А. Кузнецов

КУРС АЛГЕБРЫ

Осень 2002 – Весна 2003

Оглавление

Семестр I (Осень 2002)

Программа

На зачете каждому студенту будет предлагаться по одному вопросу из каждой темы (группы, кольца, модули, линейная алгебра, поля). После каждого вопроса указано примерное предполагаемое содержание ответа (темы, изучавшиеся на лекциях (номер лекции указан римскими цифрами), и задачи, изучавшиеся на семинарах (указана дата выдачи листка с задачами)).

- Группы.
  1. Определение моноида и группы, гомоморфизмы. — (I) 1.1–1.10, 3.1–3.5.
  2. Подгруппы, классы смежности, теорема об индексе. — (II) 1.1, 1.5, 1.6, 1.8, 1.9, (17c) 1.
  3. Нормальные подгруппы, факторгруппа. — (II) 2.3–2.9, (17c) 2, (24c) 7a.
  4. Ядро, образ, теорема о гомоморфизме. — (II) 2.1, 2.2, 2.10, 2.11.
  5. Действия групп на множествах, сопряжения, сдвиги. — (III) 1.1–1.6, (17c) 4, (24c) 4.
  6. Орбиты и стабилизаторы, формула классов. — (III) 2.2–2.9, (24c) 2a.
  7. Группа перестановок, независимые циклы. — (III) 3.1, 3.2, (24c) 2b, 3abc, 5.
  8. Транспозиции, четность, знак перестановки. — (III) 3.3–3.5, (24c) 6.
  9. Циклические группы. — (I) 1.4, 1.7, (10c) 3, 5a, 6ab.
- Кольца.
  1. Определение кольца, гомоморфизмы колец. — (I) 2.1, 2.4, 2.5, 3.1–3.5.
  2. Подкольца, идеалы, факторкольцо. — (IV) 1.1–1.8, 1.13.
  3. Ядро, образ, теорема о гомоморфизме. — (IV) 1.7–1.9, 1.14, 1.15.
- Коммутативные кольца.
  1. Делители нуля, целостность, поле частных. — (VIII) 1.1, 1.2, 1.6, 1.13, (29o) 1, 3, 4, (10c) 4abde.
  2. Простые и максимальные идеалы. — (VIII) 1.3–1.12, 1.14, (29o) 2.
  3. Кольца главных идеалов, деление с остатком. — (VIII) 2.1–2.4.
  4. Нетеровость. — (VIII) 2.8, 2.9, (29o) 5a.
  5. Делимость, наибольший общий делитель, неприводимость. — (VIII) 2.5–2.7, 3.1, 3.2, 3.5.
  6. Разложение на множители, факториальность кольца главных идеалов. — (VIII) 3.1–3.9, (29o) 6.
  7. Кольцо многочленов.
  8. Кольцо формальных степенных рядов.
  9. Гауссовы числа.
- Модули.
  1. Модули над кольцом, образующие, линейная зависимость и базисы. — (IV) 2.1–2.8.
  2. Векторные пространства, существование базиса. — (V) 1.1–1.4.

3. Подмодуль, фактормодуль, теорема о гомоморфизме. — (V) 3.1–3.7.
4. Элементарные преобразования матриц. — (V) 2.1–2.7.
5. Размерность, классификация векторных пространств. — (V) 2.8–2.10, (8о) 4.
6. Классификация конечно порожденных абелевых групп. — (8о) 5, 6.
7. Прямые суммы. — (V) 1.5–1.7, 2.11, (1о) 3bc, (8о) 2.

- Линейная алгебра.

1. Линейные отображения и матрицы, изменение матрицы при замене базиса. — (VI) 1.1–1.7.
2. След, определитель, характеристический многочлен. — (VI) 2.1–2.9, (15о) 1b, 2.
3. Присоединенная матрица, формула обращения матрицы. — (VI) 3.1–3.8.
4. Ранг оператора, матрицы, вычисление ранга. — (VI) 4.1–4.4, (15о) 4, 5.
5. Собственные векторы, корневые подпространства. — (VII) 1.1–1.6.
6. Теорема о жордановой нормальной форме. — (VII) 2.1–2.6.
7. Вычисления в жордановом базисе. — (VII) 2.5, (22о) 2, 3.
8. Полупростые и нильпотентные операторы, жорданово разложение. — (VII) 2.7, 2.8, (22о) 4, 5, 6.
9. Теорема Гамильтона-Кэли, минимальный многочлен. — (VII) 3.1–3.7.
10. Системы линейных уравнений. — (15о) 6.

- Поля.

1. Характеристика, простые поля, мультипликативная группа поля. — (IX) 1.1–1.6, (5н) 1.
2. Расширения полей, степень, конечные расширения, башни. — (IX) 2.1–2.2, (5н) 2.
3. Алгебраичекие расширения, многочлен $\mathrm{Irr}_\alpha^K(x)$. — (IX) 2.3–2.5.
4. Конечно порожденные алгебраические расширения. — (IX) 2.6–2.8.
5. Существование алгебраического замыкания. — (IX) 3.1–3.4, (5н) 7.
6. Продолжения гомоморфизмов, единственность алгебраического замыкания. — (X) 1.1–1.5.
7. Поле разложения. — (X) 2.1–2.3, (12н) 4b.
8. Нормальные расширения. — (X) 3.1–3.3, (12н) 3, 5.
9. Конечные поля и их автоморфизмы. — (X) 4.1–4.4, 4.6–4.9, (12н) 1, 2b.
10. Сепарабельная степень. — (XI) 1.1–1.5.
11. Сепарабельные расширения. — (XI) 2.1–2.11, (X) 4.5.
12. Чисто несепарабельные расширения. — (XI) 3.1–3.7.
13. Сепарабельное замыкание, совершенные поля. — (XI) 4.1–4.6, (19н) 3, 4.
14. Теорема о примитивном элементе. — (XII) 2.1–2.5.
15. Теорема Галуа. — (XII) 1.1–1.6, 2.5, 3.1, 3.2, 3.8, 3.9.
16. Свойства изоморфизма теоремы Галуа. — (XII) 3.3–3.7.
17. Группа Галуа многочлена. — (26н) 2, 3, 4, 5.

Рекоммендуемая литература

1. Ван-дер-Варден Б.Л. Современная алгебра.
2. Ленг С. Алгебра.
3. Кострикин А.И. Введение в алгебру.
4. Гельфанд И.М. Линейная алгебра.
5. Кострикин А.И., Манин Ю.И. Линейная алгебра.
6. Серр Ж.-П. Линейные представления конечных групп.
7. Серр Ж.-П. Курс арифметики.
8. Атья М., Макдональд. Коммутативная алгебра.

Лекция 1. Основные алгебраические структуры

Часть 1. Моноиды и группы

Определение 1.1. Моноид — это тройка $(M, \circ, 1)$, состоящая из множества M, бинарной операции $\circ$ на M (т.е. отображения $M \times M \to M$, $(x, y) \mapsto x \circ y$) и элемента $e \in M$, таких что выполнены следующие свойства:

M1 Ассоциативность: $\forall x, y, z \in M \quad (x \circ y) \circ z = x \circ (y \circ z)$.

M2 Аксиома единицы: $\forall x \in M \quad x \circ e = e \circ x = x$.

Примеры 1.2.

1. $(\mathbb{Z}, +, 0)$ (варианты: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_{\geqslant 0}$, $\mathbb{Q}_{\geqslant 0}$, $\mathbb{R}_{\geqslant 0}$, $\mathbb{Z}/n\mathbb{Z}$, ...).
2. $(\mathbb{Z}, \cdot, 1)$ (варианты: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_{\geqslant 0}$, $\mathbb{Q}_{\geqslant 0}$, $\mathbb{R}_{\geqslant 0}$, $\mathbb{Z}_{>0}$, $\mathbb{Q}_{>0}$, $\mathbb{R}_{>0}$, $\mathbb{Z}/n\mathbb{Z}$, ...).
3. $M = \mathrm{Map}(X, X)$ — множество отображений из множества X в себя, $\circ$ — операция композиции отображений, $e = \mathrm{Id}_X$ — тождественное отображение.
4. $M = \mathrm{Map}(X, M')$ — множество отображений из множества X в моноид M', $\circ$ — поточечное умножение ($(f \circ g)(x) = f(x) \circ' g(x)$, где $\circ'$ — операция в M'), $e \equiv e'$ — функция, тождественно равная единице моноида M'.

Легко убедиться, что единица во всяком моноиде единственна. Действительно, если e' — другая единица, то $e' = e' \cdot e = e$. Поэтому при задании моноида можно не указывать его единицу — достаточно лишь проверить ее существование.

Лемма 1.3. *Если $x_1, \ldots, x_n$ — элементы моноида, то все способы расстановки скобок в произведении $x_1 \circ \cdots \circ x_n$ дают одинаковый результат.*

Доказательство — индукция по n.

Определение 1.4. Моноид M называется коммутативным, если $\forall x, y \in M \quad x \circ y = y \circ x$.

Как правило, в коммутативных моноидах операция записывается аддитивно ($x \circ y =: x + y$), а в некоммутативных мультипликативно ($x \circ y =: xy$).

Произведение n одинаковых элементов $x \circ \cdots \circ x$ обозначается через x^n, при этом удобно положить $x^0 = e$. Легко проверить, что

$$x^n \circ x^m = x^{n+m} \tag{1.5}$$

для всех неотрицательных m и n. При аддитивной записи операции в моноиде пользуются обозначением nx вместо x^n. При этом свойство (1.5) приобретает вид $nx + mx = (n + m)x$.

Элемент x в моноиде M называется обратимым, если существуют элемент y (левый обратный), такой что $y \circ x = e$; и элемент z (правый обратный), такой что $x \circ z = e$.

Лемма 1.6. *Если x — обратим, то всякий левый обратный к x равен всякому правому обратному к x.*

Доказательство: $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z$.

Тем самым, для любого обратимого элемента x существует единственный элемент, являющийся одновременно правым и левым обратным к x. Этот элемент обозначается x^{-1} (при аддитивной записи: $-x$) и называется обратным к x. Далее, удобно обозначить $(x^{-1})^n$ через x^{-n} (при аддитивной записи $-nx$). Тогда свойство (1.5) становится верным при любых целых n и m.

Определение 1.7. Группа — это моноид, в котором все элементы обратимы.

Лемма 1.8. *Если M — моноид, то множество M^* обратимых элементов в M является группой.*

Доказательство: Достаточно проверить, что множество M^* замкнуто относительно операции $\circ$, то есть что для любых обратимых элементов $x, y \in M$ произведение $x \circ y$ — тоже обратимо. Действительно, ясно, что

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = (y^{-1} \circ x^{-1}) \circ (x \circ y) = e,$$

то есть элемент $y^{-1} \circ x^{-1}$ является обратным к $x \circ y$. □

Примеры 1.9. 1. $\mathbf{1} = \{ e \}$.

2. $(\mathbb{Z}, +)$ (варианты: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$, ...).

3. $(\mathbb{Q}^*, \cdot)$ (варианты: $\mathbb{R}^*$, $\mathbb{C}^*$, $(\mathbb{Z}/n\mathbb{Z})^*$ $\mathbb{Q}_{>0}$, $\mathbb{R}_{>0}$, $\mu_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$, $\mathbf{S}^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$, ...).

4. Группа перестановок (симметрическая группа) $\mathfrak{S}_n$ — множество изоморфизмов из n-элементного множества $\{ 1, \ldots, n \}$ на себя с операцией композиции отображений.

5. $G = \mathrm{Map}(X, G')$ — множество отображений из множества X в группу G'.

6. Группы автоморфизмов (см. лемму 3.5).

Лемма 1.10. *Если в группе G выполнено одно из равенств $x \circ y = x \circ z$ или $y \circ x = z \circ x$, то $y = z$.*

Доказательство: если $x \circ y = x \circ z$, то $y = e \circ y = (x^{-1} \circ x) \circ y = x^{-1} \circ (x \circ y) = x^{-1} \circ (x \circ z) = (x^{-1} \circ x) \circ z = e \circ z = z$. Второй случай разбирается аналогично.

Группа называется коммутативной, если она коммутативна как моноид. Коммутативные группы также называются абелевыми.

Часть 2. Кольца и поля

Определение 2.1. Кольцо— это набор $(R, +, \cdot, 0, 1)$, состоящий из множества R, бинарных операций $+$ (сложение) и $\cdot$ (умножение) на R и элементов $0, 1 \in R$, таких что выполнены следующие свойства:

R1 $(R, +, 0)$ — абелева группа.

R2 $(R, \cdot, 1)$ — моноид.

R3 Дистрибутивность (билинейность) умножения: $\forall x, y, z \in R \quad x \cdot (y + z) = x \cdot y + x \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z$.

Умножение в кольце часто записывают в виде $xy = x \cdot y$. Кольцо называется коммутативным, если коммутативна операция умножения.

Примеры 2.2. 1. $\{ 0 \}$.

2. $\mathbb{Z}$ (варианты: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$, ...).

3. $R = \mathrm{Map}(X, R')$ — множество отображений из множества X в кольцо R' с поточечными операциями.

4. $R = R'[x] = \{ a_n x^n + \cdots + a_1 x + a_0 \mid a_0, \ldots, a_n \in R' \}$ — кольцо многочленов (полиномов) с коэффициентами в кольце R'.

5. $R = R'[[x]] = \{ a_0 + a_1 x + \cdots + a_n x^n + \ldots \mid a_0, \ldots, a_n \in R' \}$ — кольцо формальных степенных рядов с коэффициентами в кольце R'.

6. $R = \mathrm{Mat}_{n \times n}(R')$ — кольцо матриц размера n на n с коэффициентами в кольце R'. Элементы R — это таблицы вида $\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$, $a_{ij} \in R'$ с покомпонентным сложением; умножением, задаваемым формулой

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix}, \text{ где } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \tag{2.3}$$

нулевой матрицей в качестве 0 и диагональной матрицей с единицами на диагонале в качестве 1.

7. Кольца эндоморфизмов (см. лемму 3.5).

Лемма 2.4. *Если R — кольцо, то* $\forall x \in R \quad 0 \cdot x = x \cdot 0 = 0$.

Доказательство: $0 + 0 \cdot x = 0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$ и остается применить лемму 1.10 к аддитивной группе кольца.

Определение 2.5. Кольцо, в котором $0 \neq 1$ и все элементы кроме нуля являются группой относительно умножения, называется телом, а если оно к тому же коммутативно, то полем.

Некоммутативные тела встречаются достаточно редко; простейший пример — тело кватернионов $\mathbb{H}$. С полями дело обстоит значительно лучше.

Примеры 2.6. Примеры полей.

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$,
2. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, где p — простое число.
3. $\mathbb{Q}[i] = \{ x + yi \in \mathbb{C} \mid x, y \in \mathbb{Q} \}$, $\mathbb{Q}[\sqrt{2}] = \{ x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Q} \}$.
4. $K = K'(x) = \left\{ \dfrac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ g(x) \not\equiv 0 \right\}$ — поле рациональных функций с коэффициентами в поле K'.
5. $K = K'((x)) = \{ a_{-n}x^{-n} + \cdots + a_{-1}x^{-1} + a_0 + a_1 x + \cdots + a_n x^n + \ldots \mid a_i \in K' \}$ — поле (формальных) рядов Лорана с коэффициентами в поле K'.

Часть 3. Гомоморфизмы

Определение 3.1. Гомоморфизм групп (моноидов) $f : G \to G'$ — это отображение, такое что $f(e) = e'$ и $\forall x, y \in G \quad f(x \circ y) = f(x) \circ' f(y)$. Гомоморфизм колец (полей) $f : R \to R'$ — это отображение, являющееся гомоморфизмом их аддитивной группы и мультипликативного моноида.

Примеры 3.2.
1. Если G — группа, а $x \in G$, то отображение $n \mapsto x^n$ является гомоморфизмом групп $\mathbb{Z} \to G$.
2. Если R — кольцо, а $x \in R$, то отображение $n \mapsto nx := x + \cdots + x$ является гомоморфизмом колец $\mathbb{Z} \to R$.
3. Проекция $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ является гомоморфизмом колец.
4. Отображения $\exp : \mathbb{R} \to \mathbb{R}_{>0}$, $\exp : \mathbb{C} \to \mathbb{C}^*$ и $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ являются гомоморфизмами групп.
5. Отображение вычисления $ev_x : \mathrm{Map}(X, G) \to G$, $f \mapsto f(x)$ является гомоморфизмом групп.
6. Если R — коммутативное кольцо, и $r \in R$, то отображение вычисления $ev_r : R[x] \to R$, $a_n x^n + \cdots + a_1 x + a_0 \mapsto a_n r^n + \cdots + a_1 r + a_0$ является гомоморфизмом колец.
7. Всякий элемент кольца R можно рассматривать как многочлен степени 0, а всякий многочлен можно рассматривать как формальный степенной ряд, все члены которого, начиная с некоторого места равны нулю. Тем самым задаются гомоморфизмы колец $R \to R[x]$ и $R[x] \to R[[x]]$.

Лемма 3.3. *Композиция гомоморфизмов является гомоморфизмом. Если $f : M \to M'$ — гомоморфизм моноидов, а $x \in M$ — обратимый элемент, то $f(x) \in M'$ — обратим и $f(x)^{-1} = f(x^{-1})$.*

Доказательство: $f(g(x \circ y)) = f(g(x) \circ g(y)) = f(g(x)) \circ f(g(y))$, откуда следует первая часть леммы. Для доказательства второй части достаточно заметить, что $f(x^{-1}) \circ f(x) = f(x^{-1} \circ x) = f(e) = e'$, $f(x) \circ f(x^{-1}) = f(x \circ x^{-1}) = f(e) = e'$, то есть $f(x^{-1}) = f(x)^{-1}$. □

Гомоморфизм (моноидов, групп, колец, полей, и т.д.) $f : M \to M'$ называется эпиморфизмом (сюръекцией, наложением), если $\forall z \in M' \ \exists x \in M$ т.ч. $f(x) = z$. Гомоморфизм f называется мономорфизмом (инъекцией, вложением), если из равенства $f(x) = f(y)$, $x, y \in M$, следует $x = y$. Гомоморфизм $f : M \to M'$ называется изоморфизмом, если существует гомоморфизм $g : M' \to M$, такой что $g \circ f = \mathrm{Id}_M$, $f \circ g = \mathrm{Id}_{M'}$.

Лемма 3.4. *Гомоморфизм групп (колец) является изоморфизмом $\Longleftrightarrow$ он является одновременно мономорфизмом и эпиморфизмом.*

Доказательство: всякий изоморфизм биективен, следовательно является мономорфизмом и эпиморфизмом. Обратно, если гомоморфизм является мономорфизмом и эпиморфизмом одновременно, то он биективен, следовательно существует обратное отображение, которое (легко проверить) является гомоморфизмом. □

Всякий гомоморфизм из (моноида, группы, кольца, поля, и т.д.) в себя называется эндоморфизмом. Эндоморфизм, являющийся изоморфизмом, называется автоморфизмом.

Лемма 3.5. *Если M — любая алгебраическая структура (моноид, группа, кольцо, поле), то множество его автоморфизмов* $\mathrm{Aut}(M)$ *является группой. Если M — абелева группа, то множество ее эндоморфизмов* $\mathrm{End}(M)$ *является кольцом.*

Доказательство: из леммы 3.3 следует, что $\mathrm{End}(M)$ является моноидом относительно операции композиции эндоморфизмов, а $\mathrm{Aut}(M)$ является множеством его обратимых эементов, следовательно $\mathrm{Aut}(M)$ — группа. Если же M является абелевой группой, то на $\mathrm{End}(M)$ есть операция поточечного сложения $((f+g)(x) := f(x)+g(x))$, так что $\mathrm{End}(M)$ становится кольцом. □

Определение 3.6. Ядром гомоморфизма групп $f : G \to G'$ называется $\mathrm{Ker}\, f = \{\, x \in G \mid f(x) = e' \,\}$. Образом гомоморфизма групп $f : G \to G'$ называется $\mathrm{Im}\, f = \{\, y \in G' \mid y = f(x), x \in G \,\}$. Аналогично, ядром гомоморфизма колец $f : R \to R'$ называется $\mathrm{Ker}\, f = \{\, x \in R \mid f(x) = 0 \,\}$. Образом гомоморфизма колец $f : R \to R'$ называется $\mathrm{Im}\, f = \{\, y \in R' \mid y = f(x), x \in R \,\}$.

Легко видеть, что ядро и образ гомоморфизма групп $f : G \to G'$ являются подгруппами (то есть подмножествами, являющимися группами относительно индуцированной операции) в G и G' соотв. Аналогично, ядро и образ гомоморфизма колец $f : R \to R'$ являются подкольцами (то есть подмножествами, являющимися кольцами относительно индуцированных операций) в R и R' соотв.

Лемма 3.7. *Гомоморфизм f групп (колец) является мономорфизмом $\Longleftrightarrow$* $\mathrm{Ker}\, f = \{\, e \,\}$ *(*$\mathrm{Ker}\, f = \{\, 0 \,\}$ *соотв.). Гомоморфизм моноидов $f : M \to M'$ является эпиморфизмом $\Longleftrightarrow$* $\mathrm{Im}\, f = M'$.

Доказательство: пусть $f : M \to M'$ — гомоморфизм групп и $f(x) = f(y)$. Тогда $f(x^{-1} \circ y) = f(x^{-1}) \circ f(y) = f(x)^{-1} \circ f(y) = (f(y))^{-1} \circ f(y) = e'$, следовательно $x^{-1} \circ y \in \mathrm{Ker}\, f$. Далее очевидно.

Следствие 3.8. *Любой гомоморфизм из поля в кольцо является вложением.*

Доказательство: по лемме 3.3 любой обратимый элемент поля (относительно мультипликативной структуры) переходит в обратимый элемент. Следовательно, всякий ненулевой элемент переходит не в ноль. В частности, ядро гомоморфизма равно нулю, следовательно гомоморфизм — вложение. □

Часть 4. Прямые произведения

Пусть $(M_1, \circ_1, e_1)$ и $(M_2, \circ_2, e_2)$ — моноиды. Тогда на произведении $M_1 \times M_2 = \{\, (x_1, x_2) \mid x_1 \in M_1,\ x_2 \in M_2 \,\}$ возникает структура моноида:

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 \circ y_1, x_2 \circ y_2), \qquad e = (e_1, e_2).$$

Этот моноид называется прямым произведением моноидов M_1 и M_2.

Лемма 4.1. *Произведение групп (колец) является группой (кольцом).*

Доказательство: очевидно.

Напротив, легко проверить, что произведение полей является кольцом, но не полем. Действительно, в произведении полей $K \times L$ имеем

$$(1_K, 0_L) \cdot (0_K, 1_L) = (1_K \cdot 0_K, 0_L \cdot 1_L) = (0_K, 0_L),$$

следовательно элементы $(1_K, 0_L)$ и $(0_K, 1_L)$ необратимы.

Лекция 2. Гомоморфизмы

Часть 1. Группы и подгруппы

Определение 1.1. Пусть G — произвольная группа. Непустое подмножество $H \subset G$ называется подгруппой, если $HH \subset H$ и $H^{-1} \subset H$, то есть для любых $h, h' \in H$ имеем $hh' \in H$, $h^{-1} \in H$.

Замечание 1.2. Из определения следует, что $e \in H$.

Примеры 1.3.

1. Если G — группа и $x \in G$, то множество $\langle x \rangle := \{ x^n \mid n \in \mathbb{Z} \}$ называется циклической подгруппой, порожденной элементом x. Вообще, группа G называется циклической, если $G = \langle x \rangle$ для некоторого $x \in G$ (покажите, что всякая циклическая группа изоморфна либо $\mathbb{Z}$, либо $\mathbb{Z}/n\mathbb{Z}$). В этом случае x называется образующей группы G.

   В частности, имеем следующие подгруппы $n\mathbb{Z} := \langle n \rangle \subset \mathbb{Z}$, $\frac{1}{n}\mathbb{Z} := \langle 1/n \rangle \subset \mathbb{Q}/\mathbb{Z}$.

2. Пусть X — любая алгебраическая структура, а $S \subset X$ — произвольное подмножество. Тогда $N_S = \{ f \in \mathrm{Aut}(X) \mid f(S) = S \}$ и $Z_S = \{ f \in \mathrm{Aut}(X) \mid \forall s \in S \ f(s) = s \}$ — подгруппы в $\mathrm{Aut}(X)$.

3. Пусть G — группа, а $S \subset G$ — подмножество. Тогда $N_S = \{ g \in G \mid gSg^{-1} = S \}$ (нормализатор множества S) и $Z_S = \{ g \in G \mid \forall s \in S \ gs = sg \}$ (централизатор множества S) — подгруппы в G.

4. Пусть G — группа, а $H_1, H_2 \subset G$ — подгруппы. Тогда $H_1 \cap H_2 \subset G$ — подгруппа. Более того, если $\{ H_i \}_{i \in I}$ — произвольное семейство подгрупп в G, то $\bigcap_{i \in I} H_i$ — подгруппа в G.

5. Пусть $H \subset G$ — подгруппа и $x \in G$. Тогда $xHx^{-1} = \{ xhx^{-1} \mid h \in H \}$ — подгруппа в G.

Упражнение 1.4. 1) Докажите, что если G — циклическая группа, то либо $G \cong \mathbb{Z}$, либо $G \cong \mathbb{Z}/n\mathbb{Z}$. 2) Покажите, что всякая подгруппа циклической группы — циклическая.

Пусть $H \subset G$ — подгруппа, $x \in G$ — произвольный элемент. Множество $xH = \{ xh \mid h \in H \} \subset G$ называется левым смежным классом группы G по подгруппе H. Аналогично, $Hx = \{ hx \mid h \in H \} \subset G$ называется правым смежным классом G по H. Заметим, что смежные классы xH и Hx не являются подгруппами (за исключением случая $x \in H$). При аддитивной записи класс смежности обозначается $x + H$.

Лемма 1.5. *Смежные классы xH и yH либо не пересекаются, либо совпадают. Умножение слева на yx^{-1} задает биекцию $xH \to yH$.*

Доказательство: пусть $xH \cap yH \neq \emptyset$. Тогда $xh_1 = yh_2$ для некоторых $h_1, h_2 \in H$. Следовательно $x = yh_2h_1^{-1}$ и $xH = yh_2h_1^{-1}H \subset yH$. Аналогично $y = xh_1h_2^{-1}$ и $yH = xh_1h_2^{-1}H \subset xH$. Значит $xH = yH$. Второе утверждение — очевидно. □

Множество всех левых смежных классов G по H обозначается через G/H, а множество всех правых смежных классов G по H обозначается через $H\backslash G$. Иногда также рассматривают двойные смежные классы G по H — множества вида $HxH = \{ h_1xh_2 \mid h_1, h_2 \in H \}$. Легко проверить, что для двойных смежных классов выполненно первое (но не второе!) утверждение леммы 1.5. Множество всех двойных смежных классов G по H обозначается через $H\backslash G/H$.

Количество различных левых смежных классов группы G по H обозначается $(G : H)$ и называется индексом подгруппы H в G. Индекс тривиальной подгруппы $(G : 1)$ равен количеству элементов в группе G и называется также порядком группы G.

Следующая теорема вытекает из леммы 1.5.

Теорема 1.6. *Если $H \subset G$ — подгруппа, то $(G : 1) = (G : H)(H : 1)$ в том смысле, что если два из индексов конечны, то конечен и третий и выполняется равенство.*

Следствие 1.7. *Если p — простое и G — группа порядка p, то $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Доказательство: возьмем произвольный $1 \neq x \in \mathbb{Z}$. По теореме 1.6 порядок подгруппы $\langle x \rangle \subset G$ — делитель числа p, следовательно $\langle x \rangle = G$, то есть G — циклическая. □

Определение 1.8. Порядком элемента $x \in G$ называется порядок подгруппы $\langle x \rangle \subset G$. Показателем элемента $x \in G$ называется любое положительное число n, такое что $x^n = e$. Аналогично, показателем группы G называется любое положительное число n, такое что $\forall x \in G \quad x^n = e$.

Лемма 1.9. *Пусть $x \in G$. Тогда (i) порядок x делит любой из его показателей; (ii) порядок x делит порядок группы G; (iii) наименьший показатель группы G равен НОК порядков всех ее элементов.*

Доказательство: рассмотрим последовательность $\{ 1, x, x^2, \dots \}$ степеней x. Если $x^n = x^m$ и $n > m$, то $x^{n-m} = 1$. Следовательно, либо все элементы в последовательности различны, либо она периодична. Пусть d — минимальный период последовательности. Тогда $x^d = 1$ и все элементы в множестве $\{ 1, x, \dots, x^{d-1} \}$ различны. Следовательно d равен порядку группы $\langle x \rangle$, то есть порядку x. Пусть теперь n — показатель элемента x. Разделим n на d с остатком: $n = qd + r$, $0 \leqslant r < d$. Тогда $x^r = x^{n-qd} = x^n (x^d)^{-q} = x^n = 1$, следовательно $r = 0$, то есть $d | n$, что доказывает утверждение (i). Утверждение (ii) немедленно следует из теоремы 1.6. Чтобы доказать утверждение (iii) заметим, что показатель группы является показателем любого из ее элементов, и, следовательно, общим кратным всех ее элементов. □

Часть 2. Гомоморфизмы групп

Определение 2.1. Ядром гомоморфизма групп $f : G \to G'$ называется $\operatorname{Ker} f = \{ x \in G \mid f(x) = e' \}$. Образом гомоморфизма групп $f : G \to G'$ называется $\operatorname{Im} f = \{ y \in G' \mid y = f(x), x \in G \}$.

Легко видеть, что ядро и образ гомоморфизма групп $f : G \to G'$ являются подгруппами.

Лемма 2.2. *Пусть $f : G \to G'$ — гомоморфизм групп. Тогда f является мономорфизмом $\iff \operatorname{Ker} f = \{ e \}$; f является эпиморфизмом $\iff \operatorname{Im} f = G'$.*

Доказательство: пусть $f : G \to G'$ — гомоморфизм групп и $f(x) = f(y)$. Тогда $f(x^{-1} \circ y) = f(x^{-1}) \circ f(y) = f(x)^{-1} \circ f(y) = (f(y))^{-1} \circ f(y) = e'$, следовательно $x^{-1} \circ y \in \operatorname{Ker} f$. Далее очевидно. □

Ясно, что всякая подгруппа является образом некоторого гомоморфизма. Действительно, если $H \subset G$ — подгруппа, то вложение $H \to G$ является мономорфизмом, образ которого равен H. Однако ядром гомоморфизма может быть уже далеко не любая подгруппа.

Определение 2.3. Подгруппа $H \subset G$ называется нормальной, если $\forall x \in G \quad xHx^{-1} = H$.

Замечание 2.4. Достаточно проверять, что $\forall x \in G \quad xHx^{-1} \subset H$.

Если H — нормальная подгруппа в G, то пишут $H \lhd G$.

Лемма 2.5. *Ядро гомоморфизма групп является нормальной подгруппой.*

Доказательство: пусть $f : G \to G'$ — гомоморфизм групп. Покажем, что $x(\operatorname{Ker} f)x^{-1} \subset \operatorname{Ker} f$. Действительно, $g \in \operatorname{Ker} f \Longrightarrow f(g) = e' \Longrightarrow f(xgx^{-1}) = f(x)f(g)f(x)^{-1} = f(x)f(x)^{-1} = e' \Longrightarrow xgx^{-1} \in \operatorname{Ker} f$. □

Примеры 2.6.

1. $\{ e \}$ и G — нормальны в G.
2. Любая подгруппа в коммутативной группе нормальна.
3. Подгруппы $\{ e \}$, $\left\langle \binom{123}{231} \right\rangle$ и $\mathfrak{S}_3$ в группе $\mathfrak{S}_3$ нормальны, а подгруппы $\left\langle \binom{123}{213} \right\rangle$, $\left\langle \binom{123}{321} \right\rangle$ и $\left\langle \binom{123}{132} \right\rangle$ — нет.
4. Подгруппа Z_S нормальна в N_S (см. пример 1.3.2).
5. Центр группы $Z_G = \{ g \in G \mid \forall x \in G \quad gx = xg \}$ — нормален.
6. Если $H \subset G$ — любая подгруппа, то $\cap_{x \in G} xHx^{-1}$ — нормальна в G.
7. Если $H_1, H_2 \lhd G$, то $H_1 \cap H_2 \lhd G$.
8. Если $K \subset H \subset G$ и $K \lhd G$, то $K \lhd H$.

9. Если $H \subset G$ — любая подгруппа, то $H \lhd N_H$. Более того, если $H \subset K \subset G$ и $H \lhd K$, то $K \subset N_H$.

10. Если $H \subset G$ — подгруппа и K — подгруппа в N_H, то KH — подгруппа в G и H — нормальна в KH.

Лемма 2.7. *Если $H \subset G$ — нормальная подгруппа, то $\forall x \in G \quad xH = Hx$.*

Доказательство: $xH = (xH)e = (xH)(x^{-1}x) = (xHx^{-1})x = Hx$. □

Пусть $H \subset G$ — нормальная подгруппа. Тогда ясно, что $(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH$. Определим на множестве левых классов смежности G/H бинарную операцию:

$$(xH) \circ (yH) := xyH. \tag{2.8}$$

Из приведенных выше рассуждений следует, что она корректно определена (результат зависит только от классов смежности xH и yH, но не от элементов x и y).

Теорема 2.9. *Если $H \subset G$ — нормальная подгруппа, то множество G/H с операцией $\circ$ является группой. Более того, проекция $f : G \to G/H$, $x \mapsto xH$ является эпиморфизмом групп, причем* $\operatorname{Ker} f = H$.

Доказательство: ассоциативность очевидна:

$$((xH) \circ (yH)) \circ (zH) = ((xy)H) \circ (zH) = ((xy)z)H = (x(yz))H = (xH) \circ ((yz)H) = (xH) \circ ((yH) \circ (zH)).$$

Далее, покажем, что класс смежности $eH = H$ является единицей:

$$(xH) \circ (eH) = (xe)H = xH, \quad (eH) \circ (xH) = (ex)H = xH.$$

Наконец, проверим, что класс $x^{-1}H$ является обратным к классу xH:

$$(xH) \circ (x^{-1}H) = (xx^{-1})H = eH, \quad (x^{-1}H) \circ (xH) = (x^{-1}x)H = eH.$$

Таким образом, G/H — действительно группа. Вторая же часть теоремы очевидна. □

Группа G/H называется факторгруппой группы G по нормальной подгруппе H. Группы $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}/\mathbb{Z}$ и $\mathbb{C}/\mathbb{Z}$ из прошлой лекции являются примерами факторгрупп.

Теорема 2.10. *Пусть $f : G \to G'$ — гомоморфизм групп. Тогда* $G/\operatorname{Ker} f \cong \operatorname{Im} f$ (канонический изоморфизм).

Доказательство: пусть $H = \operatorname{Ker} f$. Определим отображение $\bar{f} : G/H \to \operatorname{Im} f$ формулой $\bar{f}(xH) = f(x)$. Проверим корректность определения: если $xH = yH$, то $y = xh$, $h \in H$ и $f(y) = f(xh) = f(x)f(h) = f(x)e' = f(x)$, так как $h \in H = \operatorname{Ker} f$. Заметим далее, что

$$\bar{f}(xH \circ yH) = \bar{f}(xyH) = f(xy) = f(x)f(y) = \bar{f}(xH)\bar{f}(yH) \quad \text{и} \quad \bar{f}(eH) = f(e) = e',$$

следовательно $\bar{f}$ — гомоморфизм групп. Наконец, если $\bar{f}(xH) = f(x) = e'$, то $x \in \operatorname{Ker} f = H$, следовательно $xH = eH$, то есть $\bar{f}$ — мономорфизм. Кроме того, очевидно, что $\bar{f}$ — эпиморфизм. Следовательно, $\bar{f}$ — изоморфизм. □

Следствие 2.11. (*i*) *Если $f : G \to G'$ — эпиморфизм групп, то $G' \cong G/\operatorname{Ker} f$.* (*ii*) *Всякий гомоморфизм групп $f : G \to G'$ раскладывается в композицию канонических эпиморфизма, изоморфизма и мономорфизма $G \to G/\operatorname{Ker} f \to \operatorname{Im} f \to G'$.*

Лекция 3. Действия групп и группа перестановок

Часть 1. Действия групп

Определение 1.1. Действие группы G на множестве X — это отображение $a : G \times X \to X$, такое что

$$(i) \qquad \forall g, h \in G,\ x \in X \quad a(g, a(h, x)) = a(gh, x); \qquad\qquad (ii) \qquad \forall x \in X \quad a(e, x) = x.$$

Для упрощения обозначений действие группы G на множестве X часто записывается как $(g, x) \mapsto gx$.

Примеры 1.2. 1. Тривиальное действие: $(g, x) \mapsto x$.

2. Действие групп μ_n, μ, $\mathbf{S}^1$, $\mathbb{R}^+$, $\mathbb{C}^*$ на $\mathbb{C}$ умножением.
3. Действие группы перестановок $\mathfrak{S}_n$ на множестве $\{1, \ldots, n\}$.
4. Действие группы $\mathrm{Aut}(X)$ на X, где X — любая алгебраическая структура.
5. Пусть G — группа. Легко видеть, что отображение $G \times G \to G, \quad (g, x) \mapsto g \circ x$ — это действие группы G на себе. Оно называется действием левыми сдвигами.
6. Пусть G — группа, а $H \subset G$ — подгруппа. Тогда отображение $G \times G/H \to G/H, \quad (g, xH) \mapsto gxH$ — это действие группы G на множестве левых классов смежности G по H.
7. Пусть G — группа. Легко видеть, что отображение $G \times G \to G, \quad (g, x) \mapsto gxg^{-1}$ — это действие группы G на себе. Оно называется действием сопряжениями.
8. Пусть $(g, x) \mapsto gx$ — действие группы G на множестве X, а $f : H \to G$ — гомоморфизм групп. Тогда $(h, x) \mapsto f(h)x$ — действие группы H на X.
9. Пусть $(g, x) \mapsto gx$ — действие группы G на множестве X, а $Y \subset X$ — подмножество, такое что $GY \subset Y$. Тогда $(g, y) \mapsto gy$ является действием группы G на Y.
10. Пусть $(g, x) \mapsto gx$ и $(g, y) \mapsto gy$ — действия группы G на множествах X и Y. Тогда возникают действия группы G на множествах $X \times Y$, $(g, x, y) \mapsto (gx, gy)$, и $\mathrm{Map}(Y, X)$, $(g, f) \mapsto f^g$, где $f^g(y) := gf(g^{-1}y)$.
11. Пусть $(g, x) \mapsto gx$ — действие группы G на множестве X. Тогда возникает действие группы G на множестве всех подмножеств множества X: $(g, Y) \mapsto gY$, где $Y \subset X$.

Лемма 1.3. *Действия группы G на множестве X находятся в биекции с гомоморфизмами $G \to \mathrm{Aut}(X)$.*

Доказательство: пусть $a : G \times X \to X$ — действие G на X. Всякому элементу $g \in G$ сопоставим отображение $a_g : X \to X$, $x \mapsto a(g, x)$. Легко видеть, что $a_{gh}(x) = a(gh, x) = a(g, a(h, x)) = a_g(a_h(x)) = (a_g \circ a_h)(x)$, и $a_e(x) = a(e, x) = x = \mathrm{Id}_X(x)$, следовательно отображение $a : G \to \mathrm{Map}(X, X)$, $g \mapsto a_g$ является гомоморфизмом моноидов. Следовательно, $\forall g \in G\ a(g) \in \mathrm{Aut}(X)$ и $a : G \to \mathrm{Aut}(X)$ — гомоморфизм групп. Обратно, если $a : G \to \mathrm{Aut}(X)$, $g \mapsto a_g$ — гомоморфизм групп, то $(g, x) \mapsto a_g(x)$ — действие группы G на X. □

Замечание 1.4. В примере 1.2.7 отображения $S_g : G \to G$, $x \mapsto gxg^{-1}$, являются не только автоморфизмами G как множества, но и как группы (то есть согласованы с групповым законом и переводят e в e). Таким образом возникает гомоморфизм $S : G \to \mathrm{Aut}(G)$ из группы G в группу ее автоморфизмов. Автоморфизмы S_g называются внутренними автоморфизмами группы G. Легко видеть, что они образуют подгруппу в группе $\mathrm{Aut}(G)$; она обозначается $\mathrm{Inn}(G)$. Можно показать, что $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. Соответствующая факторгруппа $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ называется группой внешних автоморфизмов группы G.

Замечание 1.5. В примере 1.2.5 сдвиги $T_g : G \to G$, $x \mapsto gx$ не являются автоморфизмами группы G.

Действия групп еще называют левыми действиями. Кроме того, можно также рассматривать правые действия, то есть отображения $a' : X \times G \to X$, такие что $a'(a'(x,g),h) = a'(x,gh)$ и $a'(x,e) = x$ для любых $g,h \in G$ и $x \in X$. Примером правого действия является действие группы на себе правыми сдвигами.

Если группа G коммутативна, то всякое левое действие G является правым, и наоборот. В общем же случае это неверно. Однако, левое действие превращается в правое при обращении элемента группы.

Лемма 1.6. *Если $a : G \times X \to X$ — левое действие, то $a'(x,g) := a(g^{-1},x)$ — правое действие. Аналогично, если $a' : X \times G \to X$ — правое действие, то $a(g,x) := a'(x,g^{-1})$ — левое действие.*

Доказательство: $a'(a'(x,g),h) = a(h^{-1},a(g^{-1},x)) = a(h^{-1}g^{-1},x) = a((gh)^{-1},x) = a'(x,gh)$ и так далее. □

Часть 2. Орбиты и стабилизаторы

Пусть группа G действует на множестве X и $x \in X$. Множество $Gx = \{\, gx \mid g \in G \,\} \subset X$ называется орбитой точки x относительно действия группы G. Множество $G_x = \{\, g \in G \mid gx = x \,\} \subset G$ очевидно является подгруппой. Подгруппа G_x называется стабилизатором (стационарной подгруппой) точки x.

Пример 2.1. Пусть X — множество всех подмножеств множества $\{\,1,\ldots,n\,\}$. При действии группы $\mathfrak{S}_n$ на множестве X всякая орбита имеет вид $X \supset X_k = \{$ все k-элементные подмножества в $\{\,1,\ldots,n\,\}\}$. Стабилизатор точки $\{\,i_1,\ldots,i_k\,\} \in X_k \subset X$ — это все перестановки $\sigma \in \mathfrak{S}_n$, такие что $\sigma(\{\,i_1,\ldots,i_k\,\}) = \{\,i_1,\ldots,i_k\,\}$.

Лемма 2.2. *Любые две орбиты либо не пересекаются, либо совпадают.*

Доказательство: предположим, что $Gx \cap Gy \neq \emptyset$. Пусть $z \in Gx \cap Gy$. Тогда $z = gx$ для некоторого $g \in G$, следовательно $x = g^{-1}z$ и, значит, $Gx = Gg^{-1}z = Gz$. Аналогично $Gy = Gz$. Значит $Gy = Gx$. □

Замечание 2.3. Легко видеть, что отношение $x \sim y \iff \exists g \in G\ y = gx$ является отношением эквивалентности на множестве X. Действительно, рефлексивность отношения $\sim$ следует из наличия единицы в группе, симметричность — из существования обратного элемента, а транзитивность — из «ассоциативности» действия. Кроме того, ясно, что классы эквивалентности — это орбиты действия группы.

Если на множестве X задано действие группы G, то говорят, что X — G-множество. Морфизмом G-множеств $X \to Y$ (G-морфизмом, G-эквивариантным отображением) называется отображение $f : X \to Y$, которое коммутирует с действием группы, то есть $\forall g \in G$, $x \in X$ $f(gx) = gf(x)$.

Лемма 2.4. *Пусть группа G действует на множестве X и $x \in X$ — произвольная точка. Тогда G-множества Gx и G/G_x канонически изоморфны.*

Доказательство: легко видеть, что отображение $G/G_x \to Gx$, $gG_x \mapsto gG_xx = gx$, корректно определено. Кроме того, оно очевидно является морфизмом G-множеств. Далее, оно сюръективно по определению орбиты, так что остается проверить его инъективность. Предположим, что gG_x и $g'G_x$ переходят в одну и ту же точку орбиты Gx. Тогда $gx = g'x$, следовательно $(g^{-1}g')x = g^{-1}(g'x) = g^{-1}(gx) = (g^{-1}g)x = ex = x$, значит $g^{-1}g' \in G_x$, следовательно $gG_x = g(g^{-1}g'G_x) = g'G_x$. □

Следствие 2.5. *Длина орбиты Gx равна $(G : G_x)$.*

Лемма 2.6. *Если $y \in Gx$, то подгруппы G_y и G_x сопряжены.*

Доказательство: если $y = gx$, то ясно, что $G_y = gG_xg^{-1}$. □

Следствие 2.7. *Индексы сопряженных подгрупп равны.*

Следствие 2.8. *Пусть группа G действует на конечном множестве X. Пусть $x_1,\ldots,x_k$ — представители орбит. Тогда $|X| = \sum_{i=1}^{k}(G : G_{x_i})$.*

Важным примером действия является действие группы на себе сопряжениями. Элементы группы, лежащие в одной орбите этого действия называются сопряженными. Иначе говоря, $x,y \in G$ сопряжены $\iff$

$\exists g \in G$ так что $x = gyg^{-1}$. Сами орбиты называются классами сопряженности. Легко видеть, что стабилизатором элемента $x \in G$ является его централизатор. Следствие 2.8 в данном случае дает формулу классов:

$$(G:1) = \sum_x (G:Z_x) \qquad \text{(сумма по представителям классов сопряженности)} \tag{2.9}$$

Дадим, наконец, еще несколько определений. Действие группы называется транзитивным, если все множество X состоит из одной орбиты. Действие группы называется свободным, если стабилизатор любой точки тривиален. Действие группы называется точным, если пересечение всех стабилизаторов (т.е. ядро соответствующего гомоморфизма $G \to \mathrm{Aut}(X)$) тривиально.

Часть 3. Группа перестановок

Пусть $i_1, \ldots, i_k$ — попарно различные элементы множества $\{1, \ldots, n\}$. Перестановка, переводящая $i_1 \mapsto i_2 \mapsto i_3 \mapsto \ldots \mapsto i_k \mapsto i_1$ и оставляющая все остальные элементы множества $\{1, \ldots, n\}$ на месте, называется циклом длины n и обозначается $(i_1 i_2 \ldots i_k)$. Заметим, что $(i_1 i_2 i_3 \ldots i_{k-1} i_k) = (i_2 i_3 \ldots i_{k-1} i_k i_1)$. Циклы $(i_1 i_2 \ldots i_k)$ и $(j_1 j_2 \ldots j_l)$ называются независимыми, если $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.

Лемма 3.1. *Независимые циклы коммутируют. Любая перестановка раскладывается в произведение попарно независимых циклов. Такое разложение единственно с точностью до перестановки сомножителей и отбрасывания циклов длины* 1.

Доказательство: первая часть очевидна. Докажем теперь вторую. Пусть $\sigma \in \mathfrak{S}_n$. Рассмотрим действие подгруппы $\mathbb{Z}/m\mathbb{Z} \cong \langle\sigma\rangle \subset \mathfrak{S}_n$ на множестве $\{1 \ldots, n\}$. Пусть $\{i_1^1, \ldots, i_1^s\}$ — представители всех орбит. Для всякого $1 \leqslant t \leqslant s$ положим $i_p^t = \sigma(i_{p-1}^t)$ и пусть k_t — длина орбиты точки i_1^t. Тогда $\langle\sigma\rangle i_1^t \cong \mathbb{Z}/k_t\mathbb{Z}$, поэтому все точки i_p^t при $1 \leqslant p \leqslant k_t$ попарно различны, а $i_{k_t+1}^t = i_1^t$. Более того, легко видеть, что σ раскладывается в произведение циклов $(i_1^1 \ldots i_{k_1}^1) \cdot \ldots \cdot (i_1^s \ldots i_{k_s}^s)$ причем циклы — попарно независимы.

Остается доказать единственность такого разложения. Действительно, пусть $\sigma = (j_1^1 \ldots j_{l_1}^1) \cdot \ldots \cdot (j_1^r \ldots i_{l_r}^r)$ другое разложение. Добавляя циклы длины 1, мы можем считать, что среди чисел j_p^q содержатся все элементы множества $\{1, \ldots, n\}$. Тогда ясно, что орбиты действия группы $\langle\sigma\rangle$ — это в точности подмножества $\{j_1^1 \ldots j_{l_1}^1\}, \ldots, \{j_1^r \ldots i_{l_r}^r\}$. Поэтому $r = s$ и, переставляя циклы и меняя в них первый элемент, мы можем считать, что $j_1^t = i_1^t$ при всех $1 \leqslant t \leqslant s$. Но тогда ясно, что $l_t = k_t$ и $j_p^t = i_p^t$ при всех p. □

Пусть $\sigma = (i_1^1 \ldots i_{k_1}^1) \cdot \ldots \cdot (i_1^s \ldots i_{k_s}^s)$ — разложение перестановки σ в произведение независимых циклов. Ясно, что добавляя циклы длины 1 и переставляя сомножители, можно считать, что $k_1 \geqslant k_2 \cdots \geqslant k_s$ и $k_1 + \cdots + k_s = n$. Другими словами $(k_1, \ldots, k_s)$ — разбиение числа n. Из леммы 3.1 следует, что такое разбиение однозначно определяется перестановкой σ.

Теорема 3.2. *Перестановки σ и σ' — сопряжены, тогда и только тогда когда соответствующие им разбиения числа n совпадают.*

Доказательство: пусть $\sigma = (i_1^1 \ldots i_{k_1}^1) \cdot \ldots \cdot (i_1^s \ldots i_{k_s}^s)$, $k_1 \geqslant \cdots \geqslant k_s$ и $k_1 + \cdots + k_s = n$. Предположим, что $\sigma' = g\sigma g^{-1}$. Тогда ясно, что $\sigma' = (g(i_1^1) \ldots g(i_{k_1}^1)) \cdot \ldots \cdot (g(i_1^s) \ldots g(i_{k_s}^s))$, значит разбиение, соответствующее σ' совпадает с $(k_1, \ldots, k_s)$. Обратно, предположим, что $\sigma' = (j_1^1 \ldots j_{k_1}^1) \cdot \ldots \cdot (j_1^s \ldots j_{k_s}^s)$. Определим перестановку g правилом $g(i_p^t) = j_p^t$. Тогда ясно, что $\sigma' = g\sigma g^{-1}$. □

Цикл длины 2 называется транспозицией.

Лемма 3.3. *Любая перестановка раскладывается в произведение транспозиций.*

Доказательство: заметим, что $(i_1 i_2 i_3 \ldots i_{k-1} i_k) = (i_1 i_2) \cdot (i_2 i_3) \cdot \ldots \cdot (i_{k-1} i_k)$ и применим лемму 3.1. □

Лемма 3.4. *Пусть $\sigma = \tau_1 \cdot \ldots \cdot \tau_N$ — разложение перестановки σ в произведение транспозиций. Тогда четность числа N не зависит от выбора разложения.*

Доказательство: определим число беспорядков перестановки σ как $(\sigma) = |\{(i,j) \mid i < j \text{ и } \sigma(i) > \sigma(j)\}|$. Достаточно проверить, что $N \equiv (\sigma) \bmod 2$. Пусть σ — любая перестановка, а $\tau = (ij)$, $i < j$. Тогда,

$$\text{если } \sigma(i) < \sigma(j), \text{ то } (\sigma \cdot \tau) = (\sigma) + 2|\{k \mid i < k < j \text{ и } \sigma(i) < \sigma(k) < \sigma(j)\}| + 1;$$
$$\text{если } \sigma(i) > \sigma(j), \text{ то } (\sigma \cdot \tau) = (\sigma) - 2|\{k \mid i < k < j \text{ и } \sigma(i) < \sigma(k) < \sigma(j)\}| - 1;$$

так что в любом случае $(\sigma \cdot \tau) \equiv (\sigma) + 1 \bmod 2$, и остается применить индукцию по N. □

Перестановка называется четной, если она представляется в виде произведения четного числа транспозиций, и нечетной в противном случае. Из леммы 3.4 немедленно следует

Теорема 3.5. *Отображение $\varepsilon : \mathfrak{S}_n \to \mu_2 = \{\pm 1\}$, переводящее четные перестановки в 1, а нечетные в -1, является гомоморфизмом групп.*

Число $\varepsilon(\sigma) \in \{\pm 1\}$ называется знаком перестановки σ. Группа четных перестановок $\mathrm{A}_n = \operatorname{Ker}\varepsilon \subset \mathfrak{S}_n$ называется знакопеременной группой. Заметим, что $\mathrm{A}_n \lhd \mathfrak{S}_n$, $\mathfrak{S}_n/\mathrm{A}_n \cong \mu_2$.

Лекция 4. Кольца и модули

Часть 1. Гомоморфизмы колец

Аналогом подгрупп для колец являются подкольца, а аналогом нормальных подгрупп — идеалы.

Определение 1.1. Пусть A — произвольное кольцо. Подмножество $B \subset A$ называется подкольцом, если B — подгруппа в A относительно сложения и выполнены условия $1_A \in B$, $BB \subset B$.

Примеры 1.2.
1. Кольца $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, не имеют нетривиальных подколец.
2. Кольцо $\mathbb{Z}$ является подкольцом в $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$.
3. Кольцо R является подкольцом в кольцах $R[x]$ и $R[[x]]$.
4. Если R — коммутативное кольцо, а $f(x)$ — многочлен (формальный степенной ряд) с коэффициентами в R, то $R[f(x)]$ ($R[[f(x)]]$ соотв.) — покольцо в $R[x]$ ($R[[x]]$ соотв.).
5. Верхнетреугольные матрицы — подкольцо во всех матрицах.
6. Если A — кольцо, $S \subset A$ — подмножество, то $Z_S(A) := \{\, a \in A \mid \forall s \in S\ as = sa \,\}$ — подкольцо.
7. Если A — кольцо, то $Z(A) := Z_A(A) = \{\, a \in A \mid \forall s \in A\ as = sa \,\}$ — подкольцо (центр кольца A).

Определение 1.3. Пусть A — произвольное кольцо, а $I \subset A$ — подгруппа относительно сложения. Тогда I называется левым идеалом, если $AI \subset I$, и правым идеалом, если $IA \subset I$. Если же I является одновременно и правым и левым идеалом, то I называется двусторонним идеалом.

Двусторонние идеалы часто также называются просто идеалами.

Замечание 1.4. Заметим, что идеал (левый, правый или двусторонний) $I \subset A$ является подкольцом, только и если только $I = A$.

Замечание 1.5. Если кольцо A коммутативно, то всякий левый идеал является правым идеалом и, следовательно, двусторонним. Таким образом, в коммутативном случае все эти понятия эквивалентны.

Примеры 1.6.
1. Поле не имеет нетривиальных идеалов.
2. Всякая подгруппа (относительно сложения) в кольцах $\mathbb{Z}$ и $\mathbb{Z}/n\mathbb{Z}$ является идеалом.
3. Пусть A — кольцо и $a \in Z(A)$. Тогда $\{\, f(x) \in A[x] \mid f(a) = 0 \,\}$ — идеал.
4. Матрицы с нулевым первым столбцом образуют левый (но не правый!) идеал в кольце матриц. Аналогично, матрицы с нулевой первой строкой образуют правый (но не левый!) идеал. А нетривиальных двусторонних идеалов в кольце матриц (с коэффициентами в поле) просто нет!
5. Строго верхнетреугольные матрицы — двусторонний идеал в верхнетреугольных матрицах.
6. Если A — кольцо, $S \subset A$ — подмножество, то $AS := \{\, \sum_{i=1}^{m} a_i s_i \,\}$ — левый идеал, $SA := \{\, \sum_{i=1}^{m} s_i a_i \,\}$ — правый идеал, а $ASA := \{\, \sum_{i=1}^{m} a_i s_i a_i' \,\}$ — двусторонний идеал в кольце A (здесь $s_i \in S$, $a_i, a_i' \in A$). Говорят, что эти идеалы порождаются множеством S. Если же кольцо A коммутативно, то очевидно имеем $AS = SA = ASA$.

Определение 1.7. Ядром гомоморфизма колец $f : A \to B$ называется $\operatorname{Ker} f = \{\, a \in A \mid f(a) = 0 \,\}$. Образом гомоморфизма колец $f : A \to B$ называется $\operatorname{Im} f = \{\, b \in B \mid b = f(a),\ a \in A \,\}$.

Следующая лемма очевидно следует из определений.

Лемма 1.8. *Образ гомоморфизма колец $f : A \to B$ — подкольцо в B, а ядро — двусторонний идеал в A.*

Лемма 1.9. *Пусть $f : A \to B$ — гомоморфизм колец. Тогда f является мономорфизмом $\iff \operatorname{Ker} f = \{0\}$; f является эпиморфизмом $\iff \operatorname{Im} f = B$.*

Доказательство: аналогично утверждению о гомоморфизмах групп. □

Ясно, что всякое подкольцо $B \subset A$ является образом некоторого гомоморфизма колец. Покажем, что всякий двусторонний идеал является ядром некоторого гомоморфизма.

Пусть $I \subset A$ — идеал. Заметим, что так как аддитивная группа кольца A коммутативна, а I — подгруппа относительно сложения, то I — нормальная подгруппа, следовательно A/I является абелевой группой относительно операции сложения, заданной формулой

$$(a + I) + (b + I) = (a + b) + I. \tag{1.10}$$

Определим операцию умножения на классах смежности A/I следующим образом:

$$(a + I)(b + I) := ab + I. \tag{1.11}$$

Лемма 1.12. *Операция умножения* (1.11) *на A/I корректно определена.*

Доказательство: допустим $a' + I = a + I$, $b' + I = b + I$. Тогда $a' = a + m$, $b' = b + n$, $m, n \in I$. Следовательно $a'b' = (a + m)(b + n) = ab + mb + an + mn$, причем $mb \in IA \subset I$, $an \in AI \subset I$, $mn \in II \subset I$, следовательно $mb + an + mn \in I$ и $ab + I = a'b' + I$. □

Теорема 1.13. *Множество A/I с операциями сложения и умножения, заданными формулами* (1.10) *и* (1.11) *соотв. является кольцом. Более того, проекция $f : A \to A/I$, $a \mapsto a + I$ является эпиморфизмом колец, причем $\operatorname{Ker} f = I$.*

Доказательство: во-первых, A/I является абелевой группой относительно сложения по теореме о факторгруппе. Во-вторых, A/I является моноидом относительно умножения:

$$((a + I)(b + I))(c + I) = (ab + I)(c + I) = (ab)c + I = a(bc) + I = (a + I)(bc + I) = (a + I)((b + I)(c + I)),$$
$$(a + I)(1 + I) = a \cdot 1 + I = a + I, \quad (1 + I)(a + I) = 1 \cdot a + I = a + I.$$

Наконец, умножение в A/I дистрибутивно:

$$((a+I)+(b+I))(c+I) = ((a+b)+I)(c+I) = (a+b)c+I = (ac+bc)+I = (ac+I)+(bc+I) = (a+I)(c+I)+(b+I)(c+I).$$

Вторая часть теоремы очевидна. □

Кольцо A/I называется факторкольцом кольца A по идеалу I. Кольцо $\mathbb{Z}/n\mathbb{Z}$ является примером факторкольца.

Теорема 1.14. *Пусть $f : A \to B$ — гомоморфизм колец. Тогда $A/\operatorname{Ker} f \cong \operatorname{Im} f$* (канонический изоморфизм).

Доказательство: пусть $I = \operatorname{Ker} f$. Определим отображение $\bar{f} : A/I \to \operatorname{Im} f$ формулой $\bar{f}(a + I) = f(a)$. Далее очевидно. □

Следствие 1.15. (*i*) *Если $f : A \to B$ — эпиморфизм колец, то $B \cong A/\operatorname{Ker} f$.* (*ii*) *Всякий гомоморфизм колец $f : A \to B$ раскладывается в композицию канонических эпиморфизма, изоморфизма и мономорфизма $A \to A/\operatorname{Ker} f \to \operatorname{Im} f \to B$.*

Часть 2. Модули

Определение 2.1. Левым модулем над кольцом A (или левым A-модулем) называется абелева группа M, на которой задано линейное действие кольца A, то есть отображение $A \times M \to M$, $(a, m) \mapsto am$, такое что

$$(ab)m = a(bm), \qquad 1m = m,$$
$$(a + b)m = am + bm, \qquad a(m + n) = am + an.$$

Аналогично определяются правые A-модули.

Примеры 2.2. 1. Всякая абелева группа является $\mathbb{Z}$-модулем.

2. Если A — кольцо, то всякий левый идеал является левым A-модулем, а всякий правый идеал — правым A-модулем. В частности, само кольцо A является модулем над собой.

3. Матрицы размера $n \times m$ являются левым модулем над кольцом матриц размера $n \times n$ и правым модулем над кольцом матриц размера $m \times m$.

4. Если U и V— абелевы группы, то множество $\mathrm{Hom}(U, V)$ гомоморфизмов из U в V является левым модулем над кольцом $\mathrm{End}(V)$ и правым модулем над кольцом $\mathrm{End}(U)$.

5. Пусть M и N — A-модули. Тогда правило $a(m, n) = (am, an)$ задает на прямом произведени абелевых групп $M \times N$ структуру A-модуля. Этот A-модуль называется прямой суммой модулей M и N и обозначается $M \oplus N$.

6. Пусть $\{ M_i \}_{i \in I}$ — произвольное семейство A-модулей. Тогда множество всех наборов $\{ (m_i)_{i \in I} \}$, где $m_i \in M_i$ и во всяком наборе $\{ (m_i) \}$ все элементы кроме конечного числа равны нулю, является A-модулем относительно действия $a(m_i) = (am_i)$. Этот A-модуль называется прямой суммой A-модулей M_i и обозначается $\bigoplus_{i \in I} M_i$.

7. Прямая сумма (конечная или бесконечная) A-модулей A называется свободным A-модулем.

Замечание 2.3. Если кольцо A коммутативно, то всякий левый A-модуль является правым A-модулем и наоборот.

Упражнение 2.4. Пусть M — левый A-модуль. Покажите, что $\forall a \in A$, $m \in M$ имеем $0m = 0$, $a0 = 0$, $(-a)m = -am$.

Лемма 2.5. *Структуры A-модуля на абелевой группе M находятся в биекции с гомоморфизмами колец $A \to \mathrm{End}(M)$.*

Доказательство: пусть M — A-модуль. Всякому элементу $a \in A$ сопоставим отображение $\rho(a) : M \to M$, $m \mapsto am$. Легко видеть, что $\rho(a) \in \mathrm{End}(M)$, и что $\rho : A \to \mathrm{End}(M)$ — гомоморфизм колец. Обратно, пусть $\rho : A \to \mathrm{End}(M)$ — гомоморфизм колец. Тогда ясно, что M является A-модулем относительно действия $am := \rho(a)(m)$. □

Пусть M — левый A-модуль. Абелева подгруппа $N \subset M$ называется A-подмодулем, если $AN \subset N$. Аналогично определяются подмодули в правых модулях.

Пусть M-левый A-модуль, а $S \subset M$ — произвольное подмножество его элементов. Тогда множество $AS := \{ \sum_{s \in S} a_s s \} \subset M$, где $a_s \in A$ и во всякой сумме все слагаемые кроме конечного числа равны нулю, является подмодулем. Если $AS = M$, то говорят, что S является множеством образующих для модуля M, или что A-модуль M порождается множеством S. Если у модуля M существует конечное множество образующих, то M называется конечно порожденным.

Определение 2.6. Подмножество $S \subset M$ называется линейно независимым, если $\sum_{s \in S} a_s s = 0 \Longrightarrow \forall s$ $a_s = 0$. Множество образующих S называется базисом, если оно линейно независимо.

Лемма 2.7. *Если S — базис в M, то всякий элемент модуля M единственным образом представляется в виде суммы $\sum_{s \in S} a_s s$, в которой все слагаемые кроме конечного числа равны нулю.*

Доказательство: существование такого представления вытекает из того, что S-множество образующих, так что остается проверить единственность. Пусть $\sum_{s \in S} a_s s = \sum_{s \in S} b_s s$. Тогда $\sum_{s \in S} (a_s - b_s) s = 0$, следовательно $a_s = b_s$ при всех $s \in S$ в силу линейной независимости. □

Пусть M и N — A-модули. Гомоморфизм абелевых групп $f : M \to N$ называется гомоморфизмом A-модулей, если $f(am) = af(m)$ для всех $a \in A$, $m \in M$. Гомоморфизм A-модулей называется моно(эпи, изо, эндо, авто)морфизмом, если он является моно(эпи, изо, эндо, авто)морфизмом абелевых групп. Множество всех гомоморфизмов A-модулей $M \to N$ обозначается $\mathrm{Hom}_A(M, N)$, а множество всех эндоморфизмов A-модуля M обозначается $\mathrm{End}_A(M)$.

Теорема 2.8. *A-модуль M обладает базисом $\Longleftrightarrow$ M изоморфен свободному A-модулю.*

Доказательство: Пусть $M = \bigoplus_{i\in I} A$. Пусть $s_i \in M$ — элемент, все координаты кроме i-ой которого равны 0, а i-ая координата равна 1. Тогда легко видеть, что $S = \{ s_i \}_{i\in I}$ — базис в M. Обратно, пусть M — произвольный A-модуль с базисом S. Докажем, что он изоморфен прямой сумме $\bigoplus_{s\in S} A$. Определим отображение $f : \bigoplus_{s\in S} A \to M$ правилом $(a_s)_{s\in S} \mapsto \sum_{s\in S} a_s s$. Легко проверить, что f — гомоморфизм A-модулей, а из леммы 2.7 следует, что f — изоморфизм. □

Легко видеть, что множество $\mathrm{Hom}_A(M, N)$ является абелевой группой относительно операции поточечного сложения $(f + g)(m) = f(m) + g(m)$. Если же кольцо A-коммутативно, то множество $\mathrm{Hom}_A(M, N)$ обладает также структурой A-модуля относительно операций $(af)(m) = a(f(m))$. Действительно,

$$(af)(bm) = af(bm) = abf(m) = baf(m) = b(af)(m),$$

поэтому af является гомоморфизмом A-модулей, а остальные условия проверяются элементарно.

Лекция 5. Линейная алгебра

Часть 1. Векторные пространства

Определение 1.1. Пусть K — поле. Всякий K-модуль называется векторным пространством над полем K или K-векторным пространством. Элементы векторного пространства V называются векторами.

Лемма 1.2. *Пусть K — поле, а множество S порождает векторное пространство V. Тогда существует подмножество $S' \subset S$, являющееся базисом в V.*

Доказательство: пусть $S' \subset S$ — максимальное линейно независимое множество[1]. Докажем, что оно является базисом. Заметим, что по определению S' линейно независимо, так что остается проверить, что S' порождает V. Действительно, возьмем произвольный элемент $s \in S \setminus S'$. Ясно, что множество $S' \cup \{ s \}$ не является линейно независимым, следовательно существует линейная зависимость $a_s s + \sum_{t \in S'} a_t t = 0$. Ясно, что $a_s \neq 0$, так как иначе множество S' было бы линейно зависимым. Следовательно, $a_s \in K$ — обратим! Умножая на a_s^{-1} получаем $s = \sum_{t \in S'} (-a_s^{-1} a_t) t$. Таким образом, мы доказали, что подмодуль $KS' \subset V$ содержит все множество S, следовательно $KS' = KS = V$. □

Замечание 1.3. Аналогично доказывается, что если множество S порождает V, а подмножество $S_0 \subset S$ — линейно независимо, то существует подмножество $S_0 \subset S' \subset S$, являющееся базисом в V. Для этого достаточно взять за S' максимальное линейно независимое подмножество в S, содержащее S_0.

