\rtimes_\rho G]$ как фактор копроизведения ассоциативных унитальных колец R и $\mathbb{Z}[G]$ по соотношениям $g\lambda = {}^g\lambda g$, где $g \in G$, $\lambda \in R$.

Замечание 2. Из определения 4 сразу следует, что модуль над скрученным групповым кольцом $R[\rtimes_\rho G]$ — это R-модуль с ρ-полулинейным действием G. Примером является само R с действием G.

Наблюдение 1. Если в условиях определения 4 кольцо R коммутативно, то антиавтоморфизмы $g \mapsto g^{-1} : G \xrightarrow{\sim} G^o$ и $\lambda \mapsto \lambda : R \xrightarrow{\sim} R^o$ порядка два индуцируют антиавтоморфизм $R[\rtimes G] \xrightarrow{\sim} R[\rtimes G]^o$ порядка два, который переводит $R[\rtimes G]^o$-модули в $R[\rtimes G]$-модули, и наоборот.

Наблюдение 2. В обозначениях определения 4 гомоморфизм R-модулей $(\alpha_g)_{g\in G} \mapsto \alpha_g g : R^{\oplus G} \to R[\rtimes_\rho G]$ биективен.

Изоморфизм диагонализации

Наблюдение 3. Пусть K — поле, а I — конечное множество. Тогда гомоморфизмы K-алгебр $K^{\times I} \to K$ — это в точности проекции на сомножители.

Теорема 1. *Пусть A — конечномерная ассоциативная коммутативная унитальная алгебра над полем k, а $\theta : K \otimes_k A \xrightarrow{\sim} K^{\times I}$ — её диагонализация над расширением полей K/k. Тогда существует единственная перенумерация $I \xrightarrow{\sim} S \coloneqq \mathrm{Hom}_{k\text{-ring}}(A, K)$, которая переводит в θ гомоморфизм K-алгебр $\alpha \otimes a \mapsto (\alpha\varphi(a))_{\varphi\in S} : K \otimes_k A \xrightarrow{\sim} K^{\times S}$.*

Доказательство. Нужной перенумерацией является сквозная биекция $I \xrightarrow{\sim} \mathrm{Hom}_{K\text{-ring}}(K^{\times I}, K) \xrightarrow{\sim} \mathrm{Hom}_{K\text{-ring}}(K \otimes_k A, K) \xrightarrow{\sim} \mathrm{Hom}_{k\text{-ring}}(A, K)$. Первая из этих трёх биекций взята из наблюдения 3, а последняя следует из универсального свойства тензорного произведения. □

Наблюдение 4. В обозначениях теоремы 1 группа $G \coloneqq \mathrm{Aut}_{k\text{-ring}}(K)$ действует на $K \otimes_k A$ через левый сомножитель. Помимо этого, действия G на S и K индуцируют действие G на $K^{\times S} = \mathrm{Map}(S, K)$ сопря-

жением. Изоморфизм диагонализации $K \otimes_k A \xrightarrow{\sim} K^{\times S}$ эквивариантен относительно этих действий.

Теорема 2. *Пусть K/k — конечное расширение Галуа, G — его группа Галуа, а $K[\rtimes G]$ — скрученное групповое кольцо. Тогда гомоморфизм $K[\rtimes G]$-бимодулей $\alpha \otimes \beta \mapsto \alpha(\sum_{g\in G} g)\beta : K \otimes_k K \to K[\rtimes G]$ биективен.*

Доказательство. Отображение из формулировки теоремы 2 получается композицией отображения из формулировки теоремы 1 для $A = K$ и биективного отображения $(\alpha_g)_{g\in G} \mapsto \sum_{g\in G} \alpha_g g : K^{\times G} \to K[\rtimes G]$. □

Замечание 3. Изоморфизм теоремы 2 тоже иногда будет называться изоморфизмом диагонализации.

Основная теорема теории Галуа

Обозначение 1 (Инварианты действия)**.** Если G — группа, действующая на множестве X, то $X^G := \{x \in X \mid g(x) = x \text{ для любого } g \in G\}$.

Лемма 1. *Пусть K/k — конечное расширение Галуа, G — его группа Галуа, а $H \subset G$ — её подгруппа. Тогда $K^H = k$ тогда и только тогда, когда $H = G$.*

Доказательство. Практически очевидно из следующей цепочки изоморфизмов: $K \otimes_k (K^H) \cong (K \otimes_k K)^{\{1\}\times H} \cong (K^{\times G})^{\{1\}\times H} \cong K^{\times(G/H)}$. □

Соглашение 1. Пусть K/k — расширение полей. Условимся, что структура K-алгебры на кольце $K \otimes_k K$ по умолчанию будет задаваться гомоморфизмом $\alpha \mapsto \alpha \otimes 1 : K \to K \otimes_k K$.

Теорема 3. *Пусть $k \subset E \subset K$ — последовательность вложенных полей, причём K/k — конечное расширение Галуа. Тогда K/E — конечное расширение Галуа.*

Доказательство. Очевидная сюръекция $K^{\times I} \cong K \otimes_k K \to K \otimes_E K$ алгебр над K индуцирует изоморфизм $K^{\times J} \cong K \otimes_E K$ алгебр над K для какого-то подмножества $J \subset I$. □

Теорема 4 (Основная теорема теории Галуа)**.** *Пусть K/k — конечное расширение Галуа, G — его группа Галуа, $\mathcal{G}$ — множество подгрупп группы G, а $\mathcal{K}$ — множество подполей поля K, содержащих поле k. Тогда отображения $H \mapsto K^H : \mathcal{G} \rightleftarrows \mathcal{K} : \mathrm{Aut}_{E\text{-ring}}(K) \hookleftarrow E$ являются взаимно обратными биекциями.*

Набросок доказательства. Утверждение тривиальным образом следует из теоремы 3 и леммы 1. □

Эквивалентность категорий

Теорема 5. *Пусть K/k — конечное расширение Галуа, G — его группа Галуа, $\mathcal{S}$ — категория конечных G-множеств, $\mathcal{A}$ — категория конечномерных ассоциативных коммутативных унитальных k-алгебр, диагонализуемых над K. Тогда функторы $\mathfrak{S} : \mathcal{A} \to \mathcal{S}^o$, $A \mapsto \mathrm{Hom}_{k\text{-ring}}(A, K)$ и $\mathfrak{A} : \mathcal{S}^o \to \mathcal{A}$, $S \mapsto \mathrm{Hom}_{G\text{-sets}}(S, K)$ корректно определены и вместе с очевидными естественными преобразованиями $\eta : \mathrm{Id}_{\mathcal{A}} \to \mathfrak{A} \circ \mathfrak{S}$ и $\varepsilon : \mathfrak{S} \circ \mathfrak{A} \to \mathrm{Id}_{\mathcal{S}^o}$ задают эквивалентность категорий.*

Доказательство. Во-первых, так как кольцо K целостно, то функтор $\mathrm{Hom}_{k\text{-ring}}(-, K) : k\text{-ring} \to G\text{-sets}^o$ сохраняет конечные произведения, а $\mathrm{Hom}_{G\text{-sets}}(-, K) : G\text{-sets}^o \to k\text{-ring}$ сохраняет их тавтологически.

Во-вторых, для любого G-множества вида G/H, где $H \subset G$ — подгруппа, выполняются изоморфизмы $\varphi \mapsto \varphi([1]) : \mathrm{Hom}_{G\text{-sets}}(G/H, K) \xrightarrow{\sim} K^H$ и $K \otimes_k (K^H) \cong (K \otimes_k K)^{\{1\}\times H} \cong (K^{\times G})^{\{1\}\times H} \cong K^{\times (G/H)}$.

В-третьих, для любого $A \in \mathrm{Ob}(\mathcal{A})$ выполняются изоморфизмы $A \cong (K \otimes_k A)^{G\times\{1\}} \cong (K^{\times \mathrm{Hom}_{k\text{-ring}}(A,K)})^{G\times\{1\}} \cong \mathrm{Map}(\mathrm{Hom}_{k\text{-ring}}(A, K), K)^G \cong \mathrm{Hom}_{G\text{-sets}}(\mathrm{Hom}_{k\text{-ring}}(A, K), K)$. □

Расширения Галуа как максимально симметричные расширения

Теорема 6. *Пусть K/k и E/k — два конечных расширения полей. Тогда если $|\mathrm{Hom}_{k\text{-ring}}(E, K)| = [E : k]$, то k-алгебра E диагонализуема над K.*

Доказательство (из пяти частей).

Часть 1. Сначала предположим, что расширение E/k примитивно и зафиксируем изоморфизм $E \xrightarrow{\sim} k[X]/P(X)$. Так как $|\mathrm{Hom}_{k\text{-ring}}(E, K)| =$

$[E : k]$, то $(P(X)) = (\prod_{\alpha\in S}(X-\alpha))$ в $K[X]$, где $S \subset K$. Получаем цепочку изоморфизмов $K \otimes_k E \xrightarrow{\sim} K \otimes_k (k[X]/P(X)) \xrightarrow{\sim} K[X]/P(X) \xrightarrow{\sim} K[X]/\prod_{\alpha\in S}(X-\alpha) \xrightarrow{\sim} \prod_{\alpha\in S}(K[X]/(X-\alpha)) \xrightarrow{\sim} \prod_{\alpha\in S} K$.

Часть 2. Теперь рассмотрим общий случай. Выберем башню полей $k = E_0 \subset E_1 \subset \cdots \subset E_n = E$, такую что для любого $i = 1, \ldots, n$ расширение E_i/E_{i-1} примитивно.

Часть 3. Из условия следует, что $|\mathrm{Hom}_{E_0\text{-ring}}(E_1, K)| = [E_1 : E_0]$, поэтому, согласно части 1, имеем следующий изоморфизм алгебр над K: $K \otimes_{E_0} E_1 \xrightarrow{\sim} \bigoplus_{\varphi\in\mathrm{Hom}_{E_0\text{-ring}}(E_1,K)} K_\varphi$, где K_φ — это копия K, рассмотренная как E_1-алгебра с помощью $\varphi : E_1 \to K$.

Часть 4. Естественно, из условия также следует, что для произвольного $\varphi \in \mathrm{Hom}_{E_0\text{-ring}}(E_1, K)$ выполняется равенство $|\mathrm{Hom}_{E_1\text{-ring}}(E_2, K_\varphi)| = [E_2 : E_1]$, поэтому, согласно части 1, имеем следующий изоморфизм алгебр над K: $K_\varphi \otimes_{E_1} E_2 \xrightarrow{\sim} \bigoplus_{\psi\in\mathrm{Hom}_{E_1\text{-ring}}(E_2,K_\varphi)} K_\psi$, где K_ψ — это копия K, рассмотренная как E_2-алгебра с помощью $\psi : E_2 \to K$.