Следствие 1.4. *Всякое векторное пространство V обладает базисом. Всякое линейно независимое подмножество в V может быть дополнено до базиса. Если V — конечно порождено, то V обладает базисом из конечного числа элементов.*

Лемма 1.5. *Пусть V — векторное пространство, $U, W \subset V$ — произвольные подпространства. Тогда $U + W = \{ v \in V \mid v = u + w,\ u \in U,\ w \in W \}$ и $U \cap W$ — подпространства в V.*

Лемма 1.6. *Пусть $U, W \subset V$ — подпространства, такие что $U + W = V$ и $U \cap W = \{ 0 \}$. Тогда всякий вектор $v \in V$ единственным образом раскладывается в сумму $v = u + w$, где $u \in U$ и $w \in W$. В частности, $V \cong U \oplus W$.*

Доказательство: разложимость следует из того, что $V = U + W$. Предположим, что $u + w = u' + w'$. Тогда $u - u' = w' - w$. Но левая часть лежит в U, а правая в W, следовательно этот вектор лежит в $U \cap W = \{ 0 \}$. Значит $u' = u$ и $w' = w$ и разложение единственно. Рассмотрим теперь отображение $f : U \oplus W \to V$, $(u, w) \mapsto u + w \in V$. Легко видеть, что f — изоморфизм векторных пространств. □

В такой ситуации говорят, что пространство V раскладывается в прямую сумму подпространств U и W, а подпространство W называется дополнительным подпространством к U в V.

Теорема 1.7. *Для всякого подпространства U в векторном пространстве V существует дополнительное подпространство.*

Доказательство: выберем базис $\{ u_i \}$ в U, дополним его до базиса $\{ u_i \} \cup \{ w_j \}$ в V и положим $W = K\{ w_j \}$. Очевидно, что $U + W = V$ и $U \cap W = \{ 0 \}$. □

Заметим, что как разложение в прямую сумму, так и выбор дополнительного подпространства зависят от выбора базиса, то есть *не являются каноническими*!

[1] Если множество S конечно, то существование такого S' очевидно. Если же S бесконечно, надо воспользоватьмя леммой Цорна, то есть проверить, что для всякой возрастающей цепочки $S'_1 \subset S'_2 \subset \cdots \subset S'_n \subset \ldots$ линейно независимых подмножеств в S найдется линейно независимое подмножество S', такое что $S'_i \subset S'$ при всех i. Действительно, возьмем $S' = \bigcup_{i=1}^{\infty} S'_i$. Если $\sum_{p=1}^{m} a_p s_p = 0$ — линейное соотношение, в котором $s_1, \ldots, s_m \in S'$, то найдется i, такое что $s_1, \ldots, s_m \in S'_i$, следовательно $a_1 = \cdots = a_m = 0$, так как S'_i линейно независимо. Значит S' линейно независимо.

Замечание 1.8. В доказательстве приведенных выше утверждений коммутативность не используется. Следовательно, все утверждения справедливы также для модулей над произвольным телом.

Часть 2. Базисы и размерность

Определение 2.1. Пусть (e_i) — произвольный набор векторов в векторном пространстве V, Говорят, что набор векторов (e'_i) получен из набора (e_i) элементарным преобразованием, если

$$\text{либо } (i) \qquad \text{набор } (e'_i) \text{ является транспозицией набора } (e_i);$$

$$\text{либо } (ii) \qquad e'_i = \begin{cases} \lambda e_{i_0}, & i = i_0 \\ e_i, & i \neq i_0 \end{cases}, \text{ где } i_0 \text{ — произвольно и } \lambda \in K \text{ — обратим;}$$

$$\text{либо } (iii) \qquad e'_i = \begin{cases} e_{i_0} + \lambda e_{i_1}, & i = i_0 \\ e_i, & i \neq i_0 \end{cases}, \text{ где } i_0, i_1 \text{ и } \lambda \in K \text{ — произвольны.}$$

Лемма 2.2. *Пусть набор векторов (e'_i) в векторном пространстве V получен из набора (e_i) элементарным преобразованием. Тогда (e_i) — линейно независим (порождает V, является базисом в V) тогда и только тогда, когда соответствующие свойства выполнены для набора (e'_i).*

Доказательство: легко проверить, что наличие линейной зависимости между векторами e'_i влечет наличие линейной зависимости между векторами e_i. Следовательно, если векторы e_i линейно независимы, то и векторы e'_i линейно независимы. Далее, любой из векторов e_i выражается через векторы e'_i. Значит векторы e'_i порождают пространство V, если векторы e_i его порождали. Более того, отсюда следует, что если e_i образуют базис, то e'_i тоже образуют базис. Наконец, легко видеть, что набор (e_i) сам получается элементарным преобразованием из набора (e'_i), следовательно обратные утверждения также верны. □

Определение 2.3. Пусть (x_{ij}) — матрица с коэффициентами в произвольном кольце A. Говорят, что матрица (x'_{ij}) получена из матрицы (x_{ij}) элементарным преобразованием строк, если

$$\text{либо } (i) \qquad \text{матрица } (x'_{ij}) \text{ получена произвольной транспозицией строк матрицы } (x_{ij});$$

$$\text{либо } (ii) \qquad x'_{ij} = \begin{cases} \lambda x_{i_0 j}, & i = i_0 \\ x_{ij}, & i \neq i_0 \end{cases}, \text{ где } i_0 \text{ — произвольно и } \lambda \in A \text{ — обратим;}$$

$$\text{либо } (iii) \qquad x'_{ij} = \begin{cases} x_{i_0 j} + \lambda x_{i_1 j}, & i = i_0 \\ x_{ij}, & i \neq i_0 \end{cases}, \text{ где } i_0, i_1 \text{ и } \lambda \in A \text{ — произвольны.}$$

Аналогично определяются элементарные преобразования столбцов матрицы.

Замечание 2.4. Любое элементарное преобразование строк матрицы (x_{ij}) получается левым умножением некоторой обратимой матрицы на матрицу (x_{ij}). Любое элементарное преобразование столбцов матрицы (x_{ij}) получается правым умножением некоторой обратимой матрицы на матрицу (x_{ij}).

Определение 2.5. Матрица (x_{ij}) размера $n \times m$ называется

верхнеступенчатой, если $x_{ij} = 0$ при $j < l_i$ и $x_{il_i} = 1$, если $l_i \leqslant m$, где $1 \leqslant l_1 < l_2 < \cdots < l_n$;

нижнеступенчатой, если $x_{ij} = 0$ при $i < l_j$ и $x_{l_j j} = 1$, если $l_j \leqslant n$, где $1 \leqslant l_1 < l_2 < \cdots < l_m$;

стандартной, если $x_{ii} = 1$ при $1 \leqslant i \leqslant r$ и $x_{ij} = 0$ иначе, где $1 \leqslant r \leqslant m, n$.

Лемма 2.6. *Любая матрица с коэффициентами в поле элементарными преобразованиями строк может быть приведена к верхнеступенчатому виду, элементарными преобразованиями столбцов — к нижнеступенчатому виду, а если использовать и те и другие преобразования — то к стандартному виду.*

Докажем первое утверждение. Пусть (x_{ij}) — произвольная матрица. Пусть $l_1 = \min\{\, j \mid x_{ij} \neq 0 \,\}$ и пусть $x_{i_1,l_1} \neq 0$. Пусть (x'_{ij}) получена из (x_{ij}) перестановкой 1-ой и i_1-ой строки (элементарное преобразование первого типа); (x''_{ij}) получена из (x'_{ij}) умножением первой строки на $(x'_{1l_1})^{-1}$ (элементарное преобразование второго типа), а матрица (x'''_{ij}) получена из (x''_{ij}) прибавлением к i-ой строке первой строки, умноженной

на $-x''_{il_1}$, где $i = 2, \ldots, n$ (последовательность элементарных преобразований третьего типа). Применяя ту же процедуру еще $n-1$ раз, приводим матрицу к верхнеступенчатому виду. Второе и третье утверждения доказываются аналогично. □

Пусть (e_i) — базис в векторном пространстве V. Всякий вектор $v \in V$ может быть единственным образом представлен в виде линейной комбинации $v = \sum_{i=1}^{n} x_i e_i$. Элементы $x_i \in K$ называются координатами вектора v относительно базиса e_i. Вектор v удобно записывать в виде столбца из его координат. Соответственно, всякий набор векторов $v_1, \ldots, v_m$ можно представить в виде $n \times m$ матрицы (x_{ij}), j-ый столбец которой состоит из координат вектора v_j.

Лемма 2.7. *Пусть (x_{ij}) — матрица координат набора векторов $v_1, \ldots, v_m$ в векторном пространстве V относительно базиса $e_1, \ldots, e_n$. Тогда элементарные операции над строками матрицы (x_{ij}) соответствуют элементарным преобразованиям базиса (e_i), а элементарные операции над столбцами матрицы (x_{ij}) соответствуют элементарным преобразованиям набора векторов (v_j).*

Доказательство: непосредственна проверка. □

Следствие 2.8. *Пусть $e_1, \ldots, e_n$ — базис в V, а $v_1, \ldots, v_m$ — линейно независисмы. Тогда $m \leqslant n$. Если же $m = n$, то $v_1, \ldots, v_m$ — базис в V.*

Доказательство: выберем последовательность элементарных преобразований строк и столбцов матрицы координат набора векторов $v_1, \ldots, v_m$ относительно базиса $e_1, \ldots, e_n$, приводящую ее к стандартному виду и применим соответствующие последовательности элементарных преобразований к базису (e_i) и набору (v_j). Пусть (e'_i) и (v'_j) — полученные наборы. Тогда из леммы 2.2 следует, что e'_i — базис, а набор v'_j — линейно независим. С другой стороны, по лемме 2.7 матрица координат набора векторов v'_j относительно базиса e'_i имеет стандартный вид. Следовательно, $v'_i = e'_i$ при $1 \leqslant i \leqslant r$ и $v'_i = 0$ при $r < i \leqslant m$. Значит $m = r \leqslant n$. Более того, если $m = r = n$, то $v'_i = e'_i$ при $1 \leqslant i \leqslant n$, следовательно $v'_1, \ldots, v'_m$ образуют базис, значит по лемме 2.2 векторы $v_1, \ldots, v_m$ тоже образуют базис. □

Следствие 2.9. *Количество векторов во всех базисах векторного пространства V одинаково.*

Определение 2.10. Количество векторов в любом из базисов векторного пространства V называется размерностью V и обозначается $\dim V$.

Лемма 2.11. *Если $U \subset V$, то $\dim U \leqslant \dim V$, причем, если $\dim U = \dim V < \infty$, то $U = V$. Если $V = U \oplus W$, то $\dim V = \dim U + \dim W$.*

Доказательство: первое утверждение следует из 2.8. Пусть $V = U \oplus W$. Выберем базис $\{ u_i \}$ в U и базис $\{ w_j \}$ в W. Тогда $\{ u_i \} \cup \{ w_j \}$ — базис в $U \oplus W$. □

Часть 3. Гомоморфизмы

Определение 3.1. Гомоморфизм векторных пространств над K — это гомоморфизм K-модулей, то есть гомоморфизм абелевых групп, коммутирующий с умножением на K. Ядро гомоморфизма $f : U \to V$ — это $\operatorname{Ker} f := \{ u \in U \mid f(u) = 0 \} \subset U$, а образ — это $\operatorname{Im} f := \{ v \in V \mid v = f(u),\ u \in U \}$.

Как обычно, выполнены свойства:

Лемма 3.2. *Пусть $f : U \to V$ — гомоморфизм векторных пространств. Тогда f является мономорфизмом $\iff \operatorname{Ker} f = \{ 0 \}$; f является эпиморфизмом $\iff \operatorname{Im} f = V$.*

Теорема 3.3. *Пусть V — векторное пространство над K, $U \subset V$ — подпространство. Факторгруппа V/U обладает структурой K-векторного пространства: $\lambda(v + U) = \lambda v + U$, $\lambda \in K$. Более того, проекция $f : V \to V/U$ является эпиморфизмом векторных пространств, причем $\operatorname{Ker} f = U$.*

Векторное пространство V/U называется факторпространством V по U.

Теорема 3.4. *Пусть $f : U \to V$ — гомоморфизм колец. Тогда $U/\operatorname{Ker} f \cong \operatorname{Im} f$* (канонический изоморфизм).

Следствие 3.5. *(i) Если $f : U \to V$ — эпиморфизм колец, то $V \cong U/\operatorname{Ker} f$. (ii) Всякий гомоморфизм колец $f : U \to V$ раскладывается в композицию канонических эпиморфизма, изоморфизма и мономорфизма $U \to U/\operatorname{Ker} f \to \operatorname{Im} f \to V$.*

Важным свойством векторных пространств является

Лемма 3.6. *Пусть $e_1, \ldots, e_n$ — базис в V, а $u_1, \ldots, u_n$ — произвольный набор векторов в U. Тогда существует единственный гомоморфизм $f : V \to U$, такой что $f(e_i) = u_i$, $i = 1, \ldots, n$.*

Замечание 3.7. Свойства 3.2–3.5 выполнены для гомоморфизмов модулей над произвольным фиксированным кольцом, в частности для абелевых групп, а свойство 3.6 для свободного модуля V над любым кольцом.

Лекция 6. Операторы

Часть 1. Линейные отображения и матрицы

Пусть $A : V \to U$ — линейное отображение K-векторных пространств. Выберем базисы $f_1, \dots, f_m$ и $e_1, \dots, e_l$ в V и U соответственно. Разложим каждый из векторов $A(f_j) \in U$ по базису e_i:

$$A(f_j) = \sum_{i=1}^{l} a_{ij} e_i, \qquad a_{ij} \in K. \tag{1.1}$$

Матрица $A = (a_{ij})$ называется матрицей отображения A относительно базисов e_i и f_j.

Лемма 1.2. *Формула* (1.1) *задает биекцию* $\mathrm{Hom}_K(U, V) \cong \mathrm{Mat}_{l \times m}(K)$.

Доказательство: Заметим сначала, что если $A : V \to U$ — линейное отображение с матрицей A, то $A(\sum_{j=1}^{m} x_j f_j) = \sum_{j=1}^{m} x_j A(f_j) = \sum_{j=1}^{m} x_j (\sum_{i=1}^{l} a_{ij} e_i) = \sum_{i=1}^{l} (\sum_{j=1}^{m} a_{ij} x_j) e_i$, значит матрица определяет отображение однозначно. Более того, приведенное вычисление показывает, как по всякой матрице построить линейноне отображение, матрицей которого она являеся. □

Замечание 1.3. Как $\mathrm{Hom}_K(U, V)$, так и $\mathrm{Mat}_{l \times m}(K)$ являются векторными пространствами над полем K, а биекция (1.1) — линейна.

Пусть W — еще одно векторное пространство с базисом $g_1, \dots, g_n$, а $B : W \to V$ — линейное отображение с матрицей $B = (b_{jk})$.

Лемма 1.4. *Произведение матриц $A \cdot B$ является матрицей композиции отображений $A \circ B : W \to U$ относительно базисов e_i и g_k.*

Доказательство: $(A \circ B)(g_k) = A(B(g_k)) = A(\sum_{j=1}^{m} b_{jk} f_j) = \sum_{i=1}^{l} (\sum_{j=1}^{m} a_{ij} b_{jk}) e_i$. □

Пусть $e_1, \dots, e_l$ и $e'_1, \dots, e'_l$ — два базиса в пространстве U, а $X = (x_{ij})$ и $X' = (x'_{ij})$ — матрицы координат векторов e'_i относительно базиса e_i и векторов e_i относительно базиса e'_i соответственно. Тогда

$$e_i = \sum_{j=1}^{l} x'_{ij} e'_j = \sum_{j=1}^{l} x'_{ij} (\sum_{k=1}^{l} x_{jk} e_k) = \sum_{k=1}^{l} (\sum_{j=1}^{l} x'_{ij} x_{jk}) e_k, \quad e'_i = \sum_{j=1}^{l} x_{ij} e_j = \sum_{j=1}^{l} x_{ij} (\sum_{k=1}^{l} x'_{jk} e'_k) = \sum_{k=1}^{l} (\sum_{j=1}^{l} x_{ij} x'_{jk}) e'_k,$$

следовательно $X' \cdot X = X \cdot X' = E$, значит $X' = X^{-1}$. Матрица координат базиса e'_i относительно базиса e_i называется матрицей перехода от базиса e_i к базису e'_i. Предыдущие вычисления доказывают

Лемма 1.5. *Матрица перехода от базиса e_i к базису e'_i обратима; обратной к ней является матрица перехода от базиса e'_i к базису e_i.*

Пусть $e_1, \dots, e_m$ и $e'_1, \dots, e'_m$ — два базиса в U, $f_1, \dots, f_n$ и $f'_1, \dots, f'_n$ — два базиса в V, а X и Y — матрицы перехода от базисов e_i и f_i к базисам e'_i и f'_i — соответственно. Пусть далее $A : V \to U$ — линейное отображение, а A — его матрица относительно базисов f_i и e_i.

Лемма 1.6. *Матрица отображения A относительно базисов f'_i и e'_i равна $X^{-1} \cdot A \cdot Y$.*

Доказательство: по лемме 1.5 матрица $X^{-1} = (x'_{ij})$ является матрицей перехода от базиса e'_i к базису e_i, поэтому

$$A(f'_l) = A(\sum_{k=1}^{n} y_{kl} f_k) = \sum_{k=1}^{n} y_{kl} A(f_k) = \sum_{k=1}^{n} \sum_{j=1}^{m} a_{jk} y_{kl} e_j = \sum_{k=1}^{n} \sum_{j=1}^{m} \sum_{i=1}^{m} x'_{ij} a_{jk} y_{kl} e'_i.$$

□

Следствие 1.7. *Если e_i и e'_i — базисы в V с матрицей перехода X, а $A : V \to V$ — линейный оператор с матрицей A относительно базиса e_i, то матрица оператора A относительно базиса e'_i равана $X^{-1} \cdot A \cdot X$.*

Часть 2. След, определитель и характеристический многочлен.

Определение 2.1. Пусть $A = (a_{ij})$ — $n \times n$ матрица с коэффициентами в поле K. Следом, определителем и характеристическим многочленом матрицы A называются выражения

$$\operatorname{tr} A = \sum_{i=1}^{n} a_{ii} \in K, \qquad \det A = \sum_{\sigma \in \mathfrak{S}_n} \left(\varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \right) \in K, \qquad \chi_A(t) = \det(tE_n - A) \in K[t],$$

где E_n — единичная матрица размера $n \times n$.

Примеры 2.2. 1. Если $n = 2$, то $\operatorname{tr} A = a_{11} + a_{22}$, $\det A = a_{11}a_{22} - a_{12}a_{21}$, $\chi_A(t) = t^2 - (\operatorname{tr} A)t + \det A$.

2. Если $n = 3$, то $\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$.

Лемма 2.3. *Определитель является полилинейной знакопеременной функцией строк (столбцов) матрицы. Иначе говоря, если $A_1, \dots, A_n$ — строки матрицы A, то*

$$\det(\dots, A'_i + \lambda A''_i, \dots) = \det(\dots, A'_i, \dots) + \lambda \det(\dots, A''_i, \dots) \qquad \text{(полилинейность)},$$
$$\text{если } A_i = A_j \text{ при } i \neq j, \text{ то } \det(A_1, \dots, A_n) = 0 \qquad \text{(знакопеременность)},$$

и аналогично по отношению к столбцам.

Доказательство: полилинейность определителя по строкам следует из того, что каждое из слагаемых в формуле — полилинейно. Если же $A_i = A_j$, то слагаемые, соответствующие перестановкам σ и $\sigma \circ (ij)$ сокращаются, отсюда следует знакопеременность. Что касается полилинейности и знакопеременности по столбцам, то они доказываются аналогично с помощью формулы $\det A = \sum_{\sigma \in \mathfrak{S}_n} \left(\varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i} \right)$, которая следует из того, что $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ для любой перестановки σ. □

Замечание 2.4. Из знакопеременности и полилинейности следует кососимметричность: действительно, имеем

$$\begin{aligned}\det(\dots, A_i + A_j, \dots, A_i + A_j, \dots) = \det(\dots, A_i, \dots, A_i, \dots) + \det(\dots, A_i, \dots, A_j, \dots) \\ + \det(\dots, A_j, \dots, A_i, \dots) + \det(\dots, A_j, \dots, A_j, \dots),\end{aligned}$$

причем левая часть, а также первое и четвертое слагаемые правой части равны нулю, откуда немедленно следует, что $\det(\dots, A_i, \dots, A_j, \dots) = -\det(\dots, A_j, \dots, A_i, \dots)$.

Следствие 2.5. *Если у матрицы две строки (столбца) пропорциональны, то определитель равен нулю.*

Теорема 2.6. *Если $D : \operatorname{Mat}_{n\times n}(K) \to K$ — полилинейная знакопеременная функция строк матрицы, то $D(A) = \det(A)D(E_n)$.*

Доказательство: обозначим через e_i строку длины n с единицей на i-ом месте и нулями в сотальных местах. Тогда i-ая строка матрицы A равна $A_i = \sum_{j=1}^{n} a_{ij}e_j$. Следовательно, в силу полилинейности имеем $D(A_1, \dots, A_n) = D(\sum_{j=1}^{n} a_{1j}e_j, \dots, \sum_{j=1}^{n} a_{nj}e_j) = \sum_{j_1,\dots,j_n=1}^{n} (\prod_{i=1}^{n} a_{ij_i}) D(e_{j_1}, \dots, e_{j_n})$. Далее, в силу знакопеременности, все слагаемые, для которых $(j_1, \dots, j_n)$ не является перестановкой множества $\{1, \dots, n\}$ равны нулю, а для любой перестановки $\sigma \in \mathfrak{S}_n$ имеем в силу кососимметричности $D(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \varepsilon(\sigma)D(e_1, \dots, e_n) = \varepsilon(\sigma)D(E_n)$. Значит $D(A) = \sum_{\sigma \in \mathfrak{S}_n} (\varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}) D(E_n) = \det(A)D(E_n)$. □

Теорема 2.7. *Имеем* $\det(A \cdot B) = \det A \det B$, $\operatorname{tr}(A \cdot B) = \operatorname{tr}(B \cdot A)$.

Доказательство: зафиксируем матрицу B и рассмотрим отображение $D : \operatorname{Mat}_n(K) \to K$, $A \mapsto \det(AB)$. Легко видеть, что строки матрицы $C = AB$ имеют вид $C_i = A_i \cdot B$, то есть линейно зависят от строк матрицы A. Поэтому D является полилинейной функцией строк матрицы A. Кроме того, если $A_i = A_j$, то $C_i = C_j$, поэтому D является знакопеременной функцией строк матрицы A. Следовательно, по теореме 2.6 имеем $D(A \cdot B) = \det(A)D(E)$, но $D(E) = \det(E \cdot B) = \det(B)$ по определению фунции D. Значит $\det(A \cdot B) = \det A \det B$.

Со следом все еще проще — легко видеть, что $\operatorname{tr}(A \cdot B) = \sum_{i,j=1}^{n} a_{ij}b_{ji} = \sum_{i,j=1}^{n} b_{ij}a_{ji} = \operatorname{tr}(B \cdot A)$. □

Следствие 2.8. *Если матрица X обратима, то* $\operatorname{tr}(X^{-1}AX) = \operatorname{tr} A$, $\det(X^{-1}AX) = \det A$, $\chi_{X^{-1}AX}(t) = \chi_A(t)$.

Следствие 2.9. *След, определитель и характеристический многочлен матрицы оператора не зависят от выбора базиса в векторном пространстве.*

Тем самым, имеет смысл говорить о следе, определителе и характеристическом многочлене оператора.

Часть 3. Формула обращения матрицы

Определение 3.1. Пусть $A = (a_{ij})$ — матрица размера $m \times n$ с коэффициентами в K. Пусть $I \subset \{1, \dots, m\}$, $J \subset \{1, \dots, n\}$ — k-элементные подмножества. Определитель подматрицы $A_{IJ} = (a_{ij})_{i \in I, j \in J}$ называется минором матрицы A порядка k.

Примеры 3.2. Миноры порядка 1 — это коэффициенты матрицы; минор порядка n — определитель.

Пусть $A = (A_{ij})$ — квадратная матрица. Обозначим через A_{ij} матрицу, полученную вычеркиванием i-ой строки и j-го столбца в матрице A.

Лемма 3.3. *Для любого i имеем $\sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det A_{ik} = \det A$, $\sum_{k=1}^{n} (-1)^{k+i} a_{ki} \det A_{ki} = \det A$.*

Доказательство: следует из определения. □

Следствие 3.4. *Если $i \neq j$, то $\sum_{k=1}^{n} (-1)^{i+k} a_{jk} \det A_{ik} = 0$, $\sum_{k=1}^{n} (-1)^{k+j} \det A_{kj} a_{ki} = 0$.*

Доказательство: по предыдущей лемме эти первое из выражений равняется определителю матрицы, в которой i-ая строка равна j-ой строке, и значит равняется нулю. Аналогично со вторым выражением. □

Обозначим через $\widehat{A}$ матрицу $((-1)^{i+j} \det(A_{ji}))$ (обратите внимание на перестановку индексов!). Матрица $\widehat{A}$ называется присоединенной к матрице A.

Теорема 3.5. *Имеем $A \cdot \widehat{A} = \widehat{A} \cdot A = \det(A) \cdot E_n$.*

Доказательство: следует из 3.3 и 3.4. □

Следствие 3.6. *Если $\det A$ обратим в K, то $A^{-1} = \dfrac{1}{\det A} \widehat{A}$.*

Замечание 3.7. Все эти результаты выполняются также для операторов в произвольном конечно порожденном свободном модуле над любым коммутативным кольцом.

Теорема 3.8. *Пусть A — оператор. Следующие утверждения равносильны:*
(i) A — обратим; (ii) A — инъективен; (iii) A — сюръективен; (iv) $\det A \neq 0$.

Доказательство: заметим, что $\dim \operatorname{Ker} A + \dim \operatorname{Im} A = n$, поэтому $(ii) \iff (iii)$. Но с другой стороны, всякий инъективный и сюрьективный оператор биективен, следовательно обратим. Тем самым мы показали, что $(i) \iff (ii) \iff (iii)$. Далее, если A — обратим, то $1 = \det(E_n) = \det(A \cdot A^{-1}) = \det A \det(A^{-1})$, следовательно $\det A \neq 0$, а если $\det A \neq 0$, то A обратим по 3.6. Значит $(i) \iff (iv)$. □

Часть 4. Ранг оператора

Определение 4.1. Строчным рангом матрицы A называется максимальное число линейно независимых строк в A, а столбцовым рангом матрицы A — максимальное число линейно независимых столбцов в A.

Лемма 4.2. *Строчный ранг матрицы равен ее столбцовому рангу и равен размеру ее максимального ненулевого минора.*

Доказательство: легко проверить, что при элементарных операциях ни строчный, ни столбцовый ранг матрицы не меняются. Кроме того, миноры матрицы тоже по существу не меняются (либо переставляются, либо умножаются на обратимый элемент). Следовательно, достаточно рассмотреть очевидный случай стандартной матрицы. □

Ранг матрицы A обозначается $r(A)$.

Лемма 4.3. *Ранг матрицы линейного отображения $A : V \to U$ равен размерности его образа.*

Доказательство: образ отображения порождается столбцами его матрицы. □

Следствие 4.4. *Пусть $A : V \to U$ — линейное отображение. Тогда A — инъективен $\iff r(A) = \dim V$; A — сюръективен $\iff r(A) = \dim U$.*

Лекция 7. Операторы - 2

Часть 1. Собственные и корневые векторы

Пусть A — оператор в векторном пространстве V над полем K.

Определение 1.1. Вектор $v \in V$ называется собственным вектором оператора $A : V \to V$, если $Av = \lambda v$, $\lambda \in K$. Число $\lambda \in K$, для которого существует нетривиальный собственный вектор, называется собственным значением оператора A.

Лемма 1.2. *Множество собственных векторов оператора A с собственным значением λ является векторным подпространством в V.*

Доказательство: если $Av_1 = \lambda v_1$ и $Av_2 = \lambda v_2$, то $A(v_1 + v_2) = Av_1 + Av_2 = \lambda v_1 + \lambda v_2 = \lambda(v_1 + v_2)$. □

Лемма 1.3. *Число λ является собственным значением оператора $A \iff \chi_A(\lambda) = 0$.*

Доказательство: из определения собственного вектора следует, что λ — собственное значение $\iff$ $\operatorname{Ker}(\lambda \operatorname{Id} - A) \neq 0 \iff \det(\lambda \operatorname{Id} - A) = \chi_A(\lambda) = 0$. □

Следствие 1.4. *Если характеристический многочлен $\chi_A(t)$ имеет $n = \dim V$ различных корней, то существует базис, в котором матрица оператора A диагональна.*

Доказательство: пусть $\lambda_1, \ldots, \lambda_n$ — корни характеристического многочлена, а $v_1, \ldots, v_n$ — соответствующие собственные векторы. Тогда $v_1, \ldots, v_n$ — линейно независимы. Действительно, если $\sum x_i v_i = 0$, то $\forall i$ имеем $0 = \prod_{j \neq i}(A - \lambda_j \operatorname{Id})(\sum_{k=1}^n x_k v_k) = \sum_{k=1}^n x_k \prod_{j \neq i}(\lambda_k - \lambda_j)v_k = x_i \prod_{j \neq i}(\lambda_i - \lambda_j)v_i$, значит $x_i = 0$. Следовательно, векторы $v_1, \ldots, v_n$ образуют базис. Наконец, легко видеть, что матрица оператора A относительно этого базиса равна $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. □

Определение 1.5. Вектор $v \in V$ называется корневым вектором для оператора A относительно $\lambda \in K$, если $(A - \lambda \operatorname{Id})^k v = 0$ для какого-либо числа $k \in \mathbb{Z}$.

Лемма 1.6. *Множество V_λ корневых векторов оператора A относительно числа $\lambda \in K$ является векторным подпространством, инвариантным относительно оператора A.*

Доказателство: если $(A - \lambda \operatorname{Id})^{k_1} v_1 = 0$ и $(A - \lambda \operatorname{Id})^{k_2} v_2 = 0$, то $(A - \lambda \operatorname{Id})^{k_1 + k_2}(v_1 + v_2) = 0$, а если $(A - \lambda \operatorname{Id})^k v = 0$, то $(A - \lambda \operatorname{Id})^k Av = A(A - \lambda \operatorname{Id})^k v = 0$. □

Часть 2. Жорданова нормальная форма

В этой части лекции мы будем предполагать, что поле K алгебраически замкнуто, то есть всякий многочлен с коэффициентами в K имеет корень в K. Примером алгебраически замкнутого поля является поле $\mathbb{C}$.

Лемма 2.1. *Векторное пространство V раскладывается в прямую сумму корневых подпространств.*

Доказательство: рассмотрим цепочки векторных подпространств $V \supset \operatorname{Im}(A - \lambda \operatorname{Id}) \supset \operatorname{Im}(A - \lambda \operatorname{Id})^2 \supset \ldots$ и $0 \subset \operatorname{Ker}(A - \lambda \operatorname{Id}) \subset \operatorname{Ker}(A - \lambda \operatorname{Id})^2 \subset \ldots$ (вложения очевидны). Размерности в первой цепочке уменьшаются, а во второй — увеличиваются. Кроме того, $\dim \operatorname{Ker}(A - \lambda \operatorname{Id})^p + \dim \operatorname{Im}(A - \lambda \operatorname{Id})^p = \dim V$, следовательно, существует $k \in \mathbb{Z}$, такое что размерности (а значит, и подпространства) в цепочках при $p \geqslant k$ не меняются. Иначе говоря, при $p \geqslant k$ имеем $\operatorname{Ker}(A - \lambda \operatorname{Id})^p = \operatorname{Ker}(A - \lambda \operatorname{Id})^k$ и $\operatorname{Im}(A - \lambda \operatorname{Id})^p = \operatorname{Im}(A - \lambda \operatorname{Id})^k$. Ясно, что первое из этих подпространств совпадает с корневым подпространством V_λ. Обозначим второе подпространство через $\widehat{V}_\lambda$ и покажем, что $V = V_\lambda \oplus \widehat{V}_\lambda$. Заметим, что $\dim V_\lambda + \dim \widehat{V}_\lambda = \dim V$, поэтому достаточно проверить,

что $V_\lambda \cap \widehat{V}_\lambda = 0$. Действительно, мы знаем, что $(A-\lambda\,\mathrm{Id})\widehat{V}_\lambda = \widehat{V}_\lambda$, то есть оператор $(A-\lambda\,\mathrm{Id})$ на $\widehat{V}_\lambda$ сюръективен, следовательно обратим, следовательно все его степени обратимы, следовательно не существует вектора $0 \neq v \in \widehat{V}_\lambda$, такого что $(A-\lambda\,\mathrm{Id})^m v = 0$.

Таким образом мы показали, что $\forall \lambda \in K$ имеем разложение в прямую сумму $V = V_\lambda \oplus \widehat{V}_\lambda$. Доакажем теперь утверждение теоремы индукцией по $\dim V$. В случае $\dim V = 0$ доказывать нечего. Пусть теперь $\dim V > 0$. Преположим, что λ — собственное значение оператора A (оно существует, так как в силу алгебраической замкнутости поля K многочлен $\chi_A(t)$ имеет корень). Тогда $\dim V_\lambda > 0$, следовательно $\dim \widehat{V}_\lambda < \dim V$. Кроме того, разложение $V = V_\lambda \oplus \widehat{V}_\lambda$ по построению инвариантно относительно оператора A. Рассмотрим ограничение A на $\widehat{V}_\lambda$. Тогда по предположению индукции $\widehat{V}_\lambda = \oplus_{i=1}^m (\widehat{V}_\lambda)_{\lambda_i}$ — прямая сумма корневых подпространств. Легко видеть, что $(\widehat{V}_\lambda)_{\lambda_i}$ является корневым подпространством оператора A в V и разложение $V = V_\lambda \oplus (\oplus_{i=1}^m (\widehat{V}_\lambda)_{\lambda_i})$ — искомое. □

Квадратная матрица размера $k \times k$, у которой на диагонали стоят числа λ, над диагональю — единицы, а в остальных местах — нули, называется жордановой клеткой и обозначается $J_k(\lambda)$.

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$$

Теорема 2.2. *Пусть A — оператор в V. Тогда существует базис, в котором матрица оператора A — блочно диагональная с жордановыми клетками на диагонали.*

Доказательство: разложим V в сумму корневых подпространств. Так как корневые подпространства инвариантны относительно A, то достаточно построить жорданов базис для ограничения A на любое корневое пространство V_λ. Более того, ясно, что достаточно построить жорданов базис для оператора $A - \lambda\,\mathrm{Id}$. Таким образом, общее утверждение сводится к случаю, когда $A^k = 0$ для некоторого $k \geqslant 0$.

Преположим, что $A^{k-1} \neq 0$. Рассмотрим цепочку $0 \subset \operatorname{Ker} A \subset \operatorname{Ker} A^2 \subset \dots \subset \operatorname{Ker} A^{k-1} \subset \operatorname{Ker} A^k = V$ и докажем, что существует последовательность подпространств $W_p \subset \operatorname{Ker} A^p$, такая что условие

$$(*_p) \qquad \operatorname{Ker} A^p = [W_p \oplus A(W_{p+1}) \oplus \dots \oplus A^{k-p}(W_k)] \oplus \operatorname{Ker} A^{p-1}$$

выполняется при $p = 1, \dots, k$. Действительно, воспользуемся убывающей индукцией по p. При $p = k$ утверждение очевидно. Предположим, что $1 < p < k$ и последовательность пространств $W_p, \dots, W_k$ такова, что $(*_p)$ выполняется. Заметим, что $\big[W_p \oplus A(W_{p+1}) \oplus \dots \oplus A^{k-p}(W_k)\big] \cap \operatorname{Ker} A = 0$, следовательно

$$A(W_p) \oplus A^2(W_{p+1}) \oplus \dots \oplus A^{k-p+1}(W_k) = A(W_p \oplus A(W_{p+1}) \oplus \dots \oplus A^{k-p}(W_k)) \subset A(\operatorname{Ker} A^p) \subset \operatorname{Ker} A^{p-1}.$$

Кроме того, $\big[A(W_p) \oplus A^2(W_{p+1}) \oplus \dots \oplus A^{k-p+1}(W_k)\big] \cap \operatorname{Ker} A^{p-2} = 0$, следовательно существует W_{p-1}, так что выполняется условие $(*_{p-1})$.

Пусть теперь $W_1, \dots, W_k$ — последовательность подпространств, для которой условие $(*_p)$ выполнено при всех $1 \leqslant p \leqslant k$. Подставив равенства $(*_p)$ одно в другое, получим

$$V = \operatorname{Ker} A^k = W_k \oplus [W_{k-1} \oplus A(W_k)] \oplus [W_{k-2} \oplus A(W_{k-1}) \oplus A^2(W_k)] \oplus \dots \oplus [W_1 \oplus A(W_2) \oplus \dots \oplus A^{k-1}(W_k)].$$

Перегруппировывая члены, получаем

$$V = [W_k \oplus A(W_k) \oplus \dots \oplus A^{k-1}(W_k)] \oplus [W_{k-1} \oplus A(W_{k-1}) \oplus \dots \oplus A^{k-2}(W_{k-1})] \oplus \dots \oplus [W_2 \oplus A(W_2)] \oplus W_1.$$

Выберем теперь базис $w_{p,i}$ в каждом из пространств W_p. Заметим, что по построению $A^p(W_p) = 0$, но $W_p \cap \operatorname{Ker} A^{p-1} = 0$, поэтому векторы $e_{p,i,j} = A^j w_{p,i}$ $(j = 0, \dots, p-1)$ образуют базис в V. Более того, для любых p и i подпространство в V, порожденное векторами $e_{p,i,0}, \dots, e_{p,i,p-1}$ инвариантно относительно A, а матрица A в этом базисе является жордановой клеткой $J_p(0)$. □

Замечание 2.3. Если поле K не является алгебраически замкнутым, то жорданова базиса, вообще говоря, может и не быть. Например, оператор умножения на i в $\mathbb{C} \cong \mathbb{R}^2$ не имеет жорданова базиса над $\mathbb{R}$.

Как видно из доказательства теоремы жорданова базис не является единственным. Однако, количество жордановых клеток вида $J_k(\lambda)$ не зависит от его выбора.

Лемма 2.4. *Пусть $n_{\lambda,k}$ — количество жордановых клеток вида $J_k(\lambda)$ в матрице оператора A в некоторм жордановом базисе. Тогда $\sum_{p=1}^{k} p n_{\lambda,p} + \sum_{p=k+1}^{\infty} k n_{\lambda,p} = \dim \operatorname{Ker}(A-\lambda\,\mathrm{Id})^k$ для всех λ и k.*

Доказательство: прямое вычисление.

Замечание 2.5. Жорданов базис очень удобен для вычислений с оператором A. Например, легко видеть, что

$$\operatorname{tr} A = \sum_{\lambda,k} k n_{\lambda,k}(A)\lambda, \quad \det A = \prod_{\lambda,k} \lambda^{k n_{\lambda,k}(A)}, \quad \chi_A(t) = \prod_{\lambda,k} (t-\lambda)^{k n_{\lambda,k}(A)},$$

где $n_{\lambda,k}(A)$ — количество жордановых клеток вида $J_k(\lambda)$. Отсюда видно, что характеристический многочлен *не определяет* жорданову нормальную форму оператора.

Задание оператора A в векторном пространстве V равносильно заданию в V структуры модуля над кольцом многочленов $K[t]$ (многочлен $f(t) = a_n t^n + \cdots + a_0$ действует оператором $f(A) = a_n A^n + \cdots + a_0$). Легко видеть, что при таком соответствии оператору, состоящему из одной жордановой клетки $J_k(\lambda)$ соответствует модуль $K[t]/(t-\lambda)^k K[t]$. Поэтому теорему 2.2 можно переформулировать следующим способом.

Следствие 2.6. *Если K — алгебраически замкнутое поле и V — $K[t]$-модуль, такой что $\dim V < \infty$, то $V \cong \bigoplus_{\lambda,k} K[t]/(t-\lambda)^k K[t]$.*

Вот еще одна полезная переформулировка. Оператор называется полупростым, если его матрица диагональна в некотором базисе. Оператор A называется нильпотентным, если $A^m = 0$ для некоторого m.

Следствие 2.7. *Всякий оператор A представляется в виде $A = A_{ss} + A_n$, где A_{ss} — полупрост, A_n — нильпотентен и $A_{ss}A_n = A_n A_{ss}$.*

Замечание 2.8. Такое разложение называется жордановым. Можно показать, что оно единственно.

Часть 3. Теорема Гамильтона–Кэли

Теорема 3.1. *Пусть A — оператор в конечномерном векторном пространстве V над произвольным полем K (не обязательно алгебраически замкнутым). Тогда $\chi_A(A) = 0$.*

Доказательство: из теоремы 3.5 предыдущей лекции и определения характеристического многочлена следует, что

$$(\dagger) \qquad \chi_A(t)E = (\widehat{tE - A}) \cdot (tE - A) = (tE - A) \cdot (\widehat{tE - A})$$

(равенство в кольце $\operatorname{Mat}_{n\times n}(K[t]) \cong \operatorname{Mat}_{n\times n}(K)[t]$). Более того, это равенство выполняется также и в кольце $R = Z_A(\operatorname{Mat}_{n\times n}(K)[t]) = (Z_A(\operatorname{Mat}_{n\times n}))[t]$ (Z_A — централизатор оператора A). Действительно, ясно что $tE - A \in R$ и $\chi_A(t)E \in R$. Наконец, из (†) следует, что $(\widehat{tE - A})$ коммутирует с $tE - A$, а значит и с A, следовательно $(\widehat{tE - A}) \in R$. Заметим теперь, что отображение

$$\varphi : R \to \operatorname{Mat}_{n\times n}(K), \qquad \textstyle\sum_p B_p t^p \mapsto \sum_p B_p A^p \qquad (B_p \in Z_A(\operatorname{Mat}_{n\times n}(K)))$$

является гомоморфизмом колец. Действительно,

$$\varphi(\textstyle\sum B_p t^p)\varphi(\sum C_q t^q) = (\sum B_p A^p)(\sum C_q A^q) = \sum B_p A^p C_q A^q = \sum B_p C_q A^p A^q = \sum B_p C_q A^{p+q} = \varphi(\sum B_p C_q t^{p+q}).$$

Применяя φ к (†) получаем $\chi_A(A) = \varphi(\chi_A(t)E) = \varphi((\widehat{tE - A})) \cdot \varphi(tE - A) = \varphi((\widehat{tE - A})) \cdot (A - A) = 0$. □

Замечание 3.2. Если поле K — алгебраически замкнуто, то теорема Гамильтона–Кэли легко доказывается непосредственным вычислением оператора $\chi_A(A)$ в жордановом базисе.

Следствие 3.3. *Пусть $f_A : K[t] \to \operatorname{End}_K(A)$ — гомоморфизм, переводящий многочлен $\sum a_p t^p \in K[t]$ в оператор $\sum_p a_p A^p \in \operatorname{End}_K(A)$. Тогда $\chi_A(t) \in \operatorname{Ker} f_A$.*

Определение 3.4. Ненулевой многочлен минимальной степени со старшим коэффициентом 1 в идеале $\operatorname{Ker} f_A \subset K[t]$ называется минимальным многочленом оператора A и обозначается $m_A(t)$.

Примеры 3.5.

1. Если $m_A(t) = t - \lambda$, то $A = \lambda E$.
2. Если $m_A(t) = t^2 - t$, то A называется проектором или идемпотентным оператором.
3. Если $m_A(t) = t^n$, то A является нильпотентным оператором.

4. Если $m_A(t) = (t-1)^n$, то A называется унипотентным оператором.

Лемма 3.6. *Минимальный многочлен оператора A делит его характеристический многочлен.*

Доказательство: $\chi_A(t) = m_A(t)q(t) + r(t)$, где $\deg r(t) < \deg m_A(t)$, но $r(t) \in \operatorname{Ker} f_A$, поэтому $r(t) = 0$. □

Следствие 3.7. *Если A — оператор в n-мерном пространстве, то* $\deg m_A(t) \leqslant n$.

Замечание 3.8. Можно доказать также, что характеристический многочлен делит некоторую степень минимального многочлена.

Лекция 8. Коммутативные кольца

В этой лекции рассматриваются только коммутативные кольца.

Часть 1. Идеалы

Пусть A — коммутативное кольцо.

Определение 1.1. Элемент $a \in A$ называется делитетем нуля, если $a \neq 0$ и существует $0 \neq b \in A$, так что $ab = 0$. Кольцо A называется целостным (областью целостности), если в нем нет делителей нуля и $1 \neq 0$.

Примеры 1.2. 1. Всякое поле является целостным кольцом.

2. Кольца $\mathbb{Z}$ и $K[x]$ — целостные.

3. Кольцо $\mathbb{Z}/n\mathbb{Z}$ — целостное тогда и только тогда, когда n — простое число.

Определение 1.3. Идеал $\mathfrak{p} \subset A$ называется простым, если кольцо $A/\mathfrak{p}$ — целостное.

Пример 1.4. Идеал $n\mathbb{Z} \subset \mathbb{Z}$ — простой, тогда и только тогда, когда n — простое число.

Лемма 1.5. *Идеал $\mathfrak{p} \subset A$ — простой $\iff \mathfrak{p} \neq A$ и $\forall x, y \in A$, если $xy \in \mathfrak{p}$, то либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$.*

Доказательство: обозначим через $\bar{x}$ образ элемента $x \in A$ в кольце $A/\mathfrak{p}$. Если $\mathfrak{p}$ — простой, и $xy \in \mathfrak{p}$, то $\bar{x}\bar{y} = 0$, следовательно либо $\bar{x} = 0$, либо $\bar{y} = 0$ (так как $A/\mathfrak{p}$ — целостное), значит либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$. Аналогично доказывается обратное утверждение. □

Следствие 1.6. *Кольцо A — целостное $\iff \{0\} \subset A$ — простой идеал.*

Определение 1.7. Идеал $\mathfrak{m} \subset A$ называется максимальным, если $\mathfrak{m} \neq A$ и не существует идеала $\mathfrak{m} \subset \mathfrak{a} \subset A$, такого что $\mathfrak{m} \neq \mathfrak{a} \neq A$.

Лемма 1.8. *Идеал $\mathfrak{m} \subset A$ — максимальный $\iff A/\mathfrak{m}$ — поле.*

Доказательство: пусть $f : A \to A/\mathfrak{m}$ — каноническая проекция. Если $\mathfrak{a} \subset A$ — идеал, такой что $\mathfrak{m} \subset \mathfrak{a}$, то $\mathfrak{a}/\mathfrak{m} = f(\mathfrak{a}) \subset A/\mathfrak{m}$ — идеал. Аналогично, если $\mathfrak{b} \subset A/\mathfrak{m}$ — идеал, то $\mathfrak{a} = f^{-1}(\mathfrak{b}) \subset A$ — идеал, такой что $\mathfrak{m} \subset \mathfrak{a}$. Поэтому $\mathfrak{m}$ — максимальный $\iff A/\mathfrak{m}$ не имеет нетривиальных идеалов. Покажем, что это выполнено тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Если $A/\mathfrak{m}$ — поле, то всякий элемент $0 \neq x \in A/\mathfrak{m}$ обратим, следовательно любой ненулевой идеал в $A/\mathfrak{m}$ совпадает с $A/\mathfrak{m}$. Обратно, пусть кольцо $B = A/\mathfrak{m}$ не имеет нетривиальных идеалов. Возьмем произвольный $0 \neq x \in B$. Тогда идеал $xB \subset B$ — ненулевой, следовательно $xB = B$, то есть $1_B \in xB$, то есть $\exists y \in B$, так что $xy = 1_B$. Значит x — обратим и B — поле. □

Следствие 1.9. *Всякий максимальный идеал является простым.*

Пример 1.10. В кольце $\mathbb{Z}$ имеем $n\mathbb{Z} \subset m\mathbb{Z} \iff m|n$. Поэтому $n\mathbb{Z}$ — максимальный $\iff n$ — простое число.

Лемма 1.11. *Пусть $\mathfrak{a} \neq A$ — идеал. Тогда существует максимальный идеал $\mathfrak{a} \subset \mathfrak{m} \subset A$.*

Доказательство: по лемме Цорна достаточно проверить, что для всякой цепочки идеалов $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset A$, в которой $\forall i\ \mathfrak{a}_i \neq A$, существует идеал $\mathfrak{a} \neq A$, такой что $\forall i\ \mathfrak{a}_i \subset \mathfrak{a}$. Возьмем $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$. Нам надо проверить, что 1) $\mathfrak{a}$ — идеал; 2) $\mathfrak{a} \neq A$. Действительно, если $x, y \in \mathfrak{a}$, то $x \in \mathfrak{a}_i$, $y \in \mathfrak{a}_j$ для каких-то i, j, следовательно $x, y \in \mathfrak{a}_k$, где $k = \max(i, j)$, следовательно $x + y \in \mathfrak{a}_k \subset \mathfrak{a}$. Аналогично проверяется, что $ax \in \mathfrak{a}\ \forall a \in A$. Стало быть, $\mathfrak{a}$ — идеал. Теперь предположим, что $\mathfrak{a} = A$. Тогда $1 \in \mathfrak{a}$, следовательно $\exists i$, так что $1 \in \mathfrak{a}_i$, значит $\mathfrak{a}_i = A$ — противоречие. □

Следствие 1.12. *Всякий необратимый элемент кольца содержится в некотором максимальном идеале.*

Пусть A — целостное кольцо. Рассмотрим множество классов эквивалентности пар (a,s), $a \in A$, $s \in A \setminus \{0\}$, где $(a,s) \sim (b,t) \iff at = bs$. Обозначим класс пары (a,s) через a/s и будем называть его дробью.

Лемма 1.13. *Множество дробей $F(A) = \{a/s\}$ с операциями $a/s + b/t = (at+bs)/st$, $(a/s)\cdot(b/t) = (ab)/(st)$ является полем. Отображение $\varphi : A \to F(A)$, $a \mapsto a/1$ является мономорфизмом.*

Доказательство: непосредственная проверка.

Поле $F(A)$ называется полем частных кольца A.

Следствие 1.14. *Идеал $\mathfrak{a} \subset A$ — простой $\iff \mathfrak{a} = \operatorname{Ker} f$, где f — гомоморфизм из A в некоторое поле.*

Часть 2. Кольца главных идеалов

Определение 2.1. Идеал $I \subset A$ называется главным, если $I = aA$, $a \in A$. Коммутативное кольцо A называется кольцом главных идеалов, если $1 \neq 0$ и всякий идеал в A — главный.

Говорят, что в кольце A возможно деление с остатком, если существует функция $\varphi : A \to \mathbb{Z}_{\geqslant 0}$, такая что $\varphi^{-1}(0) = \{0\}$ и для любых $a, b \in A$, $b \neq 0$ $\exists q, r \in A$ $a = bq + r$ и $\varphi(r) < \varphi(b)$.

Пример 2.2. В кольцах $\mathbb{Z}$ и $K[x]$ возможно деление с остатком: достаточно взять $\varphi(n) = |n|$ для $n \in \mathbb{Z}$ и $\varphi(p(x)) = \deg p(x) + 1$ для $p(x) \in K[x]$ (если положить $\deg 0 = -1$).

Лемма 2.3. *Если в кольце A возможно деление с остатком, то A — кольцо главных идеалов.*

Доказательство: пусть $I \subset A$ — идеал. Если $I = 0$, то I — главный. Предположим, что $I \neq 0$. Пусть $b \in I$ таков, что $\varphi(b) = \min\{\varphi(x) \mid 0 \neq x \in I\}$. Покажем, что $I = bA$. Действительно, пусть $a \in I$. Тогда $a = bq + r$, $\varphi(r) < \varphi(b)$. Но $r \in I$, значит $r = 0$ и $a \in bA$. □

Следствие 2.4. *Кольца $\mathbb{Z}$ и $K[x]$ являются кольцами главных идеалов.*

Определение 2.5. Пусть A — целостное кольцо. Элемент $d \in A$ называется делителем элемента $a \in A$, если $a = dc$ (обозначается $d|a$). Элемент $d \in A$ называется наибольшим общим делителем элементов $a, b \in A$, если $d|a$, $d|b$ и $\forall d' \in A$ $d'|a$, $d'|b \Longrightarrow d'|d$.

Ясно, что если наибольший общий делитель существует, то определен однозначно с точностью до умножения на обратимый элемент. Будем через (a,b) обозначать любой из наибольших общих делителей.

Лемма 2.6. *Если A — кольцо главных идеалов, $a, b \in A$, то существует (a,b).*

Доказательство: рассмотрим идеал $I = aA + bA$. Так как A — кольцо главных идеалов, то $I = dA$, $d \in A$. Покажем, что $d = (a,b)$. Во-первых, $a \in aA \subset I = dA$, поэтому $d|a$. Аналогично, $d|b$. Далее, если $d'|a$ и $d'|b$, то $aA \subset d'A$, $bA \subset d'A$, поэтому $d \in dA = I = aA + bA \subset d'A$, значит $d'|d$. □

Замечание 2.7. Из доказательства леммы видно, что если $d = (a,b)$, то существуют $x, y \in A$ такие что $d = ax + by$.

Еще одним важным свойством колец главных идеалов является нётеровость.

Лемма 2.8. *Если A — кольцо главных идеалов, то A — нётерово: всякая возрастающая цепочка идеалов $I_1 \subset I_2 \subset \cdots \subset A$ стабилизируется, то есть $\exists n$ такое что $I_k = I_n$ при $k \geqslant n$.*

Доказательство: возьмем $I = \bigcup_i I_i$. Как было показано выше I — идеал, следовательно $I = aA$. Так как $a \in I$, то $a \in I_n$ для некоторого n, значит $I = aA \subset I_n$, значит $I_n = I$, значит $I_k = I_n$ при $k \geqslant n$. □

Часть 3. Факториальность

Определение 3.1. Элемент $u \in A$ называется единицей, если он обратим. Элемент $a \in A$ называется неприводимым, если a не единица, но из равенства $a = bc$ следует, что либо b, либо c — единица в A.

Пример 3.2. В кольце $\mathbb{Z}$ единицами являются числа ± 1, а неприводимыми — числа $\pm p$, где p — простое.

Лемма 3.3. *Пусть A — целостное кольцо. Тогда $aA = bA \iff a = bu$, где u — единица.*

Доказательство: $a \in aA = bA$, поэтому $a = bu$. Аналогично $b = av$. Значит $a = avu$, следовательно $vu = 1$, то есть u — единица. □

Лемма 3.4. *Если A — кольцо главных идеалов, p — неприводим и $p|ab$, то либо $p|a$, либо $p|b$.*

Доказательство: если $p \not| a$, то $(p, a) = 1$, следовательно $1 = px + ay$, значит $b = p(xb) + (ab)y$. Ясно, что p делит оба слагаемых в правой части равенства, поэтому $p|b$. □

Лемма 3.5. *Если A — целостное и главный идеал $aA \subset A$ прост, то $a \in A$ — неприводим.*

Доказательство: если $0 \neq a = bc$, то $bc \in aA$, значит либо $b \in aA$, либо $c \in aA$. Если $b \in aA$, то $b = ad$, следовательно $a = adc$, следовательно $dc = 1$ и c — единица. □

В кольце $\mathbb{Z}$ верно и обратное утверждение, однако в более общих кольцах это уже не так.

Определение 3.6. Элемент $0 \neq a \in A$ обладает однозначным разложением на неприводимые множители, если $a = u\prod_{i=1}^{n} p_i$, где u — единица, а p_i — неприводимы, и для любого другого такого разложения $a = u'\prod_{i=1}^{m} p'_i$ имеем $n = m$ и $p_i = u_i p'_i$, где u_i — единицы. Кольцо A называется факториальным, если оно целостное и всякий ненулевой элемент обладает однозначным разложением на неприводимые множители.

Пример 3.7. Хорошо известно, что в кольце $\mathbb{Z}$ всякий элемент обладает однозначным разложением на простые множители, то есть кольцо $\mathbb{Z}$ факториально. Примером не факториального кольца является кольцо $\mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \in \mathbb{C} \mid a, b \in \mathbb{Z} \,\}$. В этом кольце $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Теорема 3.8. *Если A — целостное кольцо главных идеалов, то A факториально.*

Доказательство: покажем вначале, что если $a \in A$ не является единицей, то a имеет неприводимый делитель. Преположим противное. Тогда существует разложение $a = a_1 b_1$, так что a_1 и b_1 — не единицы. Следовательно $aA \subset a_1 A$, причем по лемме 3.3 вложение строгое. Далее, если a_1 — неприводим, то все доказано, иначе же существует разложение $a_1 = a_2 b_2$, так что a_2 и b_2 — не единицы. Продолжая подобным образом, мы либо в конце концов найдем неприводимый делитель, либо построим нестабилизирующуся возрастающую цепочку идеалов $aA \subset a_1 A \subset a_2 A \subset \ldots$. Однако, из-зи нётеровости кольца A последнее невозможно. Следовательно, неприводимый делитель существует.

Докажем теперь, что a допускает разложение на неприводимые множители. Во-первых, a имеет неприводимый делитель, поэтому $a = a_1 p_1$, где p_1 неприводим. Далее, либо a_1 — единица, либо имеет неприводимый делитель, то есть $a_1 = a_2 p_2$. Продолжая подобным образом, мы либо в конце концов найдем разложение на неприводимые множители, либо построим нестабилизирующуся возрастающую цепочку идеалов $aA \subset a_1 A \subset a_2 A \subset \ldots$. Однако, из-зи нётеровости кольца A последнее невозможно. Следовательно, разложение на неприводимые множители существует.

Докажем теперь, что разложение единственно. Предположим, что $up_1 \ldots p_n = u' p'_1 \ldots p'_m$. Так как p_1 делит левую часть, то p_1 делит и правую часть, следовательно по лемме 3.4 он делит один из сомножителей правой части. Ясно, что $p_1 \not| u'$, поэтому $p_1 | p'_i$. Переставляя в правой части сомножители, можно считать, что $p_1 | p'_1$. Следовательно, $p'_1 = p_1 u_1$, где u_1 — единица. Сокращая на p_1 получаем равенство $up_2 \ldots p_n = (u' u_1) p'_2 \ldots p'_m$. Далее единственность следует по индукции. □

Следствие 3.9. *Кольца $\mathbb{Z}$ и $K[x]$ — факториальны.*

Замечание 3.10. Впоследствии мы докажем, что кольца $\mathbb{Z}[x]$ и $K[x_1, \ldots, x_n]$ факториальны, хотя и не являются кольцами главных идеалов.

Лекция 9. Поля

Часть 1. Характеристика

Пусть K — произвольное поле. Рассмотрим гомоморфизм колец $\kappa_K : \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$, где 1_K — единица поля K. Ядро гомоморфизма κ_K — идеал в $\mathbb{Z}$, следовательно имеет вид $\operatorname{Ker} \kappa_K = d\mathbb{Z} \subset \mathbb{Z}$, где $d \geqslant 0$.

Лемма 1.1. *Если $d \neq 0$, то d — простое число.*

Доказательство: образ гомоморфизма κ_K — подкольцо в поле, следовательно $\operatorname{Im} \kappa_K$ — целостное кольцо, значит $d\mathbb{Z} = \operatorname{Ker} \kappa_K$ — простой идеал, поэтому d — простое число или 0. □

Определение 1.2. Число d называется характеристикой поля K и обозначается $\operatorname{char} K$. Таким образом, либо $\operatorname{char} K = 0$, либо $\operatorname{char} K$ — простое число.

В поле характеристки 0 на всякое ненулевое целое число можно делить, а в поле характеристики $p \neq 0$ на число n можно делить, если и только если n не делится на p.

Лемма 1.3. *Если K — поле, а $I \subset K$ — идеал, то $I = 0$ или $I = K$.*

Доказательство: если $0 \neq x \in I$, то $\forall y \in K \ y = (yx^{-1})x \in I$, значит $I = K$. □

Лемма 1.4. *Всякий гомоморфизм полей является вложением.*

Доказательство: если $f : K \to L$ — гомоморфизм полей, то $f(1) = 1 \Longrightarrow \operatorname{Ker} f \neq K \Longrightarrow \operatorname{Ker} f = 0$. □

Лемма 1.5. *Если K — поле характеристики 0, то $K \supset \mathbb{Q}$, а если K — поле характеристики $p \neq 0$, то $K \supset \mathbb{F}_p$, где $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ — поле из p элементов.*

Доказательство: если $\operatorname{char} K = 0$, то отображение $\mathbb{Q} \to K$, $m/n \mapsto \kappa_K(n)^{-1} \cdot \kappa_K(m)$ является гомоморфизмом полей, следовательно $\mathbb{Q} \subset K$. Если же $\operatorname{char} K = p$, то $\operatorname{Im} \kappa_K \cong \mathbb{Z}/p\mathbb{Z} \subset K$. □

Поля $\mathbb{Q}$ и $\mathbb{F}_p$ называются простыми полями. Всякое поле содержит единственное простое подполе.

Лемма 1.6. *Если $f : K \to L$ — гомоморфизм полей, то $\operatorname{char} K = \operatorname{char} L$. Более того, f отождествляет простое подполе в K с простым подполем в L.*

Доказательство: ясно, что $\kappa_L = f \circ \kappa_K$, поэтому $\operatorname{Ker} \kappa_K \subset \operatorname{Ker} \kappa_L$. С другой стороны, из леммы 1.4 следует, что $\operatorname{Im} \kappa_K \subset \operatorname{Im} \kappa_L$. Поэтому, $\operatorname{Ker} \kappa_K = \operatorname{Ker} \kappa_L$ и $\operatorname{Im} \kappa_K = \operatorname{Im} \kappa_L$, следовательно характеристика и простые подполя совпадают. □

Часть 2. Расширения полей

Вложение полей $K \subset L$ называется также расширением полей и обозначается L/K. Если L/K — расширение полей, то поле L можно рассматривать как векторное пространство над полем K. Его размерность называется степенью расширения и обозначается $[L : K]$. Расширение L/K называется конечным, если $[L : K] < \infty$. Последовательность расширений полей $K_1 \subset K_2 \subset \cdots \subset K_n$ называется также башней полей, а расширения $K_i \subset K_{i+1}$ — этажами башни.

Лемма 2.1. *Степень расширения мультипликативна в башнях: если $F \subset K \subset L$ — расширения полей, то $[L : F] = [L : K][K : F]$.*

Доказательство: выберем базис x_i в K над F и базис y_j в L над K. Покажем, что x_iy_j образуют базис в L над F. Действительно, если $a \in L$, то $a = \sum a_jy_j$, где $a_j \in K$. Далее, имеем $a_j = \sum b_{ij}x_i$, где $b_{ij} \in F$. Подставляя, получаем $a = \sum_j(\sum_i b_{ij}x_i)y_j = \sum_{i,j} b_{ij}x_iy_j$, следовательно элементы x_iy_j порождают L над F и остается проверить их линейную независимость. Действительно, если $\sum b_{ij}x_iy_j = 0$, где $b_{ij} \in F$, то полагая $a_j = \sum b_{ij}x_i \in K$, получаем $\sum a_jy_j = 0$. Следовательно $\forall j\ a_j = 0$, но тогда $\forall i,j\ b_{ij} = 0$. □

Следствие 2.2. *Башня полей конечна, тогда и только тогда когда конечен каждый ее этаж.*

Определение 2.3. Пусть L/K — расширение полей. Элемент $\alpha \in L$ называется алгебраическим над полем K, если существует многочлен $0 \neq f(x) \in K[x]$, такой что $f(\alpha) = 0$. Расширение L/K называется алгебраическим, если всякий элемент из L алгебраичен над K.

Лемма 2.4. *Всякое конечное расширение полей алгебрачино.*

Доказательство: если $[L : K] = n$ и $\alpha \in L$, то элементы $1, \alpha, \alpha^2, \ldots, \alpha^n \in L$ не могут быть линейно независимыми над K, поэтому $\exists a_0, a_1, \ldots, a_n \in K$, так что $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Значит $f(\alpha) = 0$, где $f(x) = a_nx^n + \cdots + a_1x + a_0$. □

Пусть L/K — расширение, и $\alpha \in L$. Рассмотрим гомоморфизм $\varphi_\alpha : K[x] \to L$, $f(x) \mapsto f(\alpha)$. Его образ является подкольцом в L и обозначается $K[\alpha]$. Ясно, что $K[\alpha]$ — целостное кольцо. Его поле частных является подполем в L и обозначается $K(\alpha)$. Если α — алгебраичен над K, то гомоморфизм φ_α не является инъективным, следовательно $\operatorname{Ker}\varphi$ — нетривиальный идеал в $K[x]$. Так как $K[x]$ — кольцо главных идеалов, то $\operatorname{Ker}\varphi = p(x)K[x]$, причем $p(x)$ — неприводимый многочлен, так как $K[\alpha]$ — целостное кольцо. Более того, многочлен $p(x)$ можно выбрать так, что его старший коэффициент равен 1. Такой многочлен однозначно определяется элементом α, называется неприводимым многочленом α и обозначается $\operatorname{Irr}^K_\alpha(x)$.

Лемма 2.5. *Если $\alpha \in L$ алгебраичен над K, то $K(\alpha) = K[\alpha]$ и $[K(\alpha) : K] = \deg \operatorname{Irr}^K_\alpha(x)$.*

Доказательство: пусть $0 \neq \beta \in K[\alpha]$. Тогда $\beta = f(\alpha)$ для некоторого $f(x) \in K[x]$. Так как $p(x) = \operatorname{Irr}^K_\alpha(x)$ — неприводим, то $(p(x), f(x)) = 1$, следовательно $p(x)g(x) + f(x)h(x) = 1$ для некоторых $g(x), h(x) \in K[x]$. Подставляя α и учитывая, что $p(\alpha) = 0$, получаем $f(\alpha)h(\alpha) = 1$. Следовательно $\beta = f(\alpha)$ — обратим, значит $K[\alpha]$ — поле, откуда получаем $K(\alpha) = K[\alpha]$. Наконец, если $\deg \operatorname{Irr}^K_\alpha(x) = n$, то легко видеть, что элементы $1, \alpha, \ldots, \alpha^{n-1}$ образуют базис $K[\alpha]$ над K, следовательно $[K(\alpha) : K] = n$. □

Пусть L/K расширение полей и $\alpha_1, \ldots, \alpha_n \in L$. Рассмотрим гомоморфизм $\varphi_{\alpha_1,\ldots,\alpha_n} : K[x_1, \ldots, x_n] \to L$, $f(x_1, \ldots, x_n) \mapsto f(\alpha_1, \ldots, \alpha_n)$. Его образ является подкольцом в L и обозначается $K[\alpha_1, \ldots, \alpha_n]$. Ясно, что $K[\alpha_1, \ldots, \alpha_n]$ — целостное кольцо. Его поле частных является подполем в L и обозначается $K(\alpha_1, \ldots, \alpha_n)$.

Легко видеть, что $K(\alpha_1, \ldots, \alpha_n)$ является наименьшим подполем в L, содержащим элементы $\alpha_1, \ldots, \alpha_n$. Если $L = K(\alpha_1, \ldots, \alpha_n)$ для каких-то $\alpha_1, \ldots, \alpha_n$, то говорят, что L — конечно порождено над K.

Лемма 2.6. *Если $L = K(\alpha_1, \ldots, \alpha_n)$ и все α_i алгебраичны над K, то L конечно над K.*

Доказательство: рассмотрим башню полей $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = L$. Ясно, что α_{i+1} алгебраичен над $K(\alpha_1, \ldots, \alpha_i)$ (так как $\operatorname{Irr}^K_{\alpha_{i+1}}(x) \in K[x] \subset K(\alpha_1, \ldots, \alpha_i)[x]$), поэтому по лемме 2.5 всякий этаж башни конечен, следовательно L над K конечно. □

Теорема 2.7. *Если $F \subset K \subset L$ — расширения полей, то L/F — алгебраично $\iff$ L/K и K/F алгебраичны.*

Доказательство: импликация $\Longrightarrow$ — очевидна. Докажем обратную имплткацию. Пусть $\alpha \in L$. Рассмотрим многочлен $\operatorname{Irr}^K_\alpha(x) = x^n + a_1x^{n-1} + \cdots + a_n$, $a_i \in K$. Положим $K' = F(a_1, \ldots, a_n)$ и рассмотрим башню полей $F \subset K' \subset K'(\alpha)$. Заметим, что $K'(\alpha)$ конечно над K' по лемме 2.5. С другой стороны, $a_i \in K$, следовательно a_i алгебраичны над F, следовательно, по лемме 2.6 поле K' конечно над F. Значит $K'(\alpha)$ конечно над F, следовательно α алгебраичен над F. □

Следствие 2.8. *Если L/K — расширение полей, то $L_{\text{alg}} := \{\, \alpha \in L \mid \alpha$ алгебраичен над $K \,\}$ — подполе в L.*

Доказательство: если $\alpha, \beta \in L$ — алгебраичны над K, то поле $K(\alpha, \beta)$ конечно над K, но $\alpha + \beta$, $\alpha\beta$ и α^{-1} лежат в $K(\alpha, \beta)$ — следовательно алгебраичны над K. □

Часть 3. Алгебраическое замыкание

Лемма 3.1. *Пусть $f(x) \in K[x]$. Существует конечное расширение L/K, в котором $f(x)$ имеет корень.*

Доказательство: пусть $p(x) \in K[x]$ — неприводимый делитель многочлена $f(x)$. Возьмем $L = K[x]/p(x)K[x]$ и обозначим через α образ x в L. Тогда ясно, что $p(\alpha) = 0$, следовательно $f(\alpha) = 0$. □

Лемма 3.2. *Пусть $f_1(x), \ldots, f_n(x) \in K[x]$. Существует конечное расширение L/K, в котором каждый из многочленов $f_i(x)$ имеет корень.*

Доказательство: пусть $K_0 = K$ и K_{i+1}/K_i — конечное расширение, в котором $f_{i+1}(x)$ имеет корень. Тогда $L = K_n$ — искомое расширение. □

Теорема 3.3. *Всякое поле K можно вложить в алгебраически замкнутое поле.*

Доказательство: построим сначала расширение K_1/K, в котором любой многочлен из $K[x]$ будет иметь корень. Для этого сопоставим всякому многочлену $f(x) \in K[x]$ переменную x_f и рассмотрим кольцо многочленов $A := K[x_f]_{f \in K[x]}$ от всех этих переменных. Пусть I — идеал в кольце A, порожденный всеми многочленами $f(x_f)$. Покажем, что $I \neq A$. Действительно, если $I = A$, то существуют элементы $g_1, \ldots, g_n \in A$ и многочлены $f_1, \ldots, f_n \in K[x]$, такие что

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1. \qquad (*)$$

В каждый из многочленов $g_1, \ldots, g_n$ входит лишь конечное число переменных, поэтому $\exists N \in \mathbb{Z}$, такое что $g_1, \ldots, g_n$ лежат в подкольце $A' = K[X_{f_1}, \ldots, X_{f_n}, \ldots, X_{f_N}] \subset A$ и соотношение $(*)$ можно рассматривать как соотношение в кольце A'. Выберем теперь конечное расширение L/K, в котором каждый из многочленов $f_i(x)$ $(i = 1, \ldots, n)$ имеет корень (обозначим его α_i). Положим, далее $\alpha_i = 0$ для $n < i \leqslant N$ и рассмотрим гомоморфизм $\varphi_{\alpha_1,\ldots,\alpha_N} : A' \to L$. Применяя его к равенству $(*)$ получаем $0 = 1$ — противоречие.

Таким образом $I \neq A$. Пусть $\mathfrak{m} \subset A$ — максимальный идеал, содержащий I. Тогда $K_1 = A/\mathfrak{m}$ — поле, причем $K \subset K_1$ и всякий многочлен $f(x) \in K[x]$ имеет корень в K_1. Повторяя описанную конструкцию получаем бесконечную башню полей $K \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \ldots$, в которой всякий многочлен $f(x) \in K_i[x]$ имеет корень в K_{i+1}. Рассмотрим теперь $L = \bigcup_{i=1}^{\infty} K_i$. Покажем, что L — поле. Если $x, y \in L$, то $x, y \in K_i$ для некоторого i, значит определены $x + y, xy \in K_i$. Ясно, что заданные таким образом операции в L корректно определены. Более того, ясно, что все необходимые свойства выполняются (всякий раз их достаточно проверять в одном из полей K_i). Значит L — действительно поле. Наконец, если $f(x) \in L[x]$, то так как f имеет лишь конечное число коэффициентов, то $f(x) \in K_i[x]$ для некоторого i, значит $f(x)$ имеет корень в K_{i+1}, а следовательно и в L. □

Следствие 3.4. *Для любого поля K существует алгебраически замкнутое поле $\overline{K}$, являющееся алгебраическим расширением поля K.*

Доказательство: вложим K в алгебраически замкнутое поле L и пусть $\overline{K}$ — множество всех $\alpha \in L$, алгебраических над K. По лемме 2.8 $\overline{K}$ — подполе в L. Покажем, что $\overline{K}$ — алгебраически замкнуто. Пусть $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \overline{K}[x]$. Тогда многочлен $f(x)$ имеет корень α в L. Рассмотрим башню полей $K \subset K(a_1, \ldots, a_n) \subset K(a_1, \ldots, a_n)(\alpha)$. Первый этаж башни алгебраичен, так как a_i алгебраичны над K, а второй алгебраичен по построению. Значит $K(a_1, \ldots, a_n)(\alpha)$ алгебраично над K, следовательно $\alpha \in \overline{K}$. □

Поле $\overline{K}$ называется алгебраическим замыканием поля K.

Замечание 3.5. Позднее мы покажем, что любые два алгебраических замыкания поля K изоморфны.

Лекция 10. Нормальные расширения

Часть 1. Продолжение гомоморфизмов

Пусть $\sigma : K \to L$ — гомоморфизм полей. Часто для обозначения действия гомоморфизма используют экспоненциальную запись: $a^\sigma := \sigma(a)$, где $a \in K$. В частности, если $f(x) = \sum a_k x^k$, то $f^\sigma(x) := \sum a_k^\sigma x^k$.

Пусть K'/K и L'/L — расширения полей, а $\sigma : K \to L$ и $\tau : K' \to L'$ — гомоморфизмы. Будем говорить, что τ продолжает σ, если $\tau_{|K} = \sigma$.

Лемма 1.1. *Пусть $\sigma : K \to L$ — гомоморфизм полей, а K'/K и L'/L — расширения. Если $K' = K(\alpha)$, α — алгебраичен над K и $p(x) = \operatorname{Irr}_\alpha^K(x)$, то множество гомоморфизмов $\tau : K' \to L'$, продолжающих гомоморфизм σ, находится в биекции с множеством корней многочлена $p^\sigma(x)$ в поле L'.*

Доказательство: если τ — такой гомоморфизм, то $p^\sigma(\alpha^\tau) = p^\tau(\alpha^\tau) = (p(\alpha))^\tau = 0$, поэтому $\beta = \alpha^\tau \in L'$ — корень многочлена $p^\sigma(x) \in L[x]$. Обратно, предположим, что $\beta \in L'$ — корень $p^\sigma(x)$. Заметим, что всякий элемент в $K' = K(\alpha) = K[\alpha]$ представим в виде $f(\alpha)$, где $f(x) \in K[x]$. Положим $(f(\alpha))^\tau := f^\sigma(\beta)$. Тогда, во-первых, отображение τ определено корректно. Действительно, если $f(\alpha) = g(\alpha)$, то $(f-g)(\alpha) = 0$, следовательно $f(x) - g(x) = h(x)p(x)$, где $h(x) \in K[x]$, значит $f^\sigma(\beta) - g^\sigma(\beta) = h^\sigma(\beta)p^\sigma(\beta) = 0$. Во-вторых, легко видеть, что τ является гомоморфизмом полей. Наконец, ясно, что τ продолжает σ. □

Следствие 1.2. *Число возможных продолжений гомоморфизма $\sigma : K \to L$ на поле $K' = K(\alpha)$ не превосходит $[K' : K] = \deg \operatorname{Irr}_\alpha^K(x)$.*

Пусть K'/K и K''/K — расширения. Будем говорить, что $\sigma : K' \to K''$ — гомоморфизм полей над K, если σ продолжает тождественный гомоморфизм $K \to K$.

Лемма 1.3. *Если L/K — алгебраично, а $\sigma : L \to L$ — гомоморфизм над K, то σ — автоморфизм.*

Доказательство: достаточно проверить, что σ сюръективно. Пусть $\alpha \in L$ и $p(x) = \operatorname{Irr}_\alpha^K(x)$. Пусть $\{\alpha_1, \ldots, \alpha_m\}$ — все корни $p(x)$ в L (можно считать, что $\alpha_1 = \alpha$). Положим $L' = K(\alpha_1, \ldots, \alpha_m)$. Тогда, во-первых L' конечно порождено и алгебраично над K, следовательно $\dim_K L' = [L' : K] < \infty$. Во-вторых, ясно, что $\sigma(\alpha_i) = \alpha_j$, поэтому $\sigma(L') \subset L'$, то есть σ переводит L' в себя. Наконец, так как $\sigma : L' \to L'$ — инъективен и K-линеен, а $\dim_K L' < \infty$, то σ сюръективен на L', значит $\alpha \in \operatorname{Im}\sigma$. □

Теорема 1.4. *Если K'/K — алгебраическое расширение, а $\sigma : K \to L$ — гомоморфизм в алгебраически замкнутое поле L, то существует гомоморфизм $\sigma' : K' \to L$, продолжающий σ.*

Доказательство: пусть $K'' \subset K'$ — максимальное подполе, содержащее K, на которое можно продолжить σ[1]. Предположим, что $K'' \neq K'$. Обозначим через σ'' продолжение σ на K'' и пусть $\alpha \in K' \setminus K''$. По лемме 1.1 гомоморфизм σ'' можно продолжить на поле $K''(\alpha) \subset K'$ (так как L — алгебраически замкнуто), что противоречит максимальности поля K''. Значит $K'' = K'$ и теорема доказана. □

Следствие 1.5. *Если $\overline{K}'/K$ и $\overline{K}''/K$ — алгебраические замыкания, то $\overline{K}' \cong \overline{K}''$ (изоморфизм над K). Более того, всякий гомоморфизм $\overline{K}' \to \overline{K}''$ над K является изоморфизмом.*

Доказательство: пользуясь теоремой 1.4 строим гомоморфизмы $\sigma : \overline{K}' \to \overline{K}''$ и $\tau : \overline{K}'' \to \overline{K}'$ над K. Далее, по лемме 1.3 композиции $\tau\sigma$ и $\sigma\tau$ являются автоморфизмами, поэтому σ и τ — изоморфизмы. □

[1] Чтобы убедиться в том, что такое K'' существует воспользуемся леммой Цорна. Нам надо проверить, что для любой башни $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K'$ и любого набора гомоморфизмов $\sigma_i : K_i \to L$ ($\sigma_0 = \sigma$), продолжающих друг друга, найдется поле $\widetilde{K} \subset K'$ и гомоморфизм $\tilde{\sigma} : \widetilde{K} \to L$, такие что $\forall i$ имеем $K_i \subset \widetilde{K}$ и $\tilde{\sigma}$ продолжает σ_i. Действительно, возьмем $\widetilde{K} = \bigcup_{i=1}^\infty K_i$ и положим $\tilde{\sigma}(x) = \sigma_i(x)$, если $x \in K_i$. Ясно, что $\tilde{\sigma}$ — корректо определен (так как σ_i продолжает σ_j при $i > j$) и является гомоморфизмом. Кроме того, очевидно, что $\tilde{\sigma}$ продолжает любой из σ_i.

Часть 2. Поле разложения

Пусть K — поле и $f(x) \in K[x]$ — произвольный многочлен.

Определение 2.1. Поле L называется полем разложения многочлена f, если, во-первых, $f(x)$ над полем L раскладывается на линейные множители $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$, и, во-вторых, $L = K(\alpha_1, \dots, \alpha_n)$.

Лемма 2.2. *Всякое алгебраическое замыкание $\overline{K}$ поля K содержит единственное подполе L, являющееся полем разложения многочлена $f(x)$. Всякое вложение $\sigma : L \to \overline{K}$ над K является автоморфизмом поля L. Любые два поля разложения многочлена $f(x)$ изоморфны.*

Доказательство: Рассмотрим алгебраическое замыкание $\overline{K}$ поля K. Тогда $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$ в $\overline{K}[x]$. Ясно, что c — старший коэффициент в $f(x)$, поэтому $c \in K$. Пусть $L = K(\alpha_1, \dots, \alpha_n) \subset \overline{K}$. Тогда L является полем разложения многочлена $f(x)$. Более того, ясно что никакое другое подполе в $\overline{K}$ не может быть полем разложения этого многочлена. Тем самым, первое утверждение доказано.

Докажем теперь второе утверждение. Пусть $\alpha_1, \dots, \alpha_n$ — корни многочлена $f(x)$ в поле $\overline{K}$. Тогда ясно, что $f^\sigma(x) = f(x)$, так как σ — вложение над K, а $f(x) \in K[x]$; значит $f(\alpha_i^\sigma) = f^\sigma(\alpha_i^\sigma) = (f(\alpha_i))^\sigma = 0$, поэтому σ переводит множество корней многочлена $f(x)$ в себя. Следовательно, σ индуцирует гомоморфизм $L \to L$, который является автоморфизмом, так как $L = K(\alpha_1, \dots, \alpha_n)$.

Пусть, наконец, L' — другое поле разложения многочлена $f(x)$. Ясно, что $L' \subset \overline{K}'$ для некоторого алгебраического замыкания поля K. Выберем изоморфизм $\sigma : \overline{K} \to \overline{K}'$ над K. Повторяя те же рассуждения, что и выше, легко показать, что σ задает изоморфизм $L \to L'$. □

Аналогично определяется поле разложения произвольного семейства многочленов $\{ f_i(x) \mid f_i(x) \in K[x] \}_{i \in I}$. Полем разложения семейства $\{ f_i(x) \}$ называется поле L, такое что, во-первых, каждый из многочленов $f_i(x)$ раскладывается над полем L на линейные множители, и, во-вторых, поле L порождается корнями всех многочленов $f_i(x)$. Следующее утверждение доказывается аналогично лемме 2.2.

Лемма 2.3. *Всякое алгебраическое замыкание $\overline{K}$ поля K содержит единственное подполе L, являющееся полем разложения семейства многочленов $\{ f_i(x) \}_{i \in I}$. Всякое вложение $\sigma : L \to \overline{K}$ над K является автоморфизмом поля L. Любые два поля разложения семейства многочленов $\{ f_i(x) \}_{i \in I}$ изоморфны.*

Часть 3. Нормальные расширения

Определение 3.1. Пусть L/K — алгебраическое расширение, $L \subset \overline{K}$. Расширение L/K называется нормальным, если любой гомоморфизм $\sigma : L \to \overline{K}$ над K является автоморфизмом поля L.

Лемма 3.2. *Расширение L/K нормально $\iff$ любой неприводимый многчлен $f(x) \in K[x]$, имеющий корень в L, раскладывается в L на линейные множители.*

Доказательство: $\Longleftarrow$) Пусть $\sigma : L \to \overline{K}$ — гомоморфизм над K. Выберем произвольный элемент $\alpha \in L$ и пусть $p(x) = \mathrm{Irr}_\alpha^K(x)$. Ясно, что α^σ является корнем многочлена $p(x)$. С другой стороны, $p(x)$ раскладывается в L на линейные множители, следовательно L содержит все корни $p(x)$ в $\overline{K}$. Значит $\alpha^\sigma \in L$. Отсюда следует, что $\sigma(L) \subset L$, значит по лемме 1.3 гомоморфизм σ является автоморфизмом поля L.

$\Longrightarrow$) Пусть $f(x) \in K[x]$ — неприводим и $\alpha \in L$ — его корень. Пусть β — другой корень $p(x)$ в $\overline{K}$. Тогда по лемме 1.1 существует гомоморфизм $\sigma : L \to \overline{K}$, такой что $\alpha^\sigma = \beta$. Из нормальности поля L тут же следует, что $\beta \in L$. Значит все корни многочлена $p(x)$ содержатся в L, следовательно $p(x)$ раскладывается в L на линейные множители. □

Лемма 3.3. *Расширение L/K нормально $\iff$ L является полем разложения некоторого семейства многочленов $\{ f_i(x) \mid f_i(x) \in K[x] \}_{i \in I}$.*

Доказательство: если L/K — нормально, то L является полем разложения для семейства многочленов $\{ \mathrm{Irr}_\alpha^K(x) \}_\alpha$, где α пробегает произвольную систему образующих поля L над K, так как по лемме 3.2 каждый из многочленов $\mathrm{Irr}_\alpha^K(x)$ раскладывается в L на линейные множители. Это доказывает импликацию $\Longrightarrow$. В свою очередь импликация $\Longleftarrow$ следует из леммы 2.3. □

Часть 4. Конечные поля

Пусть p — простое число и K — поле характеристики p.

Лемма 4.1. *Отображение $\Phi : K \to K$, $x \mapsto x^p$ является гомоморфизмом поля K в себя над $\mathbb{F}_p$.*

Доказательство: очевидная проверка показывает, что $\Phi(xy) = \Phi(x)\Phi(y)$, $\Phi(x^{-1}) = \Phi(x)^{-1}$ и $\Phi(1) = 1$. Далее, заметим, что $(-1)^p = -1$ (если p — нечетно, то это очевидно, а если $p = 2$, то $(-1)^p = 1 = -1$). Значит $\Phi(-x) = (-x)^p = (-1)^p x^p = -x^p = -\Phi(x)$. Кроме того, ясно что $\Phi(0) = 0$. Остается проверить, что $\Phi(x+y) = \Phi(x)+\Phi(y)$. Действительно, $\Phi(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + y^p$. Заметим, что при $1 \leqslant k \leqslant p-1$ число $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p, следовательно равно нулю в любом поле характеристики p. Значит $\Phi(x+y) = x^p + y^p = \Phi(x) + \Phi(y)$. □

Лемма 4.2. *Если L — поле из q элементов, то $\forall \alpha \in L$ имеем $\alpha^q - \alpha = 0$.*

Доказательство: мультипликативная группа поля L имеет порядок $q-1$, поэтому $\forall \alpha \in L^*$ имеем $\alpha^{q-1} = 1$, следовательно $\alpha^q - \alpha = 0$. Остается заметить лишь, что $0^q - 0 = 0$. □

Следствие 4.3. *Если L — поле из q элементов, то L — поле разложения многочлена $f(x) = x^q - x$.*

Пусть теперь $q = p^n$ и пусть L — поле разложения многочлена $x^q - x$ над $\mathbb{F}_p$.

Лемма 4.4. *Поле L совпадает с множеством корней многочлена $f(x) = x^q - x$ и состоит из q элементов.*

Доказательство: заметим, что $x^q = x^{p^n} = \Phi^n(x)$, поэтому по лемме 4.1 множество $L_0 = \{\, \alpha \in L \mid f(\alpha) = 0 \,\}$ замкнуто относительно сложения, умножения и т.д. Иначе говоря, L_0 является подполем в L. Далее, ясно что L_0 содержит $\mathbb{F}_p$ и порождается над ним всеми корнями многочлена $f(x)$, следовательно L_0 является полем разложения $f(x)$ над $\mathbb{F}_p$, то есть $L_0 = L$. Остается проверить, что L_0 состоит из q элементов. Действительно, заметим, что $f'(x) = qx^{q-1} - 1 = -1$, поэтому $(f(x), f'(x)) = 1$, и значит $f(x)$ не имеет кратных корней в силу следующей леммы. □

Лемма 4.5. *Многочлен $f(x) \in K[x]$ имеет кратный корень в $\overline{K} \iff (f(x), f'(x)) \neq 1$.*

Доказательство: если $f(x) = (x-\alpha)g(x)$, то $f'(x) = g(x)+(x-\alpha)g'(x)$, поэтому $(x-\alpha)|f'(x) \iff (x-\alpha)|g(x)$ $\iff (x-\alpha)^2|f(x)$. □

Следствие 4.6. *Для всякого $q = p^n$ существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$ из q элементов, а именно поле разложения многочлена $x^q - x$ над $\mathbb{F}_p$.*

Займемся теперь изучением эндоморфизмов конечных полей.

Лемма 4.7. *Всякий эндоморфизм поля $\mathbb{F}_q$ является автоморфизмом.*

Доказательство: как мы знаем, всякий эндоморфизм поля является вложением, но инъективное отображение конечного множества в себя сюръективно. □

Следствие 4.8. *Гомоморфизм $\Phi : \mathbb{F}_q \to \mathbb{F}_q$ является автоморфизмом.*

Автоморфизм Φ называется автоморфизмом Фробениуса.

Теорема 4.9. *Если $q = p^n$, то группа $\mathrm{Aut}(\mathbb{F}_q)$ является циклической группой порядка n, порожденной автоморфизмом Фробениуса.*

Доказательство: покажем вначале, что Φ имеет порядок n в группе $\mathrm{Aut}(\mathbb{F}_q)$. Действительно, по лемме 4.2 $\Phi^n(\alpha) = \alpha^q = \alpha$ для любого $\alpha \in \mathbb{F}_q$, поэтому $\Phi^n = \mathrm{Id}$. С другой стороны, если $\Phi^k = \mathrm{Id}$, то $\forall \alpha \in \mathbb{F}_q$ имеем $\alpha^{p^k} = \alpha$, следовательно $\alpha \in \mathbb{F}_{p^k}$, значит $k \geqslant n$. Остается проверить, что всякий автоморфизм поля $\mathbb{F}_q$ имеет вид Φ^k. Действительно, пусть α — образующая мультипликативной группы $\mathbb{F}_q^*$. Ясно, что $\mathbb{F}_p(\alpha) = \mathbb{F}_q$, поэтому $\deg \mathrm{Irr}_\alpha^{\mathbb{F}_p}(x) = n$. Применяя следствие 1.2, получаем, что $|\mathrm{Aut}(\mathbb{F}_q)| \leqslant n$. □

Лекция 11. Сепарабельность

Часть 1. Сепарабельная степень

Лемма 1.1. *Если K/F — алгебраическое расширение, а $\sigma : F \to L$ — гомоморфизм в алгебраически замкнутое поле, то количество гомоморфизмов $\tau : K \to L$, продолжающих σ, не зависит от σ.*

Доказательство: пусть $\sigma' : F \to L'$ — другой гомоморфизм. Пусть $\overline{F}$ и $\overline{F}'$— алгебраические замыкания F в L и L' соответственно. Выберем изоморфизм $\rho : \overline{F} \to \overline{F}'$ над F. Тогда $\tau \mapsto \rho \circ \tau$ искомая биекция. □

Определение 1.2. Пусть K'/K — конечное расширение и $\sigma : K \to L$ — гомоморфизм в алгебраически замкнутое поле. Определим сепарабельную степень $[K' : K]_s$ как количество различных гомоморфизмов $K' \to L$, продолжающих σ.

Лемма 1.3. *Сепарабельная степень мультипликативна в башнях: если $K \subset K' \subset K''$ — конечные расширения полей, то $[K'' : K]_s = [K'' : K']_s[K' : K]_s$.*

Доказательство: Пусть $K \subset K' \subset K''$ — конечные расширения, L — алгебраически замкнутое поле и $\rho : K \to L$ — гомоморфизм. Пусть $\sigma_1, \ldots, \sigma_n$, $n = [K' : K]_s$ — набор различных гомоморфизмов $K' \to L$, продолжающих ρ. Пусть далее $\tau_{i1}, \ldots, \tau_{im}$, $m = [K'' : K']_s$ — набор различных гомоморфизмов $K'' \to L$, продолжающих σ_i. Покажем, что τ_{ij} различны. Действительно, если $\tau_{ij} = \tau_{kl}$, то $\sigma_i = \tau_{ij\,|K'} = \tau_{kl\,|K'} = \sigma_k$, значит $i = k$, но тогда $j = l$. Пусть теперь $\tau : K'' \to L$ — произвольный гомоморфизм, продолжающий ρ. Тогда $\tau_{|K'}$ — тоже продолжает ρ, следовательно $\tau_{|K'} = \sigma_i$ для некоторого i и, значит, $\tau = \tau_{ij}$ для некоторого j. Таким образом, мы показали, что существует ровно mn гомоморфизмов $K'' \to L$, продолжающих ρ, и тем самым доказали мультипликативность сепарабельной степени. □

Лемма 1.4. *Для любого конечного расширения K'/K имеем $[K' : K]_s \leqslant [K' : K]$.*

Доказательство: поскольку как степень, так и сепарабельная степень мультипликативны в башнях, то достаточно показать, что $[K(\alpha) : K]_s \leqslant [K(\alpha) : K]$. Но мы уже знаем, что $[K(\alpha) : K]_s$ равно количеству различных корней многочлена $\mathrm{Irr}_\alpha^K(x)$ в поле $\overline{K}$, в то время как $[K(\alpha) : K]$ равно степени этого многочлена. □

Следствие 1.5. *Пусть $K \subset K' \subset K''$ — башня конечных расширения полей. Тогда*
$[K'' : K]_s = [K'' : K] \iff [K'' : K']_s = [K'' : K']$ *и* $[K' : K]_s = [K' : K]$.

Часть 2. Сепарабельные расширения

Определение 2.1. Неприводимый многочлен $f(x) \in K[x]$ называется сепарабельным, если $f(x)$ не имеет кратных корней в $\overline{K}$.

Лемма 2.2. *Неприводимый многочлен $f(x) \in K[x]$ не сепарабелен $\iff \mathrm{char}\, K = p > 0$ и $f(x) = g(x^{p^n})$, где $g(x) \in K[x]$ — неприводимый сепарабельный многочлен.*

Доказательство: если $f(x)$ имеет кратные корни в $\overline{K}$, то $(f(x), f'(x)) \neq 1$. Но $f(x)$ — неприводим, значит[1] $(f(x), f'(x)) = f(x)$, значит $f'(x) = 0$. Отсюда следует, что $\mathrm{char}\, K = p > 0$ и $f(x) = f_1(x^p)$, где $f_1(x) \in K[x]$. Ясно, что $f_1(x)$ неприводим, поэтому по индукции $f_1(x) = g(x^{p^{\mu'}})$, где $g(x)$ неприводим и сепарабелен. Значит $f(x) = g(x^{p^{\mu'+1}})$. □

[1] если $f(x), g(x) \in K[x]$ и $h(x) = \gcd_{K[x]}(f(x), g(x))$, то $h(x) \in K[x]$. Докажите это!

Определение 2.3. Пусть L/K — расширение полей. Элемент $\alpha \in L$ называется сепарабельным над K, если многочлен $\mathrm{Irr}_\alpha^K(x)$ — сепарабелен. Алгебраическое расширение L/K называется сепарабельным, если любой элемент поля L сепарабелен над K.

Следствие 2.4. *Если* $\mathrm{char}\, K = 0$, *то всякое алгебраическое расширение поля* K *сепарабельно.*

Пусть теперь $\mathrm{char}\, K = p > 0$.

Лемма 2.5. *Элемент* α *сепарабелен над* $K \iff$ *найдется многочлен* $f(x) \in K[x]$, *такой что* $f(\alpha) = 0$ *и* $f(x)$ *не имеет кратных корней в* $\overline{K}$.

Доказательство: $\Longrightarrow$) Очевидно. $\Longleftarrow$) Ясно, что $\mathrm{Irr}_\alpha^K(x)$ делит $f(x)$, поэтому если $f(x)$ не имеет кратных корней, то и $\mathrm{Irr}_\alpha^K(x)$ не имеет кратных корней в поле $\overline{K}$. □

Лемма 2.6. *Если башня полей сепарабельна, то каждый ее этаж сепарабелен.*

Доказательство: пусть $K \subset K' \subset K''$ и K''/K сепарабельно. Все элементы в K'', а значит и в K'сепарабельны над K. С другой стороны, $\forall \alpha \in K''$ многочлен $\mathrm{Irr}_\alpha^K(x) \in K[x] \subset K'[x]$ сепарабелен, значит по лемме 2.5 элемент α сепарабелен и над K'. □

Лемма 2.7. *Пусть* α *— алгебраический элемент над полем* K, $f(x) = \mathrm{Irr}_\alpha^K(x)$ *и* $f(x) = g(x^{p^\mu})$, *где* $g(x)$ *— неприводимый и сепарабельный. Тогда* α^{p^μ} *сепарабелен над* K *и* $[K(\alpha) : K]_s = \deg g(x)$. *В частности,* $[K(\alpha) : K] = p^\mu [K(\alpha) : K]_s$.

Доказательство: Пусть $\{\, \beta_1, \ldots, \beta_m \,\}$ — множество корней многочлена $g(x)$ в $\overline{K}$. Заметим, что для каждого β_i найдется единственный $\alpha_i \in \overline{K}$, т.ч. $\alpha_i^{p^\mu} = \beta_i$ ($\alpha_i^{p^\mu} = \alpha_i'^{p^\mu} \Longrightarrow 0 = \alpha_i^{p^\mu} - \alpha_i'^{p^\mu} = (\alpha_i - \alpha_i')^{p^\mu} \Longrightarrow \alpha_i = \alpha_i'$). Тогда $f(x) = g(x^{p^\mu}) = \prod_{i=1}^m (x^{p^\mu} - \alpha_i^{p^\mu}) = \prod_{i=1}^m (x - \alpha_i)^{p^\mu}$, поэтому $[K(\alpha) : K]_s = m = \deg g(x)$. Кроме того, $[K(\alpha) : K] = \deg f(x) = p^\mu \deg g(x) = p^\mu [K(\alpha) : K]_s$. Наконец, α^{p^μ} сепарабелен так как является корнем сепарабельного многочлена $g(x)$. □

Следствие 2.8. *Элемент* α *сепарабелен* $\iff [K(\alpha) : K]_s = [K(\alpha) : K]$.

Теорема 2.9. *Конечное расширение* K'/K *сепарабельно* $\iff [K' : K]_s = [K' : K]$.

Доказательство: пусть K'/K сепарабельно. Возьмем $\alpha \in K' \setminus K$ и рассмотрим башню $K \subset K(\alpha) \subset K'$. По лемме 2.6 каждый этаж сепарабелен. Далее, в силу 2.8 имеем $[K(\alpha) : K]_s = [K(\alpha) : K]$, кроме того, по индукции имеем $[K' : K(\alpha)]_s = [K' : K(\alpha)]$, значит $[K' : K]_s = [K' : K]$ в силу мультипликативности степеней. Обратно, предположим, что $[K' : K]_s = [K' : K]$ и возьмем произвольный $\alpha \in K'$. По следствию 1.5 имеем $[K(\alpha) : K]_s = [K(\alpha) : K]$, значит в силу 2.8 элемент α сепарабелен. □

Следствие 2.10. *Расширение* $K(\alpha_1, \ldots, \alpha_n)/K$ *сепарабельно* $\iff \alpha_1, \ldots, \alpha_n$ *— сепарабельны над* K.

Доказательство: $\Longrightarrow$) По определению. $\Longleftarrow$) На каждом этаже башни $K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n)$ сепарабельная степень равна степени, поэтому $[K(\alpha_1, \ldots, \alpha_n) : K]_s = [K(\alpha_1, \ldots, \alpha_n) : K]$ в силу мультипликативности, следовательно по теореме 2.9 расширение $K(\alpha_1, \ldots, \alpha_n)/K$ сепарабельно. □

Следствие 2.11. *Башня полей сепарабельна* $\iff$ *каждый ее этаж сепарабелен.*

Доказательство: $\Longrightarrow$) Уже доказано. $\Longleftarrow$) Действительно, пусть $K \subset K' \subset K''$ — башня и $\alpha \in K''$. Пусть $\mathrm{Irr}_\alpha^{K'}(x) = x^n + a_1 x^{n-1} + \cdots + a_0$. Тогда α сепарабелен над $K(a_1, \ldots, a_n) \subset K'$, а $K(a_1, \ldots, a_n)$ сепарабельно над K. Значит $[K(a_1, \ldots, a_n, \alpha) : K]_s = [K(a_1, \ldots, a_n, \alpha) : K]$, следовательно α сепарабелен над K. □

Часть 3. Чисто несепарабельные расширения

Лемма 3.1. *Если* L/K *конечно, то* $[L : K]_s$ *делит* $[L : K]$.

Доказательство: в силу мультипликативности все следует из леммы 2.8. □

Число $[L : K]_i := [L : K]/[L : K]_s$ называется степенью несепарабельности расширения L/K.

Лемма 3.2. *Если* $\mathrm{char}\, K = 0$, *то* $[L : K]_i = 1$, *а если* $\mathrm{char}\, K = p$, *то* $[L : K]_i = p^\mu$ *для некоторого* μ.

Доказательство: в силу мультипликативности все следует из леммы 2.8. □

Определение 3.3. Элемент α называется чисто несепарабельным над K, если $\alpha^{p^\mu} \in K$. Расширение L/K называется чисто несепарабельным, если всякий $\alpha \in L$ чисто несепарабелен над K.

Лемма 3.4. *Элемент α чисто несепарабелен над $K \iff \operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, $a \in K$.*

Доказательство: если $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, то $\alpha^{p^\mu} = a \in K$, поэтому α чисто несепарабелен над K. С другой стороны, если $\mu > 0$ — минимальное число, такое что $\alpha^{p^\mu} \in K$, то $f(x) = (x-\alpha)^{p^\mu} = x^{p^\mu} - \alpha^{p^\mu} \in K[x]$, поэтому $\operatorname{Irr}_\alpha^K(x)$ делит $f(x)$, следовательн $\operatorname{Irr}_\alpha^K(x) = (x-\alpha)^n$, $n \leqslant \mu$. Наконец, если $n = mp^{\mu'}$, $(m,p) = 1$, то $(x-\alpha)^n = \left((x-\alpha)^{p^{\mu'}}\right)^m = (x^{p^{\mu'}} - \alpha^{p^{\mu'}})^m = x^n - m\alpha^{p^{\mu'}} x^{(m-1)p^{\mu'}} + \ldots$, поэтому $\alpha^{p^{\mu'}} \in K$, значит (в силу минимальности μ) имеем $\mu' = \mu$, $m = 1$ и $\operatorname{Irr}_\alpha^K(x) = (x-\alpha)^{p^\mu} = x^{p^\mu} - \alpha^{p^\mu}$. □

Следствие 3.5. *Расширение L/K чисто несепарабельно $\iff \forall \alpha \in L$ имеем $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$.*

Лемма 3.6. *Конечное расширение L/K чисто несепарабельно $\iff [L:K]_s = 1$.*

Доказательство: Пусть L/K чисто несепарабельно. Вследствии мультипликативности можно считать, что $L = K(\alpha)$. Тогда, в силу леммы 3.4 имеем $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, поэтому по лемме 2.8 имеем $[K(\alpha):K]_s = 1$. Обратно, если $[L:K]_s = 1$, то $\forall \alpha \in L$ в силу мультипликативности имеем $[K(\alpha):K]_s = 1$, поэтому по лемме 2.8 имеем $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, следовательно по лемме 3.4 элемент α чисто несепарабелен над K. □

Следствие 3.7. *Башня расширений чисто несепарабельна $\iff$ каждый ее этаж чисто несепарабелен.*

Часть 4. Сепарабельное замыкание

Лемма 4.1. *Пусть L/K — расширение. Множество элементов $\alpha \in L$, сепарабельных над K образует подполе $L^{\mathrm{sep}} \subset L$, сепарабельное над K.*

Доказательство: если $\alpha, \beta \in L^{\mathrm{sep}}$, то $K(\alpha,\beta)/K$ сепарабельно по 2.10, следовательно $\alpha+\beta, \alpha\beta, \cdots \in L^{\mathrm{sep}}$. □

Поле L^{sep} называется сепарабельным замыканием поля K в L.

Лемма 4.2. *Расширение L^{sep}/K сепарабельно, а L/L^{sep} чисто несепарабельно.*

Доказательство: первое утверждение очевидно. Докажем второе. Пусть $\alpha \in L$. По лемме 2.7 существует μ, такое что α^{p^μ} сепарабелен над K. Поэтому $\alpha^{p^\mu} \in L^{\mathrm{sep}}$, значит α чисто несепарабелен над L^{sep}. □

Замечание 4.3. Таким образом, всякое расширение представляется в виде башни, нижний этаж которой сепарабелен, а верхний — чисто несепарабелен.

Теорема 4.4. *Пусть L/K — нормальное расширение, $G = \operatorname{Aut}(L/K)$. Тогда $L^G := \{\, x \in L \mid Gx = x \,\}$ — подполе в L, причем L/L^G — сепарабельно, а L^G/K — чисто несепарабельно.*

Доказательство: Пусть $\alpha \in L$. Ясно, что орбита $G\alpha \subset L$ конечна, поэтому существует подмножество $\{\, \sigma_0, \sigma_1, \ldots, \sigma_{n-1} \,\} \subset G$, такое что $\{\, \sigma_0\alpha, \ldots, \sigma_{n-1}\alpha \,\} = G\alpha$. Рассмотрим многочлен $p(x) = \prod_{i=0}^{n-1}(x - \alpha^{\sigma_i})$. Легко видеть, что $Gp(x) = p(x)$, поэтому $p(x) \in L^G[x]$. Кроме того, по построению $p(\alpha) = 0$ и $p(x)$ не имеет кратных корней. Значит α сепарабелен над L^G. Пусть теперь $\alpha \in L^G$. Пусть $\sigma : K(\alpha) \to \overline{K}$ — произвольный гомоморфизм. Продолжим σ до гомоморфизма $\tau : L \to \overline{K}$ над K. Тогда $\tau \in G$, так как L/K нормально, значит $\alpha^\sigma = \alpha^\tau = \alpha$, так как $\alpha \in L^G$. Но тогда $\sigma = \mathrm{Id}$, значит $[K(\alpha):K]_s = 1$, значит α чисто несепарабелен над K. □

Определение 4.5. Поле K называется совершенным, если $\operatorname{char} K = 0$ или $K^p = K$, где $p = \operatorname{char} K$.

Следствие 4.6. *Любое алгебраическое расширение совершенного поля сепарабельно.*

Доказательство: если $\alpha^{p^\mu} = a \in K$, то $\alpha = \sqrt[p^\mu]{a} \in K$, значит K не имеет нетривиальных чисто несепарабельных расширений. Пусть теперь L/K — произвольное расширение. Пусть L'/K — нормальное расширение, такое что $L \subset L'$. Тогда по теореме 4.4 расширение L'/K сепарабельно, но тогда и L/K сепарабельно. □

Лекция 12. Теория Галуа

Часть 1. Теорема Галуа

Определение 1.1. Расширение L/K называется расширением Галуа, если L/K нормально и сепарабельно. Группа автоморфизмов $\mathrm{Aut}(L/K)$ называется группой Галуа поля L над K и обозначается $\mathrm{Gal}(L/K)$.

Всякой подгруппе $H \subset \mathrm{Gal}(L/K)$ можно сопоставить подполе $L^H = \{\, \alpha \in L \mid \forall \sigma \in \mathrm{Gal}(L/K)\ \alpha^\sigma = \alpha \,\}$. Аналогично, всякому подполю $F \subset L$ можно сопоставить подгруппу $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$. Основная теорема теории Галуа гласит:

Теорема 1.2. *Если L/K — конечное расширение Галуа, то сопоставления $H \mapsto L^H$, $F \mapsto \mathrm{Gal}(L/F)$ определяют взаимно однозначное соответствие между множеством $\{\, F \mid K \subset F \subset L \,\}$ промежуточных полей и множеством подгрупп $H \subset \mathrm{Gal}(L/K)$.*

Доказательство теоремы проведем в несколько этапов.

Лемма 1.3. *Если L/K — расширение Галуа, и $G = \mathrm{Gal}(L/K)$, то $L^G = K$.*

Доказательство: как было показано в прошлой лекции, если L/K нормально, то L^G/K — чисто несепарабельное расширение. Однако, если L/K сепарабельно, то и L^G/K сепарабельно, поэтому $L^G = K$. □

Лемма 1.4. *Если L/K — расширение Галуа и $K \subset F \subset L$, то L/F — расширение Галуа.*

Доказательство: L/F нормально, так как L/K нормально, и сепарабельно, так как L/K сепарабельно. □

Следствие 1.5. *Если L/K — расширение Галуа, то отображение $F \mapsto \mathrm{Gal}(L/F)$ — инъективно.*

Доказательство: если $K \subset F \subset L$, то L/F является расширением Галуа по лемме 1.4, поэтому из леммы 1.2 вытекает, что $F = L^{\mathrm{Gal}(L/F)}$. Значит, поле F восстанавливается по группе $\mathrm{Gal}(L/F)$, следовательно отображение $F \mapsto \mathrm{Gal}(L/F)$ инъективно. □

Замечание 1.6. В доказательстве инъективности конечность расширения L/K не используется. Поэтому этот результат верен и для бесконечных расширений Галуа.

Прежде чем заняться сюръективностью, докажем полезный результат.

Часть 2. Теорема о примитивном элементе

Определение 2.1. Пусть L/K — алгебраическое расширение полей. Элемент $\alpha \in L$ называется примитивным, если $L = K(\alpha)$.

Лемма 2.2. *Если для расширения полей L/K существует примитивный элемент, то L/K конечно и существует лишь конечное число различных промежуточных расширений $K \subset F \subset L$.*

Доказательство: первая часть очевидна, так как $[K(\alpha) : K] = \deg \mathrm{Irr}_\alpha^K(x)$. Докажем вторую часть. Пусть $p(x) = \mathrm{Irr}_\alpha^K(x)$. Предположим, что $K \subset F \subset L$ и рассмотрим многочлен $\mathrm{Irr}_\alpha^F(x) = x^k + a_1 x^{k-1} + \cdots + a_k$. Тогда, с одной стороны $K(a_1, \ldots, a_k) \subset F$, так как $a_1, \ldots, a_k \in F$, а с другой стороны $[K(\alpha) : K(a_1, \ldots, a_k)] \leqslant k = [K(\alpha) : F]$, значит $K(a_1, \ldots, a_k) = F$, то есть поле F восстанавливается по многочлену $\mathrm{Irr}_\alpha^F(x)$. С другой стороны, так как $p(\alpha) = 0$ и $p(x) \in K[x] \subset F[x]$, то $\mathrm{Irr}_\alpha^F(x) | p(x)$, так что достаточно показать, что многочлен $p(x)$ имеет лишь конечное число делителей в кольце $L[x]$. Однако ясно, что даже в кольце $\overline{L}[x]$ многочлен $p(x)$ имеет не больше, чем 2^n делителей, где $n = \deg p(x)$. □

Оказывается, верно и обратное утверждение.

Лемма 2.3. *Если L/K — конечное расширение и множество полей F, таких что $K \subset F \subset L$ конечно, то существует примитивный элемент.*

Доказательство: если поле K конечно, то L тоже конечно и в качестве примитивного элемента можно взять образующую группы L^*, которая, как мы знаем, циклична. Будем далее предполагать, что поле K бесконечно. Покажем, что если $L = K(\alpha, \beta)$, то найдется $\gamma \in L$, такое что $L = K(\gamma)$. Будем искать γ в виде $\gamma = \alpha + c\beta$, $c \in K$. Ясно, что в силу бесконечности поля K и конечности множества промежуточных полей, найдутся числа $c_1 \neq c_2 \in K$, такие что $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Но это поле содержит как $\beta = [(\alpha + c_1\beta) - (\alpha + c_2\beta)]/(c_1 - c_2)$, так и $\alpha = (\alpha + c_1\beta) - c_1\beta$, поэтому $K(\alpha + c_1\beta) = K(\alpha, \beta)$. Далее остается применить индукцию по количеству порождающих L над K. □

Еще одним важным классом расширений, для которого заведомо существует примитивный элемент, являются сепарабельные расширения.

Лемма 2.4. *Если L/K — конечное сепарабельное расширение, то существует примитивный элемент.*

Доказательство: как и выше, достаточно рассмотреть случай, когда K бесконечно, а $L = K(\alpha, \beta)$. Пусть $n = [L : K] = [L : K]_s$ и пусть $\sigma_1, \ldots, \sigma_n$ — различные гомоморфизмы $L \to \overline{K}$ над K. Заметим, что если $\sigma_i(\alpha) = \sigma_j(\alpha)$ и $\sigma_i(\beta) = \sigma_j(\beta)$, то $i = j$, так как $L = K(\alpha, \beta)$. Поэтому существует лишь конечное множество чисел $c \in K$, таких что $\sigma_i(\alpha + c\beta) = \sigma_j(\alpha + c\beta)$ при $i \neq j$. Выберем $c \in K$, так чтобы таких равенств при $i \neq j$ не было и рассмотрим $\gamma = \alpha + c\beta$. Тогда все числа $\sigma_i(\gamma) \in \overline{K}$ различны, следовательно σ_i — набор различных гомоморфизмов $K(\gamma) \to \overline{K}$. Значит $[K(\gamma) : K] \geqslant [K(\gamma) : K]_s \geqslant n = [L : K]$, следовательно $K(\gamma) = L$. □

Следствие 2.5. *Если L/K сепарабельно и $[K(\alpha) : K] \leqslant n$ для любого $\alpha \in L$, то $[L : K] \leqslant n$.*

Доказательство: пусть $\alpha \in L$ — таков, что $m = [K(\alpha) : K]$ — максимально возможное. Далее, если $\beta \notin K(\alpha)$, то по теореме о примитивном элементе существует γ, такое что $[K(\gamma) : K] = [K(\alpha, \beta) : K] > [K(\alpha) : K]$, что противоречит максимальности m. Значит $K(\alpha) = L$ и $[L : K] = [K(\alpha) : K] \leqslant n$. □

Часть 3. Окончание доказательства теоремы Галуа

Лемма 3.1. *Пусть L — поле и $G \subset \mathrm{Aut}(L)$ — конечная группа автоморфизмов, $|G| = n$, и $F = L^G$. Тогда L/F — конечное расширение Галуа, $G = \mathrm{Gal}(L/F)$ и $[L : F] = n$.*

Доказательство: пусть $\alpha \in L$ и $G\alpha = \{\alpha_1, \ldots, \alpha_m\}$. Ясно, что группа G переставляет числа α_i, поэтому многочлен $f(x) = \prod_{i=1}^{m}(x - \alpha_i)$ инвариантен относительно группы G, следовательно $f(x) \in F[x]$. С другой стороны, $f(\alpha) = 0$, следовательно $\mathrm{Irr}_\alpha^F(x) | f(x)$. Так как $f(x)$ раскладывается над полем L на линейные множители, и не имеет кратных корней, то то же верно и по отношению к многочлену $\mathrm{Irr}_\alpha^F(x)$. Так как α произвольно, то это означает, что расширение L/F нормально и сепарабельно, то есть является расширением Галуа. Более того, из приведенных выше рассуждений следует, что $\forall \alpha \in L$ имеем $[F(\alpha) : F] \leqslant n$, значит согласно 2.5 имеем $[L : F] \leqslant n$. С другой стороны $n = |G| \leqslant [L : F]_s \leqslant [L : F]$, значит $[L : F] = [L : F]_s = n$ и $G = \mathrm{Aut}(L/F) = \mathrm{Gal}(L/F)$. □

Теперь можно завершить доказательство теоремы Галуа. Действительно, если $H \subset \mathrm{Gal}(L/K)$ — подгруппа, то по лемме 3.1 имеем $H = \mathrm{Gal}(L/L^H)$, следовательно отображение $F \mapsto \mathrm{Gal}(L/F)$ — сюръективно.

Замечание 3.2. В доказательстве сюръективности существенным образом использована конечность расширения. Точнее говоря, использовалась конечность подшруппы $H \subset \mathrm{Gal}(L/K)$. Тем самым, даже если L/K бесконечное расширение Галуа, то образ отображения из множества подполей в множество подгрупп группы Галуа содержит все конечные подгруппы. В действительности, для бесконечных расширений отображение из множества подполей в множество подгрупп группы Галуа перестает быть сюръективным. Образ этого отображения состоит лишь из подгрупп, замкнутых относительно некоторой топологии на группе Галуа.

Теперь, закончив доказательство теоремы Галуа, займемся уточнениями. Пусть L/K — конечное расширение Галуа, и $G = \mathrm{Gal}(L/K)$. Заметим, что группа G действует как на множестве всех своих подгрупп (сопряжениями), так и на множестве всех промежуточных полей.

Лемма 3.3. *Изоморфизм теории Галуа является изоморфизмом G-множеств.*

Доказательство: пусть $\sigma \in G = \mathrm{Aut}(L/K)$ и $H \subset G$. Тогда $L^{\sigma H \sigma^{-1}} = \{\alpha \in L \mid \forall h \in H\ \sigma h \sigma^{-1}\alpha = \alpha\} = \{\alpha \in L \mid \forall h \in H\ h\sigma^{-1}\alpha = \sigma^{-1}\alpha\} = \{\alpha \in L \mid \sigma^{-1}\alpha \in L^H\} = \{\alpha = \sigma\beta \mid \beta \in L^H\} = (L^H)^\sigma$. □

Лемма 3.4. *Пусть L/K — конечное расширение Галуа, и $K \subset F \subset L$. Расширение F/K нормально $\iff$ подгруппа $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ — нормальна. В этом случае $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.*

Доказательство: всякий гомоморфизм $F \to \overline{K}$ можно продолжить до гомоморфизма $L \to \overline{K}$ над K, который в силу нормальности L/K является автоморфизмом поля L. Следовательно, расширение F/K нормально $\iff$ любой элемент группы $\mathrm{Gal}(L/K)$ оставляет F на месте, что в силу леммы 3.3 равносильно нормальности группы $\mathrm{Gal}(L/F)$.

Пусть теперь F/K нормально. Тогда всякий автоморфизм L/K оставляет F на месте, следовательно задает автоморфизм F/K. Тем самым, имеем гомоморфизм групп $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$. Этот гомоморфизм сюръективен, так как всякий автоморфизм поля F над K можно продолжить до гомоморфизма из L в $\overline{K}$ над K, который является автоморфизмом L/K в силу нормальности L/K. В свою очередь, ядро гомоморфизма состоит из всех автоморфизмов L/K, тождественных на F, то есть по теореме Галуа совпадает с группой $\mathrm{Gal}(L/F)$. □

Лемма 3.5. *Если $K \subset F, F' \subset L$, то $F \subset F' \iff \mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$. Иначе говоря, изоморфизм теории Галуа обращает отношение вложенности.*

Доказательство: если $F \subset F'$, то всякий автоморфизм поля L, тождественный на F' тождественнен и на F, поэтому $\mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$. Обратно, по теореме Галуа $L^{\mathrm{Gal}(L/F')} = F'$, поэтому вложение групп Галуа $\mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$ влечет вложение полей $F \subset F'$. □

Лемма 3.6. *Если $K \subset F \subset L$, то $[F : K] = (\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F))$. В частности, полям, конечным над K соответствуют подгруппы конечного индекса.*

Доказательство: всякий гомоморфизм $F \to \overline{K}$ продолжается до автоморфизма поля L над K, так как L/K нормально. С другой стороны, автоморфизмы σ и σ' поля L над K задают один и тот же гомоморфизм $F \to \overline{K} \iff \sigma^{-1}\sigma'$ тождественно на F, то есть лежит в $\mathrm{Gal}(L/F)$. Значит, множество гомоморфизмов $F \to \overline{K}$ совпадает с множеством смежных классов $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$, следовательно $[F : K] = [F : K]_s = (\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F))$. □

Замечание 3.7. Результаты 3.3–3.6 выполняются и для бесконечных расширений Галуа.

Замечание 3.8. Пусть $\overline{K}^{\mathrm{sep}}$ — сепарабельное замыкание поля K. Тогда $\overline{K}^{\mathrm{sep}}/K$ — максимальное сепарабельное расширение поля K. Его группа Галуа называется абсолютной группой Галуа поля K. Из теоремы Галуа следует, что сепарабельные расширения поля K находятся во взаимно однозначном соответствии с замкнутыми подгруппами абсолютной группы Галуа, при этом нормальные расширения соответствуют нормальным подгруппам, а конечные расширения соответствуют подгруппам конечного индекса.

Замечание 3.9. Изучение абсолютной группы Галуа поля рациональных чисел — одна из основных задач алгебраической теории чисел.

В завершение дадим еще одно определение.

Пусть $p(x) \in K[x]$ — неприводимый сепарабельный многочлен, а L — его поле разложения. Группа Галуа $\mathrm{Gal}(L/K)$ называется группой Галуа многочлена $p(x)$.

Семестр II (Весна 2003)

Программа

На зачете каждому студенту будет предлагаться по одному вопросу на темы «группы, поля, категории» и «теория представлений», и два вопроса по теме «линейная алгебра». После каждого вопроса указано примерное предполагаемое содержание ответа (темы, изучавшиеся на лекциях (номер лекции указан римскими цифрами), и задачи, изучавшиеся на семинарах (указана дата выдачи листка с задачами)).

- Группы, поля, категории.
  1. Разрешимые группы. — (I) 1.2, 2.2–2.4.
  2. Характеры групп. — (I) 3.1, 3.2, (15а) 13.
  3. Теорема Гильберта-90. — (I) 3.3, 3.4, 5.1, 5.2, (11ф) 4.
  4. Разрешимость уравнения в радикалах. — (I) 1.1, 1.3, 4.4, 4.5. (11ф) 1.
  5. Целые алгебраические числа. — (XI) 1.1–1.6, (22а) 3, 4.
  6. Категории. — (II) 1.1–1.5.
  7. Функторы. — (II) 3.1–3.3.
  8. Морфизмы функторов. — (II) 3.4–3.7, (18ф) 7, 8, (08а) 4.
  9. Универсальные объекты. — (II) 2.1–2.4.
  10. Произведения и копроизведения. — (II) 2.3.1–2.3.2, (18ф) 1, 2, (25ф) 7
  11. Задание группы образующими и соотношениями. — (II) 2.3.3, 2.4, (18ф) 3ab, 4, 5.
- Линейная алгебра.
  1. Двойственность. — (III) 1.1–1.9, (25ф) 1.
  2. Тензорное произведение. — (III) 2.1–2.5, (25ф) 2–4.
  3. Канонические изоморфизмы. — (III) 3.1, 3.2, (25ф) 5, 6.
  4. Билинейные формы. — (IV) 1.1–1.13, (4м) 2.
  5. Симметрические и знакопеременные формы. — (IV) 2.1–2.9, (4м) 1ab, 3.
  6. Эрмитовы формы. — (IV) 3.1–3.6, (4м) 1cd.
  7. Сигнатура. — (V) 1.1–1.3, (11м) 1.
  8. Положительная определенность. — (V) 2.1–2.7.
  9. Евклидова геометрия. — (V) 3.1–3.4, (11м) 3, 5.
  10. Ортогональная и унитарная группы. — (V) 4.1–4.5, 5, (11м) 6, 7a, (18м) 6b.
  11. Сопряженные операторы. — (VI) 1.1–1.6, 2.1–2.3.
  12. Спектральная теорема (эрмитов случай). — (VI) 3.1–3.4.
  13. Спектральная теорема (симметрический случай). — (VI) 5.1–5.3.
  14. Комплексификация и овеществление. — (VI) 4.1–4.5.
  15. Полярное разложение. — (VI) 6.1–6.3, (18м) 7.

16. Тензоры. — (VII) 1.1–1.9.
17. Симметрические и кососимметрические тензоры. — (VII) 2.1–2.10, (25м) 1.
18. Пфаффианы. — (VIII) 1.1–1.5, (01a) 2.
19. Уравнения Плюккера. — (VIII) 2.1–2.12, (01a) 5.
20. Алгебры. — (VII) 3.1–3.8, (25м) 2, 6ab, 7.

- Теория представлений.

1. Представления групп. — (IX) 1.1–1.9, 2.1, 2.2, (08a) 1, 7.
2. Теорема Машке. — (IX) 3.1–3.6, (08a) 5.
3. Лемма Шура. — (IX) 4.1–4.8, (15a) 5.
4. Характеры представлений, соотношения ортогональности. — (X) 1.1–1.4, 2.1–2.7, (15a) 1abc.
5. Следствия соотношений ортогональности. — (X) 3.1–3.8.
6. Кольцо Гротендика. — (X) 4.1–4.3, (08a) 2, (15a) 2.
7. Степени неприводимых представлений. — (XI) 1.7–1.9.
8. Ограничение и индукция. — (XI) 2.1–2.9, (22a) 6, 8, 10, 12.
9. Представления абелевых групп.
10. Представления произведения групп. — (XI) 3.1–3.5.

Лекция 1. Применения теории Галуа

Часть 1. Разрешимость в радикалах

Пусть $p(x) \in K[x]$ — неприводимый многочлен над полем K, $\operatorname{char} K = 0$.

Определение 1.1. Будем говорить, что уравнение $p(x) = 0$ разрешимо в радикалах над полем K, если поле разложения L многочлена $p(x)$ является разрешимым расширением поля K, то есть существует башня полей $K = K_0 \subset \cdots \subset K_m$, каждый этаж которой является полем разложения многочлена вида $x^{r_s} - a_s$, и $L \subset K_m$.

Определение 1.2. Цепочка подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$, называется башней подгрупп. Башня подгрупп называется нормальной, если $\forall 1 \leqslant s \leqslant m-1$ группа G_s нормальна в G_{s-1}; абелевой, если она нормальна и $\forall s$ группа G_{s-1}/G_s абелева; циклической, если она нормальна и $\forall s$ группа G_{s-1}/G_s циклическая. Конечная группа G называется разрешимой, если она обладает абелевой башней.

Теорема 1.3. *Уравнение $p(x) = 0$ разрешимо в радикалах $\iff$ группа Галуа многочлена $p(x)$ разрешима.*

Теорема будет доказана в конце лекции, пока же займемся подготовкой.

Часть 2. Разрешимые группы

Примеры 2.1.

1. Всякая абелева группа разрешима.
2. Группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$ разрешимы.
3. Группы A_n и $\mathfrak{S}_n$ при $n \geqslant 5$ неразрешимы.
4. Группа верхнетреугольных матриц разрешима.

Лемма 2.2. *Всякая подгруппа и всякая факторгруппа разрешимой группы разрешима.*

Доказательство: пусть $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ — абелева башня. Если $H \subset G$ — произвольная подгруппа, то $H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_{m-1} \supset H \cap G_m = 1$ — абелева башня. Действительно, группа $H \cap G_s$ является ядром гомоморфизма $H \cap G_{s-1} \to G_{s-1} \to G_{s-1}/G_s$, следовательно нормальна, а факторгруппа $H \cap G_{s-1}/H \cap G_s$ изоморфна образу этого гомоморфизма, следовательно изоморфна подгруппе абелевой группы G_s/G_{s-1} и, значит, сама абелева. Аналогично, если H — факторгруппа группы G и $f : G \to H$ — естественный эпиморфизм, то $H = f(G_0) \supset f(G_1) \supset \cdots \supset f(G_{m-1}) \supset f(G_m) = 1$ — абелева башня. Действительно, если $g_s \in G_s$, $g_{s-1} \in G_{s-1}$, то $f(g_s)f(g_{s-1})f(g_s)^{-1} = f(g_s g_{s-1} g_s^{-1}) \in f(G_{s-1})$, поэтому $f(G_{s-1})$ нормальна в $f(G_s)$. Кроме того, гомоморфизм $G_s \to f(G_s) \to f(G_s)/f(G_{s-1})$ сюръективен и индуцирует сюръективный гомоморфизм $G_s/G_{s-1} \to f(G_s)/f(G_{s-1})$, следовательно группа $f(G_s)/f(G_{s-1})$ изоморфна факторгруппе абелевой группы G_s/G_{s-1}, и, значит, сама абелева. □

Лемма 2.3. *Группа G разрешима $\iff$ G обладает нормальной башней, в которой все G_{s-1}/G_s разрешимы.*

Доказательство: пусть $G = G_0 \supset \cdots \supset G_m = 1$ — нормальная башня, в которой все группы $H^s := G_{s-1}/G_s$ разрешимы. Выберем абелевы башни $H^s = H_0^s \supset \cdots \supset H_{l_s}^s = 1$. Обозначим через G_t^s прообраз H_t^s относительно гомоморфизма $G_{s-1} \to G_{s-1}/G_s$. Тогда $G = G_0^1 \supset \cdots \supset G_{l_1}^1 = G_0^2 \supset \cdots \supset G_{l_{m-1}}^{m-1} = G_0^m \supset \cdots \supset G_{l_m}^m = 1$ — абелева башня. □

Лемма 2.4. *Конечная группа G разрешима $\iff$ G обладает циклической башней.*

Доказательство: достаточно заметить, что любая конечная абелева группа обладает циклической башней (докажите!), и применив конструкцию из предыдущего доказательства, собрать циклические башни факторов G_{s-1}/G_s в циклическую башню всей группы. □

Часть 3. Циклические расширения

Определение 3.1. Характером группы G со значениями в абелевой группе A называется гомоморфизм групп $G \to A$.

Теорема 3.2 (Артин). *Любое множество несовпадающих характеров группы G со значениями в K^* (мультипликативной группе поля) линейно независимо в векторном пространстве всех отображений из G в K.*

Доказательство: пусть $\chi_1, \dots, \chi_n$ — минимальный линейно зависимый набор характеров. Ясно, что $n > 1$, так как, подставляя $g = 1$ в соотношение $a_1\chi_1(g) = 0$, получаем $a_1 = 0$. Пусть $a_1\chi_1(g) + \dots + a_n\chi_n(g) = 0$ — линейная зависимость. Тогда $a_i \neq 0$ в силу минимальности. Так как $\chi_1 \neq \chi_2$, то найдется $g_1 \in G$, такое что $\chi_1(g_1) \neq \chi_2(g_1)$. Подставляя в линейную зависимость $g_1 g$, получим $a_1\chi_1(g_1)\chi_1(g) + a_2\chi_2(g_1)\chi_2(g) + \dots = 0$. Вычитая исходную зависимость, умноженную на $\chi_1(g_1)$, получаем $a_2(\chi_2(g_1) - \chi_1(g_1))\chi_2(g) + \dots = 0$. Ясно, что $a_2(\chi_2(g_1) - \chi_1(g_1)) \neq 0$ по построению, поэтому мы получили нетривиальную линейную зависимость между характерами $\chi_2, \dots, \chi_n$, что противоречит минимальности исходного набора. □

Теорема 3.3 (Гильберта-90). *Пусть L/K расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, σ — образующая группы $\mathrm{Gal}(L/K)$, и $\beta \in L^*$. Тогда $\mathrm{N}_{L/K}(\beta) := \prod_{k=0}^{n-1} \sigma^k(\beta) = 1 \iff$ найдется $\alpha \in L^*$, т.ч. $\beta = \alpha/\sigma(\alpha)$.*

Доказательство: $\Longleftarrow$) очевидно, докажем $\Longrightarrow$). Автоморфизмы σ^k поля L можно рассматривать как характеры группы L^* со значениями в группе L^*. В силу их линейной независимости найдется $a \in L^*$, такое что $\alpha = \sum_{k=0}^{n-1} b_k\sigma^k(a) \neq 0$, где $b_k = \beta\sigma(\beta)\dots\sigma^{k-1}(\beta)$. Ясно, что $b_{k+1} = \beta\sigma(b_k)$ при $0 \leqslant k \leqslant n-2$. Кроме того, из условия $\mathrm{N}_{L/K}(\beta) = 1$ следует, что $b_0 = \beta\sigma(b_{n-1})$. Поэтому $\alpha = \beta\sigma(\alpha)$ и остается разделить на $\sigma(\alpha)$. □

Следствие 3.4. *Если L/K — расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, и K содержит все корни степени n из 1, то L — поле разложения многочлена $x^n - a$, $a \in K$.*

Доказательство: пусть β — образующая группы $\mu_n(K) \cong \mathbb{Z}/n\mathbb{Z}$, а σ — образующая группы $\mathrm{Gal}(L/K)$. Тогда $\sigma^k(\beta) = \beta$, значит $\mathrm{N}_{L/K}(\beta) = \beta^n = 1$, следовательно, по теореме Гильберта-90 найдется $\alpha \in L^*$, такое что $\alpha = \beta\sigma(\alpha)$. Тогда $\sigma^k(\alpha) = \beta^{-k}\alpha$. Значит $1, \sigma, \dots, \sigma^{n-1}$ — попарно различные автоморфизмы поля $K(\alpha)$ над K, следовательно $[K(\alpha) : K] \geqslant [K(\alpha) : K]_s \geqslant n = [L : K]$, значит $K(\alpha) = L$. С другой стороны, $\sigma^k(\alpha^n) = \beta^{-kn}\alpha^n = \alpha^n$, значит $\alpha^n \in L^{\mathrm{Gal}(L/K)} = K$, то есть $\alpha^n - a = 0$, $a \in K$. □

Часть 4. Доказательство основной теоремы

Лемма 4.1. *Группа Галуа многочлена $x^r - 1$ абелева.*

Доказательство: заметим, что группа $\mu_r(\overline{K})$ — циклическая группа, а ее порядок равен r, следовательно $\mu_r(\overline{K}) \cong \mathbb{Z}/r\mathbb{Z}$. Пусть ζ — образующая группы $\mu_r(\overline{K})$. Тогда поле разложения многочлена $x^r - 1$ равно полю $K(\zeta)$. Если $\sigma \in \mathrm{Gal}(K(\zeta)/K)$, то $\sigma(\zeta) = \zeta^{k_\sigma}$, $k_\sigma \in \mathbb{Z}/r\mathbb{Z}$. Далее, легко видеть, что $k_{\tau\sigma} = k_\tau \cdot k_\sigma$ в кольце $\mathbb{Z}/r\mathbb{Z}$. Следовательно, $\sigma \mapsto k_\sigma$ — гомоморфизм группы $\mathrm{Gal}(K(\zeta)/K)$ в $(\mathbb{Z}/r\mathbb{Z})^*$, причем очевидно инъективный. Остается заметить, что группа $(\mathbb{Z}/r\mathbb{Z})^*$ абелева. □

Лемма 4.2. *Если поле K содержит все корни степени r из 1, то группа Галуа многочлена $x^r - a$ изоморфна $\mu_r(K) \cong \mathbb{Z}/r\mathbb{Z}$.*

Доказательство: если α — корень $x^r - a$, то всякий другой корень имеет вид $\alpha\zeta$, $\zeta \in \mu_r(K)$. Значит поле разложения многочлена $x^r - a$ равно полю $K(\alpha)$. Если $\sigma \in \mathrm{Gal}(K(\alpha)/K)$, то $\sigma(\alpha) = \alpha\zeta_\sigma$, $\zeta_\sigma \in \mu_r(K)$. Далее, легко видеть, что $\zeta_{\tau\sigma} = \zeta_\tau \cdot \zeta_\sigma$ в группе $\mu_r(K)$. Следовательно, $\sigma \mapsto \zeta_\sigma$ — гомоморфизм группы $\mathrm{Gal}(K(\alpha)/K)$ в $\mu_r(K)$. Более того, легко видеть, что это изоморфизм. □

Следствие 4.3. *Группа Галуа многочлена $x^r - a$ разрешима.*

Доказательство: пусть L — поле разложения многочлена $x^r - a$, а L' — поле разложения многочлена $x^r - 1$. Ясно, что $K \subset L' \subset L$, значит по теореме Галуа $\mathrm{Gal}(L/K) \supset \mathrm{Gal}(L/L')$ и $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L') \cong \mathrm{Gal}(L'/K)$. Остается заметить, что группа $\mathrm{Gal}(L'/K)$ абелева по лемме 4.1, а группа $\mathrm{Gal}(L/L')$ абелева по лемме 4.2. □

Следствие 4.4. *Если уравнение разрешимо в радикалах, то его группа Галуа разрешима.*

Доказательство: пусть $K = K_0 \subset \cdots \subset K_m$ — башня полей из определения 1.1. Пусть $G_s = \mathrm{Gal}(K_m/K_s)$. По теореме Галуа башня $G_0 \supset \cdots \supset G_m$ нормальна, а $G_{s-1}/G_s \cong \mathrm{Gal}(K_s/K_{s-1})$, то есть разрешима по следствию 4.3. Значит группа G_0 разрешима по лемме 2.3. Наконец, по теореме Галуа группа $\mathrm{Gal}(L/K)$ является факторгруппой группы G_0, и в силу леммы 2.2 тоже разрешима. □

Тем самым одно из утверждений теоремы доказано.