Часть 5. Продолжая таким образом, мы с помощью полученных изоморфизмов и изоморфизмов дистрибутивности тензорного произведения диагонализуем K-алгебру $K \otimes_k E \cong K \otimes_{E_0} E_1 \otimes_{E_1} \cdots \otimes_{E_{n-1}} E_n$. □

Следствие 1. *Пусть K/k — конечное расширение полей, такое что $|\mathrm{Aut}_{k\text{-ring}}(K)| = [K : k]$. Тогда K/k — расширение Галуа.*

Расширения Галуа и сепарабельные многочлены

Теорема 7. *Пусть k — поле, $P(X) \in k[X]$ — многочлен, E/k — поле над k, порождённое как k-алгебра корнями $P(X)$ в E, а K/k — поле над k, такое что $P(X)$ разлагается на линейные множители в $K[X]$. Тогда $N := |\mathrm{Hom}_{k\text{-ring}}(E, K)| \geqslant 1$ и $N = [E : k]$, если $P(X)$ сепарабелен.*

Доказательство (из двух частей).

Часть 1. Выберем башню полей $k = E_0 \subset E_1 \subset \cdots \subset E_n = E$, такую что $E_i := E_{i-1}[x_i] \xleftarrow{\sim} E_{i-1}[X_i]/P_i(X_i) : x_i \leftarrow X_i$ и $P(x_i) = 0$ для любого индекса $i = 1, \ldots, n$.

Часть 2. Теперь заметим, что для любого $i = 1, \ldots, n$ и любого k-гомоморфизма $\varphi : E_{i-1} \to K$ многочлен ${}^{\varphi}P_i(X)$ делит $P(X) = {}^{\varphi}P(X)$ в ${}^{\varphi}E_{i-1}[X] \subset K[X]$, а потому ${}^{\varphi}P_i(X)$ разлагается на линейные множители в $K[X]$ и сепарабелен, если $P(X)$ сепарабелен, откуда следует, что φ имеет продолжение до $E_i \to K$ и имеет $[E_i : E_{i-1}] = \deg(P_i(X))$ продолжений до $E_i \to K$, если $P(X)$ сепарабелен. □

Теорема 8. *Пусть G — конечная группа, действующая на поле K, а $\alpha \in K$ — элемент K. Тогда многочлен $P(X) \coloneqq \prod_{\beta \in O}(X - \beta) \in K[X]$, где O — это орбита α под действием G, является минимальным многочленом α над $k \coloneqq K^G$.*

Доказательство. С одной стороны, очевидно, что все коэффициенты $P(X)$ инвариантны относительно действия G, а потому лежат в k. С другой стороны, очевидно, что любой многочлен из $k[X]$ с корнем α имеет в качестве корней все $\beta \in O$, а потому делится на $P(X)$. □

Теорема 9. *Пусть E/k — конечное расширение полей, порождённое сепарабельными элементами. Тогда существует конечное расширение полей K/k, такое что k-алгебра E диагонализуема над K, вкладывающееся в любое расширение полей K'/k, обладающее тем же свойством. Более того, такое K/k — расширение Галуа.*

Набросок доказательства. Пусть $B \subset E$ — конечное множество сепарабельных элементов расширения E/k, такое что $E = k[\beta \mid \beta \in B]$, а $\mathcal{P} \subset k[X]$ — это множество унитальных минимальных многочленов над k элементов B. Тогда в качестве K/k можно взять поле разложения над k сепарабельного многочлена $\prod_{P(X) \in \mathcal{P}} P(X) \in k[X]$. □

Следствие 2. *Конечное расширение полей, порождённое сепарабельными элементами, является сепарабельным расширением. Иначе говоря, сепарабельные элементы расширения полей образуют его подполе.*

12.2. Некоторые утверждения из теории полей

Существование алгебраического замыкания

Теорема 1. *Пусть k — поле. Тогда существует алгебраическое расширение полей k^{alg}/k, такое что k^{alg} алгебраически замкнуто.*

Доказательство. Заметим, что мощность любого алгебраического расширения k ограничена сверху мощностью $k[X]$. Пусть Ω — множество, такое что $k \subset \Omega$ и мощность Ω строго больше мощности любого алгебраического расширения k. Пусть $\mathcal{S}$ — это множество алгебраических расширений k, являющихся подмножествами Ω, упорядоченное так, что быть меньше значит быть подрасширением. Тогда к $\mathcal{S}$ можно применить лемму Цорна и получить, что в $\mathcal{S}$ существует максимальный элемент. Этот максимальный элемент можно взять в качестве k^{alg}. □

Теорема о примитивном элементе

Теорема 2 (Теорема о примитивном элементе)**.** *Пусть E/k — конечное сепарабельное расширение полей. Тогда существует $\alpha \in E$, такой что $E = k[\alpha]$.*

Доказательство. Если k конечно, а α — образующая группы $E^\times$, то $E = k[\alpha]$. Предположим, что k бесконечно. Так как поле E сепарабельно, то существует расширение полей K/k, такое что $|\mathrm{Hom}_{k\text{-ring}}(E, K)| = [E : k]$, например, минимальное расширение Галуа поля k, содержащее E, или алгебраическое замыкание k. Выберем конечное подмножество $B \subset E$, такое что $E = k[\beta \,|\, \beta \in B]$, и с помощью леммы 13.2.1 найдём элемент $\alpha \in \sum_{\beta \in B} k\beta$, такой что отображение ограничения $\varphi \mapsto \varphi|_{k[\alpha]} : \mathrm{Hom}_{k\text{-ring}}(E, K) \to \mathrm{Hom}_{k\text{-ring}}(k[\alpha], K)$ инъективно. Тогда $[k[\alpha] : k] \geqslant |\mathrm{Hom}_{k\text{-ring}}(k[\alpha], K)| \geqslant |\mathrm{Hom}_{k\text{-ring}}(E, K)| = [E : k] \geqslant [k[\alpha] : k]$, откуда следует, что $[k[\alpha] : k] = [E : k]$ и $k[\alpha] = E$. □

Теорема о нормальном базисе

Наблюдение 1. Пусть M и N — артиновы и нётеровы модули над ассоциативным унитальным кольцом R. Тогда если $M^{\otimes n} \simeq N^{\otimes n}$ для какого-то $n \in \mathbb{N}_1$, то $M \simeq N$ по теореме Крулля – Шмидта.

Теорема 3 (Теорема о нормальном базисе)**.** *Пусть K/k — конечное расширение Галуа с группой Галуа G. Тогда K изоморфно $k[G]$ как $k[G]$-модуль.*

Доказательство. Кольцо $k[G]$ действует на $K \otimes_k K$ через действие на левый сомножитель и действует на $K[\rtimes G]$ левым умножением, при-

чём эти действия согласованы с изоморфизмом диагонализации теоремы 12.1.2. Осталось заметить, что $K \otimes_k K \simeq K^{\oplus[K:k]}$ и $K[\rtimes G] \simeq k[G]^{\oplus[K:k]}$ как определённые выше $k[G]$-модули, а потому $K \simeq k[G]$ как $k[G]$-модуль по наблюдению 1. □

Замечание 1. Приведённое доказательство теоремы 3 следует доказательству из учебника [14, с. 70].

Теорема Дедекинда о независимости характеров

Теорема 4 (Теорема Дедекинда о независимости характеров)**.** *Пусть S — мультипликативная полугруппа, а K — поле. Тогда множество характеров $S \to K$, то есть мультипликативных гомоморфизмов из S в K, линейно независимо над K.*

Доказательство. Полугруппа S действует на множестве S слева левыми умножениями. Это действие индуцирует правое действие S на K-модуле $V \coloneqq K^{\times S}$. Любой характер $\chi : S \to K$ как элемент V является общим собственным вектором для S относительно собственного значения χ. Осталось применить теорему о том, что сумма собственных подпространств для различных собственных значений прямая. □

Замечание 2. Я узнал об этом подходе к доказательству теоремы 4 из видеозаписи [16, лекция 5, 1:06:40].

Теорема Артина

Лемма 1. *Пусть K — поле, а G — группа, действующая на K автоморфизмами. Пусть Ω — класс $K[\rtimes G]$-модулей, у которых все ненулевые подмодули содержат ненулевые G-инвариантные элементы. Тогда $K^{\oplus I} \in \Omega$ для любого конечного множества I.*

Доказательство. Очевидно, что $K \in \Omega$ и Ω замкнуто относительно расширений: подмодуль расширения V с помощью W либо имеет нетривиальное пересечение с W, либо изоморфен подмодулю V. □

Теорема 5 (Теорема Артина)**.** *Пусть K — поле, а G — конечная группа, действующая на K автоморфизмами. Тогда $[K : K^G] \leqslant |G|$.*

Доказательство. Нам нужно доказать, что любое семейство $(\alpha_i)_{i\in I} \in K^{\oplus I}$, где I — конечное множество, такое что $|I| > |G|$, линейно зависимо над K^G. Иначе говоря, уравнение $\sum_{i\in I} \alpha_i X_i = 0$ имеет нетривиальный G-инвариантный ноль в $K^{\oplus I}$. Заметим, что такой ноль должен являться нулём системы уравнений $(\sum_{i\in I} {}^g\alpha_i X_i = 0)_{g\in G}$. Множество нулей этой системы G-инвариантно, то есть является $K[\rtimes G]$-подмодулем $K^{\oplus I}$, причём ненулевым, так как число уравнений строго меньше числа переменных. Применение леммы 1 завершает доказательство. □

12.3. Базисы трансцендентности

Теорема 1. *Пусть K — поле, $k \subset K$ — его подполе, а $(x_i)_{i\in I}$ и $(y_j)_{j\in J}$ — два конечных семейства элементов K, такие что K алгебраично над $k(x_i \mid i \in I)$ и $(y_j)_{j\in J}$ алгебраически независимо над k. Тогда $|J| \leqslant |I|$.*

Доказательство. Докажем теорему индукцией по $|J|$. Случай $|J| = 0$ тривиален. Пусть $|J| > 0$. Выберем произвольный $e \in J$. Введём обозначение $k' \coloneqq k(y_e)$. Так как y_e алгебраичен над $k(x_i \mid i \in I)$, то между y_e и $(x_i)_{i\in I}$ существует соотношение $P \in k[Y_e, X_i \mid i \in I]$, такое что $\deg_{Y_e}(P) > 0$. Так как y_e не алгебраичен над k, то существует индекс $r \in I$, такой что $\deg_{X_r}(P) > 0$, откуда следует, что x_r алгебраичен над $k'(x_i \mid i \in I\setminus\{r\})$, а потому всё поле K алгебраично над $k'(x_i \mid i \in I\setminus\{r\})$, и мы можем по индукции применить теорему к семействам $(x_i)_{i\in I\setminus\{r\}}$ и $(y_j)_{j\in J\setminus\{e\}}$ элементов расширения полей K/k'. □

Определение 1 (Базис трансцендентности)**.** Если K — поле, а $k \subset K$ — его подполе, то максимальное алгебраически независимое над k подмножество K называется *базисом трансцендентности* K над k.