Лемма 4.5. *Пусть K_1/K расширение полей и $p(x) \in K[x]$. Если L — поле разложения многочлена $p(x)$ над полем K, а L_1 — поле разложения многочлена $p(x)$ над полем K_1, то группа $\mathrm{Gal}(L_1/K_1)$ изоморфна подгруппе группы $\mathrm{Gal}(L/K)$.*

Доказательство: если $\sigma \in \mathrm{Gal}(L_1/K_1)$, то $\sigma(L) \subset L$, так как L/K нормально, следовательно $\sigma_{|L} \in \mathrm{Gal}(L/K)$. Отображение $\sigma \mapsto \sigma_{|L}$ является гоморфизмом групп $\mathrm{Gal}(L_1/K_1) \to \mathrm{Gal}(L/K)$, ядро которого есть группа всех автоморфизмов поля L_1, неподвижных на L и K_1 одновременно. Если $\alpha_1, \ldots, \alpha_n$ — корни $p(x)$, то $L = K(\alpha_1, \ldots, \alpha_n)$ и $L_1 = K_1(\alpha_1, \ldots, \alpha_n)$, поэтому автоморфизм неподвижный на K_1 и L равен Id_{L_1}. □

Теперь можно завершить доказательство теоремы 1.3. Пусть $p(x) \in K[x]$ многочлен с разрешимой группой Галуа G и L — его поле разложения над K, $[L : K] = n$. Обозначим через K_1 поле, полученное присоединением к полю K всех корней степени n из 1. Расширение $K = K_0 \subset K_1$ будет первым этажом нашей башни. Пусть далее L_1 — поле разложения многочлена $p(x)$ над K_1. По лемме 4.5 группа $\mathrm{Gal}(L_1/K_1)$ изоморфна подгруппе группы G, следовательно по лемме 2.2 разрешима. Выберем ее циклическую башню: $\mathrm{Gal}(L_1/K_1) = G_1 \supset \cdots \supset G_m = 1$. Пусть $K_s = L_1^{G_s}$ — неподвижное поле. Получаем башню $K_1 \subset \cdots \subset K_m = L_1$. По теореме Галуа каждый этаж этой башни является расширением Галуа, причем $\mathrm{Gal}(K_s/K_{s-1}) \cong \mathbb{Z}/r_s\mathbb{Z}$, а $r_s | (G_1 : 1) | (G : 1) = n$, следовательно поле K_{s-1} содержит все корни степени r_s из 1. Значит, согласно следствию 3.4 поле K_s является полем разложения многочлена $x^{r_s} - a_s$ над полем K_{s-1}. Если вспомнить, что поле K_1 является полем разложения многочлена $x^n - 1$ над полем K_0, и $L \subset L_1 = K_m$, то построенная башня полей доказывает разрешимость в радикалах уравнения $p(x) = 0$. □

Часть 5. Случай положительной характеристики

Теорема 1.3 выполняется также и для полей положительной характеристики, если немного изменить определение поля, разрешимого в радикалах. А именно, если $\mathrm{char}\, K = p$, то в башне полей, устанавливающей разрешимость в радикалах поля L, следует также разрешить этажи, в которых K_s является полем разложения многочлена $x^p - x - a_s$, $a_s \in K_{s-1}$ (расширение Артина-Шрайера).

В этом случае, полезной оказывается также аддитивная версия Теоремы Гильберта-90, а именно

Теорема 5.1 (Гильберта-90). *Пусть L/K расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, σ — образующая группы $\mathrm{Gal}(L/K)$, и $\beta \in L^*$. Тогда $\mathrm{Tr}_{L/K}(\beta) := \sum_{k=0}^{n-1} \sigma^k(\beta) = 0 \iff$ найдется $\alpha \in L^*$, т.ч. $\beta = \alpha - \sigma(\alpha)$.*

Доказательство: $\Longleftarrow$) очевидно, докажем $\Longrightarrow$). Автоморфизмы σ^k поля L можно рассматривать как характеры группы L^* со значениями в группе L^*. В силу их линейной независимости найдется $a \in L^*$, такое что $\mathrm{Tr}_{L/K}(a) = \sum_{k=0}^{n-1} \sigma^k(a) \neq 0$. Положим $\alpha = \Big(\sum_{k=0}^{n-1} b_k \sigma^k(a)\Big) / \mathrm{Tr}_{L/K}(a)$, где $b_k = \beta + \sigma(\beta) + \cdots + \sigma^{k-1}(\beta)$. Ясно, что $b_{k+1} = \beta + \sigma(b_k)$ при $0 \leqslant k \leqslant n-2$. Кроме того, из условия на $\mathrm{Tr}_{L/K}(\beta) = 0$ следует, что $b_0 = \beta + \sigma(b_{n-1})$. Поэтому $\alpha = \beta + \sigma(\alpha)$, и остается вычесть $\sigma(\alpha)$. □

Следствие 5.2. *Если $\mathrm{char}\, K = p$ и L/K — расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$, то L — поле разложения многочлена $x^p - x - a$, $a \in K$.*

Доказательство: пусть $\beta = -1$, а σ — образующая группы $\mathrm{Gal}(L/K)$. Тогда $\sigma^k(\beta) = \beta$, следовательно $\mathrm{Tr}_{L/K}(\beta) = \sum_{k=0}^{p-1} \sigma^k(\beta) = p\beta = 0$, следовательно, по теореме Гильберта-90 найдется $\alpha \in L^*$, такое что $\alpha = \sigma(\alpha) - 1$. Тогда $\sigma^k(\alpha) = \alpha + k$. Значит $1, \sigma, \ldots, \sigma^{n-1}$ — попарно различные автоморфизмы поля $K(\alpha)$ над K, следовательно $[K(\alpha) : K] \geqslant [K(\alpha) : K]_s \geqslant p = [L : K]$, значит $K(\alpha) = L$. С другой стороны, $\sigma^k(\alpha^p - \alpha) = (\alpha + k)^p - (\alpha + k) = \alpha^p - \alpha$, значит $\alpha^p - \alpha \in L^{\mathrm{Gal}(L/K)} = K$, то есть $\alpha^p - \alpha - a = 0$, $a \in K$. □

Лекция 2. Категории и функторы

Часть 1. Категории

Определение 1.1. Категория $\mathcal{C}$ — это следующие данные: 1) класс объектов $\mathrm{Ob}(\mathcal{C})$; 2) для каждой пары объектов $X, Y \in \mathrm{Ob}(\mathcal{C})$ — множество морфизмов $\mathrm{Hom}_{\mathcal{C}}(X, Y)$; и 3) закон композиции, то есть отображение $\circ : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$, $(g, f) \mapsto g \circ f$, такие что выполняются свойства:

К1 Ассоциативность: для любой четверки объектов $X, Y, Z, W \in \mathrm{Ob}(\mathcal{C})$ и любой тройки морфизмов морфизмов $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, $h \in \mathrm{Hom}_{\mathcal{C}}(Z, W)$ имеем $(h \circ g) \circ f = h \circ (g \circ f)$.

К2 Тождественный морфизм: для любого объекта $X \in \mathrm{Ob}(\mathcal{C})$ существует морфизм $\mathrm{Id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$, т.ч. для любого $Y \in \mathrm{Ob}(\mathcal{C})$ и морфизмов $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ имеем $f \circ \mathrm{Id}_X = f$, $\mathrm{Id}_X \circ g = g$.

Примеры 1.2.

1. Категория множеств $\mathcal{S}ets$: объекты — множества, морфизмы — отображения.
2. Категория групп $\mathcal{G}r$: объекты — группы, морфизмы — гомоморфизмы групп.
3. Категория G-множеств $\mathcal{S}ets^G$: объекты — G-множества, морфизмы — G-морфизмы.
4. Категория абелевых групп $\mathcal{A}b$: объекты — абелевы группы, морфизмы — гомоморфизмы групп.
5. Категории колец $\mathcal{R}ings$, коммутативных колец $\mathcal{C}omm$, полей $\mathcal{F}ields$, и т.д.
6. Категории левых A-модулей A-Mod и правых A-модулей Mod-A.
7. Категория K-векторных пространств Vect_K.
8. Всякий моноид (группу) можно рассматривать как категорию с одним объектом.
9. Категория $\mathcal{T}op$ ($\mathcal{T}op_*$) топологических пространств (с отмеченной точкой).

Морфизм $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ называется изоморфизмом, если существует $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$, такой что $f \circ g = \mathrm{Id}_Y$, $g \circ f = \mathrm{Id}_X$. Морфизм в себя называется эндоморфизмом, множество эндоморфизмов объекта X обозначается $\mathrm{End}_{\mathcal{C}}(X)$. Эндоморфизм, являющийся изоморфизмом, называется автоморфизмом. Множество автоморфизмов обозначается $\mathrm{Aut}_{\mathcal{C}}(X)$ и, как легко видеть, является группой.

Удобно объекты категории обозначать точками, а морфизмы — стрелками. Есть несколько стандартных способов «размножать» категории.

Примеры 1.3.

1. Если $\mathcal{C}$ — категория, то противоположная категория $\mathcal{C}^{\mathrm{op}}$ определяется следующим образом: $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$. Иначе говоря, «обращаются» все стрелки.
2. Пусть $\mathcal{C}$ — категория, а Q — колчан, то есть множество точек (вершин) I, и множество стрелок $A \ni \alpha : t(\alpha) \to h(\alpha)$. Категория $\mathcal{C}^Q$ представлений колчана Q в категории $\mathcal{C}$, определяется так:

$$\begin{aligned} \mathrm{Ob}(\mathcal{C}^Q) &= \{\, M_\bullet = (M_i \in \mathrm{Ob}(\mathcal{C}),\ i \in I,\ m_\alpha \in \mathrm{Hom}_{\mathcal{C}}(M_{t(\alpha)}, M_{h(\alpha)}),\ \alpha \in A) \,\} \\ \mathrm{Hom}_{\mathcal{C}^Q}(M_\bullet, N_\bullet) &= \{\, f_\bullet = (f_i \in \mathrm{Hom}_{\mathcal{C}}(M_i, N_i))_{i \in I} \mid \forall \alpha \in A\ n_\alpha \circ f_{t(\alpha)} = f_{h(\alpha)} \circ m_\alpha \,\}. \end{aligned}$$

3. Пусть $\mathcal{C}$ — категория, а G — группа. Определим $\mathcal{C}^G$ — категорию G-объектов в категории $\mathcal{C}$ — так:

$$\begin{aligned} \mathrm{Ob}(\mathcal{C}^G) &= \{\, (X, a) \mid X \in \mathrm{Ob}(\mathcal{C}),\ a \in \mathrm{Hom}_{\mathcal{G}r}(G, \mathrm{Aut}_{\mathcal{C}}(X)) \,\}, \\ \mathrm{Hom}_{\mathcal{C}^G}((X, a), (Y, b)) &= \{\, f \in \mathrm{Hom}_{\mathcal{C}}(X, Y) \mid \forall g \in G\ b(g) \circ f = f \circ a(g) \,\}. \end{aligned}$$

4. Пусть $\mathcal{C}_1$, $\mathcal{C}_2$ — категории. Определим категорию $\mathcal{C}_1 \times \mathcal{C}_2$ так:
$\mathrm{Ob}(\mathcal{C}_1 \times \mathcal{C}_2) = \{\, M = (M_1, M_2) \mid M_i \in \mathcal{C}_i \,\}$, $\mathrm{Hom}_{\mathcal{C}_1 \times \mathcal{C}_2}(M, N) = \{\, (f_1, f_2) \mid f_i \in \mathrm{Hom}_{\mathcal{C}_i}(M_i, N_i) \,\}$.

Замечание 1.4. Ясно, что $(\mathcal{C}^{\mathrm{op}})^{\mathrm{op}} = \mathcal{C}$.

Категория $\mathcal{C}'$ называется подкатегорией категории $\mathcal{C}$, если $\mathrm{Ob}(\mathcal{C}') \subset \mathrm{Ob}(\mathcal{C})$, $\mathrm{Hom}_{\mathcal{C}'}(X, Y) \subset \mathrm{Hom}_{\mathcal{C}}(X, Y)$ для всех $X, Y \in \mathcal{C}'$, и тождественный морфизм и композиция морфизмов в категории $\mathcal{C}'$ совпадает с тождественным морфизмом и композицией морфизмов в категории $\mathcal{C}$. Подкатегория $\mathcal{C}'$ называется полной, если $\mathrm{Hom}_{\mathcal{C}'}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$ для всех $X, Y \in \mathcal{C}'$. Со всяким множеством объектов категории $\mathcal{C}$ можно связать полную подкатегорию, ими образуемую.

Пример 1.5. $\mathcal{A}b \subset \mathcal{G}r$, $\mathcal{F}ields \subset \mathcal{C}omm \subset \mathcal{R}ings$ — полные подкатегории.

Часть 2. Универсальные объекты

Объект X в категории $\mathcal{C}$ называется универсальным притягивающим, если $\mathrm{Hom}_{\mathcal{C}}(Y, X)$ состоит ровно из одного элемента для всех $Y \in \mathcal{C}$. Аналогично, объект X в категории $\mathcal{C}$ называется универсальным притягивающим, если $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ состоит ровно из одного элемента для всех $Y \in \mathcal{C}$.

Примеры 2.1. 1. Точка является универсальным притягивающим, а пустое множество — универсальным отталкивающим объектом в категории $\mathcal{S}ets$.

2. $\{\,1\,\}$ является универсальным притягивающим и отталкивающим объектом в категории $\mathcal{G}r$.

3. $\{\,0\,\}$ является универсальным притягивающим и отталкивающим объектом в категории Vect_K.

4. $\mathbb{Z}$ — универсальный отталкивающий объект в категории $\mathcal{R}ings$.

5. Простое поле — универсальный отталкивающий объект в категории $\mathcal{F}ields_p$ полей характеристики p.

Следствие 2.2. *Если универсальный объект в категории $\mathcal{C}$ существует, то он определен однозначно с точностью до единственного изоморфизма.*

Доказательство: Если X и X' — универсальные отталкивающие объекты, то $\mathrm{Hom}(X, X')$ и $\mathrm{Hom}(X', X)$ состоят ровно из одного элемента, скажем f и f'. Кроме того, $\mathrm{Hom}(X, X)$ и $\mathrm{Hom}(X', X')$ тоже состоят ровно из одного элемента, значит $f' \circ f = \mathrm{Id}_X$ и $f \circ f' = \mathrm{Id}_{X'}$. □

Тем самым, если некий объект определяется «универсальным» свойством, то он однозначно определен, если существует.

Примеры 2.3. 1. Произведение. Пусть $X, Y \in \mathcal{C}$. Рассмотрим категорию троек (Z, f, g), где $Z \in \mathcal{C}$, $f : Z \to X$, $g : Z \to Y$, в которой морфизмы $(Z', f', g') \to (Z, f, g)$ — это морфизмы $\phi : Z' \to Z$, такие что $f' = f \circ \phi$, $g' = g \circ \phi$. Универсальный притягивающий объект в этой категории называется произведением $X \times Y$.

2. Копроизведение. Пусть $X, Y \in \mathcal{C}$. Рассмотрим категорию троек (Z, f, g), где $Z \in \mathcal{C}$, $f : X \to Z$, $g : Y \to Z$, в которой морфизмы $(Z, f, g) \to (Z', f', g')$ — это морфизмы $\phi : Z \to Z'$, такие что $f' = \phi \circ f$, $g' = \phi \circ g$. Универсальный отталкивающий объект в этой категории называется копроизведением $X \sqcup Y$.

3. Свободная группа. Пусть $S \in \mathcal{S}ets$. Рассмотрим категорию пар (G, f), где $G \in \mathcal{G}r$, $f \in \mathrm{Hom}_{\mathcal{S}ets}(S, G)$, в которой морфизмы $(G, f) \to (G', f')$ — это морфизмы $\phi \in \mathrm{Hom}_{\mathcal{G}r}(G, G')$, такие что $f' = \phi \circ f$. Универсальный отталкивающий объект в этой категории называется свободной группой, порожденной множеством S. Заменяя в определении свободной группы категорию $\mathcal{G}r$ на категорию $\mathcal{A}b$, $\mathcal{R}ings$, $\mathcal{C}omm$, A-Mod, ..., получаем определение свободной абелевой группы, свободного кольца, свободного коммутативного кольца, свободного A-модуля,....

Еще раз подчеркнем, что всякий раз когда мы определяем объект с помощью универсального свойства, возникает вопрос о его существовании. И этот вопрос не всегда имеет положительный ответ! Тут нужна осторожность. В качестве иллюстрации докажем:

Теорема 2.4. *Свободные группы существуют.*

Доказательство: для каждого элемента $s \in S$ введем «буквы» a_s и b_s. Пусть $\widetilde{F}$ — моноид всех «слов», состоящих из этих букв, с операцией $\tilde{\circ}$ «приписывания» слов. Обозначим через 1 — «пустое» слово, тогда 1 — единица. Пусть $\sim$ — минимальное отношение эквивалентности на моноиде $\widetilde{F}$, содержащее все «элементарные» эквивалентности $a_s b_s \sim b_s a_s \sim 1$, и замкнутое относительно приписывания, то есть такое что $w_1 \sim w_2 \Longrightarrow w\tilde{\circ}w_1 \sim w\tilde{\circ}w_2$ и $w_1\tilde{\circ}w \sim w_2\tilde{\circ}w$. Пусть $F = \widetilde{F}/\sim$ — множество классов эквивалентности. Тогда операция $\tilde{\circ}$ индуцирует операцию $\circ$ на F. Ясно, что $\circ$ — ассоциативна, так как $\tilde{\circ}$ — ассоциативна. Кроме того, ясно что 1 является единицей в F. Легко видеть, что всякий элемент в F имеет обратный (если элемент представлен словом w, то надо заменить каждую букву a_s на b_s, b_s на a_s, и обратить порядок). Таким образом, F — группа. Далее, сопоставляя всякому элементу $s \in S$ слово a_s, получаем отображение $f : S \to F$. Если же $g : S \to G$ — другое отображение, то строим сначала гомоморфизм моноидов $\tilde{\phi} : \widetilde{F} \to G$, полагая $\tilde{\phi}(a_s) = g(s)$, $\tilde{\phi}(b_s) = g(s)^{-1}$, а затем замечаем, что $\tilde{\phi}$ постоянен на классах эквивалентности, следовательно индуцирует отображение $\phi : F \to G$, которое является гомоморфизмом групп. □

Замечание 2.5. Моноид $\widetilde{F}$ — это свободный моноид, порожденный множеством S.

Часть 3. Функторы

Определение 3.1. Ковариантный функтор $F : \mathcal{C} \to \mathcal{C}'$ — это следующие данные: 1) отображение на объектах $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}')$; 2) для каждой пары объектов $X, Y \in \mathrm{Ob}(\mathcal{C})$ отображение на морфизмах $F : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X),F(Y))$, такие что выполняются свойства:

Ф1 : для любого объекта $X \in \mathrm{Ob}(\mathcal{C})$ имеем $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$.

Ф2 : для всякой пары морфизмов $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)$ имеем $F(g \circ f) = F(g) \circ F(f)$.

Аналогично, контравариантный функтор $F : \mathcal{C} \to \mathcal{C}'$ — это следующие данные: 1) отображение на объектах $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}')$; 2) для каждой пары объектов $X, Y \in \mathrm{Ob}(\mathcal{C})$ отображение на морфизмах $F : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(Y),F(X))$ (меняющее направление стрелок), такие что выполняются свойства:

Ф1′ : для любого объекта $X \in \mathrm{Ob}(\mathcal{C})$ имеем $F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}$.

Ф2′ : для всякой пары морфизмов $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y,Z)$ имеем $F(g \circ f) = F(f) \circ F(g)$.

Ясно, что функторы можно компонировать, и что композиция функторов является функтором.

Примеры 3.2. 1. Тождественный функтор $\mathrm{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$.

2. Функтор $\mathrm{Hom} : \mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathcal{S}ets$.

3. Функторы вложения $\mathcal{A}b \to \mathcal{G}r$, $\mathcal{F}ields \to \mathcal{C}omm \to \mathcal{R}ings$.

4. «Забывающие» функторы $\mathcal{G}r, \mathcal{A}b, \mathcal{R}ings, \mathcal{C}omm, \mathcal{F}ields \to \mathcal{S}ets$; A-Mod,Mod-$A \to \mathcal{A}b$; $\mathcal{C}^G \to \mathcal{C}$.

5. Функторы ограничения: $\mathcal{C}^Q \to \mathcal{C}^{Q'}$, $\mathcal{C}^G \to \mathcal{C}^{G'}$, где $Q' \subset Q$ — подколчан, а $G' \subset G$ — подгруппа.

6. Функторы проекции $\mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{C}_1$, $\mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{C}_2$.

7. Фундаментальная группа $\pi_1 : \mathcal{T}op_* \to \mathcal{G}r$, и первые гомологии $H_1 : \mathcal{T}op \to \mathcal{A}b$.

Это все примеры ковариантных функторов. Примером контравариантного функтора является «тождественный» функтор из категории $\mathcal{C}$ в категорию $\mathcal{C}^{\mathrm{op}}$.

Лемма 3.3. *Сопоставляя всякому ковариантному функтору $\mathcal{C}^{\mathrm{op}} \to \mathcal{C}'$ его композицию с «тождественным» функтором $\mathcal{C} \to \mathcal{C}^{\mathrm{op}}$, получаем биекцию между ковариантными функторами $\mathcal{C}^{\mathrm{op}} \to \mathcal{C}'$ и контравариантными функторами $\mathcal{C} \to \mathcal{C}'$.*

Функтор называется строгим (соотв. полным), если он инъективен (соотв. сюръективен) на морфизмах.

Определение 3.4. Пусть $F, G : \mathcal{C} \to \mathcal{C}'$ — ковариантные функторы. Морфизм функторов $\phi : F \to G$ — это набор морфизмов $\phi_X \in \mathrm{Hom}_{\mathcal{C}'}(F(X),G(X))$, такой что для любого морфизма $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ имеем $\phi_Y \circ F(f) = G(f) \circ \phi_X$. Аналогично, определяется морфизм контравариантных функторов.

Примеры 3.5. 1. Тождественный морфизм $\mathrm{Id}_F : F \to F$.

2. Естественное отображение $\pi_1(X, x) \to H_1(X, \mathbb{Z})$ является морфизмом функторов из π_1 в композицию функторов $\mathcal{T}op_* \to \mathcal{T}op \to \mathcal{A}b \to \mathcal{G}r$ (забывание отмеченной точки, вычисление гомологий, вложение).

3. Пусть $\mathrm{Ob}(\mathcal{C}) = \{\, (G, N) \mid G \in \mathcal{G}r,\ N \lhd G \,\}$, $\mathrm{Hom}_{\mathcal{C}}((G, N), (G', N')) = \{\, f \in \mathrm{Hom}_{\mathcal{G}r}(G, G') \mid f(N) \subset N' \,\}$. Тогда $(G, N) \mapsto G/N$ — функтор «факторизации» $\mathcal{C} \to \mathcal{G}r$, а канонический морфизм $G \to G/N$ является морфизм функторов из забывающего функтора $(G, N) \to G$ в функтор факторизации.

Вообще, то что мы называли каноническими морфизмами — это в действительности морфизмы функторов.

Ясно, что морфизмы функторов можно компонировать. Соответственно, морфизм функторов $\phi : F \to G$ называется изоморфизмом функторов, если найдется $\psi : G \to F$, такой что $\phi \circ \psi = \mathrm{Id}_G$, $\psi \circ \phi = \mathrm{Id}_F$.

Определение 3.6. Функтор $F : \mathcal{C} \to \mathcal{C}'$ называется эквивалентностью, если найдется функтор $G : \mathcal{C}' \to \mathcal{C}$, такой что $F \circ G \cong \mathrm{Id}_{\mathcal{C}'} : \mathcal{C}' \to \mathcal{C}'$ и $G \circ F \cong \mathrm{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ (изоморфизмы функторов). Категории $\mathcal{C}$ и $\mathcal{C}'$ называются в этом случае эквивалентными.

Примеры 3.7. 1. Тождественный функтор является эквивалентностью.

2. Биекция между левыми и правыми действиями группы — это эквивалентность $\mathcal{S}ets^G \to \mathcal{S}ets^{G^{\mathrm{op}}}$.

3. Аналогично для колец имеем эквивалентности A-Mod $\to$ Mod-A^{op}, Mod-$A \to A^{\mathrm{op}}$-Mod.

4. Пусть L/K — расширение Галуа. Тогда сопоставления $F \to \mathrm{Gal}(L/F)$, $H \to L^H$ задают контравариантную эквивалентность категории всех промежуточных полей $K \subset F \subset L$ (морфизмы — вложения), и категории всех подгрупп $H \subset \mathrm{Gal}(L/K)$ (морфизмы — вложения).

Лекция 3. Тензоры и двойственность

Часть 1. Двойственность

Пусть V — векторное пространство над полем K.

Определение 1.1. Векторное пространство $\mathrm{Hom}(V, K)$ линейных функций $V \to K$ называется двойственным к V и обозначается V^*. Его элементы называются функционалами на V.

Пусть $f : U \to V$ — линейное отображение векторных пространств. Сопоставляя функционалу $\xi \in V^*$ функционал $\xi \circ f \in U^*$ (то есть $(\xi \circ f)(u) = \xi(f(u))$) получаем отображение $V^* \to U^*$, которое обозначается f^* (или f^T) и называется двойственным (или сопряженным) к f.

Лемма 1.2. *Отображение $V \mapsto V^*$, $f \mapsto f^*$ является контравариантным функтором $\mathrm{Vect}_K \to \mathrm{Vect}_K$.*

Доказательство: во-первых, ясно, что f^* — линейно: $f^*(\xi+\lambda\xi') = (\xi+\lambda\xi')\circ f = \xi\circ f+\lambda\xi'\circ f = f^*(\xi)+\lambda f^*(\xi')$. Далее, легко видеть, что если $f = \mathrm{Id}_V$, то $f^*(\xi) = \xi \circ f = \xi \circ \mathrm{Id}_V = \xi$, поэтому $f^* = \mathrm{Id}_{V^*}$. Наконец, $(g \circ f)^*(\xi) = \xi \circ (g \circ f) = (\xi \circ g) \circ f = g^*(\xi) \circ f = f^*(g^*(\xi)) = (f^* \circ g^*)(\xi)$. □

Лемма 1.3. *Двойственность — аддитивный функтор, то есть существуют канонические (функториальные) изоморфизмы $(V_1 \oplus V_2)^* \cong V_1^* \oplus V_2^*$.*

Доказательство: если $\xi \in (V_1 \oplus V_2)^*$, то $\xi_{|V_1} \in V_1^*$ и $\xi_{|V_2} \in V_2^*$. Рассмотрим отображение $(V_1 \oplus V_2)^* \to V_1^* \oplus V_2^*$, $\xi \mapsto (\xi_{|V_1}, \xi_{|V_2})$. Легко видеть, что оно инъективно, сюръективно и функториально. □

Зафиксируем $v \in V$ и рассмотрим $f(v)$ как функцию от $f \in V^*$. Ясно, что она линейная по f. Тем самым, каждому вектору $v \in V$ мы сопоставили функционал на пространстве V^*, то есть построили отображение $\phi = \phi_V : V \to V^{**}$. Имеем по определению $(\phi_V(v))(\xi) = \xi(v)$, следовательно ϕ_V — линейное отображение.

Лемма 1.4. *Набор отображений ϕ_V является инъективным морфизмом функторов $\mathrm{Id} \to **$.*

Доказательство: мы должны проверить, что $f^{**} \circ \phi_U = \phi_V \circ f$ для любого линейного отображения $f : U \to V$. Действительно, возьмем произвольный $u \in U$ и $\xi \in V^*$. Тогда

$$((\phi_V \circ f)(u))(\xi) = (\phi_V(f(u)))(\xi) = \xi(f(u)) \qquad \text{и}$$

$$((f^{**} \circ \phi_U)(u))(\xi) = (f^{**}(\phi_U(u)))(\xi) = (\phi_U(u) \circ f^*)(\xi) = \phi_U(u)(f^*(\xi)) = \phi_U(u)(\xi \circ f) = (\xi \circ f)(u) = \xi(f(u)).$$

Остается заметить, что если $\phi_V(v) = 0$, то $0 = (\phi_V(v))(\xi) = \xi(v)$ для любого $\xi \in V^*$, значит $v = 0$. □

Выберем базис $\{ e_i \}$ в векторном пространстве V и определим функционал $\xi^i \in V^*$ формулой $\xi^i(e_j) = \delta^i_j$.

Лемма 1.5. *Функционалы ξ^i линейно независимы, а если V конечномерно, то ξ^i образуют базис в V^*.*

Доказательство: если $\sum \lambda_i \xi^i = 0$, то $0 = (\sum \lambda_i \xi^i)(e_j) = \lambda_j$ при всех j. Если $\dim V < \infty$, то для произвольных $\xi \in V^*$ и $v = \sum x^j e_j$ имеем $\xi(v) = \xi(\sum x^j e_j) = \sum \xi(e_j) x^j = \sum \xi(e_j) \xi^j(v)$, значит $\xi = \sum \xi(e_j) \xi^j$. Конечномерность здесь нужна для того, чтобы в разложении ξ по ξ^j получилось конечное число слагаемых. □

Базис $\{ \xi^i \}$ пространства V^* называется двойственным по отношению к базису $\{ e_i \}$ в пространстве V.

Следствие 1.6. *Если $\dim V < \infty$, то $V^* \cong V$ (не канонически).*

Следствие 1.7. *Если $\dim V < \infty$, то морфизм $\phi_V : V \to V^{**}$ является изоморфизмом (каноническим).*

Доказательство: ϕ_V инъективно, поэтому остается заметить, что $\dim V^{**} = \dim V^* = \dim V$. □

Замечание 1.8. Конечномерность очень существенна: если, например, V — счетномерно, то базис в V^* уже континуальный, поэтому ни V^*, ни, тем более, V^{**} не изоморфны V.

Следствие 1.9. *Двойственность является контравариантной аддитивной автоэквивалентностью категории Vect_K^{fd} конечномерных векторных пространств над полем K.*

Часть 2. Тензорное произведение

Пусть U, V и W — векторные пространства над полем K. Отображение $f : U \times V \to W$ называется K-билинейным, если $f(u+\lambda u', v) = f(u,v) + \lambda f(u',v)$, $f(u, v+\lambda v') = f(u,v) + \lambda f(u,v')$ для всех $\lambda \in K$.

Определение 2.1. Тензорным произведением K-векторных пространств U и V называется универсальный отталкивающий объект в категории K-билинейных отображений $U \times V \to W$.

Теорема 2.2. *Тензорное произведение существует.*

Доказательство: построим тензорное произведение явно. Пусть M — векторное пространство с базисом, состоящим из всех пар (u, v), $u \in U$, $v \in V$. Пусть N — подпространство в M, порожденное всеми элементами вида $(u+\lambda u', v) - (u,v) - \lambda(u',v)$, $(u, v+\lambda v') - (u,v) - \lambda(u,v')$. Рассмотрим отображение $f_0 : U \times V \to M/N$ — композицию естественного вложения $U \times V \to M$ и канонической проекции $M \to M/N$. Отображение f_0 билинейно по построению N. Докажем, что оно является универсальным отталкивающим объектом. Пусть $f : U \times V \to W$ — произвольное билинейное отображение. Зададим отображение $\tilde\phi : M \to W$ на базисных векторах формулой $\tilde\phi(u,v) = f(u,v)$. Тогда $\tilde\phi(N) = 0$ в силу билинейности f. Поэтому $\tilde\phi$ пропускается через M/N, то есть индуцирует морфизм $\phi : M/N \to W$. Ясно, что $\phi \circ f_0 = f$, и что морфизм ϕ — единственный удовлетворяет такому свойству (так как M/N порождается образом $U \times V$ относительно f_0). □

Тензорное произведение пространств U и V обозначается $U \otimes V$. Его элементы называются тензорами. Образы элементов $(u,v) \in U \times V$ относительно канонического морфизма $U \times V \to U \otimes V$ обозначаются $u \otimes v$ и называются разложимыми тензорами. Ясно, что всякий элемент в $U \otimes V$ представляется как линейная комбинация разложимых тензоров. Более того, в силу билинейности отображения $U \times V \to U \otimes V$ имеем $(u+\lambda u') \otimes v = u \otimes v + \lambda u' \otimes v$, $u \otimes (v + \lambda v') = u \otimes v + \lambda u \otimes v'$.

Лемма 2.3. *Если $\{u_i\}$ — базис в U, а $\{v_j\}$ — базис в V, то $\{u_i \otimes v_j\}$ — базис в $U \otimes V$.*

Доказательство: во-первых, если $u = \sum x^i u_i$, $v = \sum y^j v_j$, то $u \otimes v = (\sum x^i u_i) \otimes (\sum y^j v_j) = \sum x^i y^j u_i \otimes v_j$, значит все разложимые (а значит и вообще все) тензоры представимы в виде линейной комбинации тензоров $u_i \otimes v_j$. Остается проверить их линейную независимость. Предположим, что $\sum a^{ij} u_i \otimes v_j = 0$. Рассмотрим отображение $f^{pq} : U \times V \to K$, заданное формулой $f^{pq}(\sum x^i u_i, \sum y^j v_j) = x^p y^q$. Легко видеть, что f^{pq} билинейно, значит пропускается через морфизм $\phi^{pq} : U \otimes V \to K$. Ясно, что $\phi^{pq}(u_i \otimes v_j) = f^{pq}(u_i, v_j) = \delta_i^p \delta_j^q$, поэтому $a^{pq} = \phi^{pq}(\sum a^{ij} u_i \otimes v_j) = 0$. □

Следствие 2.4. $\dim(U \otimes V) = (\dim U)(\dim V)$.

Пусть $f : U \to U'$ и $g : V \to V'$ — линейные отображения. Легко видеть, что отображение $U \times V \to U' \otimes V'$, $(u,v) \mapsto f(u) \otimes f(v)$ — билинейно, следовательно пропускается через отображение $f \otimes g : U \otimes V \to U' \otimes V'$, причем $(f \otimes g)(u \otimes v) = f(u) \otimes g(v)$.

Лемма 2.5. *Тензорное произведения является аддитивным бифунктором, то есть существуют канонические изоморфизмы $(U_1 \oplus U_2) \otimes V \cong (U_1 \otimes V) \oplus (U_2 \otimes V)$, и $U \otimes (V_1 \oplus V_2) \cong (U \otimes V_1) \oplus (U \otimes V_2)$.*

Доказательство: функториальность очевидна, проверим аддитивность. Легко видеть, что отображение $(U_1 \oplus U_2) \times V \to (U_1 \otimes V) \oplus (U_2 \otimes V)$, $((u_1 \oplus u_2), v) \mapsto (u_1 \otimes v) \oplus (u_2 \otimes v)$ — билинейно, следовательно пропускается через отображение $(U_1 \oplus U_2) \otimes V \to (U_1 \otimes V) \oplus (U_2 \otimes V)$, которое очевидно является изоморфизмом. □

Часть 3. Тензоры и двойственность

Лемма 3.1. *Если U — конечномерно, то $\mathrm{Hom}(U,V) \cong U^* \otimes V$.*

Доказательство: для всяких $\xi \in U^*$, $v \in V$ отображение $U \to V$, $u \mapsto \xi(u)v$ — линейно. Обозначим его через $\xi \otimes v$. Легко видеть, что отображение $U^* \times V \to \mathrm{Hom}(U,V)$, $(\xi, v) \mapsto \xi \otimes v$ — билинейно, следовательно пропускается через отображение $U^* \otimes V \to \mathrm{Hom}(U,V)$. Выберем базисы $\{u_i\}$ и $\{v_j\}$ в U и V. Если U конечномерно, то рассмотрим также и двойственный базис $\{\xi^i\}$ в U^*. Тогда $\{\xi^i \otimes v_j\}$ — базис в $U^* \otimes V$. Ясно, что $\sum a_i^j \xi^i \otimes v_j$ переходит в отображение $f : U \to V$, такое что $f(u_i) = a_i^j v_j$. Поэтому $f = 0$ влечет $a_i^j = 0$ при всех i, j, что доказывает инъективность. Пусть теперь $f : U \to V$ — произвольное линейное отображение. Положим $f(e_i) = a_i^j v_j$. Ясно, что лишь конечное число a_i^j отлично от нуля, поэтому $f = \sum a_i^j \xi^i \otimes v_j$, что доказывает сюръективность. □

Теорема 3.2. *Имеем канонический изоморфизм* $\mathrm{Hom}(U, \mathrm{Hom}(V, W)) \cong \mathrm{Hom}(U \otimes V, W)$.

Доказательство: всякому линейному отображению $f : U \to \mathrm{Hom}(V, W)$ сопоставим отображение $U \times V \to W$, $(u, v) \mapsto f(u)(v)$. Оно очевидно билинейно, и, следовательно, пропускается через линейное отображение $\bar{f} : U \otimes V \to W$, причем $\bar{f}(u \otimes v) = f(u)(v)$. Ясно, что отображение $f \mapsto \bar{f}$ линейно. Обратно, если $g : U \otimes V \to W$ — линейное отображение. Тогда для всякого $u \in U$ отображение $g_u(v) = g(u \otimes v)$ является линейным отображением $V \to W$. Сопоставляя всякому $u \in U$ отображение $g_u \in \mathrm{Hom}(V, W)$, получаем отображение $\hat{g} : U \to \mathrm{Hom}(V, W)$, которое очевидно линейно. Наконец, легко видеть, что отображения $f \mapsto \bar{f}$ и $g \mapsto \hat{g}$ являются взаимно обратными и функториальными. □

Часть 4. Двойственность и тензорное произведение над кольцом

Пусть теперь A — произвольное кольцо, а U, V, W, ... — A-модули. Определим двойственный модуль V^* как $\mathrm{Hom}_A(V, A)$. Если V — левый A-модуль, то V^* — правый A-модуль (структура A-модуля на V^* задается правилом $(\xi a)(v) = \xi(v)a$), а если V — правый A-модуль, то V^* — левый A-модуль ($(a\xi)(v) := a\xi(v)$).

Аналогично случаю векторных пространств определяется сопряженный гомоморфизм f^*. При этом легко видеть, что он является гомоморфизмом A-модулей.

Лемма 4.1. *Двойственность является аддитивным контравариантным функтором* A-Mod $\to$ Mod-A *и* Mod-$A \to A$-Mod.

Доказательство: аналогично доказательству лемм 1.2 и 1.3. □

Аналогично случаю векторных пространств определяется и морфизм функторов $\phi : \mathrm{Id} \to **$ (см. 1.4), однако он уже не является инъективным — пример приводится в упражнениях. Утверждение леммы 1.5 точно так же доказывается для свободных A-модулей конечного ранга, но для произвольных A-модулей оно уже неверно. А следствие 1.6 для некоммутативных колец вообще не имеет смысла.

Что касается следствия 1.7, то тут ситуация такая. A-модуль V называется рефлексивным, если канонический морфизм $V \to V^{**}$ является изоморфизмом. Легко видно, что свободный A-модуль конечного ранга рефлексивен, но обратное, вообще говоря, неверно. Соответственно, следствие 1.9 тоже неверно, однако ему можно придать иной смысл, так что оно станет верным, но это уже область применения гомологической алгебры, которую мы оставим в стороне.

Пусть теперь кольцо A — коммутативно. Тензорным произведением A-модулей U и V называется универсальный отталкивающий объект в категории A-билинейных отображений $U \times V \to W$. Тензорное произведение A-модулей U и V обозначается $U \otimes_A V$. Существование тензорного произведения, а также его функториальность и аддитивность доказываются также, как и для векторных пространств. Более того, если A-модули U и V свободны, то аналогично лемме 2.3 доказывается, что $U \otimes_A V$ свободен, а его ранг равен произведению рангов модулей U и V. Наконец, тем же способом доказывается, что теорема 3.2 выполняется для любых A-модулей над коммутативным кольцом A, а лемма 3.1 — только если U — свободный A-модуль.

Часто полезной оказывается следующая лемма (докажите ее!).

Лемма 4.2. *Пусть* A *— подкольцо в коммутативном кольце* B*, а* U *и* V *— произвольные* B*-модули. Тогда* $U \otimes_B V \cong U \otimes_A V / \langle ub \otimes v - u \otimes bv \rangle_{u \in U, v \in V, b \in B}$ *где* $\langle \dots \rangle$ *— обозначает* A*-подмодуль, порожденный всеми элементами указанного вида.*

Замечание 4.3. Если кольцо B — некоммутативно, то можно определить тензорное произведение правого B-модуля U на левый B-модуль V с помощью формулы из предыдущей леммы (взяв $A = \mathbb{Z}$). Однако, такое произведение уже не будет B-модулем, а будет лишь абелевой группой. Тем не менее, лемма 3.1 по прежнему выполняется, если U и V — левые B-модули, причем U — свободен.

Лекция 4. Билинейные формы

Часть 1. Билинейные формы

Пусть U и V — векторные пространства над полем K.

Определение 1.1. Билинейная форма на $U \times V$ — это K-билинейное отображение $g : U \times V \to K$, то есть отображение, удовлетворяющее условиям $g(u + \lambda u', v) = g(u, v) + \lambda g(u', v)$, $g(u, v + \lambda v') = g(u, v) + \lambda g(u, v')$ для всех $\lambda \in K$.

Примеры 1.2.
1. $\langle x, y \rangle = \sum x_i y_i$ — билинейная форма на $K^n \times K^n$.
2. Отображение вычисления $\mathrm{ev} : V^* \times V \to K$, $\mathrm{ev}(\xi, v) = \xi(v)$ — билинейная форма.
3. Отображение $(A, B) \mapsto \mathrm{Tr}(AB)$ — билинейная форма $\mathrm{Mat}_{n,m}(K) \times \mathrm{Mat}_{m,n}(K) \to K$.
4. $(f, g) \mapsto \int_0^1 f(x)g(x)dx$ — билинейная форма $\mathbb{R}[x] \times \mathbb{R}[x] \to \mathbb{R}$.
5. $\omega(x, y) = \sum_{i=1}^{n} (x_{2i}y_{2i+1} - x_{2i+1}y_{2i})$ — билинейная форма $K^{2n} \times K^{2n} \to K$.

Согласно результатам предыдущей лекции, всякая билинейная форма представляется линейным отображением $U \otimes V \to K$, то есть элементом пространства $(U \otimes V)^*$.

Пусть $\{ u_i \}$ — базис в U, а $\{ v_j \}$ — базис в V. Матрица $G = (g_{ij})$, $g_{ij} := g(u_i, v_j)$ называется матрицей Грама билинейной формы g относительно базисов $\{ u_i \}$ и $\{ v_j \}$. Ясно, что всякая билинейная форма однозначно определяется своей матрицей Грама: $g(X, Y) = g(\sum x_i u_i, \sum y_j v_j) = \sum g(u_i, v_j)x_i y_j = \sum g_{ij} x_i y_j = X^T G Y$.

Лемма 1.3. *Пусть $\{ u'_i \}$ и $\{ v'_j \}$ — новые базисы с матрицами перехода A и B соответственно. Тогда матрица Грама формы g в новых базисах равна $G' = A^T G B$.*

Доказательство: $g(u'_i, v'_j) = g(\sum a_{pi} u_p, \sum b_{qj} v_q) = \sum a_{pi} g_{pq} b_{qj}$. □

Лемма 1.4. *Имеем изоморфизмы* $\mathrm{Hom}(U \otimes V, K) \cong \mathrm{Hom}(U, V^*) \cong \mathrm{Hom}(V, U^*)$.

Доказательство: сопоставим форме $g : U \times V \to K$ отображения $g_L : V \to U^*$ и $g_R : U \to V^*$, заданные формулами $(g_L(v))(u) = g(u, v)$, $(g_R(u))(v) = g(u, v)$. Эти же формулы показывают, как по отображениям восстановить билинейную форму. □

Будем называть отображения $g_L : V \to U^*$ и $g_R : U \to V^*$, соответствующие билинейной форме g, левой и правой частичными дуализациями формы g. Ясно, что матрица Грама формы g совпадает с матрицей левой дуализации $g_L : V \to U^*$, записанной относительно базиса $\{ v_i \}$ в V и двойственного базиса $\{ u^i \}$ в U^* (если $\dim U < \infty$), и транспонирована по отношению к матрице правой дуализации $g_R : U \to V^*$, записанной относительно базиса $\{ u_i \}$ в V и двойственного базиса $\{ v^i \}$ в V^* (если $\dim V < \infty$).

Определение 1.5. Левым ядром формы $g : U \otimes V \to K$ называется ${}^\perp V := \{ u \in U \mid \forall v \in V \ g(u, v) = 0 \}$. Аналогично, правым ядром формы g называется $U^\perp := \{ v \in V \mid \forall u \in U \ g(u, v) = 0 \}$. Форма g называется невырожденной, если ${}^\perp V = U^\perp = 0$.

Лемма 1.6. *Имеем* ${}^\perp V = \mathrm{Ker}\, g_R$, $U^\perp = \mathrm{Ker}\, g_L$.

Следствие 1.7. *Если $g : U \otimes V \to K$ — невырожденная форма, и одно из пространств U, V конечномерно, то $\dim U = \dim V$ и частичные дуализации формы g задают изоморфизмы $U \cong V^*$, $V \cong U^*$.*

Докзательство: пусть, например, $\dim U < \infty$. Так как $U^\perp = 0$, то $g_L : V \to U^*$ — вложение, значит $\dim V \leqslant \dim U^* = \dim U$. В частности, $\dim V < \infty$. Аналогично, из ${}^\perp V = 0$ следует, что $g_R : U \to V^*$ — вложение, значит $\dim U \leqslant \dim V^* = \dim V$. Таким образом, $\dim U = \dim V < \infty$, и частичные дуализации, будучи вложениями пространств одинаковой конечной размерности, обязаны являться изоморфизмами. □

Следствие 1.8. *Если* $\dim U, \dim V < \infty$, *то форма* g *невырождена* $\iff$ *матрица Грама формы* g *невырождена.*

Замечание 1.9. Конечномерность существенна: в примере 1.2.4 форма невырождена, однако, можно показать, что $\dim(\mathbb{R}[x])^* > \dim \mathbb{R}[x]$.

Лемма 1.10. *Всякая форма* $g : U \otimes V \to K$ *индуцирует невырожденную форму* $\bar{g} : (U/{}^\perp V) \otimes (V/U^\perp) \to K$.

Доказательство: ясно, что $g(u, v)$ не изменится, если к u прибавить любой элемент из ${}^\perp V$, а к v — любой элемент из $U^\perp$. Значит, форма g индуцирует форму $\bar{g}$. Если $\bar{u} \in U/{}^\perp V$ — элемент в левом ядре формы $\bar{g}$, то $\bar{g}(\bar{u}, \bar{v}) = 0$ для всех $\bar{v} \in V/U^\perp$, значит $g(u, v) = 0$ для всех $v \in V$, значит $u \in {}^\perp V$ и $\bar{u} = 0$, то есть левое ядро равно нулю. Аналогично доказывается тривиальность правого ядра формы $\bar{g}$. □

Определение 1.11. Пусть $g : U \otimes V \to K$ — билинейная форма, а $U_1 \subset U$, $V_1 \subset V$ — подпространства. Левым ортогоналом подпространства V_1 относительно формы g называется ${}^\perp V_1 := \{u \in U \,|\, \forall v \in V_1 \; g(u, v) = 0\}$. Аналогично, правым ортогоналом подпространства U_1 называется $U_1^\perp := \{\, v \in V \mid \forall u \in U_1 \; g(u, v) = 0 \,\}$.

Лемма 1.12. *Если* $\dim U = \dim V = n$, *то* $\dim U_1^\perp \geqslant n - \dim U_1$, $\dim {}^\perp V_1 \geqslant n - \dim V_1$. *Если же* g *невырождена, то неравенства становятся равенствами.*

Доказательство: рассмотрим индуцированную форму $U_1 \otimes V \to K$. Ясно, что ее левое ядро равно $U_1 \cap {}^\perp V$, а правое равно как раз $U_1^\perp \subset V$. Поэтому индуцированная форма $(U_1/(U_1 \cap {}^\perp V)) \otimes (V/U_1^\perp) \to K$ невырождена и $\dim U_1^\perp = \dim V - \dim(V/U_1^\perp) = n - \dim(U_1/(U_1 \cap {}^\perp V)) \geqslant n - \dim U_1$. □

Лемма 1.13. *Если форма* g *невырождена,* $\dim U = \dim V < \infty$, *то* ${}^\perp(U_1^\perp) = U_1$, $({}^\perp V_1)^\perp = V_1$.

Доказательство: ясно, что $U_1 \subset {}^\perp(U_1^\perp)$. Кроме того, $\dim({}^\perp(U_1^\perp)) = n - \dim U_1^\perp = n - (n - \dim U_1) = \dim U_1$. □

Пусть V — векторное пространство, а $V_1 \subset V$ — подпространство. Аннулятором пространства V_1 называется ${}^\perp V_1$ ортогонал к V_1 относительно билинейной формы $\mathrm{ev} : V^* \otimes V \to K$. Аналогично определятся аннулятор подпространства $U_1 \subset V^*$. Из предыдущих утверждений следует, что если V конечномерно, то аннулятор аннулятора совпадает с исходным подпространством.

Часть 2. Симметрические и знакопеременные формы

Билинейные формы $V \otimes V \to K$ называются также билинейными формами на пространстве V. Ясно, что для представления такой формы матрицей достаточно выбрать один базис в V, а при замене базиса матрица Грама формы меняется по правилу $G \mapsto A^T G A$, где A — матрица перехода.

Лемма 2.1. *Если* $\dim V < \infty$, *а* $V_1 \subset V$ *— подпространство, т.ч.* $g_{|V_1}$ *невырожденна, то* $V = V_1 \oplus V_1^\perp$.

Доказательство: во-первых, легко видеть что пространство $V_1 \cap V_1^\perp$ является правым ядром формы $g_{|V_1}$, поэтому $V_1 \cap V_1^\perp = 0$, а во-вторых, $\dim V_1^\perp \geqslant \dim V - \dim V_1$ по лемме 1.12. □

Определение 2.2. Билинейная форма на пространстве V называется симметрической, если $\forall v, v' \in V$ имеем $g(v, v') = g(v', v)$, и знакопеременной, если $\forall v \in V$ имеем $g(v, v) = 0$.

Замечание 2.3. Из знакопеременности следует кососимметричность $g(v, v') = -g(v', v)$ $\forall v, v' \in V$: действительно $0 = g(v + v', v + v') - g(v, v) - g(v', v') = g(v, v') + g(v', v)$. Если же $\mathrm{char}\, K \neq 2$, то условия знакопеременности и кососимметричности эквивалентны: $g(v, v) = -g(v, v)$, значит $g(v, v) = 0$.

Лемма 2.4. *Пусть* G *— матрица Грама формы* g *относительно некоторого базиса. Тогда*
(i) g *— симметрическая* $\iff G^T = G$; (ii) g *— кососимметрическая* $\iff G^T = -G$; (iii) g *— знакопеременная* $\iff G^T = -G$, *и* G *имеет нули на диагонали* (*второе условие нужно только при* $\mathrm{char}\, K = 2$).

Доказательство: (i) и (ii) $g(Y, X) = Y^T G X = (Y^T G X)^T = X^T G^T Y$, $g(X, Y) = X^T G Y$.
(iii) $\Longrightarrow$) имеем $0 = g(v_i, v_i) = g_{ii}$, и $0 = g(v_i + v_j, v_i + v_j) - g(v_i, v_i) - g(v_j, v_j) = g(v_i, v_j) + g(v_j, v_i) = g_{ij} + g_{ji}$.
$\Longleftarrow$) $g(\sum x_i v_i, \sum x_i v_i) = \sum x_i^2 g_{i,i} + \sum_{i<j} x_i x_j (g_{ij} + g_{ji})$. □

Следствие 2.5. *Если* $\mathrm{char}\, K \neq 2$, *то всякая билинейная форма над* K *однозначно раскладывается в сумму симметрической и знакопеременной формы.*

Докзательство: положим $g_+(v,v') = \frac{1}{2}(g(v,v') + g(v',v))$, $g_-(v,v') = \frac{1}{2}(g(v,v') - g(v',v))$. □

Очень удобным свойством симметрических и знакопеременных форм является

Лемма 2.6. *Если форма g симметрична или знакопеременна и $V_1 \subset V$, то $V_1^\perp = {}^\perp V_1$.*

Теорема 2.7. *Если $\operatorname{char} K \neq 2$, то всякая симметрическая форма над K приводится к диагональному виду.*

Доказательство: если $g(v,v) = 0$ для всех $v \in V$, то g знакопеременна, значит $g = 0$ и матрица Грама формы g диагональна. Если найдется $v \in V$, такой что $g(v,v) \neq 0$, то $V = Kv \perp v^\perp$ — ортогональная прямая сумма. Выбирая базис в $v^\perp$, в котором $g_{|v^\perp}$ диагональна, и дополняя его вектором v, получаем искомый базис. □

Теорема 2.8. *Всякая знакопеременная форма приводится к блочно-диагональному виду с блоками вида $I_2 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ и (0) на диагонали.*

Доказательство: если $g = 0$, то любой базис годится. Иначе, найдем пару векторов $v_1, v_2 \in V$, так что $g(v_1, v_2) = 1$. Ясно, что v_1 и v_2 линейно независимы. Пусть $V_{12} = Kv_1 \oplus Kv_2$. Ясно, что $g_{|V_{12}}$ имеет в базисе $\{v_1, v_2\}$ матрицу Грама I_2. В частности, $g_{|V_{12}}$ невырождена, поэтому $V = V_{12} \perp V_{12}^\perp$ — ортогональная прямая сумма. Выбирая базис в $V_{12}^\perp$, в котором $g_{|V_{12}^\perp}$ имеет искомый вид, и дополняя его векторами v_1, v_2, получаем искомый базис. □

Следствие 2.9. *Если g — невырожденная знакопеременная форма на пространстве V, то $\dim V$ — четна.*

Часть 3. Антилинейность, полуторалинейность и эрмитовость

Определение 3.1. Отображение $f : V \to W$ векторных пространств над полем $\mathbb{C}$ называется антилинейным, если f — $\mathbb{R}$-линейно и $f(zv) = \bar{z}f(v)$. Форма $g : U \times V \to \mathbb{C}$ называется полуторалинейной, если она $\mathbb{C}$-линейна по первому аргументу, и антилинейна по второму.

Замечание 3.2. Пусть V — векторное пространство над полем $\mathbb{C}$. Рассмотрим на V ту же структуру абелевой группы с новым действием поля $\mathbb{C}$: $zv := \bar{z}v$. Тем самым, получаем новое векторное пространство над полем $\mathbb{C}$, которое обозначается $\bar{V}$ и называется комплексно-сопряженным к V. Ясно, что антилинейное отображение $V \to W$ — то же самое, что линейное отображение $\bar{V} \to W$, а полуторалинейная форма $U \times V \to \mathbb{C}$ — то же самое, что билинейная форма $U \times \bar{V} \to \mathbb{C}$.

Ясно, что результаты первой части лекции с очевидными изменениями переносятся на случай полуторалинейных форм. Отметим только, что если G — матрица Грама формы g, то $g(X,Y) = X^T G \bar{Y}$, при замене базиса матрица Грама полуторалинейной формы меняется по правилу $G \mapsto A^T G \bar{B}$, а частичные дуализации формы g являются антилинейными отображениями $U \to V^*$ и $V \to U^*$.

Определение 3.3. Полуторалинейная форма h на пространстве V называется эрмитовой, если $\forall v, v' \in V$ имеем $h(v,v') = \overline{h(v',v)}$ и косоэрмитовой, если $\forall v, v' \in V$ имеем $h(v,v') = -\overline{h(v',v)}$.

Лемма 3.4. *Пусть H — матрица Грама формы h относительно некоторого базиса. Тогда (i) h — эрмитова $\iff H^T = \bar{H}$; (ii) h — косоэрмитова $\iff H^T = -\bar{H}$.*

Доказательство: $\overline{h(Y,X)} = \bar{Y}^T \bar{H} X = (\bar{Y}^T \bar{H} X)^T = X^T \bar{H}^T \bar{Y}$. □

Следствие 3.5. *Форма h — косоэрмитова $\iff ih$ — эрмитова.*

Лемма 3.6. *Всякая эрмитова (косоэрмитова) форма над K приводится к диагональному виду.*

Доказательство: пусть h — эрмитова. Если $h(v,v) = 0$ для всех $v \in V$, то для всех $u, v \in V$ и $z \in \mathbb{C}$ имеем

$$2\operatorname{Re}(zh(u,v)) = h(u, \bar{z}v) + h(\bar{z}v, u) = h(u + \bar{z}v, u + \bar{z}v) - h(u,u) - h(v,v) = 0,$$

значит $h = 0$ и матрица Грама формы h диагональна. Если найдется $v \in V$, такой что $h(v,v) \neq 0$, то $V = Kv \perp v^\perp$ — ортогональная прямая сумма. Выбирая базис в $v^\perp$, в котором $h_{|v^\perp}$ диагональна, и дополняя его вектором v, получаем искомый базис. □

Замечание 3.7. Легко видеть, что теория эрмитовых форм дословно переносится на случай произвольного расширения полей L/K степени 2 с $\operatorname{char} K \neq 2$ (в роли комплексного сопряжения выступает единственный нетривиальный автоморфизм L над K).

Лекция 5. Евклидова геометрия

Часть 1. Сигнатура

Пусть K — подполе поля $\mathbb{R}$ (например, $K = \mathbb{Q}$ или $K = \mathbb{R}$), V — n-мерное векторное пространство над полем K, а g — симметрическая билинейная форма на V. Выберем базис, в котором матрица Грама формы g диагональна (такой базис называется ортогональным), и обозначим через r_+, r_- и r_0 количество положительных, отрицательных и нулевых чисел на диагонали, так что $r_+ + r_- + r_0 = n$.

Теорема 1.1. *Числа r_+, r_- и r_0 не зависят от выбора ортогонального базиса.*

Доказательство: пусть $\{ e_i \}$ и $\{ f_i \}$ — ортогональные базисы, и обозначим $g(e_i, e_i) = a_i$, $g(f_i, f_i) = b_i$. Пусть, далее $a_1, \dots, a_{r_+} > 0 > a_{r_+ + 1}, \dots, a_{r_+ + r_-}$, $a_{r_+ + r_- + 1} = \dots = a_n = 0$; $b_1, \dots, b_{s_+} > 0 > b_{s_+ + 1}, \dots, b_{s_+ + s_-}$, $b_{s_+ + s_- + 1} = \dots = b_n = 0$; Покажем, что векторы $e_1, \dots, e_{r_+}, f_{s_+ + 1}, \dots, f_n$ линейно независимы. Действительно, если $x_1 e_1 + \dots x_{r_+} e_{r_+} = y_{s_+ + 1} f_{s_+ + 1} + \dots + y_n f_n$, то применяя к обеим частям равенства форму g получаем $x_1^2 a_1 + \dots + x_{r_+}^2 a_{r_+} = y_{s_+ + 1}^2 b_{s_+ + 1} + \dots + y_n^2 b_n$. Легко видеть, что правая часть неположительна, а левая — положительна всегда, за исключением случая $x_1 = \dots = x_{r_+} = 0$. Но тогда и $y_{s_+ + 1} = \dots = y_n = 0$, так как векторы $f_{s_+ + 1}, \dots, f_n$ линейно независимы. Из линейной независимости векторов $e_1, \dots, e_{r_+}, f_{s_+ + 1}, \dots, f_n$ следует неравенство $r_+ + (n - s_+) \leqslant n$, то есть $r_+ \leqslant s_+$. Аналогично доказывается $s_+ \leqslant r_+$. Значит $r_+ = s_+$. Аналогичные рассуждения показывают, что $r_- = s_-$. Наконец, $r_0 = n - r_+ - r_- = n - s_+ - s_- = s_0$. □

Тройка чисел (r_+, r_-, r_0) называется сигнатурой формы g. В случае, если форма g невырождена, имеем $r_0 = 0$ и сигнатурой называют пару чисел (r_+, r_-).

Лемма 1.2. *Для всякой билинейной симметрической формы g над полем $\mathbb{R}$ найдется базис, такой что матрица Грама формы g в этом базисе имеет вид* $\operatorname{diag}(1, \dots, 1, -1, \dots, -1, 0, \dots, 0)$.

Доказательство: выберем ортогональный базис $\{ e_i \}$ и заменим его на $e'_i = e_i / \sqrt{|g(e_i, e_i)|}$. □

Следствие 1.3. *Билинейные симметрические формы g и g' над полем $\mathbb{R}$ изоморфны тогда и только тогда, когда совпадают их сигнатуры.*

Часть 2. Положительно определенные формы

Определение 2.1. Билинейная симметрическая форма g называется положительно определенной, если $r_- = r_0 = 0$, и отрицательно определенной, если $r_+ = r_0 = 0$.

Лемма 2.2. *Форма g на V положительно* (отрицательно) определена $\Leftrightarrow g(v, v) > 0$ $(g(v, v) < 0)$ $\forall 0 \neq v \in V$.

Доказательство: выберем ортогональный базис $\{ e_i \}$. Если g положительно определена, то $\forall 0 \neq v = \sum x_i e_i$ имеем $g(v, v) = \sum x_i^2 g(e_i, e_i) > 0$, а если $g(v, v) > 0$ для всех $0 \neq v \in V$, то в частности $g(e_i, e_i) > 0$, значит g положительно определена. □

Следствие 2.3. *Если форма g положительно* (отрицательно) определена на V, то g положительно (отрицательно) определена и на любом его подпространстве.

Пусть теперь форма g положительно определена на V.

Следствие 2.4. *Форма $g_{|U}$ невырождена для любого $U \subset V$. В частности, $V = U \oplus U^\perp$ для любого $U \subset V$.*

Следствие 2.5. *Для любого подпространства $U \subset V$ и вектора $v \in V$ существуют единственное разложение $v = v' + v''$, такое что $v' \perp U$, $v'' \in U$.*

Вектор v'' называется ортогональной проекцией вектора v на подпространство U.

Лемма 2.6. *Если $u_1, \dots, u_k$ — ортогональный базис в U, и $v \in V$, то ортогональная проекция v на U равна $\sum_{i=1}^{k}[(v \cdot u_i)/(u_i \cdot u_i)]u_i$.*

Доказательство: предположим, что $v - \sum a_i u_i \perp U$. Тогда $0 = (v - \sum a_i u_i) \cdot u_j = v \cdot u_j - a_j u_j \cdot u_j$, откуда $a_j = (v \cdot u_j)/(u_j \cdot u_j)$. □

Теорема 2.7. *Пусть $e_1, \dots, e_n$ — базис в V. Определим векторы $e'_1, \dots, e'_n$ индуктивной формулой: $e'_k = e_k - \sum_{i=1}^{k-1}[(e_k \cdot e'_i)/(e'_i \cdot e'_i)]e'_i$. Тогда $e'_1, \dots, e'_n$ — ортогональный базис.*

Доказательство: достаточно проверить, что $\forall 1 \leqslant k \leqslant n$ векторы $e'_1, \dots, e'_k$ — линейно независимы, $e'_1, \dots, e'_k$ попарно ортогональны, и $\langle e'_1, \dots, e'_k\rangle = \langle e_1, \dots, e_k\rangle$. При $k = 1$ все очевидно. Пусть $k > 1$. Если $e'_1, \dots, e'_k$ линейно зависимы, то $e'_1, \dots, e'_{k-1}, e_k$ — тоже линейно зависимы. Но так как $e'_1, \dots, e'_{k-1}$ — линейно независимы, то это означает, что $e_k \in \langle e'_1, \dots, e'_{k-1}\rangle = \langle e_1, \dots, e_{k-1}\rangle$, что противоречит линейной независимости векторов $e_1, \dots, e_k$. Далее, из леммы 2.6 следует, что $e'_k \cdot e'_i = 0$ при $1 \leqslant i \leqslant k-1$, значит $e'_1, \dots, e'_k$ — попарно ортогональны. Наконец, $\langle e'_1, \dots, e'_k\rangle = \langle\langle e'_1, \dots, e'_{k-1}\rangle, e_k - \sum a_i e'_i\rangle = \langle\langle e_1, \dots, e_{k-1}\rangle, e_k\rangle = \langle e_1, \dots, e_k\rangle$. □

Описанный в теореме процесс называется ортогонализацией Грама–Шмидта.

Часть 3. Расстояния, углы, объем

Евклидовым пространством называется $\mathbb{R}$-векторное пространство V с положительно определенной формой g на нем. Будем для краткости обозначать $g(u, v)$ через (u, v) или даже $u \cdot v$ и называть скалярным произведением. Определим модуль или длину вектора v формулой $|v| := \sqrt{v^2}$. Заметим, что $|v| = 0 \iff v = 0$.

Всякое евклидово пространство обладает базисом, в котором матрица Грама единична (в частности, евклидовы пространства одинаковой размерности изоморфны). Такой базис называется ортонормированным. В ортонормированном базисе имеем $X \cdot Y = \sum x_i y_i$, $|X| = \sqrt{\sum x_i^2}$.

Лемма 3.1 (Неравенство Шварца). $|v \cdot w| \leqslant |v||w|$, *причем* $|v \cdot w| = |v||w| \iff v$ *и* w *коллинеарны.*

Доказательство: если $|v| = 0$ или $|w| = 0$, то неравенство очевидно. Предположим, что $|v|, |w| \neq 0$ и положим $v' = \frac{1}{|v|}v$, $w' = \frac{1}{|w|}w$, так что $|v'| = |w'| = 1$ и $v' \cdot w' = \frac{1}{|v||w|}v \cdot w$. Заметим, что $\forall t \in K$ имеем $0 \leqslant (v' + tw')^2 = v' \cdot v' + 2tv' \cdot w' + t^2 w' \cdot w' = 1 + 2tv' \cdot w' + t^2$, значит дискриминант — неположителен, то есть $(v' \cdot w')^2 \leqslant 1$, то есть $|v' \cdot w'| \leqslant 1$. Домножая на $|v||w|$ получаем искомое неравенство. Далее, если векторы v и w коллинеарны, то очевидно имеем равенство, а если неколлинеарны, то ясно что $(v' + tw')^2 > 0$, поэтому дискриминант отрицателен и получаем строгое неравенство. □

Следствие 3.2 (Неравенство треугольника). $|v + w| \leqslant |v| + |w|$.