Наблюдение 1. Пусть K — поле, а $k \subset K$ — его подполе. Тогда базисы трансцендентности K над k — это в точности минимальные подмножества $S \subset K$, такие что K алгебраично над $k(s \mid s \in S)$.

Теорема 2. *Пусть K — поле, а $k \subset K$ — его подполе. Тогда все конечные базисы трансцендентности K над k равномощны.*

Доказательство. Теорема 2 следует из теоремы 1, точнее, даже эквивалентна ей. □

Пример 1. Пусть k — поле, $A \coloneqq k[X,Y,Z]/(XY,XZ)$, а x, y и z — это образы X, Y и Z соответственно в A. Тогда $\{x\}$ и $\{y,z\}$ — два максимальных алгебраически независимых над k подмножества A.

Замечание 1. Я узнал о примере 1 из ответа [11] на «Mathematics Stack Exchange».

Глава 13

Целая зависимость

13.1. Целое замыкание

Соглашение 1. В этом разделе все кольца и алгебры считаются ассоциативными, коммутативными и унитальными.

Определение 1 (Конечная алгебра)**.** Алгебра над кольцом A называется *конечной* над A, если она конечно порождена как A-модуль.

Теорема 1 (Джойн двух конечных подалгебр конечен)**.** *Пусть B — алгебра над кольцом A, а C и D — две её конечные подалгебры. Тогда джойн C и D в решётке подалгебр алгебры B конечен над A.*

Доказательство. Джойн C и D является образом индуцированного гомоморфизма $C \otimes_A D \to B$, а тензорное произведение конечно порождённых модулей является конечно порождённым модулем. □

Определение 2 (Целое замыкание)**.** Пусть B — алгебра над кольцом A. Объединение конечных подалгебр алгебры B называется *целым замыканием* A в B. По теореме 1 оно является подалгеброй в B.

Определение 3 (Целый элемент)**.** Пусть B — алгебра над кольцом A. Элемент $b \in B$ называется *целым* над A, если порождённая им подалгебра $A[b] \subset B$ конечна над A, или, эквивалентно, b является корнем унитального многочлена с коэффициентами в A, то есть $b^n = \sum_{i=0}^{n-1} a_i b^i$ для какого-то $n \in \mathbb{N}_1$ и каких-то $a_i \in A$, где $0 \leqslant i \leqslant n-1$.

Теорема 2 (Все элементы конечной алгебры целые)**.** *Пусть B — конечная алгебра над кольцом A. Тогда любой элемент $b \in B$ является целым над A.*

Первое доказательство. Применим теорему Гамильтона – Кэли к эндоморфизму $x \mapsto bx : B \to B$ конечно порождённого A-модуля B. □

Второе доказательство. Если кольцо A нётерово, то теорема верна автоматически. Сведём общий случай к этому.

Пусть $(b_i)_{i\in I}$ — конечное семейство образующих A-модуля B, содержащее b, а $(c_{i,j,k})_{i,j,k\in I}$ — семейство элементов A, такое что $b_i b_j = \sum_{k\in I} c_{i,j,k} b_k$ для всех $i, j \in I$. Тогда кольцо $A' := \mathbb{Z}[c_{i,j,k} \mid i, j, k \in I] \subset A$ нётерово, и b лежит в конечной A'-алгебре $\sum_{i\in I} A' b_i \subset B$. По предыдущему рассуждению элемент b целый над A', а потому и над A. □

Следствие 1. *Пусть B — алгебра над кольцом A. Тогда целое замыкание A в B состоит в точности из элементов B, целых над A.*

Замечание 1. Теорему 2 можно переформулировать следующим образом: «Конечно порождённая подалгебра конечной алгебры конечна».

Пример 1. Пусть M — конечно порождённый модуль над кольцом A, а N — подмодуль в M, который не является конечно порождённым. Тогда в соответствующем A-модулю M «тривиальном расширении с квадратом ноль» $A \oplus M$, которое является конечной A-алгеброй, содержится A-подалгебра $A \oplus N$, которая не является конечной.

13.2. Лемма Нётер о нормализации

Лемма 1. *Пусть $(P_j)_{j\in J}$ — конечное семейство ненулевых полиномов от конечного семейства переменных $(X_i)_{i\in I}$ с коэффициентами в бесконечном поле Q. Пусть $Z \subset Q$ — бесконечное подмножество Q. Тогда существует точка в Z^I, не являющаяся нулём ни одного из P_j.*

Доказательство. Зафиксируем $e \in I$. Для произвольного $j \in J$ многочлен P_j, рассмотренный как многочлен от X_e с коэффициентами в поле рациональных дробей $Q((X_i)_{i\in I\setminus\{e\}})$, имеет конечное число корней. Поэтому существует число $c \in Z$, такое что после подстановки $X_e = c$

во все многочлены семейства $(P_j)_{j\in J}$ они все останутся ненулевыми, и лемма доказывается индукцией по мощности I. □

Лемма 2. *Пусть K — ассоциативное коммутативное унитальное кольцо, I — конечное множество, а $f \in K[(X_i)_{i\in I}]$ — многочлен. Тогда для любого $e \in I$, такого что $\deg_{X_e}(f) > 0$, существуют автоморфизм $\varphi \in \mathrm{Aut}_{K\text{-ring}}(K[(X_i)_{i\in I}])$ и элементы $n \in \mathbb{N}_1$ и $c \in K \setminus \{0\}$, такие что выполняется равенство $\varphi(f) = cX_e^n + (\text{члены меньшей степени по } X_e)$.*

Доказательство. Для любого семейства $(m_i)_{i\in I\setminus\{e\}} \in (\mathbb{N}_1)^{I\setminus\{e\}}$ определён автоморфизм $\varphi : K[(X_i)_{i\in I}] \to K[(X_i)_{i\in I}]$, такой что $\varphi(X_e) = X_e$ и $\varphi(X_i) = X_i + X_e^{m_i}$ для любого $i \in I \setminus \{e\}$. Тогда для любого семейства $(n_i)_{i\in I} \in (\mathbb{N}_0)^I$ выполняется равенство

$$\varphi(\textstyle\prod_{i\in I} X_i^{n_i}) = X_e^{n_e+\sum_{i\in I\setminus\{e\}} n_i m_i} + (\text{члены меньшей степени по } X_e).$$

По лемме 1, взяв $Q = \mathbb{Q}$ и $Z = \mathbb{N}_1$, мы можем выбрать $(m_i)_{i\in I\setminus\{e\}}$ таким образом, чтобы степени по X_e образов различных мономов, входящих в f, были попарно различными, так как для любых двух различных семейств $(n'_i)_{i\in I}, (n''_i)_{i\in I} \in (\mathbb{N}_0)^I$ соответствующий многочлен

$$(n'_e + \textstyle\sum_{i\in I\setminus\{e\}} n'_i M_i) - (n''_e + \sum_{i\in I\setminus\{e\}} n''_i M_i) \in \mathbb{Q}[(M_i)_{i\in I\setminus\{e\}}]$$

не равен нулю. □

Доказательство для бесконечного поля. Предположим, что K — бесконечное поле. Для любого семейства $(\lambda_i)_{i\in I\setminus\{e\}} \in K^{I\setminus\{e\}}$ определён автоморфизм $\varphi : K[(X_i)_{i\in I}] \to K[(X_i)_{i\in I}]$, такой что $\varphi(X_e) = X_e$ и $\varphi(X_i) = X_i + \lambda_i X_e$ для любого $i \in I \setminus \{e\}$. Тогда для любого семейства $(n_i)_{i\in I} \in (\mathbb{N}_0)^I$ выполняется равенство

$$\varphi(\textstyle\prod_{i\in I} X_i^{n_i}) = (\prod_{i\in I\setminus\{e\}} \lambda_i^{n_i}) X_e^{\sum_{i\in I} n_i} + (\text{члены меньшей степени по } X_e).$$

Отсюда видно, что старший по X_e коэффициент $\varphi(f)$ является ненулевым полиномом от $(\lambda_i)_{i\in I\setminus\{e\}}$. По лемме 1, взяв $Q = K$ и $Z = K$, мы можем выбрать $(\lambda_i)_{i\in I\setminus\{e\}}$ таким образом, чтобы этот коэффициент был ненулевым. □

Теорема 1 (Лемма Нётер о нормализации)**.** *Пусть A — ненулевая ассоциативная коммутативная унитальная конечно порождённая алгебра над полем K. Тогда существует K-подалгебра алгебры A, изоморфная алгебре многочленов от конечного числа переменных с коэффициентами в K, над которой A конечна.*

Доказательство. Пусть $(x_i)_{i\in I}$ — это конечное семейство образующих A как K-алгебры, то есть гомоморфизм $\pi : K[(X_i)_{i\in I}] \to A$, такой что $\pi(X_i) = x_i$ для любого $i \in I$, сюръективен. Пусть $0 \neq f \in \mathrm{Ker}(\pi)$. Применив лемму 2, получаем цепочку гомоморфизмов

$$K[(X_i)_{i\in I\setminus\{e\}}] \xrightarrow{\bar{\iota}} K[(X_i)_{i\in I}]/(\varphi(f)) \xrightarrow[\sim]{\varphi^{-1}} K[(X_i)_{i\in I}]/(f) \xrightarrow{\bar{\pi}} A,$$

где гомоморфизм $\bar{\pi}$ индуцирован π, а гомоморфизм $\bar{\iota}$ индуцирован очевидным вложением $\iota : K[(X_i)_{i\in I\setminus\{e\}}] \to K[(X_i)_{i\in I}]$. Так как кольцо $K[(X_i)_{i\in I}]/(\varphi(f))$ конечно над $K[(X_i)_{i\in I\setminus\{e\}}]$, то A — тоже. Мы получили, что K-алгебра A конечна над K-алгеброй с меньшим числом образующих. Доказательство завершается по индукции. □

13.3. Теорема Гильберта о нулях

Обобщённая лемма Зарисского

Обозначение 1 (Поле частных)**.** Поле частных ассоциативного коммутативного унитального целостного кольца A обозначается $\mathrm{Frac}(A)$.

Определение 1 (Кольцо Джекобсона)**.** Ассоциативное коммутативное унитальное кольцо A называется *кольцом Гильберта* или *кольцом Джекобсона*, если любой простой идеал в A является пересечением всех содержащих его максимальных идеалов.

Теорема 1. *Пусть A — ассоциативное коммутативное унитальное целостное кольцо, такое что $\mathrm{Frac}(A)$ цело над A. Тогда $A = \mathrm{Frac}(A)$.*

Доказательство. Пусть $a \in A \setminus \{0\}$. Так как элемент $a^{-1} \in \mathrm{Frac}(A)$ целый над A, то $a^{-n} \in \sum_{i=0}^{n-1} Aa^{-i}$ для какого-то $n \in \mathbb{N}_1$. Умножив это соотношение на a^{n-1}, получаем, что $a^{-1} \in A$. □

Теорема 2. *Пусть ассоциативное коммутативное унитальное целостное кольцо B цело над своим подкольцом A. Тогда A является полем тогда и только тогда, когда B является полем.*

Доказательство. Если B — поле, то $\mathrm{Frac}(A) \subset B$ цело над A, а потому совпадает с A. Если A — поле, то, $\mathrm{Frac}(B)$ алгебраично над A, а потому цело над B, а потому совпадает с B. □

Наблюдение 1. Пусть A — ассоциативное коммутативное унитальное целостное кольцо. Тогда A-алгебра $\mathrm{Frac}(A)$ не является конечно порождённой тогда и только тогда, когда для любого $f \in A\setminus\{0\}$ кольцо $A[f^{-1}]$ не является полем, то есть для любого $f \in A\setminus\{0\}$ существует ненулевой простой идеал $\mathfrak{p} \subset A$, не содержащий f.

Замечание 1. Для полноты отметим, что ассоциативное коммутативное унитальное целостное кольцо A, такое что A-алгебра $\mathrm{Frac}(A)$ конечно порождена, называется *областью Голдмана* или *G-областью*.

Теорема 3. *Пусть K — поле. Тогда K-алгебра $\mathrm{Frac}(K[X]) = K(X)$ не является конечно порождённой.*

Доказательство. Достаточно доказать, что $K[X][f^{-1}] \neq K(X)$ для любого $f \in K[X] \setminus K$. Из элементов $K[X]$ обратимыми в $K[X][f^{-1}]$ становятся в точности делители степеней f, а, например, $(f-1) \nmid f^n$ для любого $n \in \mathbb{N}_0$, так как $f^n \equiv 1 \not\equiv 0 \pmod{(f-1)}$. □

Пример 1. Между прочим, $K[[X]][X^{-1}] = K((X))$ для любого поля K.

Теорема 4. *Ассоциативное коммутативное унитальное кольцо A является кольцом Джекобсона тогда и только тогда, когда для любого не максимального простого идеала $\mathfrak{p} \subset A$ соответствующая A-алгебра $\mathrm{Frac}(A/\mathfrak{p})$ не является конечно порождённой.*

Доказательство. Часть «только тогда» выводится из наблюдения 1. Докажем часть «тогда». Пусть $\mathfrak{p} \subset A$ — простой идеал, $A' := A/\mathfrak{p}$, $f \in A'\setminus\{0\}$, а $\mathfrak{m} \subset A'[f^{-1}]$ — максимальный идеал. Так как $A'[f^{-1}]/\mathfrak{m} \cong (A'/(A' \cap \mathfrak{m}))[f^{-1}]$ — поле, то, по условию, $A'/(A' \cap \mathfrak{m})$ — поле, а потому $A' \cap \mathfrak{m}$ — максимальный идеал в A', не содержащий f. □

Теорема 5 (Обобщённая лемма Зарисского). *Ассоциативное коммутативное унитальное кольцо A является кольцом Джекобсона тогда и только тогда, когда любая конечно порождённая A-алгебра K, которая является полем, конечна над A.*

Доказательство (из двух частей).

Часть «тогда». Пусть $\mathfrak{p} \subset A$ — простой идеал. Тогда если A-алгебра $\mathrm{Frac}(A/\mathfrak{p})$ является конечно порождённой, то, согласно условию, она конечна над A. По теореме 2 из этого следует, что $\mathfrak{p}$ — максимальный идеал. Согласно теореме 4 мы доказали, что A — кольцо Джекобсона.

Часть «только тогда». Сначала заметим, что можно заменить кольцо A на его образ в K, и считать, что $A \subset K$. Пусть $(x_i)_{i\in I}$ — конечное семейство элементов алгебры K, такое что $K = A[x_i \,|\, i \in I]$, а $(x_j)_{j\in J}$, где $J \subset I$, — максимальное алгебраически независимое над A подсемейство семейства $(x_i)_{i\in I}$. Для каждого индекса $i \in I \setminus J$ пусть $P_i \in A[x_j \,|\, j \in J][X_i]$ — какое-то нетривиальное алгебраическое соотношение между x_i и $(x_j)_{j\in J}$, а $f_i \in A[x_j \,|\, j \in J]$ — старший по X_i коэффициент P_i. Тогда поле K цело над кольцом $A' \coloneqq A[x_j \,|\, j \in J][f_i^{-1} \,|\, i \in I \setminus J]$, откуда, по теореме 2, следует, что $A' = \mathrm{Frac}(A)(x_j \,|\, j \in J)$. Так как A' конечно порождено как A-алгебра, то $A' = \mathrm{Frac}(A)$ согласно теореме 3 и $\mathrm{Frac}(A) = A$ согласно наблюдению 1. Мы доказали, что K — конечно порождённая целая, то есть конечная, алгебра над A. □

Классическая теорема о нулях

Теорема 6 (Nullstellensatz). *Пусть k — поле, k^{alg} — его алгебраическое замыкание, A — конечно порождённая ассоциативная коммутативная унитальная алгебра над k. Тогда максимальные идеалы $\mathfrak{m} \subset A$ — это в точности ядра гомоморфизмов $A \to k^{\mathrm{alg}}$ над k.*

Доказательство (из двух частей).

Часть 1. Пусть $\mathfrak{m} \subset A$ — максимальный идеал. Тогда поле $A/\mathfrak{m}$ является конечным расширением поля k по лемме Зарисского, следовательно, вкладывается в k^{alg} над k. Идеал $\mathfrak{m}$ является ядром сквозного гомоморфизма $A \to A/\mathfrak{m} \to k^{\mathrm{alg}}$.

Часть 2. Пусть $\varphi : A \to k^{\mathrm{alg}}$ — гомоморфизм над k. Так как k-алгебра k^{alg} целостная и целая над k, то её подалгебра $\varphi(A)$ — тоже, поэтому $\varphi(A)$ является полем по теореме 2. □

Следствие 1 («Сильная теорема о нулях»). *Пусть k — поле, k^{alg} — его алгебраическое замыкание, A — конечно порождённая ассоциативная коммутативная унитальная алгебра над k, а $f \in A$ — элемент A. Если для любого гомоморфизма $\varphi : A \to k^{\mathrm{alg}}$ над k выполняется равенство $\varphi(f) = 0$, то f — нильпотент.*

Доказательство. Пусть A_f — локализация A по f. Алгебра A_f является конечно порождённой алгеброй над k: в качестве её образующих можно взять f^{-1} и образующие A, но k-гомоморфизмов $A_f \to k^{\mathrm{alg}}$ не существует. Следовательно, $A_f = 0$, то есть $f \in A$ — нильпотент. □

Замечание 2. Приведённое доказательство следствия 1 иногда называют «трюком Рабиновича».

Замечание 3. Частным случаем следствия 1 в его же обозначениях является факт, что если k-гомоморфизмов $A \to k^{\mathrm{alg}}$ не существует, то все элементы A нильпотентны, то есть $A = 0$. Это объясняет название «сильная теорема о нулях».

Часть III

Совсем сырые или мелкие тексты

Глава 14

Сырые и мелкие тексты

14.1. Категория Лямбда

Категория элементов и колчан элементов

Определение 1 (Категория элементов)**.** Если $F : \mathcal{C} \to \mathrm{Sets}$ — функтор, то его *категорией элементов* называется категория $F \int_{\mathrm{Fun}(\mathcal{C},\mathrm{Sets})^o} \mathcal{C}$, которую можно отождествить с $\mathtt{pt} \int^F \mathcal{C}$ и с $\mathcal{C} \times^F_{\mathrm{Sets}} (\mathtt{pt} \int \mathrm{Sets})$.

Замечание 1. Иногда категория $(F \int \mathcal{C})^o \cong \mathcal{C}^o \int F = \mathcal{C}^o \int_{\mathrm{Fun}(\mathcal{C},\mathrm{Sets})} F$ тоже называется категорией элементов функтора $F : \mathcal{C} \to \mathrm{Sets}$.

Определение 2 (Колчан элементов)**.** Если $F : I \to \mathrm{Sets}$ — представление колчана I, то его *колчаном элементов* называется расслоенное произведение $I \times^F_{\mathrm{Sets}} (\mathtt{pt} \int \mathrm{Sets})$ в категории колчанов.

Определение 3 (Компоненты связности)**.** Будем называть *компонентами связности* категории слои универсального функтора из данной категории в дискретную категорию. Компоненты связности топологического пространства определяются аналогично.

Пример 1. Элементы копредела функтора $F : I \to \mathrm{Sets}$, где I — малая категория, можно интерпретировать как компоненты связности категории $F \int I$, а элементы предела — как сечения проекции $F \int I \to I$.

Пример 2. Если мы рассмотрим вложение Кэли группы как представление однообъектного группоида отображениями множеств, ограничим

его на подколчан и рассмотрим колчан элементов, то получится соответствующий граф Кэли.

Пример 3. Для представлений колчана-стрелки и колчана-петли отображениями множеств изображение колчана элементов даёт традиционные картинки, связанные с морфизмами и эндоморфизмами множеств.

Пример 4. Действие группы на множестве является транзитивным действием или орбитой тогда и только тогда, когда у соответствующего группоида элементов ровно одна компонента связности.

Определение категории Лямбда

Определение 4 (Циклинар)**.** Категория, свободно порождённая колчаном элементов стандартной циклической перестановки $x \mapsto x + 1$ множества $\mathbb{Z}/n\mathbb{Z}$, где $n \in \mathbb{N}_1$, обозначается через $[n]_\Lambda$ и называется *циклинаром* порядка n.

Замечание 2. Термин «циклинар» не стандартный и придуман по аналогии с термином «ординал». Я не знаю стандартного термина.

Наблюдение 1. Для категорий $[n]$ и $[n]_\Lambda$ число n — это количество стрелок в порождающем колчане. Порождающий колчан свободной категории однозначно восстанавливается по ней.

Обозначение 1 (Группоидофикация)**.** В этом разделе локализацию малой категории $\mathcal{C}$ по всем морфизмам будем обозначать через $\mathcal{C}^{\mathrm{grp}}$.

Наблюдение 2. Группа автоморфизмов категории $[n]_\Lambda$ — это циклическая группа порядка n. Группа автоморфизмов соответствующего группоида $[n]_\Lambda^{\mathrm{grp}}$ — это диэдральная группа порядка $2n$.

Замечание 3. Обратите внимание на группы $\mathrm{Aut}([2]_\Lambda^{\mathrm{grp}})$ и $\mathrm{Aut}([1]_\Lambda^{\mathrm{grp}})$!