Доказательство: пользуясь неравенством треугольника для вещественных чисел и неравенством Шварца, получаем $(|v+w|)^2 = |(v+w)^2| = |v^2 + 2v \cdot w + w^2| \leqslant |v^2| + 2|v \cdot w| + |w^2| \leqslant |v|^2 + 2|v||w| + |w|^2 = (|v| + |w|)^2$. □

Из неравенства треугольника следует, что функция $\rho(v, w) = |v - w|$ является метрикой в пространстве V. Определим угол α между векторами v и w формулой $v \cdot w = |v||w|\cos\alpha$, $0 \leqslant \alpha \leqslant \pi$. Ясно, что α однозначно определен, за исключением случая $|v| = 0$ или $|w| = 0$.

Пусть $e_1, \dots, e_k$ — произвольный набор векторов в евклидовом пространстве. Определителем Грама набора векторов $e_1, \dots, e_k$ называется $\mathrm{G}(e_1, \dots, e_k) = \det(e_i \cdot e_j)_{i,j=1}^{k}$.

Лемма 3.3. *Объем k-мерного параллелепипеда $\{\, v = \sum_{i=1}^{k} t_i e_i \mid 0 \leqslant t_i \leqslant 1 \,\}$ равен $\sqrt{\mathrm{G}(e_1, \dots, e_k)}$.*

Доказательство: при $k = 1$ — очевидно. Пусть $k > 1$. Запишем $e_k = e'_k + e''_k$, где $e'_k \perp e_1, \dots, e_{k-1}$ и $e''_k \in \langle e_1, \dots, e_{k-1}\rangle$. Тогда ясно, что высота параллелепипеда равна $|e'_k|$, а площадь основания — $\sqrt{\mathrm{G}(e_1, \dots, e_{k-1})}$ (по предположению индукции), поэтому объем равен $|e'_k|\sqrt{\mathrm{G}(e_1, \dots, e_{k-1})}$. С другой стороны, имеем $e_k \cdot e_k = e'_k \cdot e'_k + e''_k \cdot e''_k$, и $e_k \cdot e_i = e'_k \cdot e_i + e''_k \cdot e_i = e''_k \cdot e_i$, поэтому $\mathrm{G}(e_1, \dots, e_k) = \mathrm{G}(e_1, \dots, e''_k) + |e'_k|^2\,\mathrm{G}(e_1, \dots, e_{k-1})$ и остается заметить, что первый определитель равен нулю так как векторы линейно зависимы. □

Следствие 3.4. *Если A — матрица перехода от ортонормированного базиса к произвольному базису $e_1, \dots, e_n$, то объем параллелепипеда равен $|\det(A)|$.*

Доказательство: $\mathrm{G}(e_1, \dots, e_n) = \det(A^T A) = \det(A)^2$. □

Часть 4. Ортогональная группа

Пусть V — векторное пространство над полем K с симметрической билинейной формой g. Оператор $A : V \to V$ называется ортогональным относительно формы g, если $g(Av, Av') = g(v, v')$ для всех $v, v' \in V$.

Лемма 4.1. *Пусть G — матрица Грама формы g, A — матрица оператора A в том же базисе. Оператор A ортогонален $\iff A^TGA = G$.*

Доказательство: $g(AX, AY) = (AX)^TG(AY) = X^T(A^TGA)Y$. □

Лемма 4.2. *Если форма g невырождена, а оператор A ортогонален, то A обратим.*

Доказательство: если $Av = 0$, то $g(v, v') = g(Av, Av') = g(0, Av') = 0$, значит v лежит в ядре формы g. □

Обозначим через $\mathrm{O}(V, g; K)$ множество всех обратимых операторов ортогональных относительно формы g.

Лемма 4.3. *Множество $\mathrm{O}(V, g; K)$ — группа.*

Доказательство: если $A, B \in \mathrm{O}(V, g; K)$, то $g((AB)v, (AB)v') = g(A(Bv), A(Bv')) = g(Bv, Bv') = g(v, v')$, $g(\mathrm{Id}_V v, \mathrm{Id}_V v') = g(v, v')$, $g(A^{-1}v, A^{-1}v') = g(A(A^{-1}v), A(A^{-1}v')) = g((AA^{-1})v, (AA^{-1})V') = g(v, v')$. □

Лемма 4.4. *Если формы g и h на пространствах V и W изоморфны, то $\mathrm{O}(V, g; K) \cong \mathrm{O}(W, h; K)$.*

Доказательство: пусть $f : V \to W$ — изоморфизм форм. (то есть изоморфизм пространств, такой что $h(fv, fv') = g(v, v')$ для всех $v, v' \in V$). Сопоставляя оператору $A \in \mathrm{O}(W, h)$ оператор $f^{-1}Af$ получаем гомоморфизм групп $\mathrm{O}(W, h) \to \mathrm{O}(V, g)$, так как $g(f^{-1}Afv, f^{-1}Afv') = h(ff^{-1}Afv, ff^{-1}Afv') = h(Afv, Afv') = h(fv, fv') = g(v, v')$. Обратный гомоморфизм задается формулой $B \mapsto fBf^{-1}$. □

Следствие 4.5. *Класс изоморфизма группы $\mathrm{O}(V, g; \mathbb{C})$ зависит только от ранга формы g, а класс изоморфизма группы $\mathrm{O}(V, g; \mathbb{R})$ зависит только от сигнатуры формы g.*

Группа $\mathrm{O}(V, g; K)$ называется ортогональной группой. Ортогональная группа невырожденной формы g на n-мерном векторном пространстве над полем $\mathbb{C}$ обозначается $\mathrm{O}(n, \mathbb{C})$, а ортогональная группа невырожденной формы g сигнатуры (r_+, r_-) над полем $\mathbb{R}$ обозначается $\mathrm{O}(r_+, r_-; \mathbb{R})$, при этом группа $\mathrm{O}(n, 0; \mathbb{R})$ также обозначается через $\mathrm{O}(n; \mathbb{R})$. Также часто рассматривают специальную ортогональную группу $\mathrm{SO}(n; \mathbb{R})$ ортогональных операторов с определителем 1.

Часть 5. Эрмитовы формы и унитарная группа

Положительная определенность — очень полезное с геометрической (а также, и с алгебраической) точки зрения свойство. Однако, билинейная форма над полем $\mathbb{C}$ не может быть положительно определенной — если $g(v, v) > 0$, то $g(iv, iv) = -g(v, v) < 0$. Тут на выручку приходят эрмитовы формы.

Для эрмитовых форм точно также как и для билинейных над полем $\mathbb{R}$ определяется сигнатура. Эрмитова форма h называется положительно определенной, если $h(v, v) > 0$ для всех $0 \neq v \in V$.

Лемма 5.1. *Если эрмитова форма h положительно определена, то существует базис, в котором матрица Грама формы h — единичная.*

Доказательство аналогично доказательству леммы 1.2. Аналогично, легко убедиться, что для положительно определенной эрмитовой метрики выполняется неравенство Шварца и неравенство треугольника. Таким образом, можно заниматься геометрией и в произвольном положительно определенном эрмитовом пространстве. Наконец, оператор A в комплексном векторном пространстве V с эрмитовой формой h называется унитарным, если $h(Av, Av') = h(v, v')$ для всех $v, v' \in V$. В терминах матриц условие унитарности записывается в виде $\bar{A}^TGA = G$. Легко видеть, что если h невырождена, то всякий унитарный оператор обратим и множество $\mathrm{U}(V, h)$ всех унитарных операторов является группой — унитарной группой. Класс изоморфизма унитарной группы зависит только от класса изоморфизма эрмитовой метрики, то есть от ее сигнатуры. Унитарная группа невырожденной эрмитовой формы h сигнатуры (r_+, r_-) обозначается $\mathrm{U}(r_+, r_-)$, при этом группа $\mathrm{U}(n, 0)$ также обозначается через $\mathrm{U}(n)$. Также часто рассматривают специальную унитарную группу $\mathrm{SU}(n; \mathbb{R})$ унитарных операторов с определителем 1.

Лекция 6. Сопряженность

Часть 1. Формы и операторы

Зафиксируем невырожденную билинейную форму g на конечномерном векторном пространстве V.

Лемма 1.1. *Сопоставляя оператору A форму $B_A(v,v') := g(Av,v')$, получаем изоморфизм между пространством операторов и пространством всех билинейных форм.*

Доказательство: пусть B — билинейная форма. Нам надо построить оператор A, такой что $B = B_A$. Если зафиксировать v, то $B(v,v')$ — линейная функция от v', следовательно $B(v,v') = \xi_v(v')$, где $\xi_v \in V^*$. Так как g невырождена, а V конечномерно, то найдется единственный $\hat{v} \in V$, такой что $g_R(\hat{v}) = \xi_v$, то есть $g(\hat{v},v') = \xi_v(v') = B(v,v')$. Зададим отображение $A : V \to V$ формулой $A(v) = \hat{v}$. По определению имеем равенство $g(A(v),v') = B(v,v')$. Покажем, что A — линейно. Действительно, ясно что $g(A(v_1+\lambda v_2) - A(v_1) - \lambda A(v_2), v') = g(A(v_1+\lambda v_2),v') - g(A(v_1),v') - \lambda g(A(v_2),v') = B(v_1+\lambda v_2,v') - B(v_1,v') - \lambda B(v_2,v') = B((v_1+\lambda v_2)-v_1-\lambda v_2,v') = B(0,v') = 0$, поэтому в силу невырожденности g имеем $A(v_1+\lambda v_2) = A(v_1)+\lambda A(v_2)$. Таким образом, A — оператор и $B = B_A$. Более того, из предыдущей конструкции видно, что оператор A однозначно определяется формой B. □

Следствие 1.2. *Для всякого оператора $A : V \to V$ существует единственный оператор $A^T : V \to V$, такой что $\forall v, v' \in V$ имеем $g(Av,v') = g(v,A^Tv')$.*

Оператор $A^T : V \to V$ называется оператором, сопряженным (справа) к A относительно формы g.

Замечание 1.3. Воспользовавшись определением оператора A^* и дуализации g_L, определение оператора A^T можно переписать в виде $g_L(A^Tv')(v) = g(v,A^Tv') = g(Av,v') = g_L(v')(Av) = A^*(g_L(v'))(v)$, откуда получаем $g_L \circ A^T = A^* \circ g_L$ и $A^T = g_L^{-1} \circ A^* \circ g_L$.

Следствие 1.4. *Если G — матрица Грама формы g, а A — матрица оператора, то матрица сопряженного оператора равна $G^{-1}A^TG$.*

Следствие 1.5. *Сопряжение относительно фиксированной невырожденной билинейной формы является линейным отображением* $\mathrm{End}(V) \to \mathrm{End}(V)$, *причем* $(AB)^T = B^TA^T$.

Лемма 1.6. *Если форма g симметрическая, то $A \in \mathrm{O}(V,g) \iff A^T = A^{-1}$.*

Доказательство: $A \in \mathrm{O}(V,g) \Longrightarrow g(v,v') = g(Av,Av') = g(v,A^TAv') \Longrightarrow A^TA = \mathrm{Id}$. Аналогично, $A^TA = \mathrm{Id}$ $\Longrightarrow g(Av,Av') = g(v,A^TAv') = g(v,v') \Longrightarrow A \in \mathrm{O}(V,g)$. □

Часть 2. Самосопряженные операторы

Пусть теперь форма g симметрична или кососимметрична, и $\mathrm{char}\, K \neq 2$.

Лемма 2.1. *Сопряжение является инволюцией, то есть $A^{TT} = A$.*

Доказательство: $g(A^{TT}v,v') = \pm g(v',A^{TT}v) = \pm g(A^Tv',v) = g(v,A^Tv') = g(Av,v')$. □

Определение 2.2. Оператор A называется самосопряженным относительно формы g, если $A^T = A$, и антисамосопряженным, если $A^T = -A$.

Лемма 2.3. *Всякий оператор единственным образом представляется в виде суммы сопряженного и антисамосопряженного оператора.*

Доказательство: $A = (A+A^T)/2 + (A-A^T)/2$. □

Часть 3. Спектральная теорема (эрмитов случай)

Аналогичные определения можно дать для невырожденной эрмитовой формы. Оператор, сопряженный оператору A относительно эрмитовой формы h, определяется равенством $h(Av, v') = h(v, A^\dagger v')$ и является $\mathbb{C}$-линейным. При этом сопряжение $A \mapsto A^\dagger$ является антилинейной инволюцией. Оператор A называется самосопряженным, если $A^\dagger = A$. Оператор является унитарным $\iff A^\dagger = A^{-1}$.

Замечание 3.1. Самомопряженные операторы относительно симметрической билинейной формы также называются симметрическими, а относительно эрмитовой формы также называются эрмитовыми.

Теорема 3.2. *Пусть $K = \mathbb{C}$, h — положительно определенная эрмитова форма, и A — эрмитов оператор. Тогда существует ортонормированный базис, в котором матрица оператора A диагональна.*

Доказательство: будем доказывать индукцией по размерности. Если $\dim V = 1$, то доказывать нечего. Пусть $\dim V > 1$. Пусть v_1 — собственный вектор оператора A (он существует, так как $\mathbb{C}$ — алгебраически замкнуто). Тогда $V = \mathbb{C}v_1 \perp \mathbb{C}v_1^\perp$, так как h положительно определена. Заметим, что если $v \in v_1^\perp$, то $h(v_1, Av) = h(v_1, A^\dagger v) = h(Av_1, v) = h(\lambda_1 v_1, v) = 0$, следовательно $A(v_1^\perp) \subset v_1^\perp$. Кроме того, ясно что ограничение A на $v_1^\perp$ является эрмитовым оператором относительно ограничения формы h. Значит, по предположению индукции, в $v_1^\perp$ найдется ортонормированный базис, в котором ограничение оператора A представляется диагональной матрицей. Дополняя его вектором $v_1/|v_1|$, получаем искомый ортонормированный базис пространства V. □

Множество собственных значений эрмитова оператора называется спектром.

Лемма 3.3. *Спектр эрмитова оператора — вещественный.*

Доказательство: выберем ортонормированный базис из собственных векторов. Пусть λ — собственное значение, соответствующее вектору v. Тогда $\lambda = h(\lambda v, v) = h(Av, v) = h(v, Av) = h(v, \lambda v) = \bar\lambda$. □

Следствие 3.4. *Пусть h и B — эрмитовы формы на векторном пространстве V, причем h положительно определена. Тогда найдется базис, в котором матрица Грама формы h — единична, а матрица Грама формы B — диагональна с вещественными числами на диагонали.*

Часть 4. Комплексификация и овеществление

Пусть V — векторное пространство над полем $\mathbb{R}$. Комплексификацией V называется $V_\mathbb{C} := V \otimes_\mathbb{R} \mathbb{C}$.

Лемма 4.1. *$V_\mathbb{C}$ является векторным пространством над полем $\mathbb{C}$.*

Доказательство: для всякого $\lambda \in \mathbb{C}$ отображение $V \times \mathbb{C} \to V \otimes_\mathbb{R} \mathbb{C}$, $(v, z) \mapsto v \otimes (\lambda z)$ очевидно $\mathbb{R}$-билинейно, следовательно индуцирует $\mathbb{R}$-линейное отображение $\rho_\lambda : V \otimes_\mathbb{R} \mathbb{C} \to V \otimes_\mathbb{R} \mathbb{C}$, такое что $\rho_\lambda(v \otimes z) = v \otimes (\lambda z)$. Причем, легко видеть, что $\rho_\lambda \circ \rho_\mu = \rho_{\lambda\mu}$ для всех $\lambda, \mu \in \mathbb{C}$. Значит, отображения ρ_λ задают на $V_\mathbb{C}$ структуру векторного пространства над $\mathbb{C}$. □

Лемма 4.2. *Если $\{e_p\}$ — базис V над $\mathbb{R}$, то $\{e_p \otimes 1\}$ — базис $V_\mathbb{C}$ над $\mathbb{C}$, а $\{e_p \otimes 1, e_p \otimes i\}$ — базис $V_\mathbb{C}$ над $\mathbb{R}$.*

Доказательство: вторая часть следует из леммы 2.3 лекции 3, а первая часть — из второй. Действительно, всякий элемент в $V_\mathbb{C}$ можно представить в виде $\sum x_p(e_p \otimes 1) + \sum y_p(e_p \otimes i) = \sum(x_p + y_p i)(e_p \otimes 1)$. □

Следствие 4.3. $\dim_\mathbb{C} V_\mathbb{C} = \dim_\mathbb{R} V$, $\dim_\mathbb{R} V_\mathbb{C} = 2\dim_\mathbb{R} V$.

Определение 4.4. Вещественной структурой на комплексном векторном пространстве W называется антилинейное отображение $B : W \to W$, такое что $B^2 = \mathrm{Id}$.

Легко видеть, что комплексификация всякого линейного пространства обладает канонической вещественной структурой $B(v \otimes z) = v \otimes \bar z$. Покажем, что верно и обратное.

Теорема 4.5. *Пусть W — векторное пространство над полем $\mathbb{C}$ с вещественной структурой B. Пусть $V = W^B = \{\, w \in W \mid Bw = w \,\}$. Тогда V — векторное пространство над полем $\mathbb{R}$, $W \cong V_\mathbb{C}$, а B при этом изоморфизме отождествляется с канонической вещественной структурой на $V_\mathbb{C}$.*

Доказательство: пусть $V' = \{ w \in W \mid Bw = -w \}$. Ясно, что V и V' — $\mathbb{R}$-подпространства в W. Далее, $W \cong V \oplus V'$ (изоморфизм над $\mathbb{R}$), так как $w = (w + Bw)/2 + (w - Bw)/2$. Далее ясно что $w \in V \iff iw \in V'$, так как $Biw = \bar{i}Bw = -iBw$. Наконец, отображение $V \times \mathbb{C} \to W$, $(v, z) \mapsto zv$ очевидно $\mathbb{R}$-билинейно, следовательно индуцирует $\mathbb{R}$-линейное отображение $V_{\mathbb{C}} \to W$. Остается проверить, что это отображение биективно и согласовано с комплексными и вещественными структурами. □

Комплексификация — стандартный способ сводить линейную алгебру над полем $\mathbb{R}$ к линейной алгебре над полем $\mathbb{C}$.

Часть 5. Спектральная теорема (симметрический случай)

Пусть V — векторное пространство над полем $\mathbb{R}$, а g — положительно определенная симметрическая форма.

Лемма 5.1. *Всякий самосопряженный оператор имеет вещественное собственное значение.*

Доказательство: рассмотрим комплексификацию $V_{\mathbb{C}}$ и определим на ней эрмитову форму h и оператор $A_{\mathbb{C}}$ формулами $h(v \otimes z, v' \otimes z') = z\bar{z'}g(v, v')$ и $A_{\mathbb{C}}(v \otimes z) = A(v) \otimes z$ (проверьте корректность!). Тогда форма h положительно определена, а оператор $A_{\mathbb{C}}$ — эрмитов. В самом деле, $h(v \otimes 1 + v' \otimes i, v \otimes 1 + v' \otimes i) = g(v, v) + g(v', v') > 0$ и $h(v \otimes z, A_{\mathbb{C}}(v' \otimes z')) = h(v \otimes z, A(v') \otimes z') = z\bar{z'}g(v, A(v')) = z\bar{z'}g(A(v), v') = h(A(v) \otimes z, v' \otimes z') = h(A_{\mathbb{C}}(v \otimes z), v' \otimes z')$. Значит, по лемме 3.3 оператор $A_{\mathbb{C}}$ имеет вещественное собственное значение. Наконец, выбирая базис в V легко видеть, что операторы A и $A_{\mathbb{C}}$ представляются одной и той же матрицей, следовательно, имеют одинаковые характеристические многочлены, и всякое собственное значение оператора $A_{\mathbb{C}}$ является собственным значением оператора A. □

Теорема 5.2. *Пусть A — самосопряженный оператор. Тогда существует ортонормированный базис, в котором матрица оператора A диагональна.*

Доказательство: дословно повторяет доказательство теоремы 3.2 с использованием леммы 5.1. □

Следствие 5.3. *Пусть g и B — билинейные симметрические формы на векторном пространстве V над полем $\mathbb{R}$, причем g положительно определена. Тогда найдется базис, в котором матрица Грама формы g — единична, а матрица Грама формы B — диагональна.*

Часть 6. Полярное разложение

Теорема 6.1. *Всякий невырожденный оператор A в евклидовом пространстве можно представить в виде $A = NS = S'N'$, где S, S' — самосопряженные операторы с положительным спектром, а N, N' — ортогональные операторы. Более того, операторы S, S', N, N' определены однозначно.*

Доказательство: ограничимся разложением $A = NS$ — второе разложение изучается аналогично. Рассмотрим оператор A^TA. Легко видеть, что он самосопряжен: $(A^TA)^T = A^TA^{TT} = A^TA$. Кроме того, $(A^TAv, v) = (Av, Av) = |Av|^2 > 0$, так как A невырожден. Значит, спектр оператора A^TA положителен. Отсюда следует, что существует единственный самосопряженный оператор S с положительным спектром, такой что $S^2 = A^TA$ (можно выбрать ортонормированный базис, в котором A^TA диагонален, и извлечь из элементов его матрицы корни). В частности, S — обратим. Наконец, $(AS^{-1})^T(AS^{-1}) = S^{-T}A^TAS^{-1} = S^{-1}S^2S^{-1} = \mathrm{Id}$, значит $N := AS^{-1}$ — ортогонален.

Проверим теперь однозначность. Действительно, если $A = NS$, то $A^TA = (NS)^T(NS) = S^TN^TNS = S^2$. Следовательно, оператор S определен однозначно условием положительности спектра, а в силу обратимости S оператор N также определен однозначно. □

Существует полярное разложение и для операторов в эрмитовом пространстве.

Теорема 6.2. *Всякий невырожденный оператор A в пространстве с положительно определенной эрмитовой формой h можно представить в виде $A = NS = S'N'$, где S, S' — эрмитовы с положительным спектром, а N, N' — унитарные операторы. Более того, операторы S, S', N, N' определены однозначно.*

Пример 6.3. В случае $V = \mathbb{C}$, $h(z, z') = z\bar{z'}$, полярное разложение оператора умножения на z совпадает с полярным разложением комплексного числа $z = re^{i\varphi}$.

Лекция 7. Тензоры

Часть 1. Тензоры

Пусть V — конечномерное векторное пространство над полем K. Тензорное произведение $V \otimes V \otimes \cdots \otimes V$ (p сомножителей) называется p-ой тензорной степенью пространства V и обозначается $V^{\otimes p}$. При этом полагают $V^{\otimes 0} := K$, так что $V^{\otimes p} \otimes V^{\otimes q} \cong V^{\otimes (p+q)}$ при всех $p, q \geqslant 0$. Кроме того, часто рассматривают тензорное произведение $V^{\otimes p} \otimes V^{*\otimes q}$. Его элементы называются тензорами типа (p, q) на V. Многие алгебраические объекты и структуры описываются тензорами.

Примеры 1.1. 1. Векторы — это тензоры типа $(1, 0)$.

2. Функционалы — это тензоры типа $(0, 1)$.

3. Операторы — это элементы пространства $\mathrm{Hom}(V, V) \cong V^* \otimes V$, то есть тензоры типа $(1, 1)$.

4. Билинейные формы — это линейные отображения $V \otimes V \to K$, то есть элементы пространства $(V \otimes V)^* \cong V^* \otimes V^*$, то есть тензоры типа $(0, 2)$.

Лемма 1.2. *Если* $\{ e_i \}_{i=1}^n$ *— базис в* V, *то* $\{ e_{i_1} \otimes \cdots \otimes e_{i_p} \otimes e^{j_1} \otimes \cdots \otimes e^{j_q} \}_{i_1,\ldots,i_p,j_1,\ldots,j_q=1}^n$ *— базис в* $V^{\otimes p} \otimes V^{*\otimes q}$, *где* e^j *— векторы двойственного базиса в* V^*.

Доказательство: очевидно следует из лемм 1.5 и 2.3 лекции 3. □

Соответственно, всякий тензор может быть представлен набором своих координат относительно этого базиса: $T = \sum T^{i_1,\ldots,i_p}_{j_1,\ldots,j_q} e_{i_1} \otimes \cdots \otimes e_{i_p} \otimes e^{j_1} \otimes \cdots \otimes e^{j_q}$. При этом обычно используют такую запись $T = (T^{i_1,\ldots,i_p}_{j_1,\ldots,j_q})$. С некоторыми такими представлениями мы уже хорошо знакомы, с другими еще встретимся.

Примеры 1.3. 1. Координаты оператора (a^i_j) — это его матрица.

2. Координаты билинейной формы $(g_{i,j})$ — это ее матрица Грама.

Пусть $A \in V^{\otimes p} \otimes V^{*\otimes q}$ и $B \in V^{\otimes r} \otimes V^{*\otimes s}$ — тензоры типа (p, q) и (r, s) соответственно. Их тензорным произведением называется элемент $A \otimes B \in \left(V^{\otimes p} \otimes V^{*\otimes q}\right) \otimes \left(V^{\otimes r} \otimes V^{*\otimes s}\right) \cong V^{\otimes (p+r)} \otimes V^{*\otimes (q+s)}$.

Лемма 1.4. *Если* $A = (A^{i_1,\ldots,i_p}_{j_1,\ldots,j_q})$, $B = (B^{i_1,\ldots,i_r}_{j_1,\ldots,j_s})$, *и* $C = A \otimes B$, *то* $C^{i_1,\ldots,i_p,i_{p+1},\ldots,i_{p+r}}_{j_1,\ldots,j_q,j_{q+1},\ldots,j_{q+s}} = A^{i_1,\ldots,i_p}_{j_1,\ldots,j_q} B^{i_1,\ldots,i_p}_{j_1,\ldots,j_q}$.

Следствие 1.5. *Операция* $\otimes$ *ассоциативна:* $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.

Замечание 1.6. Операция $\otimes$ на векторных пространствах коммутативна (в том смысле, что существует канонический изоморфизм $U \otimes V \cong V \otimes U$), однако операция $\otimes$ на тензорах уже некоммутативна. Действительно, если $u = (u_i)$, $v = (v_i)$, то $u \otimes v = (u_i v_j)$, а $(v \otimes u) = (v_i u_j)$, что не одно и то же!

Пусть $1 \leqslant k \leqslant p$, $1 \leqslant l \leqslant q$. Отображение $V^{\otimes p} \otimes V^{*\otimes q} = V^{\otimes (k-1)} \otimes V \otimes V^{\otimes (p-k)} \otimes V^{*\otimes (l-1)} \otimes V^* \otimes V^{*\otimes (q-l)} \cong \left(V^{\otimes (k-1)} \otimes V^{\otimes (p-k)} \otimes V^{*\otimes (l-1)} \otimes V^{*\otimes (q-l)}\right) \otimes (V \otimes V^*) \xrightarrow{\mathrm{ev}} V^{\otimes (p-1)} \otimes V^{*\otimes (q-1)}$ называется сверткой тензора типа (p, q) по индексам (k, l). Будем обозначать его $\mathrm{ev}_{k,l}$.

Лемма 1.7. *Если* $A = (A^{i_1,\ldots,i_p}_{j_1,\ldots,j_q})$ *и* $B = \mathrm{ev}_{k,l}(A)$, *то* $B^{i_1,\ldots,i_{p-1}}_{j_1,\ldots,j_{q-1}} = \sum_{i=1}^n A^{i_1,\ldots,i_{k-1},i,i_k,\ldots,i_{p-1}}_{j_1,\ldots,j_{l-1},i,j_l,\ldots,j_{q-1}}$.

В терминах тензорного произведения и свертки записываются многие важные операции.

Лемма 1.8. *Пусть* A, B *— операторы,* v *— вектор, а* f *— функционал на векторном пространстве* V. *Тогда* $f(v) = \mathrm{ev}_{1,1}(v \otimes f)$, $Av = \mathrm{ev}_{2,1}(A \otimes v)$, $AB = \mathrm{ev}_{2,1}(A \otimes B)$.

Еще одной важной операцией является действие группы $\mathfrak{S}_p \times \mathfrak{S}_q$ на пространстве $V^{\otimes p} \otimes V^{*\otimes q}$ (группа $\mathfrak{S}_p$ переставляет сомножители V, а группа $\mathfrak{S}_q$ — сомножители V^*).

Лемма 1.9. *Если* $A = (A^{i_1,\ldots,i_p}_{j_1,\ldots,j_q})$, $\sigma \in \mathfrak{S}_p$, $\tau \in \mathfrak{S}_q$ *и* $B = (\sigma, \tau)(A)$, *то* $B^{i_1,\ldots,i_p}_{j_1,\ldots,j_q} = A^{i_{\sigma_1},\ldots,i_{\sigma_p}}_{j_{\tau_1},\ldots,j_{\tau_q}}$.

Часть 2. Симметрические и кососимметрические тензоры

Ограничимся в этом разделе рассмотрением тензоров типа $(n,0)$ над полем K характеристики 0.

Определение 2.1. Тензор $T \in V^{\otimes n}$ называется симметрическим, если $\forall \sigma \in \mathfrak{S}_n$ имеем $\sigma(T) = T$, и кососимметрическим, если $\forall \sigma \in \mathfrak{S}_n$ имеем $\sigma(T) = \varepsilon(\sigma)T$.

Пространство всех симметрических тензоров типа $(n,0)$ называется симметрической степенью и обозначается S^nV, а пространство всех кососимметрических тензоров типа $(n,0)$ называется внешней степенью и обозначается Λ^nV. Кососимметрические тензоры также называются поливекторами. Заметим, что $S^0V = \Lambda^0V = V^{\otimes 0} = K$, $S^1V = \Lambda^1V = V$.

Рассмотрим на пространстве $V^{\otimes n}$ оператор симметризации $\operatorname{Sym}(T) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\sigma(T)$ и оператор альтернирования $\operatorname{Alt}(T) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\sigma(T)$. Пусть $n \geqslant 2$.

Лемма 2.2. Sym *и* Alt *— ортогональные проекторы на подпространства* $S^nV, \Lambda^nV \subset V^{\otimes n}$. *То есть,* $\operatorname{Sym}^2 = \operatorname{Sym}$, $\operatorname{Alt}^2 = \operatorname{Alt}$, $\operatorname{Sym}\operatorname{Alt} = \operatorname{Alt}\operatorname{Sym} = 0$, *и* $T \in S^nV \iff \operatorname{Sym}(T) = T$, $T \in \Lambda^nV \iff \operatorname{Alt}(T) = T$.

Доказательство: заметим, что умножение на τ дает изоморфизм $\mathfrak{S}_n \to \mathfrak{S}_n$, поэтому $\tau\circ\operatorname{Sym} = \operatorname{Sym} = \operatorname{Sym}\circ\tau$, $\tau\circ\operatorname{Alt} = \varepsilon(\tau)\operatorname{Alt} = \operatorname{Alt}\circ\tau$. Следовательно, $\operatorname{Sym}^2 = \frac{1}{n!}\sum_{\tau\in\mathfrak{S}_n}\tau\circ\operatorname{Sym} = \frac{1}{n!}\sum_{\tau\in\mathfrak{S}_n}\operatorname{Sym} = \frac{1}{n!}n!\operatorname{Sym} = \operatorname{Sym}$. Аналогично доказываются равенства $\operatorname{Alt}^2 = \operatorname{Alt}$, $\operatorname{Sym}\operatorname{Alt} = \operatorname{Alt}\operatorname{Sym} = 0$. Пусть теперь $T \in \Lambda^nV$. Тогда $\operatorname{Alt}(T) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\sigma(T) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)^2T = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}T = \frac{1}{n!}n!T = T$. Если же $\operatorname{Alt}(T) = T$, то $\tau(T) = (\tau\circ\operatorname{Alt})(T) = \varepsilon(\tau)\operatorname{Alt}(T) = \varepsilon(\tau)T$, значит $T \in \Lambda^nV$. Аналогично, $\operatorname{Sym}(T) = T \iff T \in S^nV$. □

Следствие 2.3. *При* $n \geqslant 2$ *имеем* $V^{\otimes n} = S^nV \oplus \Lambda^nV \oplus \operatorname{Ker}(\operatorname{Sym}+\operatorname{Alt})$. *В частности,* $V^{\otimes 2} = S^2V \oplus \Lambda^2V$.

Доказательство: при $n = 2$ имеем $\operatorname{Sym}+\operatorname{Alt} = \frac{1}{2}(\operatorname{Id}+\tau) + \frac{1}{2}(\operatorname{Id}-\tau) = \operatorname{Id}$, где $\tau = (12) \in \mathfrak{S}_2$. □

Лемма 2.4. *Пусть* $\dim V = N$ *и* $\{e_i\}_{i=1}^N$ *— базис в* V. *Рассмотрим* $e_{i_1}\cdot\ldots\cdot e_{i_n} := \operatorname{Sym}(e_{i_1}\otimes\cdots\otimes e_{i_n})$, $e_{i_1}\wedge\cdots\wedge e_{i_n} := \operatorname{Alt}(e_{i_1}\otimes\cdots\otimes e_{i_n})$. *Тогда* $\{e_{i_1}\cdot\ldots\cdot e_{i_n}\}_{1\leqslant i_1\leqslant\cdots\leqslant i_n\leqslant N}$ *и* $\{e_{i_1}\wedge\cdots\wedge e_{i_n}\}_{1\leqslant i_1<\cdots<i_n\leqslant N}$ *образуют базисы в* S^nV *и* Λ^nV *соответственно.*

Доказательство: линейная независимость очевидна — если предположить, что некоторая линейная комбинация равна нулю, то окажется, что аналогичная линейная комбинация векторов $e_{i_1}\otimes\cdots\otimes e_{i_n}$ в $V^{\otimes n}$ равна нулю, что невозможно. Остается заметить, что всякий элемент $e_{i_1}\otimes\cdots\otimes e_{i_n}$ операторами Sym и Alt переводится либо в один из указанных выше элементов, либо в ноль. □

Следствие 2.5. $\dim S^nV = \binom{N+n-1}{n}$, $\dim\Lambda^nV = \binom{N}{n}$.

Следствие 2.6. *При* $n > \dim V$ *имеем* $\Lambda^nV = 0$, *а при* $n = \dim V$ *имеем* $\Lambda^nV \cong K$.

Теорема 2.7. S^nV *и* Λ^nV *являются универсальными объектами в категории симметрических и кососимметрических полилинейных отображений из* $V\times\cdots\times V$.

Доказательство: пусть $f : V\times\cdots\times V \to W$ — симметрическое полилинейное отображение. Тогда оно пропускается через линейное отображение $F : V^{\otimes n} \to W$, такое что $F(a) = F(\sigma(a))$ для любых $\sigma \in \mathfrak{S}_n$, $a \in V^{\otimes n}$. Следовательно, $F(a) = F(\operatorname{Sym}(a))$, следовательно, F пропускается через S^nV. □

Замечание 2.8. Эта теорема дает правильный способ определить S^nV и Λ^nV для векторных пространств положительной характеристики, а также для модулей над произвольными кольцами, как универсальные объекты в категории симметрических и знакопеременных полилинейных отображений из $V\times\cdots\times V$.

Лемма 2.9. S^n *и* Λ^n *— функторы.*

Доказательство: если $f : U \to V$ — линейное отображение, то $f^{\otimes n}(S^nU) \subset S^nV$, $f^{\otimes n}(\Lambda^nU) \subset \Lambda^nV$. □

Теорема 2.10. *Если* $A : V \to V$ *— оператор и* $\dim V = n$, *то* Λ^nA *— умножение на* $\det A$.

Доказательство: достаточно выбрать базис и сравнить формулы. □

В связи с этим принято обозначать старшую внешнюю степень пространства V через $\det V$, а старшую линейную степень линейного отображения f векторных пространств одной размерности через $\det f$.

Часть 3. Алгебры

Определение 3.1. Алгеброй (или K-алгеброй) называется векторное пространство над полем K со структурой кольца, такой что умножение — K-билинейно.

Примеры 3.2. 1. Поле K является алгеброй над собой, а также над любым своим подполем.

2. Алгебра кватернионов $\mathbb{H}$ является $\mathbb{R}$-алгеброй (но не $\mathbb{C}$-алгеброй!).

3. Кольцо многочленов $K[x_1, \dots, x_n]$ является K-алгеброй.

4. Кольцо матриц $\mathrm{Mat}_{n\times n}(K)$ является K-алгеброй.

Замечание 3.3. Есть более общее понятие R-алгебры, где R — произвольное коммутативное кольцо. По определению R-алгебра — это произвольное кольцо A и гомоморфизм колец $R \to Z(A)$.

Ясно, что структура алгебры на пространстве A определяется билинейным отображением $m : A\otimes A \to A$, удовлетворяющим условию ассоциативности $m \circ (m \otimes \mathrm{Id}) = m \circ (\mathrm{Id} \otimes m) : A \otimes A \otimes A \to A$, и отображением $e : K \to A$, таким что $m \circ (e \otimes \mathrm{Id}) = \mathrm{Id} = m \circ (\mathrm{Id} \otimes e) : A \to A$. Выберем базис $\{ e_i \}$ в A, такой что $e_1 = e$. Координаты $c^k_{i,j}$ тензора m называются структурными константами алгебры A. Ясно, что A — алгебра $\iff$ $\sum_k c^k_{i,j}c^m_{k,l} = \sum_k c^k_{jl}c^m_{ik}$ и $c^k_{1,i} = c^k_{i,1} = \delta^k_i$. Однако, задавать структуру алгебры структурными константами на практике неудобно.

Рассмотрим пространства $T^\bullet(V) = \oplus_{n=0}^\infty V^{\otimes n}$, $S^\bullet(V) = \oplus_{n=0}^\infty S^n V$, $\Lambda^\bullet(V) = \oplus_{n=0}^\infty \Lambda^n V$ и введем на них операции $\otimes$, $\cdot$ и $\wedge$, где $a \cdot b := \mathrm{Sym}(a \otimes b)$, $a \wedge b := \mathrm{Alt}(a \otimes b)$, а операция $\otimes$ доопределена равенством $1 \otimes a = a \otimes 1 = a$, где 1 — единица в $V^{\otimes 0} = K$. Элемент a, лежащий в n-ом слагаемом, будем называть однородным и определим его степень $|a| = n$.

Лемма 3.4. *Пространства $T^\bullet(V)$, $S^\bullet(V)$ и $\Lambda^\bullet(V)$ — алгебры.*

Доказательство: $(a \cdot b) \cdot c = \mathrm{Sym}(\mathrm{Sym}(a \otimes b) \otimes c)$. Докажем, что это равно $\mathrm{Sym}(a \otimes b \otimes c)$. Действительно,

$$\mathrm{Sym}(\mathrm{Sym}(a \otimes b) \otimes c) = \mathrm{Sym}\left[\left(\frac{1}{n!}\sum\nolimits_{\tau\in\mathfrak{S}_n} \tau(a \otimes b)\right) \otimes c\right] = \frac{1}{n!}\sum\nolimits_{\tau\in\mathfrak{S}_n} \mathrm{Sym} \circ \tau(a \otimes b \otimes c) = \mathrm{Sym}(a \otimes b \otimes c),$$

где $n = |a|+|b|$, а в третьем члене мы рассматриваем $\mathfrak{S}_n$ как подгруппу в $\mathfrak{S}_{|a|+|b|+|c|}$, сосотящую из перестановок, неподвижных на последних $|c|$ элементах. Аналогично доказываются равенства $a \cdot (b \cdot c) = \mathrm{Sym}(a \otimes b \otimes c)$, $(a \wedge b) \wedge c = \mathrm{Alt}(a \otimes b \otimes c)$, $a \wedge (b \wedge c) = \mathrm{Alt}(a \otimes b \otimes c)$, из которых немедленно следует ассоциативность. □

$T^\bullet(V)$, $S^\bullet(V)$ и $\Lambda^\bullet(V)$ называются тензорной, симметрической и внешней алгебрами пространства V.

Лемма 3.5. *Алгебра $S^\bullet(V)$ коммутативна, а $\Lambda^\bullet(V)$ суперкоммутативна, то есть $a \wedge b = (-1)^{|a||b|} b \wedge a$.*

Доказательство: тензоры $a\otimes b$ и $b\otimes a$ отличаются действием перестановки, знак которой равен $(-1)^{|a||b|}$. □

Лемма 3.6. Sym *и* Alt *задают сюръективные гомоморфизмы алгебр $T^\bullet(V) \to S^\bullet(V)$ и $T^\bullet(V) \to \Lambda^\bullet(V)$.*

Доказательство: гомоморфность следует из определения операций $\cdot$ и $\wedge$, а сюръективность из леммы 2.2. □

Лемма 3.7. *Ядра гомоморфизмов* $\mathrm{Sym} : T^\bullet(V) \to S^\bullet(V)$ *и* $\mathrm{Alt} : T^\bullet(V) \to \Lambda^\bullet(V)$ *порождаются подпространствами $\Lambda^2 V \subset V \otimes V$ и $S^2 V \subset V \otimes V$ соответственно.*

Доказательство: легко видеть, что векторы $e_{i_1} \otimes \dots \otimes e_{i_k} \otimes e_{i_{k+1}} \otimes \dots \otimes e_{i_n} - e_{i_1} \otimes \dots \otimes e_{i_{k+1}} \otimes e_{i_k} \otimes \dots \otimes e_{i_n}$ порождают $\operatorname{Ker}\mathrm{Sym}$. Остается заметить, что они равны $e_{i_1} \otimes \dots \otimes e_{i_{k-1}} \otimes (2e_{i_k} \wedge e_{i_{k+1}}) \otimes e_{i_{k+2}} \otimes \dots \otimes e_{i_n}$. Аналогично, векторы $e_{i_1} \otimes \dots \otimes e_{i_k} \otimes e_{i_{k+1}} \otimes \dots \otimes e_{i_n} + e_{i_1} \otimes \dots \otimes e_{i_{k+1}} \otimes e_{i_k} \otimes \dots \otimes e_{i_n} = e_{i_1} \otimes \dots \otimes e_{i_{k-1}} \otimes (2e_{i_k} \cdot e_{i_{k+1}}) \otimes e_{i_{k+2}} \otimes \dots \otimes e_{i_n}$ порождают $\operatorname{Ker}\mathrm{Alt}$. □

Теорема 3.8. *Тензорная алгебра является свободной алгеброй, симметрическая алгебра является свободной коммутативной алгеброй, а внешняя алгебра является свободной суперкоммутативной алгеброй.*

Доказательство: пусть A — произвольная алгебра, а $\mu_1 : V \to A$ — линейное отображение. Докажем, что существует единственный гомоморфизм алгебр $\mu_\bullet : T^\bullet(V) \to A$, продолжающий μ_1. Действительно, отображение $V \times \dots \times V \to A$, $(v_1, \dots, v_n) \mapsto \mu_1(v_1) \cdot \dots \cdot \mu_1(v_n) \in A$ билинейно, следовательно, пропускается через отображение $\mu_n : V^{\otimes n} \to A$. Легко видеть, что $\mu_\bullet = \oplus\mu_n : T^\bullet(V) \to A$ — гомоморфизм алгебр, причем однозначно определенный. Пусть теперь A — коммутативная алгебра. Тогда ясно, что $\mu_2(\Lambda^2 V) = 0$, так как $\Lambda^2 V$ порождается бивекторами $v_1 \otimes v_2 - v_2 \otimes v_1$, а $\mu_2(v_1 \otimes v_2 - v_2 \otimes v_1) = \mu_1(v_1)\mu_1(v_2) - \mu_1(v_2)\mu_1(v_1) = 0$. Значит $\mu_\bullet$ пропускается через фактор по идеалу, порожденному пространством $\Lambda^2 V$, то есть через $S^\bullet V$. □

Лекция 8. Пфаффианы и уравнения Плюккера

Часть 1. Пфаффианы

Пусть $A = (a_{ij})$ — кососимметрическая матрица размера $2n \times 2n$. Будем рассматривать A как матрицу Грама кососимметрической билинейной формы. Как известно, в подходящем базисе матрица Грама такой формы приводится к стандартному виду $A_m := \begin{pmatrix} 0 & E_m & 0 \\ -E_m & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, где $2m = r(A)$. Иначе говоря, существует обратимая матрица C, такая что $A = C^T A_m C$. Следовательно, $\det A = \det A_m (\det C)^2$. В частности, если A невырождена, то $m = n$, $\det A_n = 1$ и $\det A = (\det C)^2$. Таким образом, определитель матрицы A всегда является квадратом. И это не случайно!

Теорема 1.1. *Существует единственный с точностью до знака многочлен* $\mathrm{Pf} \in \mathbb{Z}[a_{ij}]_{1 \leqslant i < j \leqslant 2n}$ *степени* n, *такой что для любой кососимметрической матрицы* A *имеем* $\det A = \mathrm{Pf}(A)^2$.

Доказательство: начнем с единственности. Если Pf_1 — многочлен, такой что $\mathrm{Pf}_1^2 = \det$, то $(\mathrm{Pf}_1 / \mathrm{Pf})^2 = 1$ в кольце $\mathbb{Q}(a_{ij})$ (поле частных кольца $\mathbb{Z}[a_{ij}]_{1 \leqslant i < j \leqslant 2n}$), то есть $\mathrm{Pf}_1 = \pm \mathrm{Pf}$.

Докажем теперь существование. Рассмотрим поле $K = \mathbb{Q}(a_{ij})_{1 \leqslant i < j \leqslant 2n}$. Матрица A, у которой на месте i, j при $i < j$ стоит a_{ij}, при $i > j$ стоит $-a_{ji}$, а при $i = j$ стоит 0, является кососимметрической матрицей с коэффициентами в поле K. Более того, ясно, что она невырождена (при подстановке $a_{ij} := \delta_{j,i+n}$ она превращается в невырожденную матрицу A_n). Следовательно, найдется невырожденная матрица C с коэффициентами в поле K, такая что $A = C^T A_n C$. Значит, $\det(A) = \det(C)^2$. Положим $\mathrm{Pf}(A) = \det(C)$. Тогда $\mathrm{Pf} \in \mathbb{Q}(a_{ij})$ и $\mathrm{Pf}^2 = \det \in \mathbb{Z}[a_{ij}]$. Покажем, что $\mathrm{Pf} \in \mathbb{Z}[a_{ij}]$. Действительно, так как $\mathbb{Q}(a_{ij})$ есть поле частных кольца $\mathbb{Z}[a_{ij}]$, то Pf можно записать в виде f/g, где $f, g \in \mathbb{Z}[a_{ij}]$. Отсюда получаем равенство $f^2 = g^2 \cdot \det$ в кольце $\mathbb{Z}[a_{ij}]$. Воспользуемся факториальностью кольца $\mathbb{Z}[a_{ij}]$. Раскладывая f, g и det на неприводимые множители и сравнивая степени, видим, что $g | f$, то есть $\mathrm{Pf} = f/g \in \mathbb{Z}[a_{ij}]$. □

Теорема 1.2. *Если целостное кольцо* A *факториально, то кольцо* $A[x]$ *тоже факториально.*

Обозначим через K поле частных кольца A. Тогда $K[x]$ — кольцо главных идеалов, в частности факториально. Кроме того, $A[x]$ — подкольцо в $K[x]$.

Лемма 1.3. *Если* $f(x)$ *неприводим в* $A[x]$, *то он неприводим и в* $K[x]$.

Доказательство: пусть $f(x) = g(x)h(x)$, $g, h \in K[x]$. Домножая на общий знаменатель коэффициентов g и h, получаем $af(x) = g_1(x)h_1(x)$, где $a \in A$, $g_1, h_1 \in A[x]$. Пусть p — неприводимый делитель a. Тогда A/pA — целостное кольцо (так как A факториально!), значит $A/pA[x]$ — тоже целостное, но в $A/pA[x]$ имеем $a = 0$, значит $g_1(x)h_1(x) = 0$, значит либо $g_1(x) = 0$, либо $h_1(x) = 0$, то есть либо $g_1(x) = pg_2(x)$ в $A[x]$, либо $h_1(x) = ph_2(x)$ в $A[x]$. Сокращая наше равенство на p и продолжая те же рассуждения, получаем равенство $f(x) = g'(x)h'(x)$ в $A[x]$, противоречащее неприводимости f. □

Доказательство теоремы: пусть $p_1(x) \cdot \dots \cdot p_r(x) = q_1(x) \cdot \dots \cdot q_s(x)$, где p_i, q_j неприводимы в $A[x]$. Тогда по лемме они неприводимы и в $K[x]$, следовательно, в силу факториальности этого кольца имеем $r = s$ и после перенумерации имеем $p_i(x) = u_i q_i(x)$, где $u_i \in (K[x])^* = K^*$. Иначе говоря, $a_i p_i(x) = b_i q_i(x)$, где $0 \neq a_i, b_i \in A$ и $(a_i, b_i) = 1$. Применяя те же рассуждения, что и в лемме получаем, что всякий неприводимый делитель a_i должен делить либо b_i, либо q_i. Но первое невозможно по условию, а второе — в силу неприводимости q_i. Значит, a_i — единица. Аналогично, b_i — единица. □

Следствие 1.4. *Кольца* $\mathbb{Z}[x_1, \dots, x_n]$ *и* $K[x_1, \dots, x_n]$ *факториальны.*

Многочлен Pf, удовлетворяющий свойствам теоремы 1.1 и свойству $\mathrm{Pf}(A_n) = 1$, называется пфаффианом.

Примеры 1.5.
1. Если $n = 1$, то $\mathrm{Pf}(A) = a_{12}$.
2. Если $n = 2$, то $\mathrm{Pf}(A) = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$.

Часть 2. Поливекторы

Лемма 2.1. *Если $w \in \Lambda^k V$, а $\xi \in V^*$, то $\mathrm{ev}_{s,1}(w \otimes \xi) = \pm \mathrm{ev}_{t,1}(w \otimes \xi)$ при всех $1 \leqslant s,t \leqslant k$. Более того, тензор $\mathrm{ev}_{s,1}(w \otimes \xi) \in V^{\otimes(k-1)}$ кососимметричен.*

Доказательство: пусть $s > t$ и $\sigma = (t, t+1, \dots, s)$ (цикл). Тогда $\mathrm{ev}_{s,1}(w \otimes \xi) = \mathrm{ev}_{t,1}(\sigma(w) \otimes \xi) = \varepsilon(\sigma)\,\mathrm{ev}_{t,1}(w \otimes \xi)$. Далее, пусть $\tau \in \mathfrak{S}_{k-1}$ и пусть $i_s : \mathfrak{S}_{k-1} \to \mathfrak{S}_k$ изоморфизм на подгруппу перестановок, неподвижных в s. Тогда $\tau(\mathrm{ev}_{s,1}(w \otimes \xi)) = \mathrm{ev}_{s,1}(i_s(\tau)(w) \otimes \xi) = \mathrm{ev}_{s,1}(\varepsilon(i_s(\tau))w \otimes \xi) = \varepsilon(i_s(\tau))\,\mathrm{ev}_{s,1}(w \otimes \xi) = \varepsilon(\tau)\,\mathrm{ev}_{s,1}(w \otimes \xi)$. □

Для всяких $w \in \Lambda^k V$ и $\xi \in \Lambda^m V^*$ определим $w \vdash \xi := \mathrm{ev}_{1,1}(\mathrm{ev}_{1,1}(\dots(\mathrm{ev}_{1,1}(w \otimes \xi))\dots))$ ($\min(m,k)$-раз).

Лемма 2.2. *Если $k > m$, то $w \vdash \xi \in \Lambda^{k-m} V$, если $k < m$, то $w \vdash \xi \in \Lambda^{m-k} V^*$, а если $k = m$, то $w \vdash \xi \in K$.*

Доказательство: пусть, например, $k > m$. Пусть $i : \mathfrak{S}_{k-m} \to \mathfrak{S}_k$ — изоморфизм на подгруппу перестановок, неподвижных на $1, \dots, m$. Тогда $\tau(w \vdash \xi)) = i(\tau)(w) \vdash \xi = \varepsilon(i(\tau))w \vdash \xi = \varepsilon(\tau)w \vdash \xi$. □

Лемма 2.3. *Спаривание $\Lambda^k V \otimes \Lambda^k V^* \to K$, $(w, \xi) \mapsto w \vdash \xi$ невырождено и, значит, $\Lambda^k V^* \cong (\Lambda^k V)^*$.*

Доказательство: легко видеть, что $(e_{i_1} \wedge \dots \wedge e_{i_k}) \vdash (e^{j_1} \wedge \dots \wedge e^{j_k}) = \delta^{j_1}_{i_1} \dots \delta^{j_k}_{i_k}/k!$. □

Замечание 2.4. При $k = 1$ спаривание $V \otimes V^* \to K$, $(w, \xi) \mapsto w \vdash \xi$ совпадает со стандартным $(w, \xi) \mapsto \xi(w)$.

Лемма 2.5. *Пусть $w \in \Lambda^k V$, $\xi_1 \in \Lambda^{m_1} V^*$, $\xi_2 \in \Lambda^{m_2} V^*$ и $m_1 + m_2 \leqslant k$. Тогда $(w \vdash \xi_1) \vdash \xi_2 = w \vdash (\xi_1 \wedge \xi_2)$.*

Доказательство: $(w \vdash \xi_1) \vdash \xi_2 = \mathrm{ev}(\mathrm{ev}(w \otimes \xi_1) \otimes \xi_2) = \mathrm{ev}(w \otimes \xi_1 \otimes \xi_2)$, а $w \vdash (\xi_1 \wedge \xi_2) = \mathrm{ev}(w \otimes \mathrm{Alt}(\xi_1 \otimes \xi_2))$, поэтому достаточно показать, что $\mathrm{ev}(w \otimes \xi)$ является кососимметрической функцией от $\xi \in V^{*\otimes m}$. Действительно, если $\sigma \in \mathfrak{S}_m \subset \mathfrak{S}_k$, то $\mathrm{ev}(w \otimes \sigma(\xi)) = \mathrm{ev}(\sigma^{-1}(w) \otimes \xi) = \mathrm{ev}(\varepsilon(\sigma^{-1})w \otimes \xi) = \varepsilon(\sigma)\,\mathrm{ev}(w \otimes \xi)$. □

Определение 2.6. k-вектор $w \in \Lambda^k V$ называется разложимым, если $w = v_1 \wedge \dots \wedge v_k$, где $v_1, \dots, v_k \in V$.

Замечание 2.7. Векторы $v_1, \dots, v_k$ в определении разложимого вектора неоднозначно определяются k-вектором w, но подпространство в V, ими порожденное, уже определяется однозначно. Это следует, например, из следующей леммы (это подпространство состоит из всех векторов $v \in V$, таких что $w \wedge v = 0$).

Лемма 2.8. *Пусть $w \in \Lambda^k V$, $v_1, \dots, v_m \in V$, $\xi_1, \dots, \xi_m \in V^*$ — линейно независимые наборы. Тогда $w \wedge v_1 = \dots = w \wedge v_m = 0 \iff w = w' \wedge v_1 \wedge \dots \wedge v_m$, $w \vdash \xi_1 = \dots = w \vdash \xi_m = 0 \iff w \in \Lambda^k(\langle \xi_1, \dots, \xi_m \rangle^\perp)$.*

Доказательство: для первого утверждения выберем базис в V, такой что $e_1 = v_1$, …, $e_m = v_m$, а для второго — такой, что $e^1 = \xi_1$, …, $e^m = \xi_m$, и перепишем условия в терминах координат w относительно индуцированного базиса в $\Lambda^k V$. □

Лемма 2.9. *Пусть $0 \neq w \in \Lambda^k V$. Тогда ранг отображения свертки $V^* \xrightarrow{w} \Lambda^{k-1} V$ не меньше чем k, причем равенство достигается тогда и только тогда, когда w разложим.*

Доказательство: пусть U — ядро. Применяя несколько раз лемму 2.8 получаем, что $w \in \Lambda^k(U^\perp)$. Поэтому, если $\dim U > n-k$, то $\dim U^\perp < k$ и $\Lambda^k(U^\perp) = 0$. Если же $\dim U = n-k$, то $\Lambda^k(U^\perp)$ порождается разложимым k-вектором $v_1 \wedge \dots \wedge v_k$, где $v_1, \dots, v_k$ — произвольный базис в $U^\perp$. □

Следствие 2.10. *Пусть $0 \neq w \in \Lambda^k V$. Тогда ранг отображения свертки $\Lambda^{k-1} V^* \xrightarrow{w} V$ не меньше чем k, причем равенство достигается тогда и только тогда, когда w разложим.*

Доказательство: достаточно показать, что это отображение двойственно по отношению к отображению из леммы с учетом изоморфизма $(\Lambda^{k-1} V)^* \cong \Lambda^{k-1} V^*$ леммы 2.3. Действительно, $\forall \xi_1 \in V^*, \xi_{k-1} \in \Lambda^{k-1} V^*$ имеем $(w \vdash \xi_{k-1})(\xi_1) = (w \vdash \xi_{k-1}) \vdash \xi_1 = w \vdash (\xi_{k-1} \wedge \xi_1) = \pm w \vdash (\xi_1 \wedge \xi_{k-1}) = \pm(w \vdash \xi_1) \vdash \xi_{k-1} = \pm(w \vdash \xi_1)(\xi_{k-1})$. □

Теорема 2.11. *k-вектор w разложим $\iff$ для любого $(k-1)$-ковектора $\xi \in \Lambda^{k-1} V^*$ имеем $w \wedge (w \vdash \xi) = 0$.*

Доказательство: $\Longrightarrow$) очевидно — если $w = v_1 \wedge \dots \wedge v_k$, то $w \vdash \xi \in \langle v_1, \dots, v_k \rangle$ и $w \wedge (w \vdash \xi) = 0$.

$\Longleftarrow$) Предположим, что w неразложим. Тогда $\dim\{\, w \vdash \xi \,\} > k$. Выберем $k+1$ линейно независимых вектора $v_1, \dots, v_{k+1} \in \{\, w \vdash \xi \,\}$. Применяя лемму 2.8, получаем, что $w = w' \wedge v_1 \wedge \dots \wedge v_{k+1}$, что невозможно. □

Замечание 2.12. Уравнения $w \wedge (w \vdash \xi) = 0$, описывающие множество разложимых k-векторов, являются уравнениями второй степени от координат. Они называются уравнения Плюккера.

Лекция 9. Теория представлений

Часть 1. Категория представлений

Определение 1.1. K-линейным представлением группы G в векторном пространстве V над полем K называется гомоморфизм групп $\rho : G \to \mathrm{GL}(V; k)$. Размерностью представления ρ называется $\dim_K V$.

Иначе говоря, K-линейное представление — это действие группы G на векторном пространстве V K-линейными преобразованиями. Когда ясно, над каким полем рассматриваются представления, символ поля будет опускаться. Кроме того, часто опускается и символ ρ, и представлением называют само пространство, в котором действует группа.

Примеры 1.2.
1. Тождественное представление $\mathrm{Id} : \mathrm{GL}(V) \to \mathrm{GL}(V)$.
2. Тривиальное представление $1_G : G \to \mathrm{GL}(1; K)$, $g \mapsto 1$.
3. Знаковое представление $\varepsilon : \mathfrak{S}_n \to \mathrm{GL}(1; K)$, $\sigma \mapsto \varepsilon(\sigma)$.
4. Стандартное представление $\mathfrak{S}_n \to \mathrm{GL}(V^{\otimes n})$.

Определение 1.3. Гомоморфизм линейных представлений $\rho_1 \to \rho_2$ — это линейное отображение $f : V_1 \to V_2$, такое что $\forall g \in G$ имеем $f \circ \rho_1(g) = \rho_2(g) \circ f$. Гомоморфизмы представлений группы G также называются G-эквивариантными гомоморфизмами. Множество всех G-эквивариантных гомоморфизмов $V_1 \to V_2$ обозначается $\mathrm{Hom}_G(V_1, V_2)$. Легко видеть, что $\mathrm{Hom}_G(V_1, V_2)$ — подпространство в пространстве $\mathrm{Hom}(V_1, V_2)$.

Пример 1.4. Если T — (косо)симметрический тензор, то $K \xrightarrow{T} V^{\otimes n}$ — гомоморфизм из тривиального (знакового) представления $\mathfrak{S}_n$ в стандартное представление.

Лемма 1.5. *K-линейные представления группы G образуют категорию* $\mathrm{Rep}_G(K)$.

Говорят, что U — подпредставление в V, если U — подпространство в V, такое что $g(U) \subset U$ для всех $g \in G$. Представление V называется неприводимым, если оно не имеет подпредставлений, кроме 0 и V.

Пример 1.6. Тривиальное и знаковое представления группы $\mathfrak{S}_n$ неприводимы. Вообще, всякое одномерное представление неприводимо.

Пусть $\rho_U : G \to \mathrm{GL}(U)$ и $\rho_V : G \to \mathrm{GL}(V)$ — представления группы G. Тогда $\rho_U \oplus \rho_V : G \to \mathrm{GL}(U \oplus V)$, $g(u, v) = (gu, gv)$ — представление группы G, которое называется прямой суммой представлений ρ_U и ρ_V.

Лемма 1.7. *Прямая сумма представлений является произведением и копроизведением в категории* Rep_G.

Пусть $f : U \to V$ — гомоморфизм представлений группы G. Легко видеть, что $\mathrm{Ker}\, f \subset U$ является подпредставлением в U, а $\mathrm{Im}\, f \subset V$ — подпредставлением в V. Действительно, если $f(u) = 0$, то $f(gu) = gf(u) = g0 = 0$, а если $v = f(u)$, то $gv = gf(u) = f(gu)$. Наконец, если $U \subset V$ — подпредставление, то на факторпространстве V/U возникает каноническое представление группы G: $g(v + U) = gv + gU = gv + U$. Оно называется факторпредставлением.

Лемма 1.8. *Если $f : U \to V$ — гомоморфизм представлений, то* $\mathrm{Im}\, f \cong U/\mathrm{Ker}\, f$.

Пусть U и V — представления группы G. Формулы $g(u \otimes v) = gu \otimes gv$ и $(gf)(u) = g(f(g^{-1}u))$ задают структуру представления группы G в пространствах $U \otimes V$ и $\mathrm{Hom}(U, V)$ соответственно. В частности, двойственное представление определяется как $U^* := \mathrm{Hom}(U, 1_G)$. Легко видеть, что все эти операции функториальны. Вот еще один важный функтор. Пусть V — представление группы G. Определим подпространство инвариантов $V^G \subset V$ формулой $V^G = \{\, v \in V \mid gv = v \ \forall g \in G \,\}$.

Очень важной операцией является усреднение по группе, т. е. оператор $\mathrm{Sym}_G = \frac{1}{|G|} \sum_{g \in G} g \in \mathrm{End}(V)$.

Лемма 1.9. *Если* $\operatorname{char} K \not| |G|$, *то* Sym_G *является* G*-эквивариантным проектором* V *на* V^G.

Доказательство: так же как и с оператором Sym проверяем, что $\forall h \in G\ h \circ \operatorname{Sym}_G = \operatorname{Sym}_G = \operatorname{Sym}_G \circ h$. □

Часть 2. Групповая алгебра

Пусть G — конечная группа. Рассмотрим векторное пространство $K[G]$ над полем K, с базисом $\{ e_g \}_{g \in G}$, занумерованным элементами группы G, и определим в нем операцию умножения формулой $(\sum_{g \in G} a_g e_g) \cdot (\sum_{h \in G} b_h e_h) = \sum_{g,h \in G} a_g b_h e_{gh}$. Легко видеть, что пространство $K[G]$ является K-алгеброй. Эта алгебра называется групповой алгеброй группы G. Заметим, что $\operatorname{Sym}_G \in K[G]$, если он имеет смысл.

Лемма 2.1. *Категория* K*-линейных представлений группы* G *эквивалентна категории* $K[G]$*-модулей.*

Доказательство: если V — линейное представление группы G, то на V вводится структура $K[G]$-модуля формулой $(\sum_{g \in G} a_g e_g)v = \sum_{g \in G} a_g g(v)$. Наоборот, если V — модуль над $K[G]$, то $g(v) := e_g v$ задает на V структуру представления группы G. Наконец, легко видеть, что гомоморфизмы представлений и гомоморфизмы $K[G]$-модулей — это одно и то же. □

Легко видеть, что понятия ядра и образа морфизма представлений, подпредставления, факторпредставления, прямой суммы представлений — эквивалентны понятиям ядра и и образа морфизма модулей, подмодуля, фактормодуля, прямой суммы модулей над алгеброй $K[G]$. Однако, тензорное произведение представлений не совпадает с тензорным произведением $K[G]$-модулей.

Замечание 2.2. Для краткости представления группы G часто называются G-модулями.

Очень важным представлением всякой группы G является ее представление в пространстве $K[G]$, которое задается формулой $g(\sum_{h \in G} a_h e_h) = \sum_{h \in G} a_h e_{gh}$, и соответствует свободному $K[G]$-модулю ранга 1. Это представление называется регулярным. Его размерность равна порядку группы G.

Часть 3. Теорема Машке

Определение 3.1. Представление V группы G называется вполне приводимым, если для любого подпредставления $U \subset V$ найдется подпредставление $U' \subset V$, такое что $V = U \oplus U'$.

Теорема 3.2. *Если группа* G *— конечна, а характеристика поля* $\operatorname{char} K$ *не делит порядок группы* $|G|$, *то всякое конечномерное представление группы* G *вполне приводимо.*

Доказательство: выберем произвольное дополнительное к U подпространство $U'' \subset V$ (не обязательно являющееся подпредставлением), и рассмотрим соответствующий проектор $p'' : V \to V$ (проектор на U вдоль U''). Далее, положим $p' := \operatorname{Sym}_G(p'') = \frac{1}{|G|} \sum_{g \in G} g p'' g^{-1}$. Заметим, что, во-первых, оператор p' эквивариантен, так как $hp'h^{-1} = \frac{1}{|G|} \sum_{g \in G} hgp''g^{-1}h^{-1} = \frac{1}{|G|} \sum_{g' \in G} g' p'' g'^{-1} = p'$, во-вторых, $p'_{|U} = \operatorname{Id}_U$, так как $p'(u) = \frac{1}{|G|} \sum_{g \in G} g p'' g^{-1} u = \frac{1}{|G|} \sum_{g \in G} g g^{-1} u = \frac{1}{|G|} \sum_{g \in G} u = u$, и наконец, $\operatorname{Im} p' = U$, так как $\operatorname{Im} g p'' g^{-1} = U$ для всех $g \in G$. Пусть теперь $U' = \operatorname{Ker} p'$. Тогда, во-первых, U' — подпредставление, так как $p'(hu') = hp'(u') = 0$ для всех $h \in G$, $u' \in U'$, во-вторых, $U' \cap U = 0$, так как $p'_{|U} = \operatorname{Id}_U$, и наконец, $\dim U' + \dim U = \dim \operatorname{Ker} p' + \dim \operatorname{Im} p' = \dim V$. Значит $V = U \oplus U'$, что и требовалось. □

Примеры 3.3.

1. Пусть $G = \mathbb{Z}$, а $K = \mathbb{C}$. Легко видеть, что структура представления группы G в пространстве V определяется одним обратимым оператором $A : V \to V$ (а именно, $\rho_A(k)v = A^k v$). При этом представление вполне приводимо $\iff$ оператор A диагонализуем, то есть полупрост.
2. $G = \mathfrak{S}_2$, $\operatorname{char} K = 2$, $V = U^* \otimes U^*$ — пространство билинейных форм на $U = K^{\oplus 2}$ не вполне приводимо.

Замечание 3.4. Приведенный пример дает правильное определение полупростоты оператора над не алгебраически замкнутыми полями. А именно, оператор называется полупростым, если для всякого инвариантного подпространства найдется инвариантное дополнительное подпространство.

Следствие 3.5. *Если группа* G *— конечна, а характеристика поля* K *не делит порядок группы* $|G|$, *то всякое конечномерное представление группы* G *является прямой суммой неприводимых представлений.*

Возникает естественный вопрос об однозначности разложения представления в сумму неприводимых. На самом деле ясно, что однозначности быть не может.