Определение 5 (Строгость/полнота на эндоморфизмах)**.** Функтор $\varphi : \mathcal{C} \to \mathcal{E}$ называется *строгим/полным на эндоморфизмах*, если для любого $C \in \mathrm{Ob}(\mathcal{C})$ индуцированный гомоморфизм моноидов $\varphi_C : \mathrm{End}_{\mathcal{C}}(C) \to \mathrm{End}_{\mathcal{E}}(\varphi(C))$ инъективен/сюръективен соответственно.

Определение 6 (Категория Лямбда)**.** Категория, объектами которой являются циклинары $[n]_\Lambda$, где $n \in \mathbb{N}_1$, а морфизмами являются функторы, строгие и полные на эндоморфизмах, обозначается символом Λ и называется *категорией Лямбда*.

Лемма 1. *Пусть $\varphi : [n]_\Lambda \to [m]_\Lambda$, где $n, m \in \mathbb{N}_1$, — функтор. Тогда индуцированные гомоморфизмы свободных циклических моноидов $\varphi_x : \mathrm{End}_{[n]_\Lambda}(x) \to \mathrm{End}_{[m]_\Lambda}(\varphi(x))$, где $x \in \mathrm{Ob}([n]_\Lambda)$, изоморфны друг другу как объекты категории стрелок категории моноидов.*

Доказательство. Для индуцированного морфизма группоидов $\varphi^{\mathrm{grp}} : [n]_\Lambda^{\mathrm{grp}} \to [m]_\Lambda^{\mathrm{grp}}$ индуцированные гомоморфизмы свободных циклических групп $\varphi_x^{\mathrm{grp}} : \mathrm{End}_{[n]_\Lambda^{\mathrm{grp}}}(x) \to \mathrm{End}_{[m]_\Lambda^{\mathrm{grp}}}(\varphi(x))$, где $x \in \mathrm{Ob}([n]_\Lambda) = \mathrm{Ob}([n]_\Lambda^{\mathrm{grp}})$, изоморфны друг другу как объекты категории стрелок категории моноидов, так как все объекты категории $[n]_\Lambda^{\mathrm{grp}}$ изоморфны друг другу. Теперь заметим, что не изоморфные гомоморфизмы свободных циклических моноидов индуцируют не изоморфные гомоморфизмы свободных циклических групп. □

14.2. Топология Гротендика

Общее определение

Определение 1 (Замкнутая слева/справа подкатегория)**.** Подкатегория $\mathcal{C}$ категории $\mathcal{E}$ называется *замкнутой слева* или *влево*, если она содержит все морфизмы из $\mathcal{E}$, кообласти которых лежат в $\mathcal{C}$, и *замкнутой справа* или *вправо*, если $\mathcal{C}^o$ замкнута слева в $\mathcal{E}^o$.

Наблюдение 1. Замкнутая слева или справа подкатегория всегда является полной подкатегорией.

Наблюдение 2. Пусть $F : \mathcal{C} \to \mathcal{E}$ — функтор, а $\mathcal{E}'$ — замкнутая слева/справа подкатегория $\mathcal{E}$. Тогда $F^{-1}(\mathcal{E}')$ — замкнутая слева/справа соответственно подкатегория $\mathcal{C}$.

Определение 2 (Сито/решето)**.** *Ситом* или *решетом* на объекте данной категории называется замкнутая слева подкатегория категории объектов над ним.

Определение 3 (Главное сито)**.** Сито всех объектов над данным объектом называется *главным ситом* на нём.

Определение 4 (Ограничение сита)**.** Любой морфизм определяет функтор из категории объектов над своей областью в категорию объектов над своей кообластью. Соответствующий функтор прообраза для сит называется *функтором ограничения* вдоль данного морфизма.

Определение 5 (Топология Гротендика)**.** *Топология Гротендика* на данной категории задаётся классом сит на её объектах, называемых *покрывающими ситами*, удовлетворяющим следующим свойствам:

а) Главные сита являются покрывающими;

б) Ограничения покрывающих сит являются покрывающими;

в) Если ограничения сита вдоль всех объектов какого-то покрывающего сита являются покрывающими, то оно само является покрывающим.

Определение 6 (Сайт)**.** Категория, снабжённая топологией Гротендика, называется *сайтом*.

Определение 7 (Коаугментация функтора)**.** Назовём *коаугментацией* функтора ко-конус над функтором, то есть его естественное преобразование в какой-то постоянный функтор.

Определение 8 (Пучок на сайте)**.** Каждое сито на объекте данной категории снабжено тавтологическим коаугментированным функтором в эту категорию. Предпучок на сайте называется *пучком*, если он переводит коаугментированые функторы, соответствующие покрывающим ситам, в диаграммы пределов.

Случай топологического пространства

Определение 9 (Пучок на топологии)**.** Пусть T — топологическое пространство, а $\mathcal{C}$ — категория. Функтор $F : \mathrm{Open}(T)^o \to \mathcal{C}$ называется *пучком*, если он сохраняет пределы замкнутых вправо подкатегорий.

Определение 10 (Кофинальный функтор)**.** Функтор $F : J \to I$ называется *кофинальным*, если для любого $i \in I$ категория $i \int^F J$ связна, и называется *ко-кофинальным*, если функтор $F^o : J^o \to I^o$ кофинален.

Наблюдение 3. Пусть $\mathcal{S}$ — подмножество множества $\mathrm{Open}(T)$, где T — топологическое пространство. Тогда полная подкатегория в $\mathrm{Open}(T)$, заданная множеством объектов $\{U \cap V \in \mathrm{Open}(T) \mid U, V \in \mathcal{S}\}$, кофинальна в замкнутой влево подкатегории в $\mathrm{Open}(T)$, порождённой $\mathcal{S}$.

14.3. Спектральная последовательность фильтрации

Соглашение 1 (Кольцо дуальных чисел)**.** В этом разделе символ R будет обозначать фиксированное ассоциативное унитальное кольцо, $R[\partial]$ — кольцо $R[X]/(X^2)$, а ∂ — образ $X \in R[X]$ в $R[\partial]$.

Замечание 1. Модули над кольцом дуальных чисел иногда называются *дифференциальными модулями*. В такой терминологии комплексы соответствуют *дифференциальным градуированным модулям*, то есть $\mathbb{Z}$-градуированным модулям над $\mathbb{N}_0$-градуированным кольцом $R[\partial]$, где $\mathbb{N}_0$-градуировка на $R[\partial]$ унаследована от $R[X]$.

Наблюдение 1. Пусть $\cdots \subset C_i \subset C_{i+1} \subset \cdots$, где $i \in \mathbb{Z}$, — ряд $R[\partial]$-модулей, $\widetilde{Z}_i^r := C_i \cap \partial^{-1}(C_{i-r})$, $\widetilde{B}_i^r := C_i \cap \partial(C_{i+r-1})$, $Z_i^r := \widetilde{Z}_i^r / \widetilde{Z}_{i-1}^{r-1}$, $B_i^r := \widetilde{B}_i^r / \widetilde{B}_{i-1}^{r+1}$, где $i, r \in \mathbb{Z}$. Тогда оператор ∂ индуцирует гомоморфизмы $d_i^r : Z_i^r \to Z_{i-r}^r / B_{i-r}^r$ с ядром Z_i^{r+1} и образом $B_{i-r}^{r+1} / B_{i-r}^r$.

Замечание 2. Чтобы доказать утверждение наблюдения 1 достаточно заметить, что ∂ индуцирует изоморфизмы $\widetilde{Z}_i^r / \widetilde{Z}_i^{r+1} \xrightarrow{\sim} \widetilde{B}_{i-r}^{r+1} / \widetilde{B}_{i-r-1}^{r+2}$, переводящие классы элементов $\widetilde{Z}_{i-1}^{r-1}$ в классы элементов $\widetilde{B}_{i-r}^r = \partial(\widetilde{Z}_{i-1}^{r-1})$.

Определение 1 (Спектральная последовательность фильтрации)**.** В обозначениях наблюдения 1 семейство $(E_i^r, d_i^r, \rho_i^r)_{i \in \mathbb{Z}, r \in \mathbb{N}_0}$, где $E_i^r := Z_i^r / B_i^r$, гомоморфизм $d_i^r : E_i^r \to E_{i-r}^r$ индуцирован d_i^r, а ρ_i^r — это очевидный изоморфизм $\mathrm{Ker}(d_i^r) / \mathrm{Im}(d_{i+r}^r) \xrightarrow{\sim} E_i^{r+1}$, называется *спектральной последовательностью фильтрации* $(C_i)_{i \in \mathbb{Z}}$.

14.4. Универсумы Гротендика

Соглашение 1. Множества, которые являются элементами $\mathcal{U}$, иногда будут называться $\mathcal{U}$-множествами. Это соглашение будет, как правило, применятся тогда, когда $\mathcal{U}$ — универсум.

Определение 1 (Универсум Гротендика)**.** Множество $\mathcal{U}$ называется *универсумом Гротендика* или просто *универсумом*, если выполняются следующие три условия:

а) Объединение всех $\mathcal{U}$-множеств совпадает с $\mathcal{U}$;

б) Для любого $\mathcal{U}$-множества множество всех его подмножеств является $\mathcal{U}$-множеством;

в) Объединение любого индексированного $\mathcal{U}$-множеством семейства $\mathcal{U}$-множеств является $\mathcal{U}$-множеством.

14.5. Категорный цилиндр

Определение и основные свойства цилиндра

Определение 1 (Категорный цилиндр)**.** Назовём *цилиндром* диаграммы категорий и функторов $\mathcal{C} \xleftarrow{\varpi} \mathcal{B} \xrightarrow{\varrho} \mathcal{E}$ категорию $\mathrm{Cyl}(\mathcal{C} \overset{\varpi}{\leftarrow}\!|^{\varrho}_{\mathcal{B}} \mathcal{E}) \coloneqq ((\mathcal{C} \times \{0\}) \sqcup (\mathcal{E} \times \{1\})) \sqcup_{(\mathcal{B}\times\{0\})\sqcup(\mathcal{B}\times\{1\})} (\mathcal{B} \times [1])$.

Замечание 1. Понятие категорного цилиндра в некотором смысле является двойственным понятию комма-категории.

Наблюдение 1. Если $\mathcal{C} \xleftarrow{\varpi} \mathcal{B} \xrightarrow{\varrho} \mathcal{E}$ — диаграмма категорий, то её цилиндр автоматически снабжён функтором $\mathrm{Cyl}(\mathcal{C} \overset{\varpi}{\leftarrow}\!|^{\varrho}_{\mathcal{B}} \mathcal{E}) \to [1]$, слои которого отождествляются с $\mathcal{C} \cong \mathcal{C} \times \{0\}$ и $\mathcal{E} \cong \mathcal{E} \times \{1\}$ соответственно.