Пример 3.6. Пусть $G = \{1\}$. Тогда представление группы G — это просто векторное пространство. Ясно, что единственное неприводимое представление — это одномерное пространство. При этом всякое пространство размерности > 1 может быть разложено в сумму одномерных далеко не одним способом!

Часть 4. Лемма Шура

В этой части ограничимся рассмотрением конечномерных представлений.

Лемма 4.1. (*i*) *Если U и V — неприводимые представления группы G, а $0 \neq f \in \mathrm{Hom}_G(U,V)$, то f является изоморфизмом.* (*ii*) *Пусть V — неприводимое представление группы G, а $f \in \mathrm{End}_G(V)$. Если поле K алгебраически замкнуто, то $f = \lambda \mathrm{Id}_V$, $\lambda \in K$, то есть $\mathrm{End}_G(V) = K$.*

Доказательство: (*i*) ясно, что $\mathrm{Ker}\, f \subset U$ и $\mathrm{Im}\, f \subset V$ — подпредставления. Если $\mathrm{Ker}\, f = U$, то $f = 0$. Если $\mathrm{Im}\, f = 0$, то также $f = 0$. Значит, в силу неприводимости U и V имеем $\mathrm{Ker}\, f = 0$, $\mathrm{Im}\, f = V$, то есть f инъективно и сюръективно. Значит, f — изоморфизм векторных пространств и существует обратное линейное отображение f^{-1}. Наконец, очевидно, что f^{-1} является G-гомоморфизмом, обратным к f, следовательно f — изоморфизм.

(*ii*) Так как K алгебраически замкнуто, то оператор f имеет собственное значение $\lambda \in K$. Ясно, что оператор $f - \lambda \mathrm{Id}_V$ является G-гомоморфизмом, причем имеет нетривиальное ядро (соответсвующее собственное подпространство), следовательно он равен нулю. Значит, $f = \lambda \mathrm{Id}_V$. □

Замечание 4.2. В случае не алгебраически замкнутого поля K часть (*ii*) леммы Шура заменяется на утверждение, что алгебра $\mathrm{End}_G(V)$ — тело. Доказательство части (*ii*) по сути сводится к проверке того, что над алгебраически замкнутым полем не бывает нетривиальных тел.

Следствие 4.3. (*i*) *Если U и V — неприводимые представления группы G и $U \ncong V$, то $\mathrm{Hom}_G(U,V) = 0$.* (*ii*) *Если U неприводимо, а K алгебраически замкнуто, то $\mathrm{Hom}_G(U^{\oplus m}, U^{\oplus n}) \cong \mathrm{Mat}_{n\times m}(K)$*

Пусть теперь V — вполне приводимое представление группы G, и $V = \oplus V_p$ — его разложение в сумму неприводимых. Пусть, далее $\rho : G \to \mathrm{GL}(U)$ — неприводимое представление группы G, а V_ρ — прямая сумма неприводимых компонент V_p, изоморфных представлению ρ. Ясно, что V_ρ — подпредставление в V и $V = \oplus_\rho V_\rho$ (прямая сумма по всем классам изоморфизма неприводимых представлений).

Лемма 4.4. *Подпредставление $V_\rho \subset V$ не зависит от исходного разложения представления V в сумму неприводимых, а зависит лишь от класса изоморфизма представления ρ.*

Доказательство: пусть $V = \oplus V'_q$ — другое разложение в сумму неприводимых. Рассмотрим отображение $f_{pq} : V'_q \to V \to V_p$ — композицию вложения и проекции, соответствующим разложениям в прямые суммы. Ясно, что f_{pq} — G-гомоморфизм. Значит, по лемме Шура f_{pq} равен нулю, если $V_p \ncong V_q$. Поэтому всякое V'_q, изоморфное представлению ρ, содержится в V_ρ. Значит, $V'_\rho \subset V_\rho$. Аналогично, $V_\rho \subset V'_\rho$, то есть $V_\rho = V'_\rho$. □

Подпредставление V_ρ называется изотипической компонентой неприводимого представления ρ в представлении V. Ясно, что изотипическая компонента раскладывается в прямую сумму нескольких экземпляров представления ρ, причем кратность, $\mathrm{mult}_\rho(V)$, не зависит от разложения.

Следствие 4.5. *Всякое вполне приводимое представление единственным образом раскладывается в сумму изотепических компонент, каждая из которых является однозначно определенной кратностью соответствующего неприводимого представления: $V = \oplus_\rho \rho^{\oplus \mathrm{mult}_\rho(V)}$.*

Пример 4.6. Пространства $S^n V$ и $\Lambda^n V$ — не что иное, как изотипические компоненты тривиального и знакового представления группы $\mathfrak{S}_n$ в $V^{\otimes n}$.

Лемма 4.7. *Пусть V и W — вполне приводимые расслоения, а $f : V \to W$ — G-гомоморфизм. Тогда для любого неприводимого ρ имеем $f(V_\rho) \subset W_\rho$.*

Доказательство: разложим V и W в сумму неприводимых и воспользуемся леммой Шура. □

Обозначив через f_ρ ограничение f на компоненту V_ρ, мы видим, что $f = \oplus_\rho f_\rho$.

Следствие 4.8. *Если V и W — вполне приводимые представления над алгебраически замкнутым полем, то* $\mathrm{Hom}_G(V,W) = \prod_\rho \mathrm{Mat}_{\mathrm{mult}_\rho(W)\times\mathrm{mult}_\rho(V)}(K)$. *В частности,* $\mathrm{mult}_\rho(V) = \dim \mathrm{Hom}_G(\rho, V)$.

Таким образом, задача описания категории конечномерных представлений конечной группы G над алгебраически замкнутым полем, характеристика которого не делит порядок группы, сводится к описанию множества классов изоморфизма неприводимых представлений. Этим мы и займемся в следующий раз.

Лекция 10. Характеры представлений

Часть 1. Характеры

Определение 1.1. Характером представления $\rho : G \to \mathrm{GL}(V)$ называется функция $\chi_\rho : G \to K$, определяемая формулой $\chi_\rho(g) := \operatorname{Tr} \rho(g)$.

Лемма 1.2. *Имеем* (i) $\chi_\rho(1) = \dim \rho$; (ii) $\chi_\rho(ghg^{-1}) = \chi_\rho(h)$ *при всех* $g, h \in G$.

Доказательство: (i) $\chi_\rho(1) = \operatorname{Tr} \rho(1) = \operatorname{Tr} \mathrm{Id}_V = \dim V = \dim \rho$. (ii) Пользуясь тем, что $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$, получаем $\chi_\rho(ghg^{-1}) = \operatorname{Tr} \rho(ghg^{-1}) = \operatorname{Tr} \rho(g)\rho(h)\rho(g)^{-1} = \operatorname{Tr} \rho(g)^{-1}\rho(g)\rho(h) = \operatorname{Tr} \rho(h) = \chi_\rho(h)$. □

Примеры 1.3. 1. Характер тривиального представления: $\chi_1 \equiv 1$.

2. Характер знакового представления: $\chi_\varepsilon(\sigma) = \varepsilon(\sigma)$.

3. Характер регулярного представления: $\chi_{K[G]}(g) = \begin{cases} |G|, & \text{если } g = 1 \\ 0, & \text{иначе} \end{cases}$.

В дальнейшем, для обозначения характера представления $\rho : G \to \mathrm{GL}(V)$ в пространстве V будем использовать также обозначение χ_V.

Лемма 1.4. *Имеем* (i) $\chi_{U \oplus V} = \chi_U + \chi_V$; (ii) $\chi_{U \otimes V} = \chi_U \chi_V$; (iii) $\chi_{V^*}(g) = \chi_V(g^{-1})$.

Доказательство: (i) Очевидно — след прямой суммы операторов равен сумме их следов.

(ii) Аналогично, нам надо показать, что след тензорного произведения операторов равен произведению их следов. Выберем базисы в пространствах U и V и рассмотрим операторы $A \in \mathrm{End}(U)$, $B \in \mathrm{End}(V)$ с матрицами (A_i^j) и (B_k^l) соответственно. Тогда матрица оператора $A \otimes B$ равна $(A_i^j B_k^l)$, а его след — сумме $\sum_{(i,k)=(j,l)} A_i^j B_k^l = \sum_{i,k} A_i^i B_k^k = (\sum_i A_i^i)(\sum_k B_k^k) = \operatorname{Tr} A \operatorname{Tr} B$.

(iii) $\chi_{V^*}(g) = \operatorname{Tr} \rho^*(g) = \operatorname{Tr} \rho(g^{-1})^* = \operatorname{Tr} \rho(g^{-1}) = \chi_V(g^{-1})$. □

Часть 2. Соотношения ортогональности

Характер представления очень полезен по следующим причинам. Во-первых, он легко вычислим. А во-вторых, как мы покажем ниже, в терминах характера можно вычислять важнейшие численные параметры представления с одной небольшой оговоркой. Дело в том, что если характеристика поля равна $p > 0$, то численые параметры вычисляются лишь по модулю p. Таким образом, теряется значительная часть информации. Поэтому, начиная с этого места будем считать, что $\operatorname{char} K = 0$.

Определение 2.1. Функция $f : G \to K$ называется центральной, если $f(ghg^{-1}) = f(h)$ при всех $g, h \in G$.

Обозначим через $C_K(G)$ пространство всех центральных K-значных функций на группе G. Ясно, что характеры представлений являются элементами пространства $C_K(G)$.

Лемма 2.2. $C_K(G)$ — *конечномерное векторное пространство, причем его размерность равна количеству классов сопряженности в группе* G.

Доказательство: всякая центральная функция по определению постоянна на классах сопряженности. □

Рассмотрим K-значную билинейную форму на $C_K(G)$:

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g^{-1}) f_2(g).$$

Лемма 2.3. *Билинейная форма $\langle -,- \rangle$ на $C_K(G)$ симметрична и невырождена.*

Доказательство: подставляя $g^{-1} = h$ и замечая, что отображение $G \to G$, $g \mapsto g^{-1}$ — биекция, получаем $\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g^{-1}) f_2(g) = \frac{1}{|G|} \sum_{h \in G} f_1(h) f_2(h^{-1}) = \langle f_2, f_1 \rangle$. Кроме того, заметим что это отображение переводит класс сопряженности в класс сопряженности, то есть индуцирует некоторую перестановку на множестве классов сопряженности. Выбирая в качестве базиса пространства $C_K(G)$ дельта-функции классов сопряженности, видим, что матрица Грама формы $\langle -,- \rangle$ в этом базисе является матрицей перестановки (умноженной на $\frac{1}{|G|}$), следовательно невырождена. □

Чуть ниже мы докажем, что характеры неприводимых представлений образуют ортогональный базис в пространстве $C_K(G)$. Для этого нам понадобится следующая лемма.

Лемма 2.4. $\frac{1}{|G|} \sum_{g \in G} \chi_V(g) = \dim V^G$.

Доказательство: так как след оператора — линейная функция, то левая часть равенства равна следу оператора Sym_G усреднения по группе. Но, как было показано, оператор Sym_G является проектором на подпространство инвариантов V^G, следовательно его след равен размерности этого пространства. □

Теорема 2.5. (*i*) *Если U и V — неприводимые представления и $U \ncong V$, то $\langle \chi_U, \chi_V \rangle = 0$.*
(*ii*) *Если U — неприводимое представление, а поле K — алгебраически замкнуто, то $\langle \chi_U, \chi_U \rangle = 1$.*

Доказательство: заметим, что $\chi_U(g^{-1})\chi_V(g) = \chi_{U^*}(g)\chi_V(g) = \chi_{U^* \otimes V}(g) = \chi_{\mathrm{Hom}(U,V)}(g)$, значит по предыдуще лемме имеем $\langle \chi_U, \chi_V \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}(U,V)}(g) = \dim \mathrm{Hom}(U,V)^G = \dim \mathrm{Hom}_G(U,V)$. Далее остается применить лемму Шура: если $U \ncong V$, то $\mathrm{Hom}_G(U,V) = 0$, значит $\langle \chi_U, \chi_V \rangle = 0$; если же $V = U$ и $\bar{K} = K$, то $\mathrm{Hom}_G(U,U)$ одномерно, значит $\langle \chi_U, \chi_U \rangle = 1$. □

Замечание 2.6. Если не предполагать алгебраическую замкнутость поля K, то можно лишь сказать, что $\langle \chi_U, \chi_U \rangle = \dim \mathrm{End}_G(U)$. В частности, $\langle \chi_U, \chi_U \rangle$ является целым положительным числом.

Следствие 2.7. *Количество классов изоморфизма неприводимых представлений группы G не превосходит количества ее классов сопряженности.*

Часть 3. Следствия соотношений ортогональности

Сначала опишем ситуацию в случае, когда поле K алгебраически замкнуто.

Следствие 3.1. *Имеем $\langle \chi_V, \chi_V \rangle \in \mathbb{Z}_{>0}$, причем V неприводимо $\iff \langle \chi_V, \chi_V \rangle = 1$.*

Доказательство: из теоремы Машке следует, что V раскладывается в прямую сумму неприводимых. Из леммы 1.4 следует, что $\chi_V = \sum_\rho \mathrm{mult}_\rho(V)\chi_\rho$. Следовательно, $\langle \chi_V, \chi_V \rangle = \sum_\rho \mathrm{mult}_\rho(V)^2$. □

Следствие 3.2. *Если U неприводимо, то $\mathrm{mult}_U(V) = \langle \chi_U, \chi_V \rangle$.*

Доказательство: аналогично, записывая $\chi_V = \sum_\rho \mathrm{mult}_\rho(V)\chi_\rho$ и вычисляя скалярное произведение с χ_U, пользуясь соотношениями ортогональности, получаем искомое равенство. □

Следствие 3.3. *Представления V и W изоморфны $\iff \chi_V = \chi_W$.*

Доказательство: равенство характеров изоморфных представлений очевидно, а если характеры равны, то по предыдущему следствию кратности всех неприводимых представлений в V и W совпадают, следовательно V и W изоморфны. □

Следствие 3.4. *Если U — неприводимо, то $\mathrm{mult}_U(K[G]) = \dim U$.*

Доказательство: согласно предыдущему следствию, нам надо вычислить скалярное произведение χ_U и $\chi_{K[G]}$. Получаем $\langle \chi_U, \chi_{K[G]} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_U(g^{-1})\chi_{K[G]}(g) = \frac{1}{|G|}\chi_U(1)|G| = \chi_U(1) = \dim U$. □

Лемма 3.5. *Характеры неприводимых представлений порождают пространство $C_K(G)$.*

Доказательство: достаточно проверить, что ортогонал ко всем характерам равен нулю. Предположим, что центральная функция φ ортогональна всем характерам. Значит $\sum_{g\in G}\varphi(g^{-1})\chi_\rho(g)=0$ для всех неприводимых ρ. Рассмотрим оператор $c_\varphi=\sum_{g\in G}\varphi(g^{-1})\rho(g)$. Легко видеть, что он коммутирует с действием группы: $c_\varphi\rho(h)=\sum_{g\in G}\varphi(g^{-1})\rho(g)\rho(h)=\sum_{g\in G}\varphi(g^{-1})\rho(h)\rho(h^{-1}gh)=\rho(h)\sum_{g\in G}\varphi((h^{-1}gh)^{-1})\rho(h^{-1}gh)=\rho(h)c_\varphi$. Следовательно, по лемме Шура оператор c_φ действует в представлении ρ умножением на константу. С другой стороны, ясно, что $\operatorname{Tr}c_\varphi=\sum_{g\in G}\varphi(g^{-1})\chi_\rho(g)=0$, значит c_φ действует нулем во всяком неприводимом представлении группы G. Но тогда c_φ действует нулем и в регулярном представлении, однако ясно, что $c_\varphi e_h=\sum_{g\in G}\varphi(g^{-1})e_{gh}$, следовательно $\varphi(g^{-1})=0$ при всех $g\in G$, то есть $\varphi=0$. □

Подытожим вышесказанное.

Теорема 3.6. *Если поле K алгебраически замкнуто, то количество классов изоморфизма неприводимых представлений группы G равно количеству ее классов сопряженности, причем всякое неприводимое представление входит в регулярное представление с кратностью равной размерности. В частности $|G|=\sum_{i=1}^s d_i^2$, где s — количество классов сопряженности, а d_i — размерность i-го неприводимого представления.*

Если не предполагать алгебраическую замкнутость поля K, то $\operatorname{mult}_U(V)=\langle\chi_U,\chi_V\rangle/\dim\operatorname{End}_G(U)$. При этом по-прежнему изоморфность представлений равносильна равенству их характеров. Далее, $\operatorname{mult}_U(K[G])=\dim U/\dim\operatorname{End}_G(U)$, следовательно всякое неприводимое представление является прямым слагаемым регулярного, причем $|G|=\sum_{i=1}^c d_i^2/e_i$, где c — количество классов изоморфизма неприводимых представлений ($c\leqslant s$), d_i — размерность i-го неприводимого представления, а e_i — размерность алгебры его G-эндоморфизмов.

Следствие 3.7. *Если поле K алгебраически замкнуто, а группа G — абелева, то всякое наприводимое представление группы G одномерно, а их количество равно порядку группы.*

Доказательство: в абелевой группе всякий класс сопряженности состоит из одного элемента, следовательно их количество равно порядку группы. Из формулы $|G|=\sum_{i=1}^s d_i^2$ тогда следует, что $d_i^2=1$ для всех i, то есть все неприводимые — одномерны. □

Замечание 3.8. Верно и обратное, если всякое неприводимое представление группы G одномерно, то группа абелева. Действительно, в этом случае все $d_i=1$, следовательно количество классов сопряженности в G равняется $|G|$, значит классы сопряженности состоят из одного элемента, то есть группа G абелева.

Часть 4. Тензорная структура и кольцо Гротендика

Обозначим через $R(G)$ абелеву группу, с образующими $[V]$, где V всевозможные (конечномерные) представления группы G, и соотношениями $[U\oplus V]=[U]+[V]$.

Лемма 4.1. *Группа $R(G)$ — свободная абелева группа ранга c.*

Доказательство: классы неприводимых представлений образуют базис в $R(G)$. □

Лемма 4.2. *Тензорное произведение индуцирует на $R(G)$ структуру коммутативного кольца.*

Доказательство: достаточно заметить, что тензорное произведение представлений ассоциативно, коммутативно и дистрибутивно (по отношению к прямой сумме), а тривиальное представление — единица. □

Кольцо $R(G)$ называется кольцом Гротендика категории конечномерных G-модулей. Ясно, что сопоставляя представлению его характер получаем вложение колец $\chi: R(G)\to C_K(G)$.

Лемма 4.3. *Классы одномерных представлений группы G с операцией $\otimes$ образуют коммутативную подгруппу в мультипликативной группе кольца $R(G)$, которая изоморфна группе $\operatorname{Hom}(G,K^*)$.*

Доказательство: ясно, что если $\dim U=\dim V=1$, то $\dim U\otimes V=1$. Более того, легко видеть, что $V\otimes 1_G\cong V$ для всех V, то есть 1_G — единица. Наконец, заметим, что гомоморфизм вычисления $\mathrm{ev}: V\otimes V^*\to 1_G$ коммутирует с действием группы G, а при $\dim V=1$ является изоморфизмом. Поэтому V^* является обратным элементом к V в группе одномерных представлений. Теперь заметим, что если ρ одномерно, то $\rho\in\operatorname{Hom}(G,\mathrm{GL}(1;K))=\operatorname{Hom}(G,K^*)$. □

Лекция 11. Индукция

Часть 1. Степени неприводимых представлений

Определение 1.1. Алгебраическое число $\alpha \in \overline{\mathbb{Q}}$ называется целым, если оно является корнем многочлена вида $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$, где $a_1, \ldots, a_n \in \mathbb{Z}$.

Лемма 1.2. *Алгебраическое число $\alpha \in \overline{\mathbb{Q}}$ — целое $\iff$ кольцо $\mathbb{Z}[\alpha] \subset \overline{\mathbb{Q}}$ — конечно порожденный $\mathbb{Z}$-модуль.*

Доказательство: $\Longrightarrow$) Если α — целое, то числа $1, \alpha, \ldots, \alpha^{n-1}$ порождают $\mathbb{Z}[\alpha]$ как $\mathbb{Z}$-модуль.
$\Longleftarrow$) Пусть $\mathbb{Z}[\alpha]$ — конечно порожденный $\mathbb{Z}$-модуль, а $\alpha_1, \ldots, \alpha_n$ — его образующие над $\mathbb{Z}$. Тогда имеем $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, где $A = (a_{ij})$ — целочисленная матрица. Заметим, что характеристический многочлен $\chi_A(x)$ матрицы A имеет целые коэффициенты. С другой стороны, по теореме Гамильтона–Кэли, имеем $\chi_A(A) = 0$. Но матрица A — это матрица умножения на α, следовательно, $\chi_A(\alpha) = 0$. □

Замечание 1.3. Аналогично доказывается следующее утверждение. Если R — коммутативное кольцо, являющееся конечно порожденным $\mathbb{Z}$-модулем, то всякий элемент $\alpha \in R$ удовлетворяет полиномиальному уравнению вида $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$, где $a_1, \ldots, a_n \in \mathbb{Z}$.

Теорема 1.4. *Целые алгебраические числа образуют подкольцо в $\overline{\mathbb{Q}}$.*

Доказательство: нам надо проверить, что если α и β — целые, то $\alpha + \beta$ и $\alpha\beta$ — тоже целые. Рассмотрим подкольцо $\mathbb{Z}[\alpha, \beta] \subset \overline{\mathbb{Q}}$. Ясно, что оно является конечно порожденным $\mathbb{Z}$-модулем (набор элементов $(\alpha^i\beta^j)_{0\leqslant i\leqslant m-1, 0\leqslant j\leqslant n-1}$ при подходящих m и n порождает его). Следовательно, подкольца $\mathbb{Z}[\alpha + \beta] \subset \mathbb{Z}[\alpha, \beta]$ и $\mathbb{Z}[\alpha\beta] \subset \mathbb{Z}[\alpha, \beta]$ тоже являются конечно порожденными $\mathbb{Z}$-модулями. □

Лемма 1.5. *Поле $\overline{\mathbb{Q}}$ является полем частных кольца целых алгебраических чисел.*

Доказательство: пусть $\alpha \in \overline{\mathbb{Q}}$ и $\mathrm{Irr}_\alpha^{\mathbb{Q}}(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$. Ясно, что $a_i \in \mathbb{Q}$ при всех i. Пусть m — НОК их знаменателей. Тогда многочлен $\mathrm{Irr}_{m\alpha}^{\mathbb{Q}}(x) = x^n + ma_1 x^{n-1} + \cdots + m^{n-1}a_{n-1}x + m^n a_n$ имеет целые коэффициенты, значит $m\alpha$ — целое алгебраической число, а $\alpha = \frac{m\alpha}{m}$. □

Лемма 1.6. *Рациональное число является целым алгебраическим $\iff$ оно целое.*

Доказательство: пусть $\alpha = r/s$ — корень многочлена $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$. Тогда $r^n + a_1 r^{n-1}s + \cdots + a_{n-1}rs^{n-1} + a_n s^n = 0$. Можно считать, что r и s взаимно просты. Однако, если p — простой делитель числа s, то $p|r^n$, значит $p|r$. Следовательно, $s = \pm 1$ и α — целое. □

Лемма 1.7. *Если χ — характер представления конечной группы G над полем K характеристики 0, то $\chi(g)$ — целое алгебраическое число $\forall g \in G$.*

Доказательство: $\chi(g)$ — след оператора $\rho(g)$, то есть сумма его собственных значений (над полем $\overline{K}$). Однако, $\rho(g)^{|G|} = \rho(g^{|G|}) = \rho(1) = \mathrm{Id}$, поэтому все собственные значения являются корнями из единицы. В частности, они целые алгебраические числа. Следовательно и $\chi(g)$ — целое алгебраическое число. □

Лемма 1.8. *Если V — неприводимое представление конечной группы G над полем $K = \overline{K}$, $\mathrm{char}\, K = 0$, а C — класс сопряженности то $\frac{1}{\dim V}\sum_{g\in C}\chi_V(g)$ — целое алгебраическое число.*

Доказательство: рассмотрим элемент $e_C := \sum_{g\in C} g \in K[G]$. Заметим, что e_C лежит в $Z(\mathbb{Z}[G])$ — центре целочисленного группового кольца. Однако, $Z(\mathbb{Z}[G])$ является $\mathbb{Z}$-подмодулем в $\mathbb{Z}[G]$, следовательно является $\mathbb{Z}$-модулем конечного типа. Значит, e_C удовлетворяет полиномиальному уравнению с целыми коэффициентами. Так как этому же уравению удовлетворяют и собственные числа оператора e_C в любом представлении группы G, то все они целые алгебраические числа. С другой стороны, так как e_C лежит в центре алгебры $K[G]$, то e_C действует в V умножением на некоторое число λ, причем $\lambda = \frac{\mathrm{Tr}\, e_C}{\dim V} = \frac{1}{\dim V}\sum_{g\in C}\chi_V(g)$. Остается заметить, что λ — собственное число для e_C. □

Теорема 1.9. *Если V — неприводимое представление конечной группы G над полем $K = \overline{K}$, $\operatorname{char} K = 0$, то размерность V делит порядок G.*

Доказательство: $\frac{|G|}{\dim V} = \frac{1}{\dim V}\sum_{g\in G}\chi_V(g^{-1})\chi(g) = \sum_C \chi_V(g^{-1})\left(\frac{1}{\dim V}\sum_{g\in C}\chi(g)\right)$ — целое алгебраическое число. Однако, оно рациональное, значит оно целое. □

Часть 2. Ограничение и индукция

Пусть $\rho : G \to \mathrm{GL}(V)$ представление группы G, а $H \subset G$ – подгруппа. Тогда $\rho_{|H} : H \to \mathrm{GL}(V)$ — представление группы H, которое называется ограничением представления ρ на подгруппу H.

Лемма 2.1. *Ограничение является функтором из категории Rep_G в категорию Rep_H.*

Функтор ограничения обозначается Res^G_H.

Пусть теперь наоборот, $H \subset G$ – подгруппа, а U — представление группы H. Выберем представителей $1 = g_1, \dots, g_k$ в левых классах смежности G по H и рассмотрим пространство $K[G/H]$ с базисом $\{e_i\}_{i=1}^k$, занумерованном классами смежности. Далее, рассмотрим пространство $K[G/H]\otimes U = \bigoplus_{i=1}^k e_i\otimes U$ и введем в нем структуру G-модуля следующим образом. Для всякого $g \in G$ и $1 \leqslant i \leqslant k$ определим число $1 \leqslant s(g,i) \leqslant k$ как номер класса смежности элемента $g\cdot g_i \in G$, и определим элемент $h(g,i) \in H$ формулой $g\cdot g_i = g_{s(g,i)}\cdot h(g,i)$. Положим теперь $g(e_i \otimes u) = e_{s(g,i)} \otimes h(g,i)u$.

Ясно, что $s(g'g,i) = s(g', s(g,i))$, $h(g'g,i) = h(g', s(g,i))h(g,i)$. Отсюда сразу следует, что $K[G/H] \otimes U$ — представление группы G. Более того, ясно, что $s(h,1) = 1$, $h(h,1) = h$, поэтому естественное вложение $f_U : U \to K[G/H] \otimes U$, $u \mapsto e_1 \otimes u$, является морфизмом H-модулей. Покажем, что оно обладает следующим универсальным свойством:

> *если V — представление группы G, а $f : U \to V$ — морфизм H-модулей, то существует единственный морфизм G-модулей $\tilde f : K[G/H] \otimes U \to V$, такой что $\tilde f \circ f_U = f$.*

Действительно, если $\tilde f$ — такой морфизм, то $\tilde f(e_i \otimes u) = \tilde f(g_i(e_1 \otimes u)) = g_i\tilde f(f_U(u)) = g_i f(u)$, поэтому $\tilde f$ — единственный. С другой стороны, определяя $\tilde f$ формулой $\tilde f(\sum e_i \otimes u_i) = \sum g_i f(u_i)$, получаем морфизм G-модулей: $\tilde f(g\sum e_i \otimes u_i) = \tilde f(\sum e_{s(g,i)} \otimes h(g,i)u_i) = \sum g_{s(g,i)} f(h(g,i)u_i) = \sum g_{s(g,i)}h(g,i)f(u_i) = \sum (g\cdot g_i)f(u_i) = g\sum g_i f(u_i) = g\tilde f(\sum e_i \otimes u_i)$.

Построенное нами представление группы G называется представлением, индуцированным с представления U группы H, и обозначается $\mathrm{Ind}^G_H(U)$, а доказанное нами универсальное свойство может быть переформулировано следующим образом:

Теорема 2.2. *Если U и V — представления групп H и G, то $\mathrm{Hom}_H(U, \mathrm{Res}^G_H(V)) = \mathrm{Hom}_G(\mathrm{Ind}^G_H(U), V)$.*

Следствие 2.3. *Индуцированное представление не зависит от выбора представителей классов сопряженности.*

Пример 2.4. Легко видеть, что $\mathrm{Ind}^G_{\{1\}} K \cong K[G]$ — представление группы G, индуцированное с тривиального представления единичной подгруппы является регулярным представлением. Обобщением этого примера является изоморфизм $\mathrm{Ind}^G_H K[H] \cong K[G]$.

Следствие 2.5. *Индукция является функтором из категории Rep_H в категорию Rep_G.*

Доказательство: пусть $f : U \to U'$ — морфизм H-модулей. Определим $\mathrm{Ind}^G_H(f)$ как морфизм G-модулей $\mathrm{Ind}^G_H U \to \mathrm{Ind}^G_H U'$, соответствующий композиции $U \xrightarrow{f} U' \xrightarrow{f_{U'}} \mathrm{Res}^G_H \mathrm{Ind}^G_H(U')$. □

Замечание 2.6. Свойство $\mathrm{Hom}_H(U, \mathrm{Res}^G_H(V)) = \mathrm{Hom}_G(\mathrm{Ind}^G_H(U), V)$ называется сопряженностью этих функторов. Оно аналогично свойству сопряженности операторов относительно билинейной формы. Пары сопряженных функторов часто встречаются в математике. Например, функтор $\mathcal{S}ets \to \mathcal{G}r$, сопоставляющий множеству порожденную им свободную группу, сопряжен к забывающему структуру группы функтору $\mathcal{G}r \to \mathcal{S}ets$.

Лемма 2.7. *Имеем* $\chi_{\mathrm{Ind}^G_H U}(g) = \dfrac{1}{|H|}\displaystyle\sum_{\substack{s\in G\\ s^{-1}gs\in H}} \chi_U(s^{-1}gs)$.

Доказательство: выберем базис $\{ u_j \}$ в пространстве U и рассмотрим базис $\{ e_i \otimes u_j \}$ пространства $\mathrm{Ind}_H^G U$. Ясно, что матрица оператора g в этом базисе является блочно-перестановочной, соответствующей перестановке $i \mapsto s(g,i)$. Значит ее след равен сумме следов блоков, таких что $s(g,i) = i$, то есть $g \cdot g_i = g_i \cdot h$, то есть $g_i^{-1} \cdot g \cdot g_i \in H$. Значит, $\chi(g) = \sum_{i \mid g_i^{-1} g g_i \in H} \chi_U(g_i^{-1} g g_i)$. Заметим, теперь, что если $s = g_i h$, то $s^{-1} g s = h^{-1} g_i^{-1} g g_i h$. В частности, $s^{-1} g s \in H \iff g_i^{-1} g g_i \in H$, причем $\chi_U(s^{-1} g s) = \chi_U(g_i^{-1} g g_i)$, откуда и получаем искомую формулу. □

Замечание 2.8. Поведение характера при ограничении еще проще. Легко видеть, что $\chi_{\mathrm{Res}_H^G V}(h) = \chi_V(h)$.

Индукция помогает строить представления.

Пример 2.9. Пусть $G = \mathfrak{S}_3$, $H = A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Рассмотрим любое нетривиальное линейное представление группы H. Вычисляя характер, видим, что индуцированное представление является неприводимым двумерным представлением группы $\mathfrak{S}_3$.

Часть 3. Дополнения

Пусть $G = G_1 \times G_2$, а V_1 и V_2 — представления групп G_1 и G_2 соответственно. В тензорном произведении $V_1 \otimes V_2$ зададим структуру представления группы G формулой $(g_1, g_2)(v_1 \otimes v_2) = (g_1 v_1) \otimes (g_2 v_2)$.

Лемма 3.1. *Пусть V_1 и V_1' — неприводимые G_1-модули, а V_2 и V_2' — неприводимые G_2-модули.*
(i) $V_1 \otimes V_2 \cong V_1' \otimes V_2' \iff V_1 \cong V_1'$, $V_2 \cong V_2'$. (ii) Если $\overline{K} = K$, то $V_1 \otimes V_2$ неприводимо над $G_1 \times G_2$.

Доказательство: заметим, что $\chi_{V_1 \otimes V_2}(g_1, g_2) = \chi_{V_1}(g_1)\chi_{V_2}(g_2)$.
(i) Имеем очевидное равенство $\langle \chi_{V_1 \otimes V_2}, \chi_{V_1' \otimes V_2'} \rangle = \frac{1}{|G_1 \times G_2|} \sum_{(g_1,g_2) \in G_1 \times G_2} \chi_{V_1}(g_1^{-1}) \chi_{V_2}(g_2^{-1}) \chi_{V_1'}(g_1) \chi_{V_2'}(g_2) = \left(\frac{1}{|G_1|} \sum_{g_1 \in G_1} \chi_{V_1}(g_1^{-1}) \chi_{V_1'}(g_1) \right) \left(\frac{1}{|G_2|} \sum_{g_2 \in G_2} \chi_{V_2}(g_2^{-1}) \chi_{V_2'}(g_2) \right) = \langle \chi_{V_1}, \chi_{V_1'} \rangle \langle \chi_{V_2}, \chi_{V_2'} \rangle$. Если теперь при $i = 1$ или $i = 2$ имеем $V_i \ncong V_i'$, то $\langle \chi_{V_i}, \chi_{V_i'} \rangle = 0$, значит $\langle \chi_{V_1 \otimes V_2}, \chi_{V_1' \otimes V_2'} \rangle = 0$ и $V_1 \otimes V_2 \ncong V_1' \otimes V_2'$.
(ii) Предыдущее равенство показывает, что $\langle \chi_{V_1 \otimes V_2}, \chi_{V_1 \otimes V_2} \rangle = \langle \chi_{V_1}, \chi_{V_1} \rangle \langle \chi_{V_2}, \chi_{V_2} \rangle = 1$. □

Замечание 3.2. Над незамкнутым полем утверждение *(ii)* предыдущей леммы вообще говоря неверно. Например, если $K = \mathbb{R}$, $G_1 = \mathbb{Z}/3\mathbb{Z}$, $G_2 = \mathbb{Z}/5\mathbb{Z}$, а V_1 и V_2 — двумерные неприводимые представления.

Лемма 3.3. *Имеем изоморфизм $(G_1 \times G_2)$-модулей $K[G_1 \times G_2] \cong K[G_1] \otimes K[G_2]$.*

Доказательство: отображение $e_{(g_1,g_2)} \mapsto e_{g_1} \otimes e_{g_2}$ является искомым изоморфизмом. □

Теорема 3.4. *Если $\overline{K} = K$, то всякое неприводимое представление группы $G_1 \times G_2$ однозначно представляется в виде $V_1 \otimes V_2$, где V_1 и V_2 — неприводимые представления групп G_1 и G_2.*

Доказательство: нам осталось проверить, что всякое неприводимое представление группы $G_1 \otimes G_2$ имеет указанный вид. Действительно, $K[G_1 \times G_2] = K[G_1] \otimes K[G_2] = (\oplus V_{1,i}) \otimes (\oplus V_{2,j}) = \oplus (V_{1,i} \otimes V_{2,j})$.
Еще одно доказательство получается, если вычислить сумму квадратов размерностей представлений вида $V_{1,i} \otimes V_{2,j}$: имеем $\sum_{i,j} (d_{1,i} d_{2,j})^2 = (\sum_i d_{1,i}^2)(\sum_j d_{2,j}^2) = |G_1||G_2| = |G_1 \times G_2|$. □

Замечание 3.5. Над незамкнутым полем утверждение теоремы вообще говоря неверно. Можно утверждать лишь то, что всякое неприводимое представление группы $G_1 \times G_2$ является прямым слагаемым в представлении вида $V_1 \otimes V_2$.

Семестр III (Осень 2003)

Программа

На зачете каждому студенту будет предлагаться по одному вопросу на темы «группы, коммутативная алгебра, некоммутативные кольца и модули, когомологии». После каждого вопроса указано примерное предполагаемое содержание ответа (темы, изучавшиеся на лекциях (номер лекции указан римскими цифрами), и задачи, изучавшиеся на семинарах (указана дата выдачи листка с задачами)). Знак $*$ у номера задачи означает, что на зачете может быть спрошена часть этой задачи.

- Группы.
  1. Теорема Жордана–Гельдера для групп. — (I) 1.1–1.7.
  2. Разрешимые и нильпотентные группы. — (I) 2.1–2.9, (08c) 2, 6, 7.
  3. Силовские подгруппы. — (I) 3.1–3.3, (08c) 3, 4*.
  4. Расширения групп. — (III) 3.1–3.3, (22c) 5, 6, 10*.
  5. Абелевы расширения. — (III) 3.4–3.5, (22c) 7–9, (08c) 5b.
  6. Когомологии групп. — (II) 3.1–3.5, (III) 1.1–1.3, (15c) 7, (22c) 1.
  7. Свойства когомологий групп. — (III) 2.1–2.4, (22c) 2, (13o) 12.
  8. Когомологии циклических групп. — (III) 2.5–2.6, (22c) 3, 4a.
  9. Когомологии Галуа. — (X) 3.3–3.4, (10н) 7, 9.
- Коммутативная алгебра.
  1. Идеалы. — (IV) 1.1–1.3, (29c) 1–4, 8.
  2. Радикалы. — (IV) 2.1–2.9 (29c) 5, 9.
  3. Аффинные алгебраические многообразия. — (IV) 3.1–3.3, 3.5–3.11 (29c) 10.
  4. Морфизмы алгебраических многообразий. — (IV) 3.12, 3.13.
  5. Нетеровы модули. — (V) 1.1–1.6, (06o) 1, 10a.
  6. Нетеровы кольца. — (V) 1.7–1.11, 2.1–2.5 (06o) 11, 5a.
  7. Артиновость. — (06o) 2–4, 5bcde, 6, 10b.
  8. Теорема Гильберта о нулях. — (V) 3.1–3.6.
  9. Целые расширения колец. — (VII) 1.1–1.9, (20o) 2, 4, 6a, 8.
  10. Конечные морфизмы. — (VII) 2.1–2.6.
  11. Лемма Нетер о нормализации. — (VII) 4.1–4.3, (20o) 7*.
  12. Кольцо инвариантов. — (VIII) 1.1–1.6.
  13. Фактормногообразия. — (VIII) 1.7–1.9, 2.4, (27o) 1–3.
  14. Симметрические многочлены. — (VIII) 2.1–2.4, (27o) 4–6.
  15. Результант и дискриминант. — (VIII) 3.1–3.4, (27o) 7.
- Некоммутативные кольца и модули.

1. Теорема Жордана–Гельдера для модулей. — (08о) 7, 8, (03н) 4.
2. Точность функтора Hom. — (VI) 1.1–1.7, (13о) 1, 2ab.
3. Определение функтора Ext. — (VI) 2.1–2.4.
4. Свойства функтора Ext. — (VI) 2.5–2.7, (13о) 2c, 3h, 8.
5. Расширения модулей. — (VI) 3.1–3.2, (13о) 7.
6. Тензорное произведение и функтор Tor. — (VI) 4.1–4.2, (13о) 10–12.
7. Полупростые модули. — (IX) 1.1–1.12, (03н) 4, 5.
8. Полупростые кольца. — (IX) 2.1–2.9, (X) 1.9*, (03н) 7.
9. Простые кольца. — (IX) 3.1–3.8, (X) 1.10*.
10. Радикал Джекобсона. — (X) 1.1–1.10, (10н) 1, (03н) 8, 9.
11. Алгебра матриц. — (IX) 3.4, (X) 2.3, 3.1, (03н) 6.
12. Тела. — (X) 2.1–2.2, 3.4, (03н) 1, 2, (10н) 8.
13. Центральные простые алгебры. — (X) 2.5–2.8.
14. Группа Брауэра. (X) 3.2–3.4, (10н) 2*–6*, 7.

- Когомологии.

1. Комплексы. — (II) 1.1–1.10, (15c) 1, 2, 3abc, 4.
2. Лемма о змее. — (II) 2.1–2.6, (15c) 1, 2, 3abc, 4.
3. Цилиндр и конус морфизма. — (13о) 4–6.
4. Когомологии групп. — (II) 3.1–3.5, (III) 1.1–1.3, (15c) 7, (22c) 1.
5. Точность функтора Hom. — (VI) 1.1–1.7, (13о) 1, 2ab.
6. Определение функтора Ext. — (VI) 2.1–2.4.
7. Свойства функтора Ext. — (VI) 2.5–2.7, (13о) 2c, 3h, 8.
8. Тензорное произведение и функтор Tor. — (VI) 4.1–4.2, (13о) 10–12.

Лекция 1. Группы

Часть 1. Теорема Жордана–Гельдера

Определение 1.1. Группа G называется простой, если она не имеет нетривиальных нормальных подгрупп.

Примеры 1.2. 1. Коммутативная группа G проста $\iff G = \mathbb{Z}/p\mathbb{Z}$, где p — простое;

2. Знакопеременная группа A_n проста при $n = 2$ и $n \geqslant 5$.

Определение 1.3. Башня подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$, называется простой, если $\forall s \leqslant m$ группа G_s нормальна в G_{s-1} и группа G_{s-1}/G_s проста.

Определение 1.4. Одна башня подгрупп называется уплотнением другой башни, если последовательность подгрупп из второй башни является подпоследовательностью последовательности подгрупп первой башни.

Лемма 1.5. *Всякая нормальная башня конечной группы может быть уплотнена до простой башни.*

Доказательство: Рассмотрим нормальную башню с максимальным количеством нетривиальных факторов, являющуюся уплотнением исходной. Если бы один из факторов G_{s-1}/G_s в этой башне не являлся простой группой, то башню можно было бы уплотнить следующим образом. Выберем нетривиальную нормальную подгруппу $H \lhd G_{s-1}/G_s$ и положим $G'_i = G_i$ при $i \leqslant s-1$, $G'_i = G_{i-1}$ при $i \geqslant s+1$ и обозначим через G'_s прообраз подгруппы H в G_{s-1} относительно канонического эпиморфизма $G_{s-1} \to G_{s-1}/G_s$. Ясно, что новая башня нормальна, является уплотнением предыдущей, и имеет больше нетривиальных факторов, что противоречит выбору предыдущей башни. Следовательно, предыдущая башня являлась простой. □

Возникает вопрос, насколько единственна простая башня данной группы. Ясно, что ответ отрицательный: например, $\mathbb{Z}/6\mathbb{Z} \supset 2\mathbb{Z}/6\mathbb{Z} \supset 1$ и $\mathbb{Z}/6\mathbb{Z} \supset 3\mathbb{Z}/6\mathbb{Z} \supset 1$ — различные простые башни группы $\mathbb{Z}/6\mathbb{Z}$. Однако видно, что хоть башни и различны, но множества факторгрупп, встречающихся в них, совпадают.

Теорема 1.6. *Если $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ и $G = G'_0 \supset G'_1 \supset \cdots \supset G'_{n-1} \supset G'_n = 1$ — простые башни группы G, в которых все включения строгие, то $m = n$ и последовательности их факторов отличаются перестановкой.*

Начнем с леммы.

Лемма 1.7. *Пусть $G_2 \lhd G_1 \subset G$ и $G'_2 \lhd G'_1 \subset G$. Тогда* $\dfrac{G_2(G_1 \cap G'_1)}{G_2(G_1 \cap G'_2)} \cong \dfrac{(G_1 \cap G'_1)G'_2}{(G_2 \cap G'_1)G'_2}$.

Доказательство: рассмотрим сначала левую дробь. Ясно, что $G_1 \cap G'_2 \subset G_1 \cap G'_1 \subset G_1 \subset N_{G_2}$, поэтому произведения групп в ее числителе и знаменателе являются подгруппами в G. Кроме того, $(g_2 g_{11})(h_2 g_{12})(g_2 g_{11})^{-1} = g_2(g_{11} h_2 g_{11}^{-1})(g_{11} g_{12} g_{11}^{-1})g_2 \in G_2 G_2(G_1 \cap G'_2)G_2 = G_2(G_1 \cap G'_2)$, где $g_{11} \in G_1 \cap G'_1$, $g_{12} \in G_1 \cap G'_2$ и $g_2, h_2 \in G_2$, поэтому знаменатель является нормальной подгруппой в числителе и левая факторгруппа имеет смысл. Рассмотрим теперь композицию гомоморфизмов

$$f : G_1 \cap G'_1 \to G_2(G_1 \cap G'_1) \to \frac{G_2(G_1 \cap G'_1)}{G_2(G_1 \cap G'_2)}.$$

Так как $G_2(G_1 \cap G'_2)(G_1 \cap G'_1) = G_2(G_1 \cap G'_1)$, то f сюръективен. Далее, $\operatorname{Ker} f = (G_1 \cap G'_1) \cap G_2(G_1 \cap G'_2)$. Покажем, что

$$(G_1 \cap G'_1) \cap G_2(G_1 \cap G'_2) = (G_2 \cap G'_1)(G_1 \cap G'_2).$$

Действительно, легко видеть, что каждый из сомножителей правой части лежит в каждом из сомножителей левой части, откуда получаем включение $\supset$. Возьмем теперь произвольный элемент в левой части. Его

можно записать в виде g_2g_{12}, где $g_2 \in G_2$, $g_{12} \in G_1 \cap G_2'$, причем $g_2g_{12} \in G_1 \cap G_1' \subset G_1'$. Следовательно, $g_2 = (g_2g_{12})g_{12}^{-1} \in G_1'(G_1 \cap G_2') \subset G_1'G_2' \subset G_1'$, значит $g_2 \in G_2 \cap G_1'$ и $g_2g_{12} \in (G_2 \cap G_1')(G_1 \cap G_2')$. Тем самым доказано включение $\subset$, а стало быть и равенство.

Получаем $\dfrac{G_2(G_1 \cap G_1')}{G_2(G_1 \cap G_2')} \cong \dfrac{G_1 \cap G_1'}{(G_2 \cap G_1')(G_1 \cap G_2')}$. Аналогично $\dfrac{(G_1 \cap G_1')G_2'}{(G_2 \cap G_1')G_2'} \cong \dfrac{G_1 \cap G_1'}{(G_1 \cap G_2')(G_2 \cap G_1')}$. Остается заметить, что $G_1 \cap G_2' \subset G_1 \cap G_1' \subset N_{G_2} \cap N_{G_1'} \subset N_{G_2 \cap G_1'}$, поэтому $(G_1 \cap G_2')(G_2 \cap G_1') \cong (G_2 \cap G_1')(G_1 \cap G_2')$. □

Доказательство теоремы: положив $G_{ij} := G_{i+1}(G_i \cap G_j')$, получаем уплотнение $G = G_0 = G_{00} \supset G_{01} \supset \cdots \supset G_{0n} = G_1 = G_{10} \supset G_{11} \supset \cdots \supset G_{m-1,n} = 1$ первой башни. Аналогично, положив $G_{ij}' := (G_j \cap G_i')G_{i+1}'$, получаем уплотнение $G = G_0' = G_{00}' \supset G_{01}' \supset \cdots \supset G_{0m}' = G_1' = G_{10}' \supset G_{11}' \supset \cdots \supset G_{n-1,m}' = 1$ второй башни. Из леммы следует, что

$$\frac{G_{ij}}{G_{i,j+1}} = \frac{G_{i+1}(G_j' \cap G_i)}{G_{i+1}(G_{j+1}' \cap G_i)} \cong \frac{(G_j \cap G_i')G_{i+1}'}{(G_{j+1} \cap G_i')G_{i+1}'} = \frac{G_{ij}'}{G_{i,j+1}'},$$

следовательно факторы в этих башнях попарно изоморфны. Остается заметить, что так как исходные башни были простыми, то наборы факторов в исходных башнях и их уплотнениях совпадают. □

Простая башня группы также называется рядом Жордана–Гельдера или композиционным рядом.

Часть 2. Разрешимые и нильпотентные группы

Напомним, что группа G называется разрешимой, если она обладает абелевой башней подгрупп, то есть башней $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$, в которой $\forall s \leqslant m\ G_s \lhd G_{s-1}$ и группа G_{s-1}/G_s абелева. Иначе говоря, группа разрешима, если все простые факторы в ее ряде Жордана–Гельдера коммутативны.

Пусть G — произвольная группа, а $H_1, H_2 \subset G$ — ее подгруппы. Обозначим через $[H_1, H_2]$ подгруппу в G, порожденную всеми коммутаторами $[h_1, h_2] := h_1h_2h_1^{-1}h_2^{-1}$, где $h_1 \in H_1$, $h_2 \in H_2$. В частности, группа $[G, G]$ называется коммутантом группы G и обозначается G'.

Лемма 2.1. *Если подгруппы H_1 и H_2 нормальны в G, то подгруппа $[H_1, H_2] \subset G$ тоже нормальна.*

Доказательство: $g[h_1, h_2]g^{-1} = gh_1h_2h_1^{-1}h_2^{-1}g^{-1} = (gh_1g^{-1})(gh_2g^{-1})(gh_1^{-1}g^{-1})(gh_1^{-1}g^{-1}) = [gh_1g^{-1}, gh_2g^{-1}]$. □

Лемма 2.2. *Коммутант всякой группы G является нормальной подгруппой, а факторгруппа G/G' абелева. Более того, если $f : G \to A$ — гомоморфизм группы G в абелеву группу A, то $G' \subset \operatorname{Ker} f$.*

Доказательство: во-первых, коммутант нормален в силу предыдущей леммы. Во-вторых, ясно что в факторгруппе G/G' всякий коммутатор равен 1, значит группа G/G' — абелева. Наконец, если A — произвольная абелева группа, а $f : G \to A$ — гомоморфизм, то $f([g_1, g_2]) = f(g_1g_2g_1^{-1}g_2^{-1}) = f(g_1)f(g_2)f(g_1)^{-1}f(g_2)^{-1} = [f(g_1), f(g_2)] = 1$, значит $G' \subset \operatorname{Ker} f$. □

Пусть теперь G — произвольная группа и рассмотрим следующую башню ее подгрупп: $G^{(0)} = G$, $G^{(1)} = [G, G] = G'$, …, $G^{(s)} = [G^{(s-1)}, G^{(s-1)}] = (G^{(s-1)})'$.

Теорема 2.3. *Группа G разрешима $\iff G^{(s)} = 1$ для некоторого s.*

Доказательство: Из предыдущей леммы следует, что башня из коммутантов является абелевой башней, откуда вытекает ($\Longleftarrow$). Пусть теперь $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ — произвольная абелева башня. Покажем, что $G^{(s)} \subset G_s$ для всех s. Воспользуемся индукцией по s. Случай $s = 0$ очевиден. Теперь предположим, что $G^{(s-1)} \subset G_{s-1}$ и рассмотрим композицию гомоморфизмов $G^{(s-1)} \to G_{s-1} \to G_{s-1}/G_s$. Так как G_{s-1}/G_s — абелева группа, то $G^{(s)}$ лежит в ядре композиции, следовательно $G^{(s)} \subset G_s$. □

Определение 2.4. Башня подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ называется центральным рядом, если $\forall s \leqslant m$ группа G_s нормальна в G, и G_{s-1}/G_s лежит в центре группы G/G_s.

Определение 2.5. Группа G называется нильпотентной, если она обладает конечным центральным рядом.

Примеры 2.6. 1. Коммутативная группа нильпотентна;

2. если G — p-группа (т.е. $|G| = p^n$), то G — нильпотентна (доказывается индукцией по n, используя тот факт, что центр p-группы всегда нетривиален).

Определение 2.7. Последовательность групп $Z_0G = G$, $Z_1G = [G, G]$, ..., $Z_sG = [Z_{s-1}G, G]$ называется нижним центральным рядом группы G.

Последовательность групп $Z^0G = 1$, $Z^1G = Z(G)$, $Z^sG = \phi_{s-1}^{-1}(Z(G/Z^{s-1}G))$, где $\phi_{s-1} : G \to G/Z^{s-1}G$ — канонический эпиморфизм, называется верхним центральным рядом группы G.

Лемма 2.8. *Построенные ряды являются центральными.*

Доказательство: начнем с нижнего центрального ряда. Во-первых, ясно что Z_sG — подгруппа в G, порожденная элементами вида $[\dots[[g_1, g_2], g_3], \dots, g_s]$, следовательно $Z_sG \subset Z_{s-1}G$. Во-вторых, из леммы 2.1 следует, что группа Z_sG нормальна в G. Наконец, коммутатор любого элемента из $Z_{s-1}G$ с любым элементом из G лежит в Z_sG, поэтому группа $Z_{s-1}G/Z_sG$ содержится в центре группы G/Z_sG. Значит нижний центральный ряд действительно является центральным.

Что касается верхнего центрального ряда, то здесь надо проверить лишь то, что $Z^sG \lhd G$. Воспользуемся индукцией. Случай $s = 0$ очевиден. Предположим теперь, что $Z^{s-1}G \lhd G$ и пусть $g \in G$, $h \in Z^sG$. Тогда, так как $\phi_{s-1}(h)$ лежит в центре группы $G/Z^{s-1}G$, то $\phi_{s-1}(ghg^{-1}) = \phi_{s-1}(g)\phi_{s-1}(h)\phi_{s-1}(g)^{-1} = \phi_{s-1}(h)$, значит $\phi_{s-1}(ghg^{-1})$ тоже лежит в центре группы $G/Z^{s-1}G$, следовательно $ghg^{-1} \in Z^sG$ и $Z^sG \lhd G$. □

Будем говорить, что верхний (нижний) центральный ряд группы G обрывается, если для некоторого s имеем $Z^sG = G$ (соотв. $Z_sG = 1$). Минимальное такое s называется длиной соответствующего центрального ряда.

Теорема 2.9. *Следующие условия эквивалентны: (i) группа G нильпотентна; (ii) верхний центральный ряд группы G обрывается; (iii) нижний центральный ряд группы G обрывается.*

Часть 3. Силовские подгруппы

Пусть p — простое число. Группа H называется p-группой, если ее порядок есть степень числа p. Пусть теперь G — конечная группа. Подгруппа $H \subset G$ называется силовской p-подгруппой, если H — p-группа и ее индекс не делится на p. Иначе говоря, если $|G| = p^km$ и $(p, m) = 1$, то H — силовская, если $|H| = p^k$.

Теорема 3.1. *Всякая конечная группа G имеет силовскую p-подгруппу для любого p.*

Доказательство: индукция по $n = |G|$. Если $p \not| n$, то $H = 1$ и доказывать нечего. Пусть $p|n$. По формуле классов имеем $n = (Z : 1) + \sum_{x \in G \setminus Z}(G : G_x)$, значит, либо $p|(Z : 1)$, либо найдется $x \in G$, такое что $p \not|(G : G_x)$. Во втором случае имеем $|G_x| < |G|$, значит, по предположению индукции G_x имеет силовскую p-подгруппу, которая будет силовской и в G. В первом же случае выберем в абелевой группе Z подгруппу Z' порядка p и рассмотрим $G' = G/Z'$ (Z' нормальна, так как лежит в центре). Если $H' \subset G'$ — силовская p-подгруппа, то ее прообраз в G тоже является силовской p-подгруппой. □

Теорема 3.2. *(i) Всякая p-подгруппа $H \subset G$ содержится в силовской p-подгруппе. (ii) Все силовские p-подгруппы в G сопряжены. (iii) Количество силовских p-подгрупп в G равно 1 по модулю p.*

Доказательство: рассмотрим действие группы G сопряжениями на множестве всех своих p-подгрупп.

(*i*) Пусть $H \subset G$ — p-подгруппа, P — силовская p-подгруппа, а S — орбита P под действием G. Тогда $|S| = (G : N_P)$, где N_P — нормализатор P. Но ясно, что $P \subset N_P$, поэтому $|S|$ взаимно прост с p. Рассмотрим теперь действие H на S. Порядок S равен сумме длин орбит. С другой стороны, всякая орбита группы H имеет порядок равный p^s, следовательно, найдется орбита порядка 1. Пусть она состоит из группы P'. Тогда $H \subset N_{P'}$, следовательно, $HP' \subset G$ — подгруппа и, так как $HP'/P' \cong H/(H \cap P')$, то HP' является p-группой. Но так как $P' \subset HP'$ и P' силовская, то $HP' = P'$, значит, $H \subset P'$.

(*ii*) Заметим, что в (*i*) мы доказали даже более сильное утверждение. А именно, если H — p-подгруппа, а P — силовская p-подгруппа, то H лежит в силовской подгруппе, сопряженной к P. Если H — сама силовская, то получаем, что H и P сопряжены.

(*iii*) Рассмотрим действие силовской группы P на множестве всех силовских групп. Длина любой орбиты — это степень p, причем орбита группы P' состоит из одной точки $\iff P \subset N_{P'}$, но как показано в (*i*) из этого следует $P' = P$. Таким образом, длина всех орбит, кроме орбиты $\{P\}$ делится на p. □

Замечание 3.3. Так как множество всех силовских p-подгрупп — орбита группы G, то их количество равно индексу нормализатора силовской p-подгруппы P, следовательно делит $(G : P) = |G|/p^n$.

Лекция 2. Гомологии

Часть 1. Комплексы

Определение 1.1. Комплексом векторных пространств называется (конечная или бесконечная) последовательность векторных пространств и линейных отображений

$$\dots \xrightarrow{d^{i-1}} C^i \xrightarrow{d^i} C^{i+1} \xrightarrow{d^{i+1}} C^{i+2} \xrightarrow{d^{i+2}} \dots, \qquad \text{в которой } \boxed{d^{i+1} \circ d^i = 0} \text{ для всех } i \in \mathbb{Z}.$$

Пространство C^i называется i-ым членом комплекса $(C^\bullet, d^\bullet)$, а гомоморфизм d^i — i-ым дифференциалом.

Замечание 1.2. Аналогично определяется комплекс абелевых групп, модулей над фиксированным кольцом, и т.д. Кроме того, заменяя условие $d^{i+1} \circ d^i = 0$ условием $d^{i+1} \circ d^i = 1$ можно определить комплекс групп.

Замечание 1.3. Можно также сказать, что комплекс — это векторное пространство $C^\bullet$

- $\mathbb{Z}$-градуированное, то есть разложенное в прямую сумму $C^\bullet = \bigoplus_{i\in\mathbb{Z}} C^i$,
- снабженное дифференциалом $d : C^\bullet \to C^\bullet$, повышающим градуировку на единицу, т.е. $d(C^i) \subset C^{i+1}$,
- с условием $\boxed{d \circ d = 0}$.

Такие комплексы называют когомологическими или коцепными. Помимо них используются и гомологические или цепными комплексы, которые отличаются тем, что в них дифференциал понижает градуировку (градуировка в гомологических комплексах обозначается нижним индексом).

Примеры 1.4.

1. Пусть X — топологическое пространство, а $C_p(X)$ — группа сингулярных p-цепей (свободная абелева группа, порожденная множеством всех непрерывных отображений из p-мерного стандартного симплекса Δ^p в X), а $d = \partial$ — отображение взятия границы (p-мерному симплексу сопоставляется знакопеременная сумма его $(p-1)$-мерных граней). Тогда $(C_\bullet(X), \partial)$ — (гомологический) комплекс абелевых групп, который называется комплексом сингулярных цепей пространства X.

2. Пусть $C^p(X) := C_p(X)^* = \mathrm{Hom}(C_p(X), \mathbb{Z})$ — группа сингулярных p-коцепей, а $d = \partial^*$ — отображение кограницы. Тогда $(C^\bullet(X), \partial^*)$ — (когомологический) комплекс абелевых групп, который называется комплексом сингулярных коцепей пространства X.

3. Пусть X — гладкое многообразие, $\Omega^p X$ — пространство гладких дифференциальных p-форм на X, а $d^p : \Omega^p X \to \Omega^{p+1} X$ — внешний дифференциал. Тогда $(\Omega^\bullet X, d^\bullet)$ — комплекс векторных пространств, который называется комплексом де Рама.

Определение 1.5. Пусть $(C^\bullet, d^\bullet)$ — комплекс векторных пространств. Подпространства $Z^i = \mathrm{Ker}\, d^i \subset C^i$ и $B^i = \mathrm{Im}\, d^{i-1} \subset C^i$ называются пространством i-коциклов и пространством i-кограниц соответственно.

Лемма 1.6. *Всякая кограница является коциклом, то есть $B^i \subset Z^i$.*

Доказательство: $x \in B^i \Longrightarrow x = d^{i-1}(y) \Longrightarrow d^i(x) = d^i(d^{i-1}(y)) = (d^i \circ d^{i-1})(y) = 0 \Longrightarrow x \in Z^i$. □

Определение 1.7. Факторпространство $H^i = H^i(C^\bullet, d^\bullet) := Z^i/B^i$ называется пространством i-ых когомологий комплекса $(C^\bullet, d^\bullet)$. Для гомологического комплекса $(C_\bullet, d_\bullet)$ анлогичным образом определяется понятие циклов $Z_i = \mathrm{Ker}\, d_i$, границ $B_i = \mathrm{Im}\, d_{i+1}$ и гомологий $H_i = H_i(C_\bullet, d_\bullet) := Z_i/B_i$. Для всякого (ко)цикла $x \in Z^i$ будем обозначать его класс (ко)гомологий через $\bar{x} \in H^i$.

Примеры 1.8. 1. Гомологии комплекса $(C_\bullet(X), \partial)$ называются сингулярными гомологиями пространства X и обозначаются $H_i(X, \mathbb{Z})$. Когомологии комплекса $(C^\bullet(X), \partial^*)$ называются сингулярными когомологиями пространства X и обозначаются $H^i(X, \mathbb{Z})$.

2. Пусть F — произвольная абелева группа. Гомологии комплекса $(C_\bullet(X) \otimes_{\mathbb{Z}} F, \partial \otimes \mathrm{Id}_F)$ называются сингулярными гомологиями с коэффициентами в F пространства X и обозначаются $H_i(X, F)$. Когомологии комплекса $(\mathrm{Hom}(C_\bullet(X), F), \partial^*)$ называются сингулярными когомологиями с коэффициентами в F пространства X и обозначаются $H^i(X, F)$.

3. Когомологии комплекса де Рама называются когомологиями де Рама и обозначаются $H^i_{DR}(X)$. Теорема де Рама утверждает, что $H^i_{DR}(X) \cong H^i(X, \mathbb{R})$.

Определение 1.9. Комплекс $C^\bullet$ называется ацикличным комплексом или точной последовательностью, если $H^i(C^\bullet) = 0$ при всех i. Иначе говоря, если $Z^i = B^i$, то есть $\mathrm{Ker}\, d^i = \mathrm{Im}\, d^{i-1}$.

Примеры 1.10. 1. Комплекс $0 \to A \to 0$ точен $\iff A = 0$.

2. Комплекс $0 \to A \xrightarrow{f} B \to 0$ точен $\iff f$ — изоморфизм.

3. Комплекс $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ точен $\iff f$ — мономорфизм, g — эпиморфизм и $\mathrm{Ker}\, g = f(A)$ (следовательно, $C = B/A$). Такие точные последовательности называются точными тройками или короткими точными последовательностями.

Часть 2. Лемма о змее

Определение 2.1. Морфизмом комплексов $f^\bullet : E^\bullet \to F^\bullet$ называется набор морфизмов $f^i : E^i \to F^i$, такой что $d^i_F \circ f^i = f^{i+1} \circ d^i_E$ для всех i.

Лемма 2.2. *Если $f^\bullet : E^\bullet \to F^\bullet$ — морфизм комплексов, то $f^i(Z^i(E^\bullet)) \subset Z^i(F^\bullet)$, $f^i(B^i(E^\bullet)) \subset B^i(F^\bullet)$.*

Доказательство: если $x \in Z^i(E^\bullet)$, то $d^i_F(f^i(x)) = f^{i+1}(d^i_A(x)) = 0$, то есть $f^i(x) \in Z^i(F^\bullet)$. Если же $x \in B^i(E^\bullet)$, то есть $x = d^{i-1}_E(y)$, то $f^i(x) = f^i(d^{i-1}_A(y)) = d^{i-1}_B(f^{i-1}(y)) \in B^i(F^\bullet)$. □

Пусть $f^\bullet : E^\bullet \to F^\bullet$ — морфизм копмлексов, а $h \in H^i(E^\bullet) = Z^i(E^\bullet)/B^i(E^\bullet)$ — класс когомологий. Выберем коцикл $x \in Z^i(E^\bullet)$, представляющий класс h и рассмотрим элемент $f^i(x) \in F^i$. Согласно предыдущей лемме $f^i(x)$ является коциклом, причем при замене коцикла x другим коциклом, представляющим тот же класс когомологий, коцикл $f^i(x)$ изменится на когранicу. Следовательно, класс когомологий коцикла $f^i(x)$ зависит лишь от класса h. Таким образом, всякий морфизм комплексов индуцирует морфизм когомологий $H^i(E^\bullet) \to H^i(F^\bullet)$, который обозначается $H^i f^\bullet$, такой что

$$H^i f(\bar{x}) = \overline{f^i(x)}.$$

Упражнение 2.3. Покажите, что $H^i f$ является гомоморфизмом.

Пусть $0 \to E^\bullet \xrightarrow{f^\bullet} F^\bullet \xrightarrow{g^\bullet} G^\bullet \to 0$ — точная тройка комплексов (то есть $f^\bullet$ и $g^\bullet$ — морфизмы комплексов, а последовательности $0 \to E^i \xrightarrow{f^i} F^i \xrightarrow{g^i} G^i \to 0$ точны при всех i). Рассмотрим произвольный класс когомологий $h \in H^i(G^\bullet)$ и проделаем следующую последовательность операций:

1. выберем $x \in G^i$, такой что $\bar{x} = h$ (заметим, что $d^i_G(x) = 0$);
2. выберем $x' \in F^i$, такой что $g^i(x') = x$ (это возможно, так как g^i — эпиморфизм);
3. положим $x'' := d^i_F(x'')$;
4. выберем $x''' \in E^{i+1}$, такой что $f^{i+1}(x''') = x''$ (это возможно, так как $g^{i+1}(x'') = g^{i+1}(d^i_F(x')) = d^i_G(g^i(x')) = d^i_G(x) = 0$, то есть $x'' \in \mathrm{Ker}\, g^{i+1} = \mathrm{Im}\, f^{i+1}$).

Лемма 2.4. *Элемент x''' является коциклом, а его класс когомологий $\overline{x'''}$ зависит лишь от класса $\bar{x}$, и не зависит от произвола в производимых выборах.*

Доказательство: $f^{i+2}(d_E^{i+1}(x''')) = d_F^{i+1}(f^{i+1}(x''')) = d_F^{i+1}(x'') = d_F^{i+1}(d_F^i(x')) = 0$, поэтому, так как f^{i+2} — мономорфизм, то $d_E^{i+1}(x''') = 0$, то есть x''' — коцикл.