Наблюдение 2. Пусть $\mathcal{S} \to [1]$ — функтор, а $\mathcal{S}_0$ и $\mathcal{S}_1$ — его слои над 0 и 1 соответственно. Тогда $\mathcal{S} \cong \mathrm{Cyl}(\mathcal{S}_0 \,|_{\mathcal{S}_0 \lceil_{\mathcal{S}} \mathcal{S}_1}\, \mathcal{S}_1)$.

Определение 2 (Образующие цилиндра)**.** Если $\mathrm{Cyl}(\mathcal{C} \overset{\varpi}{\leftarrow}\!|^{\varrho}_{\mathcal{B}} \mathcal{E})$ — цилиндр диаграммы $\mathcal{C} \xleftarrow{\varpi} \mathcal{B} \xrightarrow{\varrho} \mathcal{E}$, то компоненты естественного преобразования $\mathcal{B} \times [1] \to \mathrm{Cyl}(\mathcal{C} \overset{\varpi}{\leftarrow}\!|^{\varrho}_{\mathcal{B}} \mathcal{E})$ называются его *образующими*.

Наблюдение 3. Пусть $F : \mathcal{C} \to I$ — функтор. Тогда $\mathrm{Cyl}(\mathcal{C} \mid^F I)$ существует и любой морфизм $\varphi : c \to i$ в $\mathrm{Cyl}(\mathcal{C} \mid^F I)$, где $c \in \mathcal{C}$, $i \in I$, единственным образом пропускается через образующую $\overrightarrow{F}(c) : c \to F(c)$.

Наблюдение 4. Пусть функторы $\alpha : \mathcal{C} \to \mathcal{C}'$, $\beta : \mathcal{E} \to \mathcal{E}'$ и $\gamma : \mathcal{B} \to \mathcal{B}'$ — компоненты морфизма из диаграммы категорий $\mathcal{C} \xleftarrow{\varpi} \mathcal{B} \xrightarrow{\varrho} \mathcal{E}$ в диаграмму категорий $\mathcal{C}' \xleftarrow{\varpi'} \mathcal{B}' \xrightarrow{\varrho'} \mathcal{E}'$. Тогда α, β и γ индуцируют функтор $\mathrm{Cyl}(\alpha \mid_\gamma \beta) : \mathrm{Cyl}(\mathcal{C} \,{}^{\varpi}|^{\varrho}_{\mathcal{B}}\, \mathcal{E}) \to \mathrm{Cyl}(\mathcal{C}' \,{}^{\varpi'}|^{\varrho'}_{\mathcal{B}'}\, \mathcal{E}')$.

Пример 1. Пусть $\rho : \mathcal{C} \to \mathcal{E}$ — функтор. В качестве иллюстрации к введённым обозначениям приведём следующий декартов квадрат:

$$\begin{array}{ccc} \mathrm{Cyl}(\mathcal{C} \mid^{\rho}_{\mathcal{C}} \mathcal{E}) & \xrightarrow{\mathrm{Cyl}(\mathrm{Id}|_{\mathrm{Id}}(\mathcal{E}\to\mathtt{pt}))} & \mathrm{Cyl}(\mathcal{C} \mid_{\mathcal{C}} \mathtt{pt}) \\ {\scriptstyle \mathrm{Cyl}(\rho|_{\rho}\mathrm{Id})}\downarrow & & \downarrow{\scriptstyle \mathrm{Cyl}(\rho|_{\rho}\mathrm{Id})} \\ \mathrm{Cyl}(\mathcal{E} \mid_{\mathcal{E}} \mathcal{E}) & \xrightarrow{\mathrm{Cyl}(\mathrm{Id}|_{\mathrm{Id}}(\mathcal{E}\to\mathtt{pt}))} & \mathrm{Cyl}(\mathcal{E} \mid_{\mathcal{E}} \mathtt{pt}). \end{array}$$

Определение расслоения Гротендика

Определение 3 (Замкнутость относительно пуллбэков)**.** Если $\mathcal{C}$ — категория, а B и P — два класса морфизмов в $\mathcal{C}$, то P называется замкнутым относительно пуллбэков вдоль морфизмов из B, если любая диаграмма вида $\beta : c' \to c \leftarrow c'' : \pi$, где $\pi \in P$, а $\beta \in B$, достраивается до декартового квадрата, в котором морфизм $c' \times_c c'' \to c'$ лежит в P.

Определение 4 (Расслоение Гротендика)**.** Функтор $F : \mathcal{C} \to I$ называется *расслоением Гротендика*, если класс образующих цилиндра $\mathrm{Cyl}(\mathcal{C} \mid^F I)$ замкнут относительно пуллбэков вдоль морфизмов из I.

Определение 5 (Расслоение Стрита)**.** Функтор $F : \mathcal{C} \to I$ называется *расслоением Стрита* или *расслоением Стрита-Гротендика*, если класс композиций образующих и изоморфизмов в $\mathrm{Cyl}(\mathcal{C} \mid^F I)$ замкнут относительно пуллбэков вдоль морфизмов из I.

14.6. Окольцованный спектр кольца

Леммы о покрытиях локализациями

Соглашение 1. В этом подразделе A — это фиксированное коммутативное ассоциативное унитальное кольцо, а $(S_i)_{i\in I}$ — семейство мультипликативных подмножеств A, такое что множества $\operatorname{Spec}(A_{S_i})$ покрывают множество $\operatorname{Spec}(A)$.

Лемма 1. *Пусть M — A-модуль. Тогда канонический гомоморфизм $m \mapsto (\frac{m}{1})_{i\in I} : M \to \prod_{i\in I} M_{S_i}$ инъективен.*

Доказательство. Пусть $m \in M$ переходит в 0 во всех M_{S_i}. Тогда аннулятор m в A не дизъюнктен ни с каким из S_i, а потому не содержится ни в каком простом идеале кольца A, а потому равен A. □

Следствие 1. *Пусть M — A-модуль. Тогда если $M_{S_i} = 0$ для всех $i \in I$, то $M = 0$.*

Следствие 2. *Пусть $M^\bullet$ — коцепной комплекс A-модулей. Тогда если $(\mathrm{H}^0(M^\bullet))_{S_i} \cong \mathrm{H}^0(M^\bullet_{S_i}) = 0$ для всех $i \in I$, то $\mathrm{H}^0(M^\bullet) = 0$.*

Наблюдение 1. Пусть $S_1, S_2 \subset A$ — мультипликативные множества, M — A-модуль, $\frac{m_1}{s_1} \in M_{S_1}$ и $\frac{m_2}{s_2} \in M_{S_2}$. Тогда если $\frac{m_1}{s_1} = \frac{m_2}{s_2}$ в $M_{S_1S_2}$, то существуют $r_1 \in S_1$ и $r_2 \in S_2$, такие что для формальных дробей $\frac{r_1m_1}{r_1s_1}$ и $\frac{r_2m_2}{r_2s_2}$ выполняется равенство $(r_2s_2)(r_1m_1) = (r_1s_1)(r_2m_2)$.

Лемма 2. *Пусть M — A-модуль. Пусть множество I конечно. Тогда гомоморфизм $M \xrightarrow{\iota} M' := \operatorname{Ker}(\prod_{i\in I} M_{S_i} \xrightarrow{\alpha} \prod_{(i,j)\in I\times I} M_{S_iS_j})$, где $\iota(m) := (\frac{m}{1})_{i\in I}$, а $\alpha((\frac{m_i}{s_i})_{i\in I}) := (\frac{m_i}{s_i} - \frac{m_j}{s_j})_{(i,j)\in I\times I}$, биективен.*

Первое доказательство. После применения функтора локализации по S_e для произвольного $e \in I$ заданная гомоморфизмами ι и α короткая последовательность $M \to \bigoplus_{i\in I} M_{S_i} \to \bigoplus_{(i,j)\in I\times I} M_{S_iS_j}$ станет точной слева по тривиальным причинам. Осталось применить следствие 2. □

Второе доказательство. Инъективность ι следует из леммы 1. Докажем сюръективность ι. Пусть $(\frac{m_i}{s_i})_{i\in I} \in M'$. Тогда, согласно наблюдению 1, можно предположить, что $s_im_j = s_jm_i$ для любых $i, j \in I$.

Выберем семейство $(a_i)_{i\in I}$ элементов A, такое что $\sum_{i\in I} s_i a_i = 1$. Возьмём $m \coloneqq \sum_{i\in I} a_i m_i \in M$. Тогда $s_i m = \sum_{j\in I} s_i a_j m_j = \sum_{j\in I} s_j a_j m_i = m_i$ для любого $i \in I$, откуда следует, что образ m в M' равен $(\frac{m_i}{s_i})_{i\in I}$. □

Замечание 1. Первое доказательство леммы 2 основано на доказательстве леммы 7.13 из [7, лекция 7].

Определение окольцованного спектра

Наблюдение 2. Если база топологии состоит из компактных подмножеств, то условия отделимости и склейки для предпучков на этой базе достаточно проверять для конечных покрытий.

Определение 1 (Окольцованный спектр)**.** Если A — ассоциативное коммутативное унитальное кольцо, то его *окольцованным спектром* называется топологическое пространство $X \coloneqq \mathrm{Spec}(A)$, снабжённое пучком колец $\mathcal{O}_X$, заданным на стандартной базе топологии Зарисского равенствами $\mathcal{O}_X(D(f)) \coloneqq A_{A\setminus(\bigcup_{\mathfrak{p}\in D(f)}\mathfrak{p})} \cong A_f$, где $f \in A$, и отображениями ограничения, являющимися гомоморфизмами A-алгебр.

Замечание 2. В случае определения 1 с учётом наблюдения 2 условия отделимости и склейки следуют из леммы 2.

14.7. Мнемоники о единицах измерения

Наблюдение 1 (Метр)**.** Один метр — это примерно одна десятимиллионная расстояния между полюсом и экватором по поверхности сферического приближения к Земле. Десять — это количество пальцев на обеих руках человека, а семь нулей нужны для того, чтобы метр был максимально близок к росту человека.

Наблюдение 2 (Человек, клетка и атом)**.** Размер человека — примерно 1 метр. Размер атома — примерно 1 ангстрем, то есть 10^{-10} метра. Размер клетки составляет примерно 1 «сотку», то есть одну сотую миллиметра, то есть 10^{-5} метра — ровно посередине между метром и ангстремом.[1] Сотка приблизительно совпадает с толщиной стандартной бытовой алюминиевой фольги.

[1]Разумеется, у разных клеток разный размер. Например, человеческая яйцеклетка

имеет диаметр примерно в одну десятую миллиметра и видна невооружённым глазом как маленькая песчинка.

Глава 15

Совсем мелкие тексты

15.1. Не сгруппированные мелочи I

Наблюдение 1 (Предупорядочения и упорядочения)**.** Если рассматривать предупорядоченные множества как категории, то это в точности категории, эквивалентные частично упорядоченным множествам.

Наблюдение 2 (Решётка разбиений)**.** Разбиения данного множества образуют полную решётку, так же, как и подмножества.

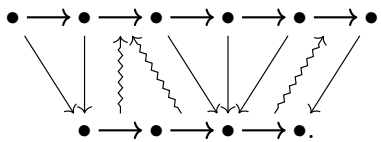
Соглашение 1 (Кольцоиды)**.** Категории, обогащённые структурой абелевой группы/моноида на Hom-ах, стоит называть *кольцоидами*/*полукольцоидами*, а не аддитивными/преаддитивными категориями.

Определение 1 (p-Адическая норма)**.** Пусть $p \in \mathbb{Z}$ — простое число. Норма $x \mapsto \|x\|_p : \mathbb{Q} \to \mathbb{R}$, такая что $\|p\|_p = p^{-1}$ и $\|l\|_p = 1$ для любого простого $l \in \mathbb{Z}$, отличного от p, называется *p-адической нормой*.

Наблюдение 3 (Базис лежит в полупространстве)**.** Пусть $(e_i)_{i\in I}$ — произвольный базис в евклидовом пространстве E. Тогда существует вектор $v \in E$, такой что $\langle v, e_i\rangle = 1 > 0$ для любого $i \in I$, потому что структурная билинейная форма в E невырождена.

Наблюдение 4. Разложение конечномерной полупростой алгебры Ли над алгебраически замкнутым полем характеристики ноль в прямую сумму простых идеалов очень каноническое.

Наблюдение 5. Дуальность Жуаяля можно иллюстрировать так:



Факт 1. Гаусс обнаружил следующую формулу для $16\cos(2\pi/17)$:

$$\sqrt{17}-1+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

Наблюдение 6. Выполняется следующая важная формула для элементарных трансвекций, где $ab=ba=-1$:

$$\begin{pmatrix}1&a\\0&1\end{pmatrix}\begin{pmatrix}1&0\\b&1\end{pmatrix}\begin{pmatrix}1&a\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\b&1\end{pmatrix}\begin{pmatrix}1&a\\0&1\end{pmatrix}\begin{pmatrix}1&0\\b&1\end{pmatrix}=\begin{pmatrix}0&a\\b&0\end{pmatrix}.$$

Наблюдение 7 (Тождества Ньютона – Жирара)**.** Зная, что логарифмическая производная геометрической прогрессии равна ей самой, получаем:

$$-t\frac{d}{dt}\log\prod_{\lambda\in\Lambda}(1-\lambda t)=\frac{-t\frac{d}{dt}\prod_{\lambda\in\Lambda}(1-\lambda t)}{\prod_{\lambda\in\Lambda}(1-\lambda t)}=\sum_{\lambda\in\Lambda}\sum_{n\geqslant 1}\lambda^n t^n\implies$$

$$\implies -k\sigma_k=\sum_{i=1}^{k}\gamma_i\sigma_{k-i},\text{ где }\prod_{\lambda\in\Lambda}(1-\lambda t)=\sum_{n\geqslant 0}\sigma_n t^n,\ \gamma_n\coloneqq\sum_{\lambda\in\Lambda}\lambda^n.$$

Обозначение 1. В обозначениях $N\rtimes H$ и $N\ltimes H$ активная группа тычет вилками в пассивную.

Наблюдение 8. Закон инерции Сильвестра абсолютно тривиален: у положительного и отрицательного подпространства тривиальное пересечение, поэтому сумма их размерностей меньше или равна размерности всего пространства.

Наблюдение 9. Евклидово самосопряжённый оператор расширением скаляров даёт положительно эрмитово самосопряжённый оператор, а у таких операторов все собственные числа вещественные. Для самосопряжённого оператора ортогонал к инвариантному подпространству инвариантен. Эти два утверждения дают ортогональную диагонализацию квадратичных форм на евклидовых пространствах.

Соглашение 2. Для квадратичных форм, возможно, стоит говорить «положительная», «отрицательная», «полуположительная», «полуотрицательная». Вместо «знакоопределённая» говорить «анизотропная».

Наблюдение 10 (Фробениус абелевой группы)**.** Пусть $p \in \mathbb{Z}$ — простое число, а V — абелева группа. Тогда мы имеем гомоморфизм абелевых групп $a \mapsto [a^{\otimes [p]_\Lambda}] : V \to \operatorname{Coker}(\Sigma_{C_p} : (V^{\otimes [p]_\Lambda})_{C_p} \to (V^{\otimes [p]_\Lambda})^{C_p})$, где $C_p \coloneqq \operatorname{Aut}([p]_\Lambda)$, а Σ_{C_p} — отображение суммирования по действию конечной группы C_p из её коинвариантов в инварианты.

Наблюдение 11 (Функториальность жорданова разложения)**.** Пусть K — поле, а $\varphi : V \to W$ — гомоморфизм $K[X]$-модулей. Тогда φ отображает жорданово подпространство $\bigcup_{n \geqslant 0} \operatorname{Ker}((X-\lambda)^n : V \to V)$, где $\lambda \in K$, в жорданово подпространство $\bigcup_{n \geqslant 0} \operatorname{Ker}((X-\lambda)^n : W \to W)$.

Пример 1. Алгебра $k[X,Y]/(XY)$, где k — ассоциативное коммутативное унитальное кольцо, не является амальгамированной суммой в категории ассоциативных коммутативных унитальных колец своих подалгебр $k[X]$ и $k[Y]$ над их пересечением $k[X] \cap k[Y] = k$.

Замечание 1. Пример 1 был подсказан Дмитрием Калединым по интернету 20 июля 2023 года.

Утверждение 1. *Пусть $\alpha : S^{-1}R \rightleftarrows T^{-1}E : \beta$ — кольцевые гомоморфизмы между локализациями ассоциативных унитальных колец R и E по множествам S и T. Если $\beta \circ \alpha : S^{-1}R \to S^{-1}R$ является эндоморфизмом над R, а образ α содержит образ канонического гомоморфизма $E \to T^{-1}E$, то $\beta \circ \alpha = \mathrm{Id}$ и $\alpha \circ \beta = \mathrm{Id}$.*

Доказательство. Так как все эндоморфизмы $S^{-1}R$ над R тождественные, то $\beta \circ \alpha = \mathrm{Id}$. Так как $\beta \circ \alpha = \mathrm{Id}$, то $\alpha \circ \beta$ переводит образ α в себя тождественно, в частности, является эндоморфизмом над E, откуда следует, что $\alpha \circ \beta = \mathrm{Id}$. □

Теорема 1 (Основная теорема арифметики)**.** *Каждый ненулевой идеал области главных идеалов однозначно представляется в виде конечного произведения ненулевых простых идеалов.*

Определение 2 (Консервативный функтор)**.** Функтор называется *консервативным*, если он переводит морфизмы, не являющиеся изоморфизмами, в морфизмы, не являющиеся изоморфизмами.

Обозначение 2 (Мультипликативный моноид кольца)**.** Пусть R — ассоциативное унитальное кольцо. Моноид всех элементов R с операцией умножения обозначается через R^{mult}.

Определение 3 (Характер Дирихле)**.** Отображение $\chi : \mathbb{Z} \to \mathbb{C}$ называется *характером Дирихле* модуля m, где $m \in \mathbb{N}_1$, если оно разлагается в композицию стандартной редукции $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ и консервативного гомоморфизма мультипликативных моноидов $(\mathbb{Z}/m\mathbb{Z})^{\mathrm{mult}} \to \mathbb{C}^{\mathrm{mult}}$.

Наблюдение 12 (Лист Мёбиуса)**.** Определим *раздутие* $\mathbb{R}^n$ в точке $0 \in \mathbb{R}^n$, где $n \in \mathbb{N}_1$, как множество $\mathcal{M}^n \coloneqq \{(x, l) \in \mathbb{R}^n \times \mathrm{Gr}(1, \mathbb{R}^n) \mid x \in l\}$ с индуцированной топологией, где $\mathrm{Gr}(1, \mathbb{R}^n)$ — это грассманиан прямых в $\mathbb{R}^n$, проходящих через $0 \in \mathbb{R}^n$. Отображение $\pi : \mathcal{M}^n \to \mathbb{R}^n$, $(x, l) \mapsto x$ задаёт гомеоморфизм между дополнением *особого слоя* $\pi^{-1}(0)$ в $\mathcal{M}^n$ и $\mathbb{R}^n \setminus \{0\}$. Инверсия относительно единичной сферы на $\mathbb{R}^n \setminus \{0\}$ однозначно продолжается до гомеоморфизма $\mathcal{M}^n \xrightarrow{\sim} \mathbb{R}\mathrm{P}^n \setminus \{0\}$. Проколотое проективное пространство $\mathbb{R}\mathrm{P}^n \setminus \{0\}$, в свою очередь, гомеоморфно пространству аффинных гиперплоскостей в $\mathbb{R}^n$ по проективной двойственности. Топологическое пространство $\mathcal{M}^2$ называется *листом Мёбиуса*.

Соглашение 3 (Аксиоматическая алгебра)**.** Возможно, стоит называть алгебру, которую сейчас, в первой четверти XXI века, преподают на первых курсах университетов, *аксиоматической алгеброй*.

Определение 4 (Внешние степени спаривания)**.** Пусть I — конечное множество, A — коммутативное ассоциативное унитальное кольцо, $v \otimes w \mapsto v \cdot w : V \otimes_A W \to A$ — спаривание между двумя A-модулями. Спаривание $\Lambda^I(V) \otimes_A \Lambda^I(W) \to A$, индуцированное спариванием $(\bigotimes_{i \in I} v_i) \otimes (\bigotimes_{i \in I} w_i) \mapsto \det((v_i \cdot w_j)_{i,j \in I}) : V^{\otimes I} \otimes_A W^{\otimes I} \to A$, называется *$I$-ой внешней степенью* спаривания $v \otimes w \mapsto v \cdot w : V \otimes_A W \to A$.

Определение 5 (Дискриминант билинейной формы)**.** В условиях определения 4 при дополнительном предположении $V = W \simeq A^I$ спаривание $(\bigwedge_{i \in I} v_i) \otimes (\bigwedge_{i \in I} w_i) \mapsto \det((v_i \cdot w_j)_{i,j \in I}) : \Lambda^I(V) \otimes_A \Lambda^I(V) \to A$ называется *дискриминантом* спаривания $v \otimes w \mapsto v \cdot w : V \otimes_A V \to A$.

Наблюдение 13 (Два определения экспоненты)**.** Доказательства сходимости ряда $\sum_{n=0}^{\infty}\frac{1}{n!}x^n$ и равенства $\lim_{m\to\infty}(1+\frac{x}{m})^m=\sum_{n=0}^{\infty}\frac{1}{n!}x^n$ довольно простые.