Изучим теперь насколько x''' зависит от произвола в выборах. Во-первых, выбор элемента x''' на шаге (4) однозначен в силу мономорфности морфизма f^{i+1}, стало быть здесь произвола нет. Во-вторых, произвол в выборе элемента x' на шаге (2) сводится к замене $x' \mapsto x' + f^i(y)$, которая влечет замену $x'' \mapsto x'' + d_F^i(f^i(y)) = x'' + f^{i+1}(d_E^i(y)) = f^{i+1}(x''' + d_E^i(y))$ и, следовательно, $x''' \mapsto x''' + d_E^i(y)$, то есть x''' меняется на кограницу, а класс $\overline{x'''}$ не меняется. Наконец, произвол в выборе элемента x на шаге (1) сводится к замене $x \mapsto x + d_G^{i-1}(z) = x + d_G^{i-1}(g^{i-1}(z')) = x + g^i(d_F^{i-1}(z'))$, где $z' \in F^{i-1}$, которая на шаге (2) сводится к замене $x' \mapsto x' + d_F^{i-1}(z')$, а на шаге (3) — к замене $x'' \mapsto x'' + d_F^i(d_F^{i-1}(z')) = x''$, то есть элемент x'' не меняется. □

Итак, описанная выше конструкция дает отображение $\delta : H^i(G^\bullet) \to H^{i+1}(E^\bullet)$, называемое связывающим гомоморфизмом

$$\delta(\bar{x}) = \overline{x'''}.$$

Упражнение 2.5. Покажите, что δ является гомоморфизмом.

Теорема 2.6. *Если $0 \to E^\bullet \xrightarrow{f^\bullet} F^\bullet \xrightarrow{g^\bullet} G^\bullet \to 0$ — точная тройка комплексов, то последовательность когомологий $\cdots \to H^i(E^\bullet) \xrightarrow{H^i f} H^i(F^\bullet) \xrightarrow{H^i g} H^i(G^\bullet) \xrightarrow{\delta} H^{i+1}(E^\bullet) \xrightarrow{H^{i+1} f} H^{i+1}(F^\bullet) \to \dots$ точна.*

Доказательство: нам нужно проверить, что это комплекс, причем ацикличный.

- $(H^i g \circ H^i f)(\bar{x}) = \overline{g^i(f^i(x))} = \bar{0} = 0$;
- если $\bar{x} = H^i g(\bar{y})$, то $x = g^i(y)$, $x' = y$, $x'' = d_F^i(y) = 0$, $x''' = 0$ и $\delta(\bar{x}) = \bar{x'''} = 0$;
- $(H^{i+1} f \circ \delta)(\bar{x}) = \overline{f^{i+1}(x''')} = \overline{x''} = \overline{d_F^i(x')} = 0$.
- **Точность в $H^i(F^\bullet)$:** если $H^i g(\bar{x}) = 0$, то $g^i(x) = d_G^{i-1}(y) = d_G^{i-1}(g^{i-1}(y')) = g^i(d_F^{i-1}(y'))$, значит $g^i(x - d_F^{i-1}(y')) = 0$, то есть $x - d_F^{i-1}(y') = f^i(z)$ и $\bar{x} = \overline{f^i(z) + d_F^{i-1}(y')} = \overline{f^i(z)} = H^i f(\bar{z})$.
- **Точность в $H^i(G^\bullet)$:** если $\delta\bar{x} = 0$, то $x''' = d_E^i(y)$, значит $x'' = f^{i+1}(x''') = f^{i+1}(d_E^i(y)) = d_F^i(f^i(y))$, но $x'' = d_F^i(x')$, значит $d_F^i(x' - f^i(y)) = 0$, значит $\bar{x} = \overline{g^i(x')} = \overline{g^i(x' - f^i(y))} = H^i g(x' - f^i(y))$.
- **Точность в $H^{i+1}(E^\bullet)$:** если $H^{i+1} f(\bar{y}) = 0$, то $f^{i+1}(y) = d_F^i(z)$, значит, $d_G^i(g^i(z)) = g^{i+1}(d_F^i(z)) = g^{i+1}(f^{i+1}(y)) = 0$, и полагая $x := g^i(z)$, получаем $x' = z$, $x'' = d_F^i(z) = f^{i+1}(y)$ и $x''' = y$, т.е. $\bar{y} = \delta(\bar{x})$.

□

Часть 3. Когомологии групп

Пусть G — конечная группа. G-модулем будем называть абелеву группу, на которой задано линейное левое действие группы G. Иначе говоря, G-модуль — это левый модуль над групповой алгеброй $\mathbb{Z}[G]$.

Для каждого n рассмотрим свободную абелеву группу $F_n := \mathbb{Z}\langle G^{n+1}\rangle = \mathbb{Z}\langle G \times G \times \cdots \times G\rangle$, порожденную множеством G^{n+1}. Диагональное действие G на G^{n+1} индуцирует на F_n структуру G-модуля.

Лемма 3.1. *F_n является свободным G-модулем.*

Доказательство: группа G переставляет базисные (над $\mathbb{Z}$) элементы $e_{g_0,\dots,g_n} \in F_n$, действуя на базисе свободно. Выбирая в каждой из орбит по представителю (например, $e_{1,g_1,\dots,g_n}$) получаем базис F_n над $\mathbb{Z}[G]$. □

Ясно, что при всех $i, n \in \mathbb{Z}$ проекция $p_{n,i} : G^{n+1} \to G^n$, $(g_0, \dots, g_n) \mapsto (g_0, \dots, g_{i-1}, \hat{g_i}, g_{i+1}, \dots, g_n)$ (забывание i-ой координаты) коммутирует с действием группы G, следовательно индуцирует гомоморфизм G-модулей $\partial_{n,i} : F_n \to F_{n-1}$, $e_{g_0,\dots,g_n} \mapsto e_{g_0,\dots,g_{i-1},\hat{g_i},g_{i+1},\dots,g_n}$.

Лемма 3.2. *Имеем $\partial_{n-1,i} \circ \partial_{n,j} = \partial_{n-1,j-1} \circ \partial_{n,i}$ при $i < j$ и $\partial_{n-1,i} \circ \partial_{n,j} = \partial_{n-1,j} \circ \partial_{n,i+1}$ при $i \geqslant j$.*

Доказательство: очевидная проверка. □

Положим теперь $\partial_n := \sum_{i=0}^n (-1)^i \partial_{n,i}$.

Лемма 3.3. *$(F_\bullet, \partial_\bullet)$ — комплекс G-модулей.*

Доказательство: $\partial_{n-1}\circ\partial_n = \sum_{i<j}(-1)^{i+j}\partial_{n-1,i}\circ\partial_{n,j} + \sum_{i\geqslant j}(-1)^{i+j}\partial_{n-1,i}\circ\partial_{n,j} = \sum_{i<j}(-1)^{i+j}\partial_{n-1,i}\circ\partial_{n,j} + \sum_{i\geqslant j}(-1)^{i+j}\partial_{n-1,j}\circ\partial_{n,i+1}$ и ясно, что слагаемое (i,j) из первой суммы сокращается со слагаемым $(j-1,i)$ из второй суммы. □

Лемма 3.4. *Комплекс $(F_\bullet)$ ацикличен вне члена F_0, а $H_0(F_\bullet)\cong\mathbb{Z}$ с тривиальной структурой G-модуля.*

Доказательство: дополним комплекс $F_\bullet$ членом $F_{-1}=\mathbb{Z}e_\emptyset$ и рассмотрим отображение $h_n : F_n \to F_{n+1}$, $e_{g_0,\dots,g_n}\mapsto e_{1,g_0,\dots,g_{n+1}}$. Легко видеть, что $h_{n-1}\partial_n+\partial_{n+1}h_n = \mathrm{Id}_{F_n}$, поэтому если $\partial_n(x)=0$, то $x=\partial_{n+1}(h_n(x))$. Значит, дополненный комплекс ацикличен, а когомология исходного комплекса совпадает с $F_{-1}\cong\mathbb{Z}$. □

Ацикличный комплекс $(F_\bullet,\partial_\bullet)$ называется стандартной резольвентой для группы G.

Пусть M — произвольный G-модуль. Применяя к стандартной резольвенте функторы $-\otimes_G M$ и $\mathrm{Hom}_G(-,M)$ получаем комплексы (по функториальности) абелевых групп

$$0\leftarrow F_0\otimes_G M\leftarrow F_1\otimes_G M\leftarrow F_2\otimes_G M\leftarrow\dots \quad\text{и}\quad 0\to\mathrm{Hom}_G(F_0,M)\to\mathrm{Hom}_G(F_1,M)\to\mathrm{Hom}_G(F_2,M)\to\dots,$$

Определение 3.5. Группа $H_i(G,M) := H_i(F_\bullet\otimes_G M)$ называется группой гомологий группы G с коэффициентами в G-модуле M. Группа $H^i(G,M) := H^i(\mathrm{Hom}_G(F_\bullet,M))$ называется группой гомологий группы G с коэффициентами в G-модуле M.

Лекция 3. Когомологии групп

Часть 1. Когомологии групп

Напомним определение (ко)гомологий групп. Стандартной резольвентой для группы G называется комплекс G-модулей $0 \leftarrow F_0 \xleftarrow{\partial} F_1 \xleftarrow{\partial} F_2 \xleftarrow{\partial} \dots$, где $F_n := \mathbb{Z}\langle G^{n+1}\rangle$, а $\partial(e_{g_0,\dots,g_n}) = \sum_{i=0}^{n}(-1)^i e_{g_0,\dots,\hat{g_i},\dots,g_n}$. Далее, для всякого левого G-модуля M рассматриваются два комплекса абелевых групп:

$$0 \leftarrow F_0 \otimes_G M \xleftarrow{\partial} F_1 \otimes_G M \xleftarrow{\partial} F_2 \otimes_G M \xleftarrow{\partial} \dots \quad \text{и} \quad 0 \to \mathrm{Hom}_G(F_0, M) \xrightarrow{\partial^*} \mathrm{Hom}_G(F_1, M) \xrightarrow{\partial^*} \mathrm{Hom}_G(F_2, M) \xrightarrow{\partial^*} \dots,$$

(в первом случае мы пользуемся структурой правых G-модулей на F_n, а во втором — структурой левых G-модулей). Соответственно, (ко)гомологиями группы G с коэффициентами в M называются (ко)гомологии этих комплексов: $H_i(G, M) := H_i(F_\bullet \otimes_G M)$, $H^i(G, M) := H^i(\mathrm{Hom}_G(F_\bullet, M))$.

Лемма 1.1. *Имеем* $H_0(G, M) \cong M_G := M/\langle m - gm\rangle_{g\in G, m\in M}$, $H^0(G, M) \cong M^G = \{\, m \in M \mid gm = m\ \forall g \in G \,\}$.

Доказательство: F_0 — свободный G-модуль ранга 1, поэтому $F_0 \otimes_G M \cong M$, а F_1 — свободный G-модуль с базисом $(e_{1,g})_{g\in G}$ над $\mathbb{Z}[G]$, поэтому $F_1 \otimes_G M \cong \oplus_{g\in G}(e_{1,g} \otimes M)$, а $\partial(e_{1,g} \otimes m) = gm - m$.

Аналогично, $\mathrm{Hom}_G(F_0, M) \cong M$: всякому $m \in M$ соответствует отображение $f_m : e_g \mapsto gm$. Ясно, что $\partial^*(f_m)(e_{g_0,g_1}) = f_m(\partial(e_{g_0,g_1})) = f_m(e_{g_1} - e_{g_0}) = g_1 m - g_0 m$, поэтому $H^0(G, M) = \mathrm{Ker}\,\partial^* = M^G$. □

Лемма 1.2. *Существует изоморфизм* $\mathrm{Hom}_G(F_n, M) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}\langle G^n\rangle, M)$, *при котором* ∂^* *принимает вид*

$$(\partial^* f)(g_1, \dots, g_{n+1}) = g_1 f(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n}(-1)^i f(\dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots) + (-1)^{n+1} f(g_1, \dots, g_n). \qquad (*)$$

Доказательство: выберем в качестве базиса модуля $\mathbb{Z}\langle G^{n+1}\rangle$ над $\mathbb{Z}[G]$ векторы $e_{1,g_1,g_1g_2,\dots,g_1\cdots g_n}$. Каждый G-гомоморфизм $\mathbb{Z}\langle G^{n+1}\rangle \to M$ однозначно определяется своими значениями на этих векторах. Переписывая в этих терминах определение, получаем формулу $(*)$.

$$\begin{aligned}(\partial^* f)(g_1, \dots, g_{n+1}) = (\partial^* f)(e_{1,g_1,g_1g_2,\dots,g_1\cdots g_{n+1}}) = \\ f(e_{g_1,g_1g_2,\dots,g_1\cdots g_{n+1}}) + \textstyle\sum_{i=1}^{n}(-1)^i f(e_{1,\dots,g_1\cdots g_{i-1},g_1\cdots g_{i+1},\dots}) + (-1)^{n+1} f(e_{1,g_1,g_1g_2,\dots,g_1\cdots g_n}) = \\ g_1 f(g_2, \dots, g_{n+1}) + \textstyle\sum_{i=1}^{n}(-1)^i f(\dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots) + (-1)^{n+1} f(g_1, \dots, g_n).\end{aligned}$$

Следствие 1.3. *Имеем* $H^1(G, M) = \{\, f \in \mathrm{Hom}(\mathbb{Z}\langle G\rangle, M) \mid f(g_1g_2) = g_1 f(g_2) + f(g_1) \,\}/\{\, f \mid f(g_1) = g_1 f_0 - f_0 \,\}$; $H^2(G, M) = \{\, f \in \mathrm{Hom}(\mathbb{Z}\langle G^2\rangle, M) \mid f(g_1g_2, g_3) + f(g_1, g_2) = g_1 f(g_2, g_3) + f(g_1, g_2g_3) \,\}/\{\, g_1 f(g_2) - f(g_1g_2) + f(g_1) \,\}$.

Часть 2. Свойства когомологий

Лемма 2.1. (*i*) *(Ко)гомологии являются ковариантными функторами* G-Mod $\to \mathcal{A}b$.
(*ii*) *(Ко)гомологии коммутируют с прямыми суммами.*
(*iii*) $H_i(G, \mathbb{Z}[G]) = H^i(G, \mathbb{Z}[G]) = 0$ *при* $i > 0$. (*iv*) $H_0(G, \mathbb{Z}[G]) = H^0(G, \mathbb{Z}[G]) = \mathbb{Z}$.

Доказательство: первое утверждение следует из функториальности операций $F_\bullet \otimes_G -$ и $\mathrm{Hom}_G(F_\bullet, -)$, а второе — из того, что функторы $F_\bullet \otimes_G -$, $\mathrm{Hom}_G(F_\bullet, -)$, $H_i(-)$ и $H^i(-)$ коммутируют с прямыми суммами. Третье утверждение следует из того, что функтор $- \otimes_G \mathbb{Z}[G]$ есть забывание структуры G-модуля, а функтор $\mathrm{Hom}_G(-, \mathbb{Z}[G])$ есть двойственность в категории абелевых групп. Наконец, последнее утверждение получается применением леммы 1.1:

$$H_0(G, \mathbb{Z}[G]) = \mathbb{Z}[G]_G = \mathbb{Z}[G]/\langle e_1 - e_g\rangle_{g\in G} = \mathbb{Z}, \quad H^0(G, \mathbb{Z}[G]) = \mathbb{Z}[G]^G = \{\, \textstyle\sum a_g e_g \mid \forall g \in G\ a_g = a_1 \,\} = \mathbb{Z}.$$

Теорема 2.2. *Пусть* $0 \to M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \to 0$ *— точная тройка G-модулей. Тогда возникают точные последовательности*

$$\dots \xrightarrow{\delta} H_1(G,M_1) \xrightarrow{H_1 f_1} H_1(G,M_2) \xrightarrow{H_1 f_2} H_1(G,M_3) \xrightarrow{\delta} H_0(G,M_1) \xrightarrow{H_0 f_1} H_0(G,M_2) \xrightarrow{H_0 f_2} H_0(G,M_3) \to 0,$$
$$0 \to H^0(G,M_1) \xrightarrow{H^0 f_1} H^0(G,M_2) \xrightarrow{H^0 f_2} H^0(G,M_3) \xrightarrow{\delta} H^1(G,M_1) \xrightarrow{H^1 f_1} H^1(G,M_2) \xrightarrow{H^1 f_2} H^1(G,M_3) \xrightarrow{\delta} \dots,$$

где δ — связывающий гомоморфизм.

Доказательство: G-модуль F_n свободен, поэтому последовательности комплексов $0 \to F_\bullet \otimes_G M_1 \xrightarrow{f_1} F_\bullet \otimes_G M_2 \xrightarrow{f_2} F_\bullet \otimes_G M_3 \to 0$ и $0 \to \mathrm{Hom}_G(F_\bullet, M_1) \xrightarrow{f_1} \mathrm{Hom}_G(F_\bullet, M_2) \xrightarrow{f_2} \mathrm{Hom}_G(F_\bullet, M_3) \to 0$ точны. Остается применить лемму о змее. □

Эта теорема дает удобное средство для вычисления (ко)гомологий.

Определение 2.3. Точная последовательность G-модулей $\dots \to P_2 \to P_1 \to P_0 \to M \to 0$, в которой все G-модули P_n свободны, называется левой свободной резольвентой G-модуля M. Аналогично, точная последовательность G-модулей $0 \to M \to P^0 \to P^1 \to P^2 \to \dots$, в которой все G-модули P^n свободны, называется правой свободной резольвентой G-модуля M.

Теорема 2.4. (*i*) *Если* $0 \to M \to P^0 \xrightarrow{f^0} P^1 \xrightarrow{f^1} P^2 \xrightarrow{f^2} \dots$ *— свободная резольвента, то когомологии G с коэффициентами в M вычисляются применением функтора инвариантов: $H^i(G,M) = H^i(P^{\bullet G}, f^{\bullet G})$.*
(*ii*) *Если* $\dots \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \to M \to 0$ *— свободная резольвента, то гомологии G с коэффициентами в M вычисляются применением функтора коинвариантов: $H_i(G,M) = H_i(P_{\bullet G}, f_{\bullet G})$.*

Доказательство: (*i*) разрежем резольвенту на точные тройки

$$0 \to M \to P^0 \to M^1 \to 0, \quad 0 \to M^1 \to P^0 \to M^2 \to 0, \quad 0 \to M^2 \to P^0 \to M^3 \to 0, \quad \dots,$$

где $M^i = \mathrm{Im}\, f^{i-1} = \mathrm{Ker}\, f^i$. Применяя к первой из них предыдущую теорему и лемму 2.1 (iii), получаем

$$0 \to H^0(G,M) \to P^{0G} \to H^0(G,M^1) \to H^1(G,M) \to 0, \qquad H^{i+1}(G,M_1) = H^{i+2}(G,M) \quad \text{при } i \geqslant 0.$$

Применяя те же рассуждения ко второй тройке, и учитывая предыдущие равенства, получаем

$$0 \to H^0(G,M^1) \to P^{1G} \to H^0(G,M^2) \to H^2(G,M) \to 0, \qquad H^{i+1}(G,M_2) = H^{i+3}(G,M) \quad \text{при } i \geqslant 0.$$

Продолжая таким же образом, получаем

$$0 \to H^0(G,M^n) \to P^{nG} \to H^0(G,M^{n+1}) \to H^{n+1}(G,M) \to 0, \qquad H^{i+1}(G,M_{n+1}) = H^{i+n+2}(G,M) \quad \text{при } i \geqslant 0.$$

Так как морфизм $f^n : P^n \to P^{n+1}$ пропускается через M^{n+1}, то следующая диаграмма коммутативна

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(G,M^{n-1}) & \longrightarrow & P^{n-1\,G} & \longrightarrow & H^0(G,M^n) & \longrightarrow & H^n(G,M) \longrightarrow 0 \\
 & & & & \downarrow{\scriptstyle f^{n-1G}} & & & & \\
0 & \longrightarrow & H^0(G,M^n) & \longrightarrow & P^{nG} & \longrightarrow & H^0(G,M^{n+1}) & \longrightarrow & H^{n+1}(G,M) \longrightarrow 0 \\
 & & & & \downarrow{\scriptstyle f^{nG}} & & & & \\
0 & \longrightarrow & H^0(G,M^{n+1}) & \longrightarrow & P^{n+1\,G} & \longrightarrow & H^0(G,M^{n+2}) & \longrightarrow & H^{n+2}(G,M) \longrightarrow 0
\end{array}$$

Значит, $\mathrm{Ker}\, f^{nG} = H^0(G,M^n)$, $\mathrm{Im}\, f^{n-1\,G} = \mathrm{Ker}(H^0(G,M^n) \to H^n(G,M))$, то есть $H^n(P^{\bullet G}, f^{\bullet G}) = H^n(G,M)$. Утверждение (*ii*) доказывается аналогично. □

В качестве примера использования резольвент для вычисления (ко)гомологий вычислим (ко)гомологии циклической группы. Пусть $G = \mathbb{Z}/m\mathbb{Z}$, а $t \in G$ — образующая группы G. Рассмотрим следующие элементы групповой алгебры: $1 - t \in \mathbb{Z}[G]$ и $N = 1 + t + \dots + t^{m-1} \in \mathbb{Z}[G]$.

Лемма 2.5. *Имеем* $\mathrm{Ker}(1-t) = \mathbb{Z}N = \mathrm{Im}\, N$, $\mathrm{Ker}\, N = \mathrm{Im}(1-t)$.

Доказательство: $(1-t)(\sum a_k t^k) = \sum (a_k - a_{k-1}) t^k$, $N(\sum a_k t^k) = (\sum a_k) N$, далее очевидно. □

Следствие 2.6. *Тривиальный модуль $\mathbb{Z}$ имеет следующие резольвенты:*

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{1-t} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{1-t} \mathbb{Z}[G] \xrightarrow{N} \dots \quad \text{и} \quad \dots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{1-t} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{1-t} \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

Теперь заметим, что $\mathbb{Z}[G]_G = \mathbb{Z}[G]^G = \mathbb{Z}$, причем $t_G = t^G = 1$, а $N_G = N^G = m$. Следовательно, когомологии и гомологии группы G с коэффициентами в $\mathbb{Z}$ вычисляются комплексами

$$0 \to \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{m} \dots \quad \text{и} \quad \dots \xrightarrow{m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{m} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0.$$

Окончательно, получаем

$$H^i(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \begin{cases} \mathbb{Z}, & \text{при } i = 0 \\ 0, & \text{при нечетном } i \\ \mathbb{Z}/m\mathbb{Z}, & \text{при четном } i \geqslant 2 \end{cases}, \qquad H_i(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \begin{cases} \mathbb{Z}, & \text{при } i = 0 \\ \mathbb{Z}/m\mathbb{Z}, & \text{при нечетном } i \\ 0, & \text{при четном } i \geqslant 2 \end{cases}$$

Часть 3. Расширения групп

Определение 3.1. Расширением группы G с помощью группы N называется точная последовательность (в категории групп) $1 \to N \to E \xrightarrow{f} G \to 1$. Расширение называется расщепимым, если существует гомоморфизм групп $\phi : G \to E$ (называемый расщеплением), такой что $f \circ \phi = \mathrm{Id}_G$.

Простейшим примером расширения групп является полупрямое произведение. Если $A : G \to \mathrm{Aut}(N)$ действие группы G на N, то группа $N \leftthreetimes G$ определяется как множество $N \times G$ с операцией $(n_1, g_1)(n_2, g_2) = (n_1 A(g_1)(n_2), g_1 g_2)$. Ясно, что отображения $n \mapsto (n, 1)$, $(n, g) \mapsto g$ задают на $N \leftthreetimes G$ структуру расширения. Можно показать, что всякое расщепимое расширение является полупрямым произведением.

Пусть группа E является произвольным расширением G с помощью N. Тогда $N \subset E$ нормальная подгруппа и $G \cong E/N$. Выберем какое-нибудь отображение множеств $\phi : G \to E$, такое что $f \circ \phi = \mathrm{Id}_G$. Иначе говоря, для каждого элемента $g \in G$ мы выбираем элемент $\phi(g) \in E$, такой что $f(\phi(g)) = g$. Так как $N \subset E$ нормальна, то $\mathrm{Ad}_{\phi(g)} N = N$, где $\mathrm{Ad}_g(x) = gxg^{-1}$ — сопряжение. Следовательно, $\mathrm{Ad}_{\phi(g)}$ является автоморфизмом группы N.

Лемма 3.2. *Класс автоморфизм $\mathrm{Ad}_{\phi(g)} \in \mathrm{Aut}\, N$ по модулю внутренних автоморфизмов группы N определен однозначно, т.е. не зависит от выбора ϕ.*

Доказательство: если $\phi' : G \to E$ — другое такое отображение, то $\phi'(g) = n\phi(g)$, где $n \in N$, следовательно $\mathrm{Ad}_{\phi'(g)} = \mathrm{Ad}_{n\phi(g)} = \mathrm{Ad}_n \circ \mathrm{Ad}_{\phi(g)}$, а $\mathrm{Ad}_n \in \mathrm{Inn}\, N$. □

Таким образом, сопоставляя всякому элементу $g \in G$ автоморфизм $\mathrm{Ad}_{\phi(g)}$ с точностью до внутреннего автоморфизма получаем отображение $\overline{\mathrm{Ad}} : G \to \mathrm{Out}(N) = \mathrm{Aut}(N)/\mathrm{Inn}(N)$, не зависящее от выбора ϕ.

Лемма 3.3. *Отображение $\overline{\mathrm{Ad}} : G \to \mathrm{Out}(N)$ является гомоморфизмом групп.*

Доказательство: $f(\phi(g_1)\phi(g_2)) = f(\phi(g_1))f(\phi(g_2)) = g_1 g_2 = f(\phi(g_1 g_2))$, поэтому

$$\phi(g_1 g_2) = \xi(g_1, g_2)\phi(g_1)\phi(g_2), \qquad \text{где } \xi(g_1, g_2) \in N,$$

значит $\mathrm{Ad}_{\phi(g_1 g_2)} = \mathrm{Ad}_{\xi(g_1,g_2)\phi(g_1)\phi(g_2)} = \mathrm{Ad}_{\xi(g_1,g_2)} \circ \mathrm{Ad}_{\phi(g_1)} \circ \mathrm{Ad}_{\phi(g_2)}$, значит $\overline{\mathrm{Ad}}(g_1 g_2) = \overline{\mathrm{Ad}}(g_1)\overline{\mathrm{Ad}}(g_2)$. □

Пусть группа N — абелева. Тогда $\mathrm{Inn}(N) = 1$, то есть $\mathrm{Out}(N) = \mathrm{Aut}(N)$ и гомоморфизм $\overline{\mathrm{Ad}}$ задает на N структуру G-модуля. Более того, $(\phi(g_1)\phi(g_2))\phi(g_3) = \xi(g_1, g_2)\phi(g_1 g_2)\phi(g_3) = \xi(g_1, g_2)\xi(g_1 g_2, g_3)\phi(g_1 g_2 g_3)$, $\phi(g_1)(\phi(g_2)\phi(g_3)) = \phi(g_1)\xi(g_2, g_3)\phi(g_2 g_3) = \overline{\mathrm{Ad}}_{g_1}\xi(g_2, g_3)\phi(g_1)\phi(g_2 g_3) = \overline{\mathrm{Ad}}_{g_1}\xi(g_2, g_3)\xi(g_1, g_2 g_3)\phi(g_1 g_2 g_3)$. Значит, $\xi(g_1, g_2)\xi(g_1 g_2, g_3) = \overline{\mathrm{Ad}}_{g_1}\xi(g_2, g_3)\xi(g_1, g_2 g_3)$, что при аддитивной записи становится условием 2-коцикла. Далее, если заменить отображение ϕ на ϕ', то $\phi'(g) = \eta(g)\phi(g)$, значит $\phi'(g_1)\phi'(g_2) = \eta(g_1)\phi(g_1)\eta(g_2)\phi(g_2) = \eta(g_1)\overline{\mathrm{Ad}}_{g_1}(\eta(g_2))\phi(g_1)\phi(g_2) = \eta(g_1)\overline{\mathrm{Ad}}_{g_1}(\eta(g_2))\xi(g_1, g_2)\phi(g_1 g_2) = \eta(g_1)\overline{\mathrm{Ad}}_{g_1}(\eta(g_2))\xi(g_1, g_2)\eta(g_1 g_2)^{-1}\phi'(g_1 g_2)$, значит $\xi'(g_1, g_2) = \eta(g_1)\overline{\mathrm{Ad}}_{g_1}(\eta(g_2))\xi(g_1, g_2)\eta(g_1 g_2)^{-1}$, что при аддитивной записи означает, что $\xi' - \xi = \partial^* \eta$. Отсюда заключаем, что каждому расширению группы G с помощью абелевой группы N можно сопоставить класс когомологий $\bar{\xi} \in H^2(G, N)$, который не зависит от выбора ϕ.

Обратно, если $\bar{\xi} \in H^2(G, N)$, то множество $E = N \times G$ с операцией $(n_1, g_1) \cdot (n_2, g_2) = (n_1 + g_1 n_2 + \xi(g_1, g_2), g_1 g_2)$ является искомой группой (проверьте, это не вполне тривиально!)

Теорема 3.4. *Множество расширений группы G с помощью абелевой группы N, индуцирующих данное действие группы G на N совпадает с группой $H^2(G, N)$.*

Замечание 3.5. Легко видеть, что нулевому классу когомологий соответсвует полупрямое произведение.

Лекция 4. Коммутативная алгебра

Часть 1. Идеалы

Пусть A — коммутативное кольцо. Напомним, что идеалом в A называется подгруппа (относительно сложения) $\mathfrak{a} \subset A$, такая что $A\mathfrak{a} = \mathfrak{a}$.

Определение 1.1. Суммой идеалов $\mathfrak{a} + \mathfrak{b}$ называется множество элементов кольца A вида $a + b$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Произведением идеалов $\mathfrak{ab}$ называется множество элементов кольца A вида $\sum a_i b_i$, где $a_i \in \mathfrak{a}$, $b_i \in \mathfrak{b}$.

Лемма 1.2. *Сумма, произведение и пересечение идеалов — идеалы. Все указанные операции коммутативны и ассоциативны, а произведение — билинейно:* $(\mathfrak{a}_1 + \mathfrak{a}_2)\mathfrak{b} = \mathfrak{a}_1\mathfrak{b} + \mathfrak{a}_2\mathfrak{b}$. *Наконец,* $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}$.

Если $a \in A$, то идеал $(a) = aA := \{ x = ay \mid y \in A \}$ называется главным идеалом. Идеал $(a_1) + \cdots + (a_m)$ обозначается также $(a_1, \ldots, a_m)$. Заметим, что $(a) = A \iff a$ обратим.

Идеал $\mathfrak{m} \subset A$ — максимальный, если для всякого идеала $\mathfrak{a} \subset A$, такого что $\mathfrak{m} \subset \mathfrak{a} \subset A$, имеем либо $\mathfrak{a} = \mathfrak{m}$, либо $\mathfrak{a} = A$. Идеал $\mathfrak{p} \subset A$ — простой, если $\forall x, y \in A$, $x \notin \mathfrak{p}$, $y \notin \mathfrak{p} \Longrightarrow xy \notin \mathfrak{p}$. Идеал $\mathfrak{m} \subset A$ максимален $\iff$ $A/\mathfrak{m}$ — поле. Идеал $\mathfrak{p} \subset A$ прост $\iff$ $A/\mathfrak{p}$ — целостное кольцо. Макисмальный идеал прост.

Напомним, что прообраз простого идеала при гомоморфизме колец всегда прост, а прообраз максимального идеала максимален, если дополнительно предположить, что гомоморфизм сюръективен.

Лемма 1.3. *Всякое кольцо обладает максимальным идеалом.*

Доказательство: если $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset A$ — возрастающая цепочка идеалов $\mathfrak{a}_i \neq A$, то идеал $\mathfrak{a} = \bigcup_i \mathfrak{a}_i \subset A$ нетривиален: $\mathfrak{a} = A \Longrightarrow 1 \in \mathfrak{a} \Longrightarrow 1 \in \mathfrak{a}_i \Longrightarrow \mathfrak{a}_i = A$ для некоторого i. Остается применить лемму Цорна. □

Рассматривая прообразы максимальных идеалов в $A/\mathfrak{a}$ относительно проекции $A \to A/\mathfrak{a}$, заключаем, что всякий нетривиальный идеал содержится в максимальном идеале. Рассматривая $\mathfrak{a} = (a)$, заключаем, что всякий необратимый элемент кольца A содержится в максимальном идеале.

Часть 2. Радикалы

Напомним, что $x \in A$ называется нильпотентом, если $x^n = 0$ для некоторого n.

Лемма 2.1. *Множество всех нильпотентов в A является идеалом.*

Доказательство: $x^n = y^m = 0 \Longrightarrow (x+y)^{n+m} = \sum \binom{n+m}{k} x^k y^{n+m-k} = 0$; $(ax)^n = a^n x^n = 0$. □

Идеал $\mathfrak{N}$, образованный всеми нильпотентами кольца A называется нильрадикалом.

Лемма 2.2. *Нильрадикал равен пересечению всех простых идеалов.*

Доказательство: пусть $x \in A$ — нильпотент, а $\mathfrak{p} \subset A$ — простой идеал. Если $x \notin \mathfrak{p}$, то по индукции $x^n \notin \mathfrak{p}$, но $x^n = 0 \in \mathfrak{p}$, значит $x \in \mathfrak{p}$, то есть $\mathfrak{N} \subset \bigcap \mathfrak{p}$. Обратно, предположим, что x — не нильпотент и рассмотрим множество идеалов, не пересекающихся с множеством $\{ x^n \}_{n \in \mathbb{N}}$. Согласно лемме Цорна в множестве таких идеалов найдется макисмальный идеал $\mathfrak{p}$. Покажем, что $\mathfrak{p}$ — простой. Пусть $y, z \notin \mathfrak{p}$. Тогда по построению $\mathfrak{p}$ имеем $x^k \in \mathfrak{p} + (y)$, $x^l \in \mathfrak{p} + (z)$. Перемножая, получаем $x^{k+l} \in \mathfrak{p} + (yz)$. Если $yz \in \mathfrak{p}$, то $\mathfrak{p} + (yz) = \mathfrak{p}$, то есть $x^{k+l} \in \mathfrak{p}$, что противоречит выбору $\mathfrak{p}$. Значит $yz \notin \mathfrak{p}$ и $\mathfrak{p}$ — прост. □

Определение 2.3. Радикалом идеала $\mathfrak{a} \subset A$ называется множество $\mathfrak{r}(\mathfrak{a}) := \{ x \in A \mid x^n \in \mathfrak{a} \text{ для некотого } n \}$.

Лемма 2.4. *Если $\pi : A \to A/\mathfrak{a}$ — канонический эпиморфизм, то $\mathfrak{r}(\mathfrak{a}) = \pi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$.*

Доказательство: $x^n \in \mathfrak{a} \iff \pi(x)^n = 0$ в $A/\mathfrak{a}$. □

Следствие 2.5. *Радикал* $\mathfrak{r}(\mathfrak{a})$ *является идеалом,* $\mathfrak{a} \subset \mathfrak{r}(\mathfrak{a})$*, и* $\mathfrak{r}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

Следствие 2.6. *Имеем* $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$.

Доказательство: $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \bigcap_{\mathfrak{p} \supset \mathfrak{r}(\mathfrak{a})} \mathfrak{p} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p} = \mathfrak{r}(\mathfrak{a})$. □

Определение 2.7. Идеал $\mathfrak{a} \subset A$ называется радикальным, если $\mathfrak{a} = \mathfrak{r}(\mathfrak{a})$.

Предыдущее следствие показывает, что радикал идеала является радикальным идеалом.

Следствие 2.8. *Идеал* $\mathfrak{a}$ *— радикальный* $\iff$ *кольцо* $A/\mathfrak{a}$ *не имеет нетривиальных нильпотентов.*

Следствие 2.9. *Простой идеал радикален.*

Часть 3. Алгебраические многообразия

Коммутативная алгебра очень тесно связана с геометрией алгебраических многообразий. Пусть k — алгебраически замкнутое поле. Обозначим через $\mathbb{A}^n = \mathsf{k}^n$ — n-мерное аффинное пространство с координатами $x_1, \ldots, x_n$, и пусть $X \subset \mathbb{A}^n$ — аффинное алгебраическое многообразиенад полем k, то есть множество, заданное полиномиальными уравнениями: $X = \{\, x = (x_1, \ldots, x_n) \in \mathbb{A}^n \mid f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0 \,\}$, где $f_1, \ldots, f_m \in \mathsf{k}[x_1, \ldots, x_n]$. Тогда $A_X := \mathsf{k}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ — типичное коммутативное кольцо. Точнее говоря, k-алгебра A называется конечно порожденной над полем k, если найдется конечный набор элементов $a_1, \ldots, a_n \in A$, такой что всякий элемент из A представляется в виде многочлена от a_i с коэффицентами в k.

Лемма 3.1. *Если* k*-алгебра* A *— конечно порождена над* k*, то* $A \cong \mathsf{k}[x_1, \ldots, x_n]/I$*. Более того, если* A *не имеет нетривиальных нильпотентов, то идеал* I *— радикальный.*

Доказательство: если $a_1, \ldots, a_n$ порождают A, то отображение $f : \mathsf{k}[x_1, \ldots, x_n] \to A$, $f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$ является эпиморфизмом, значит $A \cong \mathsf{k}[x_1, \ldots, x_n]/\operatorname{Ker} f$. Остается применить следствие 2.8. □

Позднее мы покажем, что всякий идеал $I \subset \mathsf{k}[x_1, \ldots, x_n]$ представляется в виде $I = (f_1, \ldots, f_m)$ (теорема Гильберта о базисе).

Всякому идеалу $\mathfrak{a} \subset A_X$ сопоставим подмножество $V(\mathfrak{a}) = \{\, x \in X \mid \forall f \in \mathfrak{a}\ f(x) = 0 \,\}$. Подмножества вида $V(\mathfrak{a}) \subset X$ называются алгебраическими подмногообразиями. Обратно, всякому подмножеству $Y \subset X$ сопоставим идеал $I_Y := \{\, f \in A_X \mid f_{|Y} \equiv 0 \,\} \subset A_X$.

Лемма 3.2. *Обе конструкции монотонны по отношению к включению: если* $\mathfrak{a} \subset \mathfrak{b}$*, то* $V(\mathfrak{b}) \subset V(\mathfrak{a})$*, а если* $Y \subset Z$*, то* $I_Z \subset I_Y$.

Доказательство: если $\mathfrak{a} \subset \mathfrak{b}$ и $x \in V(\mathfrak{b})$, то всякая функция из $\mathfrak{a}$ лежит в $\mathfrak{b}$, следовательно зануляется на $V(\mathfrak{b})$, значит $x \in V(\mathfrak{a})$, значит $V(\mathfrak{b}) \subset V(\mathfrak{a})$. Если $Y \subset Z$ и $f \in I_Z$, то f зануляется на Z, а значит и на Y, значит $f \in I_Y$, значит $I_Z \subset I_Y$. □

Лемма 3.3. *Операции сложения, умножения и пересечения идеалов соответствуют пересечению и объединению подмногообразий. Иначе говоря,* $V(\mathfrak{a}_1 + \mathfrak{a}_2) = V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$*,* $V(\mathfrak{a}_1\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2) = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$.

Доказательство: если $x \in V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$, то $\forall f \in \mathfrak{a}_1, g \in \mathfrak{a}_2$ имеем $f(x) = g(x) = 0$, значит $(f+g)(x) = 0$, то есть $V(\mathfrak{a}_1 + \mathfrak{a}_2) \supset V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$. Далее, $V(\mathfrak{a}_1 + \mathfrak{a}_2) \subset V(\mathfrak{a}_1), V(\mathfrak{a}_2) \subset V(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subset V(\mathfrak{a}_1\mathfrak{a}_2)$, так как $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \mathfrak{a}_1, \mathfrak{a}_2 \subset \mathfrak{a}_1 + \mathfrak{a}_2$. Остается проверить, что $V(\mathfrak{a}_1\mathfrak{a}_2) \subset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$. Действительно, если $x \in V(\mathfrak{a}_1\mathfrak{a}_2) \setminus V(\mathfrak{a}_1)$, то $\exists f \in \mathfrak{a}_1$, так что $f(x) \neq 0$. Значит $\forall g \in \mathfrak{a}_2$ имеем $fg \in \mathfrak{a}_1\mathfrak{a}_2 \Longrightarrow (fg)(x) = 0 \Longrightarrow g(x) = 0$, т.е. $x \in V(\mathfrak{a}_2)$. □

Одним из основных результатов в коммутативной алгебре является

Теорема 3.4. *Имеем* $I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a})$.

Эта теорема известна как Теорема Гильберта о нулях (Hilbert Nullstellensatz). Ее мы докажем позднее, а пока выведем из нее следствия.

Следствие 3.5. *Если* $Y \subset X$ *— алгебраическое подмногообразие, то идеал* I_Y *радикален, а* $Y = V(I_Y)$.

Доказательство: Y по определению подмногообразия имеет вид $Y = V(\mathfrak{a})$, поэтому $I_Y = I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a})$ — радикальный идеал, а $V(I_Y) = V(\mathfrak{r}(\mathfrak{a})) = V(\mathfrak{a}) = Y$. □

Следствие 3.6. *Соответствия $\mathfrak{a} \mapsto V(\mathfrak{a})$, $Y \mapsto I_Y$ задают биекцию между множеством всех подмногообразий $Y \subset X$ и множеством всех радикальных идеалов $\mathfrak{a} \subset A_X$.*

Доказательство: если $\mathfrak{a}$ радикален, то $I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a}) = \mathfrak{a}$, а все остальное доказано выше. □

Следствие 3.7. *Всякий максимальный идеал в кольце $A = A_X$ имеет вид $\mathfrak{m} = I_x$, где $x \in X$.*

Доказательство: $I_{V(\mathfrak{m})} = \mathfrak{r}(\mathfrak{m}) = \mathfrak{m}$. Так как $I_\emptyset = A$, то $V(\mathfrak{m}) \neq \emptyset$. Если $x \in V(\mathfrak{m})$, то $\mathfrak{m} = I_{V(\mathfrak{m})} \subset I_x \neq A$. Но $\mathfrak{m}$ максимальный, значит $\mathfrak{m} = I_x$. □

Таким образом, точки многообразия находятся во взаимно-однозначном соответствии с максимальными идеалами кольца.

Определение 3.8. Подмножество $Y \subset X$ называется неприводимым, если $Y \subset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) \Longrightarrow Y \subset V(\mathfrak{a}_1)$ или $Y \subset V(\mathfrak{a}_2)$.

Лемма 3.9. *Подмногообразие Y — неприводимо $\Longleftrightarrow$ идеал I_Y прост.*

Доказательство: ($\Longrightarrow$) $Y = V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) \Longrightarrow Y = V(\mathfrak{a}_1\mathfrak{a}_2)$. Если $\mathfrak{a}_1 \not\subset I_Y$, то найдется $f \in \mathfrak{a}_1 \setminus I_Y$. Тогда для всякого $g \in \mathfrak{a}_2$ имеем $fg \in \mathfrak{a}_1\mathfrak{a}_2 \Longrightarrow fg \in I_Y \Longrightarrow g \in I_Y$, то есть $\mathfrak{a}_2 \subset I_Y \Longrightarrow Y \subset V(\mathfrak{a}_2)$. Иначе $\mathfrak{a}_1 \subset I_Y \Longrightarrow Y \subset V(\mathfrak{a}_1)$. ($\Longleftarrow$) Пусть I_Y — не прост. Тогда найдутся $f_1, f_2 \notin I_Y$, так что $f_1 f_2 \in I_Y$. Тогда $I_Y + (f_1 f_2) = I_Y$ и $Y = V(I_Y) = V(I_Y + (f_1 f_2)) = V((I_Y + (f_1))(I_Y + (f_2))) = V(I_Y + (f_1)) \cup V(I_Y + (f_2))$, но $Y \not\subset V(I_Y + (f_i))$, так как $f_i \notin I_Y$. □

Следствие 3.10. *Многообразие X неприводимо $\Longleftrightarrow$ кольцо A_X целостное.*

Таким образом, неприводимые подмногообразия в X находятся во взаимно-однозначном соответствии с простыми идеалами кольца A_X. При этом точки, лежащие на подмногообразии $V(\mathfrak{p})$ соответствуют максимальным идеалам, содержащим идеал $\mathfrak{p}$.

Изучим теперь геометрический смысл факторизации.

Лемма 3.11. *Все (простые, максимальные) идеалы кольца $A/\mathfrak{a}$ находятся во взаимно-однозначном соответствии со всеми (простыми, максимальными) идеалами кольца A, содержащими $\mathfrak{a}$.*

Доказательство: если $\pi : A \to A/\mathfrak{a}$ — канонический эпиморфизм, а $\mathfrak{b} \subset A/\mathfrak{a}$ — идеал, то $\mathfrak{b} = \pi^{-1}(\mathfrak{a})/\mathfrak{a}$. Обратно, если $\mathfrak{c} \subset A$ — идеал и $\mathfrak{a} \subset \mathfrak{c}$, то $\mathfrak{c}/\mathfrak{a} \subset A/\mathfrak{a}$ — идеал и $\mathfrak{c} = \pi^{-1}(\mathfrak{c}/\mathfrak{a})$. Наконец, $(A/\mathfrak{a})/\mathfrak{b} = A/\pi^{-1}(\mathfrak{b})$, поэтому $\mathfrak{b}$ — прост (максимален) $\Longleftrightarrow \pi^{-1}(\mathfrak{b})$ — прост (максимален). □

Таким образом, точки многообразия, соответствующего кольцу $A/\mathfrak{a}$, это точки, лежащие на $V(\mathfrak{a})$. Иначе говоря, переход к факторкольцу соответствует переходу к подмногообразию.

Пусть $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ — алгебраические многообразия. Отображение $\phi : X \to Y$ называется алгебраическим, если оно имеет вид $\phi(x_1, \ldots, x_n) = (\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots, x_n))$ и $\phi_1, \ldots, \phi_m \in \mathsf{k}[x_1, \ldots, x_n]$. Если $\phi : X \to Y$ — алгебраическое отображение и $f \in \mathsf{k}[y_1, \ldots, y_m]$, то $\phi^*(f) := f \circ \phi = f(\phi_1, \ldots, \phi_m) \in \mathsf{k}[x_1, \ldots, x_n]$. Более того, если $f_{|Y} = 0$, то $\phi^*(f)_{|X} = 0$, поэтому ϕ^* индуцирует отображение $A_Y \to A_X$, которое очевидно является гомоморфизмом.

Лемма 3.12. *Сопоставления $X \mapsto A_X$, $\phi \mapsto \phi^*$ задают контравариантный функтор из категории алгебраических многообразий над полем k в категорию конечно порожденных коммутативных k-алгебр.*

Обратно, пусть $\Phi : A_Y \to A_X$ — гомоморфизм колец. Каждая из переменных $y_1, \ldots, y_m$ является функцией на Y, поэтому $\Phi(y_i) \in A_X = \mathsf{k}[x_1, \ldots, x_n]/I_X$. Поднимая $\Phi(y_i)$ до многочленов $\phi_i(x) \in \mathsf{k}[x_1, \ldots, x_n]$, получаем отображение $\phi : X \to \mathbb{A}^m$. Ясно, что при этом $\phi^*(f)_{|X} = \Phi(f_{|Y})$, поэтому если $f \in I_Y$, то $f \circ \phi = 0$, значит $\phi(X) \subset Y$. Таким образом, всякий гомоморфизм колец индуцирован алгебраическим отображением многообразий. Наконец, вспоминая, что всякая конечно порожденная коммутативная алгебра без нильпотентов является алгеброй функций на аффинном многообразии, получаем.

Теорема 3.13. *Категория аффинных алгебраических многообразий над полем k эквивалентна категории конечно порожденных коммутативных k-алгебр без нильпотентов.*

Лекция 5. Теорема Гильберта

Часть 1. Нетеровость

Определение 1.1. Модуль M над кольцом A называется нетеровым, если всякая возрастающая цепочка подмодулей $M_1 \subset M_2 \subset M_3 \subset \dots$ в M стабилизируется, то есть $M_{i+1} = M_i$ для $i \gg 0$.

Пример 1.2. Векторное пространство V над полем нетерово $\iff \dim V < \infty$.

Определение 1.3. Модуль M конечно порожден над кольцом A, если найдется конечное число элементов $m_1, \dots, m_n \in M$, такие что всякий элемент из M представляется в виде конечной линейной комбинации элементов m_i с коэффициентами в A. Иначе говоря, M изоморфен фактормодулю свободного A-модуля конечного ранга.

Лемма 1.4. *Модуль M нетеров $\iff$ любой подмодуль в M конечно порожден.*

Доказательство: ($\Longrightarrow$) Пусть M нетеров и $M' \subset M$. Рассмотрим цепочку подмодулей $0 = M_0 \subset M_2 \subset \dots$ в M', в которой если $M_i \neq M'$, то $M_{i+1} = M_i + Am_{i+1}$, где $m_{i+1} \in M' \setminus M_i$. Так как цепочка стабилизируется, то $M_i = M'$ при некотором i, но тогда $m_1, \dots, m_i$ порождают M'.

($\Longleftarrow$) Пусть $M_1 \subset M_2 \subset \dots$ — возрастающая цепочка в M. Рассмотрим $M' = \bigcup M_i \subset M$. Ясно, что M' — подмодуль. Пусть $m_1, \dots, m_n$ — его образующие. Тогда для каждого i имеем $m_i \in M_j$ при $j \gg 0$, откуда $M' = M_j$ при $j \gg 0$ и цепочка стабилизируется. □

Лемма 1.5. *Если $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ — точная тройка, то M нетеров $\iff$ M' и M'' нетеровы.*

Доказательство: ($\Longrightarrow$) если $M'_1 \subset M'_2 \subset \dots$ и $M''_1 \subset M''_2 \subset \dots$ — возрастающие цепочки в M' и M'', то $f(M'_1) \subset f(M'_2) \subset \dots$ и $g^{-1}(M''_1) \subset g^{-1}(M''_2) \subset \dots$ — возрастающие цепочки в M. Следовательно $f(M'_{i+1}) = f(M'_i)$ и $g^{-1}(M''_{i+1}) = g^{-1}(M''_i)$ при $i \gg 0$. Но тогда $M'_{i+1} = M'_i$ и $M''_{i+1} = M''_i$, так как f — моно, а g — эпиморфизм.

($\Longleftarrow$) если $M_1 \subset M_2 \subset \dots$ — возрастающая цепочка в M, то $g(M_1) \subset g(M_2) \subset \dots$ и $f^{-1}(M_1) \subset f^{-1}(M_2) \subset \dots$ — возрастающие цепочки в M'' и M', поэтому $g(M_{i+1}) = g(M_i)$ и $f^{-1}(M_{i+1}) = f^{-1}(M_i)$ при $i \gg 0$. Но тогда $M_{i+1} = M_i$. Действительно, если $x \in M_{i+1}$, то $g(x) \in g(M_{i+1}) = g(M_i)$, значит найдется $y \in M_i$, так что $g(x) = g(y)$. Тогда $g(x - y) = 0$, значит $x - y \in \operatorname{Ker} g = \operatorname{Im} f$, то есть $x - y \in f(f^{-1}(M_{i+1})) = f(f^{-1}(M_i))$, следовательно найдется $z \in f^{-1}(M_i)$, такой что $x = y + f(z)$. Но $f(z) \in M_i$, значит $x \in M_i$. □

Следствие 1.6. *Прямая сумма конечного числа нетеровых модулей нетерова.*

Доказательство: индукция, использующая точные тройки $0 \to M_n \to \oplus_{i=1}^{n} M_i \to \oplus_{i=1}^{n-1} M_i \to 0$. □

Определение 1.7. Кольцо A называется нетеровым, если свободный A-модуль A нетеров. Иначе говоря, если всякая возрастающая цепочка идеалов в A стабилизируется.

Примеры 1.8.

1. Поле нетерово.
2. Конечное кольцо нетерово.
3. Кольцо главных идеалов нетерово (все идеалы главные $\Longrightarrow$ значит все идеалы конечно порождены).

Лемма 1.9. *Факторкольцо нетерова кольца нетерово.*

Доказательство: $A/\mathfrak{a}$ является нетеровым A-модулем, а значит и нетеровым $A/\mathfrak{a}$-модулем. □

Теорема 1.10. *Модуль M над нетеровым кольцом A нетеров $\iff$ M конечно порожден.*

Доказательство: ($\Longrightarrow$) Следует из леммы 1.4. ($\Longleftarrow$) Выберем в M образующие, рассмотрим сюръекцию $A^{\oplus n} \to M$ и заметим, что по следствию 1.6 модуль $A^{\oplus n}$ нетеров, а по лемме 1.5 модуль M нетеров. □

Следствие 1.11. *Подмодуль и фактормодуль конечно порожденного модуля над нетеровым кольцом конечно порождены.*

Часть 2. Теорема Гильберта о базисе

Когда-то, нетеровость всякого кольца приходилось проверять по отдельности. Теорема Гильберта позволила избавиться от этого.

Теорема 2.1. *Если кольцо A — нетерово, то кольцо $A[x]$ — тоже нетерово.*

Доказательство: пусть $I \subset A[x]$ — идеал. Рассмотрим множество $I_0 \subset A$, состоящее из старших коэффициентов многочленов, входящих в A. Ясно, что I_0 — идеал в A, так как $f(x) = ax^n + \dots \in I$, $g(x) = bx^m + \dots \in I$ $\Longrightarrow f(x)x^m + g(x)x^n = (a+b)x^{n+m} + \dots \in I$, $cf(x) = cax^n + \dots \in I \Longrightarrow a + b \in I_0$, $ca \in I_0$ для всех $c \in A$. Идеал I_0 конечно порожден над A. Выберем конечный набор образующих $a_1, \dots, a_n$ идеала I_0 над A и пусть $f_1, \dots, f_n \in A[x]$ — многочлены из I, старшие коэффициенты которых равны $a_1, \dots, a_n$. Пусть $N = \max \deg f_i$ Пусть далее $M = I \cap A\langle 1, x, \dots, x^{N-1}\rangle \subset A[x]$. Тогда M является A-подмодулем в свободном A-модуле конечного ранга, значит M конечно порожден над A. Выберем конечный набор образующих $g_1, \dots, g_m$ модуля M над A и докажем, что многочлены $f_1, \dots, f_n, g_1, \dots, g_m$ порождают идеал I над $A[x]$. Для этого надо любой многочлен $h(x) \in I$ представить в виде линейной комбинации многочленов f_i, g_j. Действительно, если $\deg h < N$, то $h \in M$ и представляется в виде линейной комбинации многочленов g_j. Пусть теперь $\deg h > N$, $h = ax^k + \dots$. Тогда $a \in I_0$, значит $a = \sum c_i a_i$, $c_i \in A$, следовательно если $h'(x) = h(x) - \sum c_i x^{k - \deg f_i} f_i$, то $h'(x) \in I$, причем $\deg h' < \deg h$. Повторяя это рассуждение заключаем, что h представляется в виде линейной комбинации многочленов f_i и многочлена, лежащего в I, степень которого меньше чем N. □

Следствие 2.2. *Кольцо многочленов $\mathsf{k}[x_1, \dots, x_n]$ нетерово.*

Следствие 2.3. *Любая конечно порожденная коммутативная k-алгебра нетерова.*

Следствие 2.4. *Если A нетерово, то любая конечно порожденная коммутативная A-алгебра нетерова.*

Следствие 2.5. *Любой идеал в конечно порожденной коммутативной k-алгебре конечно порожден.*

Часть 3. Теорема Гильберта о нулях

Теорема 3.1. *Если $X \subset \mathbb{A}^n$ — аффинное алгебраическое многообразие над алгебраически замкнутым полем k, $\mathfrak{a} \subset A_X$ — идеал в его координатной алгебре, то $I_{V(\mathfrak{a})} = \mathfrak{r}(\mathfrak{a})$.*

Покажем, что условие алгебраической замкнутости поля k в формулировке теоремы существенно. Рассмотрим идеал $\mathfrak{a} := (x^2+1)\mathbb{R}[x] \subset \mathbb{R}[x]$. Тогда $V(\mathfrak{a}) \subset \mathbb{R}$ задается уравнением $x^2 + 1 = 0$, которое не имеет вещественных решений. Поэтому $V(\mathfrak{a}) = \emptyset$ и $I_{V(\mathfrak{a})} = \mathbb{R}[x] \neq \mathfrak{r}(\mathfrak{a})$. Причина в том, что $V(\mathfrak{a})$ не имеет вещественных точек, но имеет две комплексные точки i и $-i$, поэтому при переходе к полю $\mathbb{C}$ получаем $V(\mathfrak{a}) = \{\, i, -i \,\}$ и $I_{V(\mathfrak{a})} = \{\, f(x) \in \mathbb{C}[x] \mid (x-i)|f(x), (x+i)|f(x) \,\} = \{\, f(x) \in \mathbb{C}[x] \mid (x^2+1)|f(x) \,\} = \mathfrak{a}$. Разобранный факт является иллюстрацией следующего принципа:

> *алгебраическое многообразие над незамкнутым полем k следует рассматривать как множество точек соответствующего многообразия над $\bar{\mathsf{k}}$, имеющих координаты в k.*

Тот же пример показывает, что в формулировке "слабой формы" теоремы Гильберта о нулях, утверждающей что всякий максимальный идеал в алгебре A_X функций на многообразии X имеет вид I_x, где $x \in X$, существенно условие алгебраической замкнутости поля. А именно, идеал $\mathfrak{a}$ рассмотренный выше максимален ($\mathbb{R}[x]/\mathfrak{a} \cong \mathbb{C}$), однако, чтобы его представить в виде I_x, надо в качестве точки x взять точку с комплексными координатами.

Прежде чем приступить к доказательству теоремы Гильберта, нам потребуются приготовления.

Лемма 3.2. *Если $A \subset B \subset C$ и B — конечно порожденная A-алгебра, а C — конечно порожденная B-алгебра, то C — конечно порожденная A-алгебра.*

Доказательство: если $b_1, \dots, b_n$ порождают B над A, а $c_1, \dots, c_m$ порождают C над B, то $b_1, \dots, b_n, c_1, \dots, c_m$ порождают C над A. □

Лемма 3.3. *Поле $K = \mathsf{k}(x_1, \dots, x_m)$ является конечно порожденной k-алгеброй только при $m = 0$.*

Доказательство: предположим, что $\phi_1, \dots, \phi_n$ порождают K над k, $\phi_i = f_i/g_i$. Выберем неприводимый многочлен $p \in \mathsf{k}[x_1, \dots, x_m]$, не являющийся делителем ни одного из многочленов g_i (неприводимых делителей у многочленов g_i лишь конечное число в силу факториальности кольца $\mathsf{k}[x_1, \dots, x_m]$, а различных неприводимых — бесконечное (для любого множества $p_1, \dots, p_N$ неприводимых многочленов всякий неприводимый делитель многочлена $p_1 \cdots p_N + 1$ взаимно прост с каждым из p_i)). Тогда $1/p$ не лежит в подкольце поля K, порожденном над k элементами ϕ_i. □

Определение 3.4. Набор элементов $a_1, \dots, a_n$ в коммутативной k-алгебре A называется алгебраически независимым над k, если для любого многочлена $0 \neq f(x_1, \dots, x_n) \in \mathsf{k}[x_1, \dots, x_n]$ имеем $f(a_1, \dots, a_n) \neq 0$.

Лемма 3.5. *Если конечно порожденная коммутативная k-алгебра A является полем, то A/k — конечное расширение полей.*

Доказательство: выберем конечный набор образующих $a_1, \dots, a_n$ алгебры A над k. Можно считать, что образующие перенумерованы таким образом, что $a_1, \dots, a_m$ алгебраически независимы над k, а $a_1, \dots, a_m, a_i$ при $m < i \leqslant n$ уже алгебраически зависимы. Далее, гомоморфизм $\mathsf{k}[x_1, \dots, x_m] \to A$, $x_i \mapsto a_i$ является вложением, значит индуцирует изоморфизм поля $\mathsf{k}(x_1, \dots, x_m)$ и подполя $K \subset A$, порожденного элементами $a_1, \dots, a_m$. При этом все a_i при $m < i \leqslant n$ алгебраичны над K, следовательно A алгебраично над K, следовательно $\dim_K A < \infty$. Пусть $e_1, \dots, e_l$ — базис A над K. Тогда для всех $1 \leqslant i, j \leqslant n$ имеем

$$a_i = \sum_{k=1}^{l} \lambda_{ik} e_k, \qquad e_i e_j = \sum_{k=1}^{l} \mu_{ijk} e_k, \qquad \lambda_{ik}, \mu_{ijk} \in K.$$

Пусть $B \subset A$ — алгебра, порожденная над k элементами λ_{ik}, μ_{ijk}. Тогда B — нетерова. Из предыдущих равенств следует, что элементы $e_1, \dots, e_l$ порождают A как B-модуль, то есть A конечно порожденный B-модуль, следовательно K — тоже конечно порожденный B-модуль, так как $K \subset A$, следовательно K — конечно порожденная B-алгебра, следовательно K — конечно порожденная k-алгебра. Но $K \cong \mathsf{k}(x_1, \dots, x_m)$, следовательно $m = 0$, $K = \mathsf{k}$ и $\dim_{\mathsf{k}} A < \infty$. □

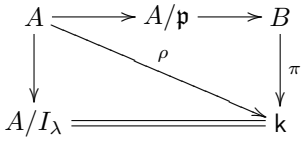
Следствие 3.6. *Если $\mathfrak{m}$ — максимальный идеал в конечно порожденной коммутативной k-алгебре A, то поле $A/\mathfrak{m}$ является конечным расширением поля k.*

Если $A = A_X$, $X \subset \mathbb{A}^n$, $x_1, \dots, x_n$ — координаты в $\mathbb{A}^n$, $A/\mathfrak{m} = F$ и $\pi : A \to F$ — соответствующий эпиморфизм, и $\lambda_i := \pi(x_i) \in F$, то $\mathfrak{m} = \{ f \in \mathsf{k}[x_1, \dots, x_n] \mid f(\lambda_1, \dots, \lambda_n) = 0 \} = I_{(\lambda_1, \dots, \lambda_n)}$. Иначе говоря, максимальный идеал $\mathfrak{m}$ соответствует точке многообразия X с координатами в расширении F поля k.

Теперь можно приступить к доказательству теоремы Гильберта.

Шаг 1. Предположим, что теорема доказана для простых идеалов. Тогда для любого $\mathfrak{a}$, если $\mathfrak{a} \subset \mathfrak{p}$, то $V(\mathfrak{p}) \subset V(\mathfrak{a})$, значит $I_{V(\mathfrak{a})} \subset I_{V(\mathfrak{p})} = \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$, следовательно $I_{V(\mathfrak{a})} \subset \bigcup_{\mathfrak{a} \subset \mathfrak{p}} \mathfrak{p} = \mathfrak{r}(\mathfrak{a})$.

Шаг 2. Предположим, что $f \in I_{V(\mathfrak{p})}$, $f \notin \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$. Рассмотрим подкольцо в поле частных целостного кольца $A/\mathfrak{p}$, порожденное элементом $1/f$: $B = A/\mathfrak{p}[1/f]$. Так как $f \neq 0$ в $A/\mathfrak{p}$, то $B \neq 0$. Выберем максимальный идеал $\mathfrak{m}$ в кольце B. Кольцо B конечно порождено над A, поэтому B конечно порождено над k, поэтому $B/\mathfrak{m}$ является конечно порожденной k-алгеброй. Следовательно, поле $B/\mathfrak{m}$ является конечным расширением поля k. Но k алгебраически замкнуто, поэтому $B/\mathfrak{m} \cong \mathsf{k}$. Пусть $\pi : B \to \mathsf{k}$ — соответствующий эпиморфизм, а ρ — композиция $A \to A/\mathfrak{p} \to A/\mathfrak{p}[1/f] = B \to \mathsf{k}$. Ясно, что $\mathfrak{p} \subset \operatorname{Ker} \rho$. Пусть также $\lambda_i = \rho(x_i) \in \mathsf{k}$, где $x_1, \dots, x_n$ — координаты в аффинном пространстве, в которм лежит X. Тогда если $\lambda = (\lambda_1, \dots, \lambda_n)$, то эпиморфизм ρ совпадает с эпиморфизмом $A \to A/I_\lambda \cong \mathsf{k}$



(эпиморфизм однозначно определяется значениями на образующих кольца), поэтому $\mathfrak{p} \subset I_\lambda$, следовательно $\lambda \in V(I_\lambda) \subset V(\mathfrak{p})$. Однако, $\pi(1/f) = 1/f(\lambda_1, \dots, \lambda_n)$, поэтому $f(\lambda_1, \dots, \lambda_n) \neq 0$, значит $f \notin I_{V(\mathfrak{p})}$. □

Лекция 6. Когомологии модулей

Часть 1. Свойства точности функтора Hom

Определение 1.1. Комплекс $0 \to M_1 \to M_2 \to M_3 \to 0$ называется точным слева, если он точен в членах M_1 и M_2, и точным справа, если он точен в членах M_2 и M_3.