Абсолютная сходимость ряда $\sum_{n=0}^{\infty}\frac{1}{n!}x^n$ доказывается через банальное сравнение с геометрической прогрессией, так как $|\frac{x^n}{n!}|\leqslant|\frac{x^{n-1}}{(n-1)!}||\frac{x}{n}|$, а при ограниченном x число $|\frac{x}{n}|$ стремится к 0 когда n стремится к ∞.

По биному Ньютона $(1+\frac{x}{m})^m=\sum_{n=0}^{\infty}\frac{m(m-1)\cdots(m-(n-1))}{m^n}\frac{1}{n!}x^n$. Коэффициенты этих рядов по модулю не больше соответствующих коэффициентов абсолютно сходящегося ряда $\sum_{n=0}^{\infty}\frac{1}{n!}x^n$ и стремятся к ним когда m стремится к ∞, откуда и следует, что $\lim_{m\to\infty}(1+\frac{x}{m})^m=\sum_{n=0}^{\infty}\frac{1}{n!}x^n$.

15.2. Не сгруппированные мелочи II

Наблюдение 1 (Предаддитивная категория)**.** Предаддитивная категория в смысле раздела 1.3 статьи [13] — это то же самое, что категория, в которой конечные произведения и копроизведения существуют и коммутируют друг с другом.

Определение 1 (Абелева категория)**.** Аддитивная категория называется *абелевой*, если она конечно полна и кополна, и для любого морфизма $X\to Y$ индуцированный морфизм $X\sqcup_{X\times_Y X}X\to Y\times_{Y\sqcup_X Y}Y$ из кообраза в образ является изоморфизмом.

Наблюдение 2. Категория малых категорий содержит все малые пределы и копределы.

Наблюдение 3. Пусть R — ассоциативное унитальное кольцо. Тогда гомоморфизм $a\mapsto(v\mapsto av:M\to M)_{M\in\mathrm{Ob}(R\text{-mod})}:\mathrm{Z}(R)\to\mathrm{End}(\mathrm{Id}_{R\text{-mod}})$ является изоморфизмом.

Наблюдение 4 (Аппроксимация $99/70\approx\sqrt{2}$)**.** Так как $7^2=49\approx50$, то имеем очевидную пару приближений $7/5<\sqrt{2}<10/7$ к $\sqrt{2}$, такую что $(7/5)(10/7)=2$. По формуле $(a-b)(a+b)=a^2-b^2$ квадрат среднего арифметического двух чисел больше квадрата их среднего геометрического на квадрат полуразности, в частности, квадрат числа $(7/5+10/7)/2=99/70$ больше 2 на $((10/7-7/5)/2)^2=1/70^2=1/4900$.

Замечание 1. Стороны листа бумаги A4 имеют длину 297 мм и 210 мм, а $297/210 = 99/70$.

Определение 2 (Групповой объект)**.** *Групповым объектом* в категории $\mathcal{C}$ называется пара (G, μ) из объекта $G \in \mathrm{Ob}(\mathcal{C})$ и естественного преобразования $(\mu_X : \mathrm{Hom}_{\mathcal{C}}(X, G) \times \mathrm{Hom}_{\mathcal{C}}(X, G) \to \mathrm{Hom}_{\mathcal{C}}(X, G))_{X \in \mathrm{Ob}(\mathcal{C})}$, которое превращает каждое из множеств $\mathrm{Hom}_{\mathcal{C}}(X, G)$ в группу.

Наблюдение 5 (Обратный Мура – Пенроуза)**.** Пусть $x : V \rightleftarrows U : y$ — гомоморфизмы $\mathbb{Z}$-модулей, такие что $xyx = x$ и $yxy = y$. Тогда $yxyx = yx$ и $xyxy = xy$, то есть xy и yx — проекторы. При этом, так как $xyx = x$, то $\mathrm{Ker}(yx) \subset \mathrm{Ker}(x)$, а потому $\mathrm{Ker}(yx) = \mathrm{Ker}(x)$. Аналогично, $\mathrm{Im}(yx) = \mathrm{Im}(y)$, и всё то же с заменой $x \leftrightarrow y$. Отсюда получаем разложения $V = \mathrm{Ker}(x) \oplus \mathrm{Im}(y)$ и $U = \mathrm{Ker}(y) \oplus \mathrm{Im}(x)$, и взаимно обратные изоморфизмы $v \mapsto x(v) : \mathrm{Im}(y) \rightleftarrows \mathrm{Im}(x) : y(u) \mapsfrom u$. Если V и U — это модули над $\mathbb{R}$ или $\mathbb{C}$ с невырожденными скалярными произведениями, то x однозначно определяет y, для которого описанные разложения ортогональны. Это и есть «обратный Мура – Пенроуза».

Список иллюстраций

Список литературы

[1] J. J. Sylvester. “On the Relation between the Minor Determinants of Linearly Equivalent Quadratic Functions”. В: *The Collected Mathematical Papers of James Joseph Sylvester*. Т. I (1837–1853). 37. Cambridge, University press, 1904, с. 241—250. URL: https://archive.org/details/collectedmathem01sylvrich/page/241/mode/1up (дата обр. 23.08.2024) (цит. на с. 13). Переизд. “On the Relation between the Minor Determinants of Linearly Equivalent Quadratic Functions”. В: *Philosophical Magazine*. 4-я сер. I.XXXVII (1851), с. 295—305. URL: https://babel.hathitrust.org/cgi/pt?id=umn.31951000614090i&view=1up&seq=317 (дата обр. 23.08.2024).

[2] В. И. Арнольд. *Гюйгенс и Барроу, Ньютон и Гук. Первые шаги математического анализа и теории катастроф, от эвольвент до квазикристаллов*. Современная математика для студентов. Москва: Наука. Гл. ред. физ.-мат. лит., 1989. 96 с. ISBN: 5-02-013935-1 (цит. на с. 73).

[3] В. И. Арнольд. *Математические методы классической механики*. 3-е изд. испр. и доп. Москва: Наука. Гл. ред. физ.-мат. лит., 1989. 472 с. ISBN: 5-02-014282-4 (цит. на с. 73).

[4] Waldemar Hołubowski. “An inverse matrix of an upper triangular matrix can be lower triangular”. В: *Discussiones Mathematicae. General Algebra and Applications* 22.2 (2002), с. 161—166. DOI: https://doi.org/10.7151/dmgaa.1055. URL: https://www.dmgaa.uz.zgora.pl/publish/article.php?doi=1055 (дата обр. 07.01.2025) (цит. на с. 69).

[5] Jean-Pierre Serre. “On a theorem of Jordan”. В: *Bulletin of the American Mathematical Society* 40.4 (2003), с. 429—440. URL: https://

www.ams.org/journals/bull/2003-40-04/S0273-0979-03-00992-3/ (дата обр. 22.03.2024) (цит. на с. 100).

[6] F. W. Lawvere. “Functorial Semantics of Algebraic Theories...” В: *Reprints in Theory and Applications of Categories* 5 (2004), с. 1—121. URL: http://www.tac.mta.ca/tac/reprints/articles/5/tr5abs.html (дата обр. 16.02.2024) (цит. на с. 11).

[7] Д. Каледин. *Введение в алгебраическую геометрию (конспекты лекций в НОЦ МИАН)*. 2005—2006. URL: https://homepage.mi-ras.ru/~kaledin/noc/ (дата обр. 20.11.2024) (цит. на с. 171).

[8] В. И. Арнольд. *Математическое понимание природы. Очерки удивительных физических явлений и их понимания математиками (с рисунками автора)*. Издание третье, стереотипное. Москва: МЦНМО, 2011. 144 с. ISBN: 978-5-94057-744-7 (цит. на с. 73).

[9] PseudoNeo (https://math.stackexchange.com/users/7085/pseudoneo). *Center of the unit group $R^\times$ of a ring.* 27 марта 2013. URL: https://math.stackexchange.com/q/342817 (дата обр. 24.09.2024) (цит. на с. 110).

[10] М. Вербицкий. *Теория Галуа*. 2013. URL: http://verbit.ru/MATH/GALOIS-2013/ (дата обр. 02.03.2024) (цит. на с. 143).

[11] user26857 (https://math.stackexchange.com/users/121097/user26857). *maximal algebraically independent sets in ring extensions.* 23 сент. 2014. URL: https://math.stackexchange.com/q/942910 (дата обр. 17.11.2024) (цит. на с. 152).

[12] Michael Müger. “Notes on the theorem of Baker-Campbell-Hausdorff-Dynkin”. Work in progress! 22 апр. 2020. URL: https://www.math.ru.nl/~mueger/PDF/BCHD.pdf (дата обр. 19.01.2025) (цит. на с. 135).

[13] D. B. Kaledin. “What do Abelian categories form?” В: *Russian Mathematical Surveys* 77.1 (февр. 2022), с. 1—45. ISSN: 1468-4829. DOI: 10.1070/rm10044. arXiv: 2112.02155v2 [math.CT]. URL: http://dx.doi.org/10.1070/RM10044 (цит. на с. 177).

[14] James S. Milne. *Fields and Galois Theory (v5.10)*. Available at www.jmilne.org/math/. 2022, с. 1—144. URL: https://jmilne.org/math/CourseNotes/ft.html (дата обр. 03.03.2024) (цит. на с. 143, 150).

[15] Alexey Muranov. "Proof of Cayley-Hamilton theorem using polynomials over the algebra of module endomorphisms". В: *Linear Algebra and its Applications* 645 (июль 2022), с. 165—169. ISSN: 0024-3795. DOI: 10.1016/j.laa.2022.03.012. arXiv: 2105.09285v2 [math.HO]. URL: http://dx.doi.org/10.1016/j.laa.2022.03.012 (цит. на с. 45).

[16] С. О. Горчинский. *Теория Галуа, алгебраические группы и дифференциальные уравнения*. 2022. URL: https://teach-in.ru/course/galois-theory-algebraic-groups-and-differential-equations (дата обр. 30.04.2025) (цит. на с. 150).

[17] Pavel Etingof. *Lie Groups and Lie Algebras*. AMR Research Monographs 4. Association for Mathematical Research, 2024. DOI: https://doi.org/10.48550/arXiv.2201.09397. arXiv: 2201.09397v4 [math.RT]. URL: https://amathr.org/books/books_etingof_1/ (дата обр. 30.04.2025) (цит. на с. 135).

[18] Коллектив авторов. *Matrix (mathematics). History*. Wikipedia (english). Авг. 2024. URL: https://en.wikipedia.org/wiki/Matrix_(mathematics)#History (дата обр. 23.08.2024) (цит. на с. 13).

[19] Д. Терешкин. *Алгебраическая теория категорий. Лекция 1*. 2024. URL: https://www.youtube.com/live/oZ9hKNNP5Sk (дата обр. 16.05.2025) (цит. на с. 67).