Лемма 1.2. (*i*) *Последовательность* $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ *точна слева* $\iff$ *для любого* A*-модуля* N *последовательность* $0 \to \operatorname{Hom}_A(N, M_1) \xrightarrow{f_*} \operatorname{Hom}_A(N, M_2) \xrightarrow{g_*} \operatorname{Hom}_A(N, M_3)$ *точна слева.*
(*ii*) *Последовательность* $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ *точна справа* $\iff$ *для любого* A*-модуля* N *последовательность* $0 \to \operatorname{Hom}_A(M_3, N) \xrightarrow{g^*} \operatorname{Hom}_A(M_2, N) \xrightarrow{f^*} \operatorname{Hom}_A(M_1, N)$ *точна слева.*

Доказательство: (*i*) ($\Longrightarrow$) Если $\phi_1 \in \operatorname{Hom}_A(N, M_1)$, $f_*(\phi_1) = f \circ \phi_1 = 0$, то $\operatorname{Im}\phi_1 \subset \operatorname{Ker} f = 0$, поэтому $\phi_1 = 0$. Если $\phi_2 \in \operatorname{Hom}_A(N, M_2)$, $g_*(\phi_2) = g \circ \phi_2 = 0$, то $\operatorname{Im}\phi_2 \subset \operatorname{Ker} g = \operatorname{Im} f \cong M_1$, поэтому найдется $\phi_1 \in \operatorname{Hom}_A(N, M_1)$, такой что $\phi_2 = f_*(\phi_1)$. ($\Longleftarrow$) Возьмем $N = M_1$, $\phi_1 = 1$. Тогда $0 = (g_* \circ f_*)(\phi_1) = g_*(f_*(\phi_1)) = g \circ f \circ 1 = g \circ f$, поэтому $\operatorname{Im} f \subset \operatorname{Ker} g$. Возьмем $N = \operatorname{Ker} f$ и естественное вложение $\phi_1 : N \to M_1$. Тогда $f_*(\phi_1) = f \circ \phi_1 = 0$, поэтому $\phi_1 = 0$, то есть $N = \operatorname{Ker} f = 0$. Наконец, возьмем $N = \operatorname{Ker} g$ и естественное вложение $\phi_2 : N \to M_2$. Тогда $g_*(\phi_2) = g \circ \phi_2 = 0$, поэтому $\phi_2 = f_*(\phi_1) = f \circ \phi_1$. Значит $\operatorname{Ker} g = \operatorname{Im}\phi_2 \subset \operatorname{Im} f$.
(*ii*) ($\Longrightarrow$) Аналогично, если $\psi_3 \in \operatorname{Hom}_A(M_3, N)$, $g^*(\psi_3) = \psi_3 \circ g = 0$, то $\operatorname{Ker}\psi_3 \supset \operatorname{Im} g = M_3$, поэтому $\psi_3 = 0$. Если $\psi_2 \in \operatorname{Hom}_A(M_2, N)$, $f^*(\psi_2) = \psi_2 \circ f = 0$, то $\operatorname{Ker}\psi_2 \supset \operatorname{Im} f = \operatorname{Ker} g$, поэтому ψ_2 пропускается через $M_2/\operatorname{Ker} g = M_3$. Иначе говоря, найдется $\psi_3 \in \operatorname{Hom}_A(M_3, N)$, такой что $\psi_2 = g^*(\psi_3)$. ($\Longleftarrow$) Возьмем $N = M_3$, $\psi_3 = 1$. Тогда $0 = (f^* \circ g^*)(\psi_3) = f^*(g^*(\psi_3)) = 1 \circ g \circ f = g \circ f$, поэтому $\operatorname{Im} f \subset \operatorname{Ker} g$. Возьмем $N = M_3/\operatorname{Im} g$ и естественную проекцию $\psi_3 : M_3 \to N$. Тогда $g^*(\psi_3) = \psi_3 \circ g = 0$, поэтому $\psi_3 = 0$, то есть $N = 0$, то есть $\operatorname{Im} g = M_3$. Наконец, возьмем $N = M_2/\operatorname{Im} f$ и естественное вложение $\psi_2 : M_2 \to N$. Тогда $f^*(\psi_2) = \psi_2 \circ f = 0$, поэтому $\psi_2 = g^*(\psi_3) = \psi_3 \circ g$. Значит $\operatorname{Im} f = \operatorname{Ker}\psi_2 \supset \operatorname{Ker} g$. □

Лемма 1.3. *Если* P *— свободный модуль, а* $f : M \to M'$ *— эпиморфизм, то для всякого морфизма* $\phi' : P \to M'$ *найдется морфизм* $\phi : P \to M$*, такой что* $\phi' = f \circ \phi$*.*

Доказательство: всякий морфизм из P однозначно задается своими значениями на произвольном базисе $\{e_i\}$ модуля P, поэтому достаточно выбрать прообразы элементов $\phi'(e_i)$ относительно f. □

Лемма 1.4. *Пусть последовательность* $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ *точна.*
(*i*) *Если* N *свободен, то* $0 \to \operatorname{Hom}_A(N, M_1) \xrightarrow{f_*} \operatorname{Hom}_A(N, M_2) \xrightarrow{g_*} \operatorname{Hom}_A(N, M_3) \to 0$ *точная тройка.*
(*ii*) *Если* M_3 *свободен, то* $0 \to \operatorname{Hom}_A(M_3, N) \xrightarrow{g^*} \operatorname{Hom}_A(M_2, N) \xrightarrow{f^*} \operatorname{Hom}_A(M_1, N) \to 0$ *точная тройка.*

Доказательство: (*i*) Достаточно проверить сюръективность морфизма g_*, но она равносильна тому, что всякий морфизм из Nв M_3 можно поднять вдоль g.
(*ii*) Достаточно проверить сюръективность морфизма f^*. Поднимая тождественный морфизм $M_3 \to M_3$ вдоль g, получаем морфизм $s : M_3 \to M_2$, такой что $g \circ s = 1_{M_3}$. Ясно, что s — вложение. Докажем, что композиция $\bar{f} : M_1 \xrightarrow{f} M_2 \to M_2/s(M_3)$ — изоморфизм. Действительно, $\bar{f}(m_1) = 0 \Longrightarrow f(m_1) = s(m_3) \Longrightarrow m_3 = g(s(m_3)) = g(f(m_1)) = 0 \Longrightarrow m_1 \in \operatorname{Ker} f = 0$. Кроме того, если $m_2 \in M_2$, то $g(m_2 - s(g(m_2))) = g(m_2) - g(s(g(m_2))) = g(m_2) - g(m_2) = 0$, поэтому $m_2 - s(g(m_2)) = f(m_1)$ и $m_2 = f(m_1) + s(g(m_2))$. Следовательно, $\bar{f}$ — эпиморфизм. Обозначим через p композицию $M_2 \to M_2/s(M_3) \xrightarrow{\bar{f}^{-1}} M_1$. Тогда $p \circ f = 1_{M_1}$ и для всякого морфизма $\psi : M_1 \to N$ имеем $\psi = \psi \circ p \circ f = f^*(\psi \circ p)$, поэтому f^* сюръективен. □

Замечание 1.5. Фактически, мы доказали, всякая точная тройка со свободным M_3 расщепляется, то есть изоморфна тройке $0 \to M_1 \xrightarrow{(1,0)} M_1 \oplus M_3 \xrightarrow{(0,1)} M_3 \to 0$.

Определение 1.6. Функтор называется точным слева (точным справа, точным), если он переводит всякую точную последовательность в последовательность точную слева (точную справа, точную).

Следствие 1.7. *Функтор* Hom *точен слева как по первому, так и по второму аргументу.*

Часть 2. Функторы Ext

Определение 2.1. Пусть $\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$ — левая свободная резольвента, то есть точная последовательность A-модулей, в которой все модули P^i свободные. Определим группы расширений

$$\operatorname{Ext}^p_A(M,N) := H^p(\operatorname{Hom}_A(P_\bullet, N))$$

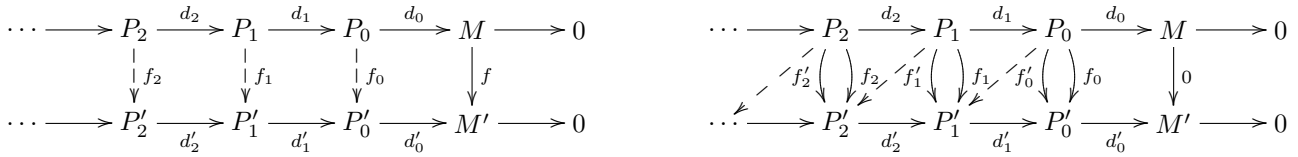
как когомологии комплекса $0 \to \operatorname{Hom}_A(P_0,N) \to \operatorname{Hom}_A(P_1,N) \to \operatorname{Hom}_A(P_2,N) \to \dots$.

Лемма 2.2. *Всякий модуль над кольцом имеет свободную резольвенту.*

Доказательство: если $\{m_i\}_{i\in I}$ — набор (возможно бесконечный) образующих A-модуля M, то гомоморфизм $\oplus_{i\in I} A \to M$ сюръективен. Иначе говоря, у всякого A-модуля есть "свободная накрывающая". Пользуясь этим фактом строим резольвенту последовательно: в качестве P_0 берем свободную накрывающую M, в качестве P_1 берем свободную накрывающую A-модуля $\operatorname{Ker}(P_0 \to M)$, в качестве P_2 берем свободную накрывающую A-модуля $\operatorname{Ker}(P_1 \to P_0)$ и т.д. □

Возникает вопрос, зависит ли группа $\operatorname{Ext}^p_A(M,N)$ от выбора резольвенты.

Лемма 2.3. *Если $P_\bullet \to M$ и $P'_\bullet \to M'$ — свободные резольвенты, а $f : M \to M'$ — гомоморфизм, то существует морфизм комплексов $f_\bullet : P_\bullet \to P'_\bullet$, коммутирующий с f. Более того, если $f'_\bullet : P_\bullet \to P'_\bullet$ — другой такой морфизм комплексов, то морфизмы $f'_\bullet$ и $f_\bullet$ гомотопны, то есть существует последовательность морфизмов $h_i : P_i \to P'_{i+1}$, так что $f'_i - f_i = h_{i-1}d_i + d_{i+1}h_i$.*



Доказательство: морфизмы f_i будем строить последовательно, положив $f_{-1} = f$. Если f_i уже построен, то заметим, что $d'_i f_i d_{i+1} = f_{i-1} d_i d_{i+1} = 0$, поэтому $\operatorname{Im}(d_{i+1}f_i) \subset \operatorname{Ker} d'_i = \operatorname{Im} d'_{i+1}$, следовательно найдется f_{i+1}, такой что $d'_{i+1}f_{i+1} = f_i d_{i+1}$. Морфизмы h_i будем строить последовательно, положив $h_{-1} = 0$. Если h_{i-1} уже построен, то заметим, что $d'_i(f'_i - f_i - h_{i-1}d_i) = d'_i f'_i - d'_i f_i - d'_i h_{i-1} d_i = f'_{i-1}d_i - f_{i-1}d_i - d'_i h_{i-1} d_i = (f'_{i-1} - f_{i-1} - d'_i h_{i-1}) d_i = h_{i-2} d_{i-1} d_i = 0$, поэтому $\operatorname{Im}(f'_i - f_i - h_{i-1}d_i) \subset \operatorname{Ker} d'_i = \operatorname{Im} d'_{i+1}$, следовательно найдется h_i, такой что $d'_{i+1}h_i = f'_i - f_i - h_{i-1}d_i$. □

Следствие 2.4. *Группы $\operatorname{Ext}^p_A(M,N)$ определены однозначно с точностью до канонического изоморфизма.*

Доказательство: пусть $P^\bullet \to M$ и $P'_\bullet \to M$ — свободные резольвенты. Тождественный морфизм 1_M можно продолжить до морфизма резольвент $f_\bullet : P_\bullet \to P'_\bullet$, который индуцирует морфизм комплексов $f^*_\bullet : \operatorname{Hom}_A(P'_\bullet, N) \to \operatorname{Hom}_A(P_\bullet, N)$ и их когомологий $H^p f^*_\bullet : \operatorname{Ext}^p_A(M,N) \to \operatorname{Ext}^p_A(M,N)$. При этом, если $f'_\bullet$ — другой морфизм резольвент, то гомотопия $h_\bullet$, соединяющая $f_\bullet$ и $f'_\bullet$ индуцирует гомотопию, соединяющую $f^*_\bullet$ и $f'^*_\bullet$, следовательно $H^p f^*_\bullet = H^p f'^*_\bullet$. Таким образом, мы получаем канонический морфизм. Чтобы проверить, что он является изоморфизмом, рассмотрим морфизм резольвент $g_\bullet : P'_\bullet \to P_\bullet$, продолжающий 1_M. Тогда $H^p f^*_\bullet \circ H^p g^*_\bullet = H^p(f^*_\bullet \circ g^*_\bullet) = H^p((g_\bullet \circ f_\bullet)^*)$, но морфизм резольвент $g_\bullet \circ f_\bullet : P_\bullet \to P_\bullet$ продолжает морфизм 1_M, также как и $1_{P_\bullet}$, поэтому $H^p((g_\bullet \circ f_\bullet)^*) = H^p(1^*_{P_\bullet}) = \mathrm{Id}$. Таким образом, $H^p f^*_\bullet \circ H^p g^*_\bullet = \mathrm{Id}$. Аналогично доказывается $H^p g^*_\bullet \circ H^p f^*_\bullet = \mathrm{Id}$. □

Следствие 2.5. Ext^p_A *является функтором как по первому, так и по второму аргументам.*

Лемма 2.6. *(i) Функторы Ext^p_A коммутируют с прямыми суммами; (ii) $\operatorname{Ext}^0(M,N) = \operatorname{Hom}_A(M,N)$; (iii) если M свободен, то $\operatorname{Ext}^p(M,N) = 0$ при $p > 0$ для всех N.*

Доказательство: (*i*) Если $P_\bullet \to M$ и $P'_\bullet \to M'$ — свободные резольвенты, то $P_\bullet \oplus P'_\bullet \to M \oplus M'$ — свободная резольвента, значит $\operatorname{Ext}^p_A(M \oplus M', N) = H^p(\operatorname{Hom}_A(P_\bullet \oplus P'_\bullet, N)) = H^p(\operatorname{Hom}_A(P_\bullet, N) \oplus \operatorname{Hom}_A(P'_\bullet, N)) = H^p(\operatorname{Hom}_A(P_\bullet, N)) \oplus (\operatorname{Hom}_A(P'_\bullet, N)) = \operatorname{Ext}^p_A(M,N) \oplus \operatorname{Ext}^p_A(M',N)$. (*ii*) Применяя к точной последовательности $P_1 \to P_0 \to M \to 0$ точный слева функтор $\operatorname{Hom}_A(-,N)$, получаем точную слева последовательность

$0 \to \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(P_0,N) \to \mathrm{Hom}_A(P_1,N)$, откуда $\mathrm{Ext}^0_A(M,N) = H^0(\mathrm{Hom}_A(P_\bullet,N)) = \mathrm{Hom}_A(M,N)$. (*iii*) Если M свободен, то полагая $P_0 = M$, $P_{>0} = 0$ получаем свободную резольвенту, и в комплексе $\mathrm{Hom}_A(P_\bullet,N)$ все члены, начиная с первого зануляются, значит $\mathrm{Ext}^p_A(M,N) = 0$ при $p > 0$. □

Легко видеть, что когомологии групп являются частным случаем функтора Ext. А именно, стандартная резольвента является свободной резольвентой тривиального G-модуля $\mathbb{Z}$ в категории $\mathbb{Z}[G]$-модулей. Поэтому,

$$H^p(G,M) = \mathrm{Ext}^p_{\mathbb{Z}[G]}(\mathbb{Z},M).$$

Теорема 2.7. *Всякой точной тройке* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *соответствуют функториальные точные последовательности*

$$0 \to \mathrm{Hom}(M'',N) \to \mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N) \xrightarrow{\delta} \mathrm{Ext}^1(M'',N) \to \mathrm{Ext}^1(M,N) \to \mathrm{Ext}^1(M',N) \xrightarrow{\delta} \mathrm{Ext}^2(M'',N) \to \dots$$
$$0 \to \mathrm{Hom}(N,M') \to \mathrm{Hom}(N,M) \to \mathrm{Hom}(N,M'') \xrightarrow{\delta} \mathrm{Ext}^1(N,M') \to \mathrm{Ext}^1(N,M) \to \mathrm{Ext}^1(N,M'') \xrightarrow{\delta} \mathrm{Ext}^2(N,M') \to \dots$$

Доказательство: можно выбрать свободные резольвенты $P'_\bullet \to M'$, $P''_\bullet \to M''$ и $P_\bullet \to M$, а также морфизмы резольвент $f_\bullet : P'_\bullet \to P_\bullet$ и $g_\bullet : P_\bullet \to P''_\bullet$ таким образом, что последовательность $0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$ будет точна. Применяя функтор $\mathrm{Hom}_A(-,N)$ получим точную последовательность $0 \to \mathrm{Hom}_A(P''_\bullet,N) \to \mathrm{Hom}_A(P_\bullet,N) \to \mathrm{Hom}_A(P'_\bullet,N) \to 0$ так как $P''_\bullet$ свободен. Теперь первая точная последовательность групп Ext получается применением леммы о змее. Вторая последовательность групп Ext строится так же как и точная последовательность когомологий группы. Выбираем свободную резольвенту $Q_\bullet \to N$, применяем функтор $\mathrm{Hom}_A(Q_\bullet,-)$, получаем точную последовательность комплексов $0 \to \mathrm{Hom}_A(Q_\bullet,M') \to \mathrm{Hom}_A(Q_\bullet,M) \to \mathrm{Hom}_A(Q_\bullet,M'') \to 0$ и пользуемся леммой о змее. □

Часть 3. Расширения

Определение 3.1. Расширением A-модуля M с помощью A-модуля N называется точная тройка A-модулей вида $0 \to N \xrightarrow{i} E \xrightarrow{\pi} M \to 0$. Расширения (E,i,π) и (E',i',π') называются эквивалентными, если существует изоморфизм $\phi : E \to E'$, такой что $i' = \phi \circ i$, $\pi = \pi' \circ \phi$. Расширение называется тривиальным, если оно эквивалентно расширению $0 \to N \xrightarrow{(1,0)} N \oplus M \xrightarrow{(0,1)} M \to 0$.

Теорема 3.2. *Расширения A-модуля M с помощью N нумеруются элементами группы* $\mathrm{Ext}^1_A(M,N)$.

Доказательство: пусть $0 \to N \to E \to M \to 0$ — расширение. Применяя функтор $\mathrm{Hom}_A(M,-)$ получаем точную последовательность $0 \to \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,E) \to \mathrm{Hom}(M,M) \xrightarrow{\delta} \mathrm{Ext}^1(M,N) \to \dots$. Сопоставим расширению элемент $\delta(1_M) \in \mathrm{Ext}^1(M,N)$. Из функториальности следует, что эквивалентным расширениям соответствуют одинаковые элементы в группе $\mathrm{Ext}^1(M,N)$. Обратно, всякому элементу $\varepsilon \in \mathrm{Ext}^1(M,N)$ сопоставим расширение таким образом. Выберем свободную резольвенту $\dots \to P_2 \to P_1 \to P_0 \to M \to 0$ и морфизм $f : P_1 \to N$, представляющий ε. Тогда $d_1^* f = f \circ d_2 = 0$. Рассмотрим отображение $\phi : P_1 \to N \oplus P_0$, $p_1 \mapsto (fp_1, d_1p_1)$, и определим $E = \mathrm{Coker}\,\phi := (N \oplus P_0)/\mathrm{Im}\,\phi$. Пусть, наконец $i : N \to E$ формулой $i(n) = (n,0) \pmod{\mathrm{Im}\,\phi}$, и $\pi : E \to M$ формулой $\pi(n,p_0) = d_0p_0$ (если $(n,p_0) \in \mathrm{Im}\,\phi$, то $(n,p_0) = (fp_1, d_1p_1)$ и $d_0p_0 = d_0d_1p_1 = 0$). Докажем, что $0 \to N \xrightarrow{i} E \xrightarrow{\pi} M \to 0$ — точная последовательность. Действительно, $\pi(i(n)) = \pi(n,0) = d_00 = 0$, значит $\mathrm{Im}\,i \subset \mathrm{Ker}\,\pi$. Кроме того, если $i(n) = 0$, то $(n,0) = (fp_1, d_1p_1)$, в частности $d_1p_1 = 0$, то есть $p_1 = d_2p_2$, и $n = fp_1 = fd_2p_2 = 0$. Значит i — вложение. Далее, π — сюръекция, так как $d_0 : P_0 \to M$ — сюръекция. Наконец, если $\pi(n,p_0) = 0$, то $d_0p_0 = 0$, значит $p_0 = d_1p_1$, следовательно $(n,p_0) = (n - fp_1, 0) + (fp_1, d_1p_1) = i(n - fp_1) \pmod{\mathrm{Im}\,\phi}$, то есть $\mathrm{Ker}\,\pi = \mathrm{Im}\,i$.

Часть 4. Тензорное произведение

Лемма 4.1. *Последовательность* $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ *точна справа* $\iff$ *для любого A-модуля N последовательность* $M_1 \otimes_A N \xrightarrow{f\otimes 1} M_2 \otimes_A N \xrightarrow{g\otimes 1} M_3 \otimes_A N \to 0$ *точна справа.*

Доказательство: согласно предыдущей лемме последовательнсоть $M_\bullet \otimes_A N$ точна справа $\iff \forall P$ последовательность $\mathrm{Hom}_A(M_\bullet \otimes_A N, P) \cong \mathrm{Hom}_A(M_\bullet, \mathrm{Hom}_A(N,P))$ точна слева $\iff$ последовательнсоть $M_\bullet$ точна сплева, так как всякий A-модуль можно представить в виде $\mathrm{Hom}_A(N,P)$ (так как $\mathrm{Hom}_A(A,P) \cong P$). □

Эта лемма дает простой способ вычисления тензорного произведения модулей. Представим модуль M как коядро отображения свободных модулей: $A^m \xrightarrow{f} A^n \to M \to 0$, где $f = (f_{ij})$ — матрица с коэффициентами в A. Тогда имеем точную последовательность $N^{\oplus m} \xrightarrow{f} N^{\oplus n} \to M \otimes_A N \to 0$.

Следствие 4.2. *Имеем* $A/\mathfrak{a} \otimes_A M \cong M/\mathfrak{a}M$.

Лекция 7. Расширения колец и полей

Часть 1. Целые расширения колец

Пусть $A \subset B$ — вложение (расширение) колец. Для вского $x \in B$ будем обозначать через $A[x]$ подкольцо в B, порожденное над A элементом x, то есть образ кольца $A[X]$ при гомоморфизме $A[X] \to B$, $X \mapsto x$.

Определение 1.1. Элемент $x \in B$ называется целым над A, если он является корнем многочлена с коэффициентами в A и старшим коэффициентом 1, то есть $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.

Лемма 1.2. *Следующие условия равносильны:*
(i) элемент $x \in B$ цел над A;
(ii) подкольцо $A[x] \subset B$ является конечно порожденным A-модулем;
(iii) x содержится в подкольце $C \subset B$, являющемся конечно порожденным A-модулем.

Доказательство: $(i) \Longrightarrow (ii)$ элементы $1, \ldots, x^{n-1}$ порождают $A[x]$ над A. $(ii) \Longrightarrow (iii)$ Возьмем $C = A[x]$. $(iii) \Longrightarrow (i)$ Пусть элементы $e_1, \ldots, e_n \in C$ порождают C как A-модуль, причем будем считать, что $e_1 = 1$. Тогда $xe_i = \sum a_{ij} e_j$, поэтому матрица $(x\delta_{ij} - a_{ij})$ действует нулем на каждый из элементов e_i. Следовательно, многочлен $f(x) = \det(x\delta_{ij} - a_{ij}) = \widehat{(x\delta_{ij} - a_{ij})}(x\delta_{ij} - a_{ij})$ действует нулем на каждый из e_i. В частности, $f(x) = f(x) \cdot 1 = f(x)e_1 = 0$. Остается заметить, что $f(x)$ имеет коэффициенты в A, а его старший коэффициент равен 1. □

Лемма 1.3. *Сумма и произведение целых элементов цело.*

Доказательство: если x и y целы над A, то $A[x, y]$ является конечно порожденным A-модулем (мономы $x^i y^j$, $i \leqslant m$, $j \leqslant n$ порождают $A[x, y]$ над A). Кроме того, $A[x, y]$— подкольцо, содержащее как $x + y$, так и xy. □

Следствие 1.4. *Если $A \subset B$ — расширение колец, то множество элементов кольца B, целых над A является подкольцом в B.*

Подкольцо элементов кольца B, целых над A называется целым замыканием A в B. Если целое замыкание A в B совпадает с B, то говорят, что B цело над A (является целым расширением кольца A).

Лемма 1.5. *Если $A \subset B \subset C$ — расширения колец, B цело над A, и $x \in C$ цел над B, то x цел над A.*

Доказательство: пусть $x^n + b_1 x^{n-1} + \cdots + b_n = 0$, $b_i \in B$. Тогда $A[x, b_1, \ldots, b_n]$ является конечно порожденным $A[b_1, \ldots, b_n]$-модулем, но $A[b_1, \ldots, b_n]$ является конечно порожденным A-модулем (так как b_i целы над A). Значит $A[x, b_1, \ldots, b_n]$ является конечно порожденным A-модулем, следовательно x цел над A. □

Следствие 1.6. *Если $A \subset B \subset C$ — расширения колец, и B цело над A, то целое замыкание A в C совпадает с целым замыканием B в C.*

Если целое замыкание A в B совпадает с A, то говорят, что A целозамкнуто в B. Целостное кольцо A называется целозамкнутым, если оно целозамкнуто в своем поле частных $F(A)$.

Лемма 1.7. *Целое замыкание A в B целозамкнуто в B.*

Доказательство: если $x \in B$ цел над целым замыканием $\bar{A}$ кольца A в B, то x цел над A, то есть $x \in \bar{A}$. □

Следствие 1.8. *Целое замыкание целостного кольца A в поле его частных целозамкнуто.*

Лемма 1.9. *Если $A \subset B$— целое расширение целостных колец, то расширение полей $F(A) \subset F(B)$ — алгебраическое.*

Доказательство: если $x \in B$, то $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, то x алгебраичен над $F(A)$. Кроме того, если $y \in B$, то $y^m + a'_1 y^{m-1} + \cdots + a'_m = 0$, поэтому $a'_m y^{-m} + \cdots + a'_1 y^{-1} + 1 = 0$, значит y^{-1} алгебраичен над $F(A)$. Значит x/y алгебраичен над $F(A)$, то есть $F(A) \subset F(B)$ алгебраическое расширение. □

Часть 2. Конечные морфизмы

Лемма 2.1. *Если $A \subset B$ — целое расширение целостных колец, то A — поле $\iff$ B — поле.*

Доказательство: если A — поле, $x \in B$ и $X^n + a_1X^{n-1} + \cdots + a_n$ — многочлен минимальной степени со старшим коэфициентом 1, корнем которого является x, то $a_n \neq 0$, значит $-a_n^{-1}(x^{n-1}+a_1x^{n-2}+\cdots+a_{n-1})x = 1$, значит x — обратим. Если же B — поле, и $x \in A$, то $x^{-1} \in B$, значит $x^{-n}+a_1x^{1-n}+\cdots+a_n = 0$ для некоторых $a_1, \ldots, a_n \in A$, значит $x^{-1} = -a_1 - \cdots - a_nx^{n-1} \in A$. □

Гомоморфизм колец $f : A \to B$ называется целым, если кольцо B цело над $f(A)$.

Лемма 2.2. *Если $f : A \to B$ — целый морфизм, $\mathfrak{b} \subset B$ — идеал, и $\mathfrak{a} = f^{-1}(\mathfrak{b})$, то $A/\mathfrak{a} \subset B/\mathfrak{b}$ — целое расширение.*

Доказательство: поднимем элемент $\bar{x} \in B/\mathfrak{b}$ до элемента $x \in B$ и найдем элементы $a_i \in A$, такие что $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Тогда $\bar{x}^n + \bar{a_1}\bar{x}^{n-1} + \cdots + \bar{a_n} = 0$. □

Следствие 2.3. *Если $f : A \to B$ — целый морфизм, то $\mathfrak{b} \subset B$ максимален $\iff$ $f^{-1}(\mathfrak{b}) \subset A$ максимален.*

Лемма 2.4. *Если $f : A \to B$ — целый морфизм, $\mathfrak{a} \subset A$ — идеал, и $\mathfrak{b} = Bf(\mathfrak{a}) \subset B$, то $A/\mathfrak{a} \to B/\mathfrak{b}$ — целое расширение.*

Доказательство: $B/\mathfrak{b}$ цело над $A/f^{-1}(\mathfrak{b})$, а $A/f^{-1}(\mathfrak{b})$ цело над $A/\mathfrak{a}$, так как $\mathfrak{a} \subset f^{-1}(f(\mathfrak{a})) \subset f^{-1}(Bf(\mathfrak{a})) = f^{-1}(\mathfrak{b})$. Значит $B/\mathfrak{b}$ цело над $A/\mathfrak{a}$. □

Лемма 2.5. *Если кольцо A является целым расширением поля k и конечно порождено над k, то A имеет лишь конечное число максимальных идеалов.*

Доказательство: пусть $x_1, \ldots, x_n$ порождают A над k, и $X \subset \mathbb{A}^n$ — соответствующее алгебраическое многообразие. Так как каждое из x_i является корнем многочлена с коэффициентами в k, то каждая координата точки из X может принимать лишь конечное число значений (корней соответствующего многочлена). Поэтому число точек в X конечно, а значит, по теореме Гильберта о нулях, конечно и количество максимальных идеалов в A. □

Теорема 2.6. *Пусть X, Y — аффинные алгебраические многообразия, $f : X \to Y$ — морфизм, такой что морфизм колец $f^* : A_Y \to A_X$ целый. Тогда каждая точка многообразия Y имеет конечное число прообразов в X.*

Доказательство: если $f(x) = y$, то $f^*(\mathfrak{m}_y) \subset \mathfrak{m}_x$, поэтому достаточно проверить, что существует лишь конечное число максимальных идеалов в A_X, содержащих $f^*(\mathfrak{m}_y)$. Однако, ясно что эти идеалы находятся в биекции с максимальными идеалами кольца $A_X/A_Xf^*(\mathfrak{m}_y)$, которое является конечно порожденным целым расширением поля $A_Y/\mathfrak{m}_y$. □

Морфизмы алгебраических многообразий, соответствующие целым морфизмам колец, называются конечными морфизмами.

Часть 3. Трансцендентные расширения полей

Пусть K/k — расширение полей. Набор элементов $\{ x_i \}_{i \in I}$ называется алгебраически независимым над k, если не существует нетривиального многочлена с коэффициентами в k, обращающегося в нуль при подстановке в него x_i. Иначе говоря, если гомоморфизм $\mathsf{k}[X_i]_{i \in I} \to K$, $X_i \mapsto x_i$ инъективен.

Лемма 3.1. *Если набор элементов $\{ x_i \}_{i \in I}$ алгебраически независимым над k, то гомоморфизм $\mathsf{k}[X_i]_{i \in I} \to K$, $X_i \mapsto x_i$ продолжается до вложения полей $\mathsf{k}(X_i)_{i \in I} \to K$.*

Доказательство: поле $\mathsf{k}(X_i)_{i \in I}$ является полем частных кольца $\mathsf{k}[X_i]_{i \in I}$, поэтому вложение $\mathsf{k}[X_i]_{i \in I} \to K$ продолжается до вложения полей $\mathsf{k}(X_i)_{i \in I} \to K$. □

Определение 3.2. Набор элементов $\{ x_i \}_{i \in I}$ порождает поле K над k, если всякий элемент из k можно представить в виде рациональной функции от x_i с коэффициентами в k. Расширение полей K/k называется конечно порожденным, если найдется конечное множество элементов $x_1, \ldots, x_n \in K$, порождающих K над k.

Лемма 3.3. *Если K/k расширение полей, то в любой системе образующих K над k найдется набор алгебраически независимых элементов $\{x_i\}_{i\in I}$, такой что расширение $K/\mathsf{k}(x_i)_{i\in I}$ является алгебраическим.*

Доказательство: возьмем произвольный набор образующих $\{x_j\}_{j\in J}$ и выберем в нем максимальный алгебраически независимый поднабор $\{x_i\}_{i\in I}$ $(I\subset J)$ (для доказательства его существования надо воспользоваться леммой Цорна). Тогда любая из образующих x_j поля K над k алгебраична над $\mathsf{k}(x_i)_{i\in I}$. Кроме того, любой элемент поля K лежит в подполе, порожденным конечным количеством элементов x_j над $\mathsf{k}(x_i)_{i\in I}$. Следовательно, все элементы поля K алгебраичны над $\mathsf{k}(x_i)_{i\in I}$. □

Набор алгебраически независимых над k элементов $\{x_i\}_{i\in I}$, поля K такой что расширение $K/\mathsf{k}(x_i)_{i\in I}$ алгебраическое, называется базисом трансцендентности K над k.

Следствие 3.4. *Если K конечно порождено над k, то K обладает конечным базисом трансцендентности.*

Теорема 3.5. *Любые два базиса транцендентности равномощны.*

Доказательство: докажем утверждение в случае, когда один из базисов конечен. Пусть $\{x_1,\dots,x_m\}$ — базис трансцендентности. Достаточно проверить, что если набор $\{y_1,\dots,y_n\}$ алгебраически независим, то $n\leqslant m$. Действительно, y_1 алгебраичен над $\mathsf{k}(x_1,\dots,x_m)$, поэтому найдется многочлен f_1, такой что $f_1(y_1,x_1,\dots,x_m)=0$. Ясно, что хотя бы один из элементов x_i входит в f (иначе y_1 был бы алгебраичен над k, что протеворечит алгебраической независимости набора $\{y_1,\dots,y_n\}$). Перенумеровав x_i можно считать, что это x_1. Следовательно, x_1 алгебраичен над $\mathsf{k}(y_1,x_2,\dots,x_m)$, а значит K алгебраично над $\mathsf{k}(y_1,x_2,\dots,x_m)$. Далее, y_2 алгебраичен над $\mathsf{k}(y_1,x_2,\dots,x_m)$, поэтому найдется многочлен f_2, такой что $f_2(y_1,y_2,x_2,\dots,x_m)=0$. Ясно, что хотя бы один из элементов x_i входит в f (иначе y_1 и y_2 были бы алгебраически зависимы). Перенумеровав x_i можно считать, что это x_2. Следовательно, x_2 алгебраичен над $\mathsf{k}(y_1,y_2,x_3,\dots,x_m)$, а значит K алгебраично над $\mathsf{k}(y_1,y_2,x_3,\dots,x_m)$. Если $n>m$ то подобными рассуждениями доказываем, что K алгебраично над $\mathsf{k}(y_1,\dots,y_m)$, что противоречит алгебраической независимости набора $\{y_1,\dots,y_n\}$. □

Мощность базиса трансцендентности K над k называется его степенью трансцендентности над k и обозначается $\operatorname{degtr} K/\mathsf{k}$.

Часть 4. Лемма Нетер о нормализации

Теорема 4.1. *Если A — конечно порожденная k-алгебра, то существует конечное число алгебраически независимых над k элементов $y_1,\dots,y_r\in A$, таких что A цело над $\mathsf{k}[y_1,\dots,y_r]$.*

Доказательство: докажем утверждение для бесконечного поля k. Выберем конечный набор образующих $x_1,\dots,x_n$ алгебры A над k и докажем утверждение индукцией по n. Если $x_1,\dots,x_n$ алгебраически независимы, то доказывать нечего. Иначе, пусть $f(x_1,\dots,x_n)=0$. Пусть $F(x_1,\dots,x_n)$ — однородная компонента старшей степени и пусть $F(\lambda_1,\dots,\lambda_n)\neq 0$. Перенумеровав переменные, можно считать, что $\lambda_n\neq 0$. Пусть $x_i'=x_i-\lambda_i/\lambda_n x_n$. Тогда $f(x_1,\dots,x_n)=F(x_1,\dots,x_n)+\dots=F(x_1'+\lambda_1/\lambda_n x_n,\dots,x_{n-1}'+\lambda_{n-1}/\lambda_n x_n,x_n)+\dots=F(\lambda_1/\lambda_n,\dots,\lambda_{n-1}/\lambda_n,1)x_n^N+\dots=F(\lambda_1,\dots,\lambda_n)\lambda_n^{-N}x_n^N+\dots$, поэтому x_n цел над $\mathsf{k}[x_1',\dots,x_{n-1}']$, то есть A цело над $\mathsf{k}[x_1',\dots,x_{n-1}']$. По предположению индукции найдется алгебраически независимый набор $y_1,\dots,y_r\in\mathsf{k}[x_1',\dots,x_{n-1}']$, такой что $\mathsf{k}[x_1',\dots,x_{n-1}']$ цело над $\mathsf{k}[y_1,\dots,y_r]$. Но тогда и A цело над $\mathsf{k}[y_1,\dots,y_r]$. □

Замечание 4.2. Геометрический смысл доказательства таков: мы рассматриваем соответствующее алгебре A многообразие $X\subset\mathbb{A}^n$, выбираем гиперповерхность $f(x)=0$, содержащую X, и рассматриваем проекцию из точки, не лежащей на этой гиепрповерхности.

Лемма 4.3. *Если A — целостное кольцо, элементы $y_1,\dots,y_r\in A$ алгебраически независимы над k и A цело над $\mathsf{k}[y_1,\dots,y_r]$, то $\operatorname{degtr} F(A)/k=r$.*

Доказательство: $F(A)$ алгебраично над $\mathsf{k}(y_1,\dots,y_r)$, а $\operatorname{degtr}\mathsf{k}(y_1,\dots,y_r)/\mathsf{k}=r$, так как $y_1,\dots,y_r$ образуют базис трансцендентности. □

Таким образом, степень трансцендентности поля частных кольца функций на неприводимом алгебраическом многообразии является алгебраическим способом определить размерность многообразия: $\dim X=\operatorname{degtr} A_X$.

Лекция 8. Симметрические многочлены

Часть 1. Кольца инвариантов

Пусть G — конечная группа автоморфизмов k-алгебры A (то есть $g(a+b) = ga+gb$, $g(ab) = (ga)(gb)$ и $g\lambda = \lambda$ для всех $g \in G$, $\lambda \in \mathsf{k}$). Например, $A = \mathsf{k}[x_1, \ldots, x_n]$, а $G = \mathfrak{S}_n$ действует на A перестановками переменных.

Алгеброй инвариантов называется множество $A^G = \{\, a \in A \mid ga = a \ \forall g \in G \,\}$. Легко видеть, что A^G является подалгеброй в A. Заметим, что поле k содержится в алгебре инвариантов.

Лемма 1.1. *Расширение колец $A^G \subset A$ целое.*

Доказательство: для всякого $a \in A$ многочлен $f(x) = \prod_{g\in G}(x - ga) \in A[x]$ инвариантен относительно действия группы G, следовательно $f(x) \in A^G[x]$. Кроме того, старший коэффициент $f(x)$ равен 1, и $f(a) = 0$. Значит a цел над A^G. □

Лемма 1.2. *Если алгебра A конечно порождена, то A является конечно порожденным A^G-модулем.*

Доказательство: пусть $x_1, \ldots, x_n$ порождают A над k. Каждый из x_i целый над A^G, то есть $x_i^{d_i} = \sum_{j=0}^{d_i-1} b_{ij}x_i^j$, где $b_{ij} \in A^G$. Следовательно, мономы $\prod_{i=1}^n x_i^{k_i}$, $0 \leqslant k_i < d_i$ порождают A как A^G-модуль. □

Теорема 1.3. *Если алгебра A конечно порождена, то алгебра инвариантов A^G тоже конечно порождена.*

Доказательство: воспользуемся тем же рассуждением, что и при доказательстве теоремы Гильберта о нулях. Пусть $a_1, \ldots, a_n$ порождают A как k-алгебру, а $e_1, \ldots, e_l$ — порождают A как A^G-модуль. Тогда для всех $1 \leqslant i, j \leqslant n$ имеем

$$a_i = \sum_{k=1}^{l} \lambda_{ik}e_k, \qquad e_ie_j = \sum_{k=1}^{l} \mu_{ijk}e_k, \qquad \lambda_{ik}, \mu_{ijk} \in A^G.$$

Пусть $B \subset A^G$ — алгебра, порожденная над k элементами λ_{ik}, μ_{ijk}. Тогда B конечно порождена, следовательно нетерова. Из предыдущих равенств следует, что не только a_i, но и все их произведения представляются в виде линейной комбинации элементов e_i с коэффициентами в B, следовательно элементы $e_1, \ldots, e_l$ порождают A как B-модуль. Значит A — конечно порожденный B-модуль, следовательно A^G — тоже конечно порожденный B-модуль, так как $A^G \subset A$, следовательно A^G — конечно порожденная B-алгебра, следовательно A^G — конечно порожденная k-алгебра. □

В частности, алгебра инвариантов нетерова, если алгебра A конечно порождена, а группа G конечна. Можно однако показать, что алгебра инвариантов нетерова и в более общих предположениях. Всякому идеалу $I \subset A^G$ сопоставим идеал $AI \subset A$, а идеалу $J \subset A$ сопоставим идеал $J \cap A^G \subset A^G$.

Лемма 1.4. *Если порядок группы G взаимно прост с $\operatorname{char}\mathsf{k}$, то $I = AI \cap A^G$.*

Доказательство: вложение $I \subset AI \cap A^G$ очевидно. С другой стороны, всякий элемент идеала AI имеет вид $a = \sum a_ki_k$, где $a_k \in A$, $i_k \in I$. Применяя к нему оператор симметризации, получаем $\frac{1}{|G|}\sum_{g\in G} ga = \sum(\frac{1}{|G|}\sum_{g\in G} ga_k)i_k$, так как $i_k \in I \subset A^G$. Теперь, если $a \in AI \cap A^G$, то левая часть равна a, а правая лежит в $A^GI = I$, поэтому $a \in I$ и $AI \cap A^G = I$. □

Замечание 1.5. В доказательстве леммы фактически использовалсь не конечность группы G, а свойство полной приводимости ее представлений над полем k (оператор симметризации — это G-эквивариантный функториальный проектор на подпространство инвариантов). Группа, любое представление которой над полем k вполне приводимо, называется редуктивной (над полем k). Таким образом, предположение о взаимной простоте характеристики поля и порядка группы можно заменить на предположение о редуктивности группы G.

Следствие 1.6. *Если алгебра A нетерова, а группа G редуктивна, то алгебра инвариантов A^G нетерова.*

Доказательство: пусть $I_1 \subset I_2 \subset \cdots \subset A^G$ — возрастающая цепочка идеалов в A^G. Тогда $AI_1 \subset AI_2 \subset \cdots \subset A$ — возрастающая цепочка идеалов в A. Из нетеровости A следует, что $AI_{k+1} = AI_k$ при $k \gg 0$. Но тогда $I_{k+1} = AI_{k+1} \cap A^G = AI_k \cap A^G = I_k$, значит A^G нетерово. □

Изучим теперь геометрический смысл кольца инвариантов. Пусть $A = A_X$ — координатная алгебра многоюразия $X \subset \mathbb{A}^m$. Напомним, что функтор перехода от многообразия к его координатной алгебре вполне строгий (т.е. индуцирует биекцию на множестве морфизмов), поэтому действие группы G на A задает действие группы G на X. Далее, поскольку алгебра инвариантов A^G коммутативна и конечно порождена, то она является координатной алгеброй многообразия $Y \subset \mathbb{A}^n$, а вложение алгебр $A^G \to A$ индуцирует отображение многообразий $X \to Y$. Ясно, что при этом отображении точка, соответствующая максимальному идеалу $\mathfrak{m} \subset A$ переходит в точку, соответствующую максимальному идеалу $\mathfrak{m} \cap A^G \subset A^G$.

Лемма 1.7. *Пусть $\mathfrak{m}_0 \subset A^G$ — максимальный идеал. Всякий простой идеал $\mathfrak{p} \subset A$, такой что $\mathfrak{p} \cap A^G = \mathfrak{m}_0$ максимален, а группа G действует на множестве таких идеалов транзитивно.*

Доказательство: пусть $\mathfrak{m}, \mathfrak{p} \subset A$ — максимальный и простой идеалы, такие что $\mathfrak{m} \cap A^G = \mathfrak{p} \cap A^G = \mathfrak{m}_0$ и предположим, что $\forall g \in G$ имеем $\mathfrak{m} \not\subset g\mathfrak{p}$ (в противном случае $\mathfrak{m} \subset g\mathfrak{p}$ влечет $\mathfrak{m} = g\mathfrak{p}$ так как $\mathfrak{m}$ максимален, откуда следует как максимальность идеала $\mathfrak{p}$, так и транзитивность действия группы G). Тогда, согласно приведенной ниже лемме имеем $\mathfrak{m} \not\subset \bigcup_{g\in G} g\mathfrak{p}$. Выберем $a \in \mathfrak{m}$, так что $a \notin g\mathfrak{p}$ при всех $g \in G$ и рассмотрим $b = \prod_{g\in G} ga$. Ясно, что $b \in A^G$. Кроме того, $a \in \mathfrak{m}$, значит $b \in \mathfrak{m}$, значит $b \in \mathfrak{m} \cap A^G = \mathfrak{m}_0$. С другой стороны, при всех $g \in G$ имеем $ga \notin \mathfrak{p}$ (иначе $a \in g^{-1}\mathfrak{p}$), следовательно $b \notin \mathfrak{p}$ в силу простоты $\mathfrak{p}$, что противоречит тому, что $b \in \mathfrak{m}_0 = \mathfrak{p} \cap A^G$. □

Лемма 1.8. *Если $\mathfrak{a}$ — идеал, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ — простые идеалы и $\mathfrak{a} \not\subset \mathfrak{p}_i$ для всех i, то $\mathfrak{a} \not\subset \bigcup_{i=1}^n \mathfrak{p}_i$.*

Доказательство: воспользуемся индукцией по n. Случай $n = 1$ очевиден. Предположим, что утверждение доказано для $n-1$. Тогда для всех j имеем $\mathfrak{a} \not\subset \bigcup_{i\neq j} \mathfrak{p}_i$. Выберем элементы $x_j \in \mathfrak{a}$, $x_j \notin \bigcup_{i\neq j} \mathfrak{p}_i$, то есть $x_j \notin \mathfrak{p}_i$ при $i \neq j$. Если при каком-то j имеем $x_j \notin \mathfrak{p}_j$, то $x_j \in \mathfrak{a}$ и $x_j \notin \bigcup_{i=1}^n \mathfrak{p}_i$, и утверждение доказано. Иначе имеем $x_j \in \mathfrak{p}_j$ при всех j. Положим $x = \sum_{j=1}^n \prod_{i\neq j} x_i$. Тогда $x \in \mathfrak{a}$, но каждое из слагаемых $\prod_{i\neq j} x_i$ лежит в каждом из $\mathfrak{p}_i$ при $i \neq j$ и не лежит в $\mathfrak{p}_j$ (так как $\mathfrak{p}_j$ — простой). Следовательно $x \notin \bigcup_{j=1}^n \mathfrak{p}_j$ и утверждение доказано. □

Следствие 1.9. *Если $A = A_X$, где X — аффинное алгебраическое многообразие, то $A^G = A_Y$, где Y — аффинное алгебраическое многообразие, вложение $A^G \to A$ индуцирует отображение $X \to Y$, которое задает биекцию между множеством орбит действия G на X и множеством точек Y.*

Иначе говоря, многообразие Y является фактором многообразия X по действию конечной группы G и обозначается $X//G$.

Часть 2. Симметрические многочлены

Рассмотрим действие группы $\mathfrak{S}_n$ на аффинном пространстве $\mathbb{A}^n$ перестановками координат. Координатной алгеброй аффинного пространства является алгебра многочленов $\mathsf{k}[x_1, \ldots, x_n]$, поэтому координатной алгеброй фактора $\mathbb{A}^n//\mathfrak{S}_n$ является алгебра симметрических многочленов

$$\mathsf{k}[x_1, \ldots, x_n]^{\mathfrak{S}_n} := \{\, f(x_1, \ldots, x_n) \mid f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})\ \forall \sigma \in \mathfrak{S}_n \,\}.$$

Элементарными симметрическими многочленами называются многчлены

$$s_1 = x_1 + \cdots + x_n, \qquad \ldots \qquad s_k = \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} x_{i_1} \cdot \cdots \cdot x_{i_k}, \qquad \ldots \qquad s_n = x_1 \cdot \cdots \cdot x_n.$$

Лемма 2.1. *Элементарные симметрические многочлены порождают алгебру $\mathsf{k}[x_1, \ldots, x_n]^{\mathfrak{S}_n}$.*

Доказательство: поскольку элементарные симметрические многочлены однородны, то достаточно проверить, что всякий однородный симметрический многочлен степени d представляет как многочлен от симметрических. Воспользуемся одновременной индукцией по n и d. Основание индукции ($d = 1$) очевидно —

всякий однородный симметрический многочлен степени 1 равен λs_1, $\lambda \in \mathsf{k}$. Пусть теперь $f(x_1,\dots,x_n)$ — однородный симметрический многочлен степени d. Подставляя $x_n = 0$ получаем однородный симметрический многочлен степени d от переменных $x_1,\dots,x_{n-1}$, поэтому, по предположению индукции найдется многочлен $g(y_1,\dots,y_{n-1})$, такой что $f(x_1,\dots,x_{n-1},0) = g(s_1(x_1,\dots,x_{n-1},0),\dots,s_{n-1}(x_1,\dots,x_{n-1},0))$. Рассмотрим разность $f'(x_1,\dots,x_n) = f(x_1,\dots,x_n) - g(s_1(x_1,\dots,x_n),\dots,s_{n-1}(x_1,\dots,x_n))$. Ясно, что $f'(x_1,\dots,x_{n-1},0) = 0$, поэтому f' делится на x_n. Кроме того, f' симметрический многочлен, поэтому f' также делится и на каждое из x_i, $1 \leqslant i \leqslant n$. Но все x_i попарно взаимно просты, поэтому f' делится на $s_n = x_1 \cdot \dots \cdot x_n$, следовательно $f = g(s_1,\dots,s_{n-1}) + s_n f''$, причем f'' — однородный симметрический многочлен меньшей степени. Остается еще раз воспользоваться предположением индукции. □

Лемма 2.2. *Элементарные симметрические многочлены алгебраически независимы над* k.

Доказательство: определим $\deg' y_1^{k_1} \cdot \ldots \cdot y_n^{k_n} = \sum ik_i$. Тогда $\deg f(s_1,\dots,s_n) = \deg' f(y_1,\dots,y_n)$, поэтому достаточно проверить, что не существует однородного (относительно $\deg'$) многочлена $f(y_1,\dots,y_n) \neq 0$, такого что $f(s_1,\dots,s_n) = 0$. Воспользуемся одновременной индукцией по n и $d = \deg' f$. Основание индукции ($d = 1$) очевидно — если $\deg' f(y_1,\dots,y_n) = 1$, то $f(y_1,\dots,y_n) = \lambda y_1$ и $f(s_1,\dots,s_n) = \lambda s_1$. Пусть теперь $\deg' f(y_1,\dots,y_n) = d$, и $f(s_1,\dots,s_n) = 0$. Положим $g(y_1,\dots,y_{n-1}) = f(y_1,\dots,y_{n-1},0)$. Тогда $g(s_1(x_1,\dots,x_{n-1}),\dots,s_{n-1}(x_1,\dots,x_{n-1})) = f((x_1,\dots,x_{n-1},0),\dots,s_n(x_1,\dots,x_{n-1},0)) = 0$, поэтому по предположению индукции $g = 0$. Значит, f делится на y_n, то есть $f = y_n f'$. Следовательно, $s_n f'(s_1,\dots,s_n) = 0$ и в силу целосности кольца многочленов $f'(s_1,\dots,s_n) = 0$. Но степень многочлена f' меньше d, значит по предположению индукции $f' = 0$, то есть $f = 0$. □

Из доказанных утверждений немедленно вытекает теорема.

Теорема 2.3. *Алгебра симметрических многочленов изоморфна алгебре многочленов от n переменных.*

Доказательство: гомоморфизм алгебр $\mathsf{k}[y_1,\dots,y_n] \to \mathsf{k}[x_1,\dots,x_n]^{\mathfrak{S}_n}$, $y_i \mapsto s_i(x_1,\dots,x_n)$ сюръективен по первой лемме и инъективен по второй. □

Следствие 2.4. *Имеем* $\mathbb{A}^n//\mathfrak{S}_n \cong \mathbb{A}^n$.

Часть 3. Дискриминант и результант

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_m$, $g(x) = b_0x^n + b_1x^{n-1} + \dots + b_n$ — многочлены с коэффициентами в поле k. Рассмотрим матрицу $\mathfrak{R}$ размера $(m+n)\times(m+n)$ и ее определитель $R(f,g) = \det\mathfrak{R}$. Ясно, что $R(f,g)$ является многочленом от a_i, b_j с коэффициентами в $\mathbb{Z}$. Он называется результантом многчленов $f(x)$ и $g(x)$.

$$\mathfrak{R} = \begin{pmatrix} a_0 & a_1 & \dots & a_m & & & \\ & a_0 & a_1 & \dots & a_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \dots & a_m \\ b_0 & b_1 & \dots & \dots & b_n & & \\ & b_0 & b_1 & \dots & \dots & b_n & \\ & & \ddots & \ddots & & & \ddots \\ & & & b_0 & b_1 & \dots & \dots & b_m \end{pmatrix}$$

Лемма 3.1. *Найдутся многочлены $\phi, \psi \in \mathbb{Z}[a_0,\dots,a_m,b_0,\dots,b_n,x]$, такие что $\phi\cdot f + \psi\cdot g = R(f,g)$.*

Доказательство: рассмотрим матрицу $\mathfrak{R}$ как матрицу с коэффициентами в кольце $\mathbb{Z}[a_0,\dots,a_m,b_0,\dots,b_n,x]$, прибавим к последнему столбцу первый, умноженный на x^{m+n-1}, второй, умноженный на x^{m+n-2}, …, предпоследний, умноженный на x, и разложим определитель по последнему столбцу. □

Следствие 3.2. *Если f и g имеют общий корень в $\bar{\mathsf{k}}$, то $R(f,g) = 0$.*

Доказательство: подставим общий корень f и g вместо x в равенство $\phi\cdot f + \psi\cdot g = R(f,g)$. □

Лемма 3.3. *Если $f(x) = a_0(x-\alpha_1)\cdot\dots\cdot(x-\alpha_m)$, $g(x) = b_0(x-\beta_1)\cdot\dots\cdot(x-\beta_n)$, то $R(f,g) = a_0^n b_0^m \prod_{i,j=1}^n(\alpha_i-\beta_j)$.*

Доказательство: разделив первые n строк матрицы $\mathfrak{R}$ на a_0, а последние m строк — на b_0 мы сводим утверждение к случаю $a_0 = b_0 = 1$. В этом случае, как левая, так и правая части являются многочленами от α_i, β_j с коэффициентами в $\mathbb{Q}$, причем левая часть делится на правую, так как при $\alpha_i = \beta_j$ имеем $R(f,g) = 0$. Кроме того, обе части однородны степени mn, поэтому частное является константой. Наконец, константа равна 1, так как член $b_n^m = ((-1)^m\prod_i\beta_i)^n$ входит в обе части с коэффициентом 1. □

Теорема 3.4. *Результант обращается в ноль $\iff$ многочлены имеют общий корень.*

Дискриминантом многчлена $f(x) = a_0(x-\alpha_1)\dots(x-\alpha_m)$ назывется $D(f) = a_0^{2n-2}\prod_{i\neq j}(\alpha_i-\alpha_j)$. Ясно, что правая часть является симметрическим многочленом от $\alpha_1,\dots,\alpha_n$, поэтому дискриминант $D(f)$ является многочленом от коэффициентов многочлена f с целыми коэффициентами. Дискриминант обращается в ноль $\iff$ многочлен имеет кратный корень.

Лекция 9. Полупростые алгебры

Часть 1. Полупростые модули

Пусть A — алгебра, не обязательно коммутативная. В дальнейшем мы рассматриваем левые A-модули и левые идеалы (если не оговорено иное), хотя аналогичные рассуждения легко переносятся на случай правых A-модулей и правых идеалов.

Определение 1.1. A-модуль M называется простым, если он не содержит подмодулей, кроме 0 и M.

Примеры 1.2. 1. Если A — тело, то модуль M прост $\iff \dim_A M = 1$;

2. если $A = \mathrm{End}_{\mathsf{k}}(V)$, то V — простой A-модуль;

3. если $A = \mathsf{k}[G]$ — групповая алгебра, а M — представление, то M — прост $\iff M$ — неприводимо.

Лемма 1.3. *Если $f : M \to N$ — гомоморфизм простых A-модулей, то либо $f = 0$, либо f — изоморфизм.*

Доказательство: ядро и образ f — подмодули в M и N, поэтому если $f \neq 0$, то $\operatorname{Ker} f = 0$, $\operatorname{Im} f = N$, то есть f — изоморфизм. □

Следствие 1.4. *Если M — простой A-модуль, то $\mathrm{End}_A(M)$ — тело.*

Определение 1.5. A-модуль M называется полупростым, если для всякого подмодуля $M' \subset M$ найдется подмодуль $M'' \subset M$, такой что $M = M' \oplus M''$.

Примеры 1.6. 1. Если A — тело, то любой A-модуль полупрост;

2. если $A = \mathrm{End}_{\mathsf{k}}(V)$, то V — простой A-модуль;

3. если G конечная группа и $\operatorname{char} \mathsf{k} = 0$ (то есть G редуктивна), то любой $\mathsf{k}[G]$-модуль полупрост.

Лемма 1.7. *Прямая сумма простых модулей полупроста.*

Доказательство: пусть $M = \oplus_{i\in I} M_i$, M_i — простые, и $M' \subset M$. Пусть $I_0 \subset I$ — максимальное подмножество, такое что $(\oplus_{i\in I_0} M_i) \cap M' = 0$ (для доказательства его существования придется воспользоваться леммой Цорна). Положим $M'' = \oplus_{i\in I_0} M_i$ и покажем, что $M = M' \oplus M''$. Действительно, $M' \cap M'' = 0$ по определению. С другой стороны, $M_i \cap (M' \oplus M'')$ — подмодуль в M_i. Если он равен нулю, то $(M'' \oplus M_i) \cap M' = 0$, значит I_0 не максимально. Значит он равен M_i, значит $M_i \subset M' \oplus M''$, значит $M = \oplus_{i\in I} M_i \subset M' \oplus M''$, то есть $M' \oplus M'' = M$. □

Лемма 1.8. *Подмодуль и фактормодуль полупростого модуля полупросты.*

Доказательство: пусть $N \subset M$, M — полупрост и $N' \subset N$. Так как M полупрост, существует $M'' \subset M$, так что $M = N' \oplus M''$. Тогда $N = N' \oplus (N \cap M'')$, значит N полупрост. Аналогично, пусть $f : M \to N$ — эпиморфизм, и $N' \subset N$. Тогда $f^{-1}(N') \subset M$ и найдется $M'' \subset M$, так что $M = f^{-1}(N') \oplus M''$. Тогда $N = N' \oplus f(M'')$, значит N полупрост. □

Лемма 1.9. *Всякий полупростой модуль содержит простой подмодуль.*

Доказательство: рассмотрим ненулевой подмодуль $Am \subset M$. Ясно, что $Am \cong A/I$, где $I \subset A$ — идеал. Выберем максимальный идеал $\mathfrak{m} \subset A$, такой что $I \subset \mathfrak{m}$. Ясно, что $\mathfrak{m}/I \subset A/I$ — подмодуль, но $A/I \subset M$, поэтому A/I полупрост, значит найдется подмодуль $M' \subset A/I$, такой что $A/I = \mathfrak{m}/I \oplus M'$. Покажем, что M' — простой модуль. Действительно, если $M'' \subset M'$, то $\mathfrak{m}/I \oplus M'' \subset A/I$, что в силу максимальности $\mathfrak{m}$ влечет либо $M'' = 0$, либо $M'' = M$. □

Замечание 1.10. Условие полупростоты здесь существенно. Например, если $A = \mathsf{k}[x]$, $M = A$, то всякий подмодуль в M изоморфен A (т.к. A — область главных идеалов), поэтому не является простым.

Теорема 1.11. *Модуль M полупрост $\Longleftrightarrow$ он является прямой суммой простых модулей.*

Доказательство: $\Longleftarrow$) уже доказано, докажем $\Longrightarrow$). Идея такая: выберем простой подмодуль $M_1 \subset M$, отщепим его прямым слагаемым $M = M_1 \oplus M'$, выберем простой подмодуль $M_2 \subset M'$, отщепим его прямым слагаемым $M' = M_2 \oplus M''$, и т.д. Формализуется это рассуждение так: рассмотрим множество подмодулей в M, являющихся прямыми суммами простых, и введем на нем отношение порядка, положив $M' < M''$, если $M'' = M' \oplus (\oplus M_i)$, где все M_i простые. Ясно, что всякая возрастающая цепочка содержит наибольший элемент — им является прямая сумма всех простых модулей, в сумму которых раскладываются дополнительные прямые слагаемые. Поэтому найдется максимальный подмодуль $M' \subset M$, являющийся прямой суммой простых. Покажем, что $M' = M$. Действительно, в противном случае найдется ненулевой подмодуль $M'' \subset M$, такой что $M = M' \oplus M''$. Так как M'' полупрост, то он содержит простой подмодуль $M''' \subset M''$ и модуль $M' \oplus M''' \subset M$ строго больше чем M'. □

Следствие 1.12. *Прямая сумма полупростых модулей полупроста.*

Часть 2. Полупростые кольца

Определение 2.1. Кольцо A называется полупростым, если всякий A является полупростым A-модулем.

Примеры 2.2.
1. Тело является полупростым кольцом;
2. кольцо матриц с коэффициентами в поле полупросто;
3. прямое произведение полупростых колец полупросто.

Лемма 2.3. *Любой модуль над полупростым кольцом полупрост.*

Доказательство: любой модуль является фатором свободного модуля. □

Пусть A полупростое кольцо. Каждый идеал в кольце A является A-модулем. Обратно, всякий подмодуль в A-модуле A — это идеал. Идеал называется простым, если он является простым A-модулем. Ясно, что A раскладывается в прямую сумму простых идеалов.

Лемма 2.4. *Если L — простой идеал, а M — простой модуль, то либо $M \cong L$, либо $LM = 0$.*

Доказателство: так как L идеал, то LM есть подмодуль в M, поэтому либо $LM = 0$, либо $LM = M$. Если $LM = M$, то найдется $m \in M$, так что $Lm \neq 0$, но Lm — подмодуль в M, поэтому $Lm = M$. Значит, умножение на m является эпиморфизмом $L \to M$. Его ядро есть подмодуль в L, следовательно равно нулю, следовательно $L \cong M$. □

Следствие 2.5. *Всякий простой A-модуль изоморфен простому идеалу.*

Доказательство: если $M \ncong L$ для всех простых идеалов L в A, то $M = AM = (\oplus L)M = \oplus LM = 0$. □

Следствие 2.6. *Если L, L' — идеалы в A, неизоморфные как A-модули, то $LL' = 0$.*

Пусть L_i — простые идеалы, представляющие разные классы изоморфизма простых A-модулей, и A_i — сумма всех простых идеалов в A, изоморфных L_i.

Лемма 2.7. *Имеем $A = \oplus A_i$.*

Доказательство: разложим A в прямую сумму простых идеалов и обозначим через A'_i сумму тех из них, которые изоморфны идеалу L_i. Тогда $A = \oplus A'_i$. Ясно, что $\mathrm{Hom}_A(L_i, A'_j) = 0$ при $i \neq j$, поэтому всякий простой идеал, изоморфный идеалу L_i содержится в слагаемом $A'_i = \mathrm{Ker}(A \to \oplus_{j \neq i} A'_j)$. Значит $A'_i = A_i$ и $A = \oplus A_i$.

Лемма 2.8. *Имеем $A_i A_j = 0$ при $i \neq j$ и $A_i A_i = A_i$.*

Доказательство: $A_i A_j = (\oplus L_{is})(\oplus L_{jt}) = \oplus L_{is} L_{jt} = 0$ при $i \neq j$, а $A_i A_i = (\oplus A_j) A_i = A A_i = A_i$. □

Теорема 2.9. *Количество классов изоморфизма простых идеалов конечно, каждый идеал A_i двусторонний, является кольцом, и $A = \prod A_i$. В каждом из колец A_i все простые идеалы изоморфны.*

Доказательство: разложим единицу кольца A относительно разложения $A = \oplus A_i$: $1 = \sum e_i$, количество ненулевых слагаемых конечно по определению прямой суммы. Ясно, что $e_i e_j = 0$ при $i \neq j$, поэтому $\sum e_i = 1 = 1 \cdot 1 = (\sum e_i)(\sum e_i) = \sum e_i^2$, значит $e_i^2 = e_i$. Наконец, $A_i = 1A_i = (\sum e_j)A_i = e_i A_i = e_i A$, поэтому A_i только конечное число, каждый из них является правым (а значит и двусторонним) идеалом, и кольцом (единица — это e_i). Так как e_i — ортогональные идемпотенты, то A раскладывается в произведение колец A_i. Наконец, каждый простой идеал в A_i является простым A-модулем, следовательно все они изоморфны как A-модули, а значит и как A_i-модули. □

Часть 3. Простые кольца

Определение 3.1. Полупростое кольцо называется простым, если в нем все простые идеалы изоморфны.

Лемма 3.2. *Простое кольцо является прямой суммой конечного числа простых идеалов, не содержит нетривиальных двусторонних идеалов, и для любых простых иделов $L, L' \subset A$ найдется элемент $a \in A$, так что $La = L'$.*

Доказательство: разложим A в прямую сумму простых левых идеалов $A = \oplus L_i$, и разложим единицу $1 = \sum e_i$. В этом разложении лишь конечное число ненулевых слагаемых. Кроме того, $A = A \cdot 1 = A(\sum e_i) \subset \oplus_{e_i \neq 0} L_i$, поэтому лишь конечное число L_i отлично от нуля. Далее, если L, L' — простые идеалы, и $f : L \to L'$ — их изоморфизм как A-модулей, а $\pi : A \to L$, $i : L' \to A$ — проекция и вложение, то $i \circ f \circ \pi$ — эдоморфизм A, а всякий эндоморфизм A — это правое умножение, поэтому найдется $a \in A$, такое что $L' = (i \circ f \circ \pi)(L) = La$. Наконец, если $I \subset A$ — нетривиальный идеал, то $A = I \oplus M$, выберем простые идеалы $L \subset I$, $L' \subset M$ и найдем элемент $a \in A$, такой что $La = L'$. Тогда $Ia \not\subset I$, поэтому I не двусторонний. □

Теорема 3.3. *Пусть $D = \mathrm{End}_A(L)$ — тело эндоморфзмов простого идеала. Тогда L — конечномерный D-модуль и $A \cong \mathrm{End}_D(L)$.*

Доказательство: действие всякого элемента из A на L коммутирует с действием всякого элемента из D, поэтому существует канонический гомоморфизм $\lambda : A \to \mathrm{End}_D(L)$. Его ядро — двусторонний идеал, поэтому $\mathrm{Ker}\,\lambda = 0$ ($\mathrm{Ker}\,\lambda \neq A$, так как $1 \notin \mathrm{Ker}\,\lambda$), значит λ — вложение. Наконец, $LA \subset A$ — двусторонний идеал, поэтому $LA = A$, а $\lambda(L) \subset \mathrm{End}_D(L)$ — идеал, так как для любого эндоморфизма $f \in \mathrm{End}_D(L)$ и $l, x \in L$ имеем $(f \circ \lambda(l))(x) = f(lx) = f(l)x = \lambda(f(l))(x)$. Следовательно, $\mathrm{End}_D(L) = \mathrm{End}_D(L)\lambda(A) = \mathrm{End}_D(L)\lambda(LA) = \mathrm{End}_D(L)\lambda(L)\lambda(A) = \lambda(L)\lambda(A) = \lambda(LA) = \lambda(A)$, поэтому λ сюръективно. Остается проверить, что L является D-модулем конечного ранга. Действительно, если бы L имел бесконечный ранг над D, то алгебра $A \cong \mathrm{End}_D(L)$ раскладывалась бы в бесконечную прямую сумму простых идеалов, что противоречит доказанному выше утверждению. □

Лемма 3.4. *Если L — конечномерный D-модуль, то алгебра $A = \mathrm{End}_D(L)$ проста и $D = \mathrm{End}_A(L)$.*

Доказательство: так как L является свободным D-модулем, и любой ненулевой элемент в L дополняется до базиса, то алгебра $A = \mathrm{End}_D(L)$ действует транзитивно на множестве ненулевых элементов, поэтому L является простым A-модулем. Далее, выберем базис $(v_1, \ldots, v_n)$ модуля L над D. Тогда $A = \oplus_{i=1}^n L_i$, где $L_i \subset \mathrm{End}_D(L)$ — эндоморфзмы, зануляющиеся на всех v_j при $j \neq i$. При этом отображение $f \mapsto f(v_i)$ задает изоморфизм модуля L_i с L. Наконец, пусть $\phi \in \mathrm{End}_A(L)$. Коммутируя его с элементарными матрицами E_{ij} заключаем, что ϕ есть умножение на элемент из D. □

Следствие 3.5. *Если A — полупростая алгебра над полем k, то A есть конечное произведение матричных алгебр над телами над k.*

Следствие 3.6. *Если A — коммутативная полупростая алгебра над полем k, то A есть конечное произведение полей, являющихся расширениями поля k.*

Лемма 3.7. *Если поле k алгебраически замкнуто, а D — конечномерное тело над k, то $D = \mathsf{k}$.*

Доказательство: всякий элемент из D алгебраичен над k. □

Следствие 3.8. *Если A — полупростая алгебра конечномерная над алгебраически замкнутым полем, то A есть конечное произведение матричных алгебр.*

Лекция 10. Центральные простые алгебры

Часть 1. Критерий простоты

Напомним, что радикалом Джекобсона алгебры A называется пресечение всех левых максимальных идеалов в A. Радикал Джекобсона алгебры A обозначается $\mathfrak{R}_A$.

Лемма 1.1. *Радикал Джекобсона является двусторонним идеалом.*

Доказательство: пусть $x \in \mathfrak{R}_A$, $a \in A$ и $xa \notin \mathfrak{R}_A$. Тогда найдется левый максимальный идеал $\mathfrak{m} \subset A$, такой что $xa \notin \mathfrak{m}$. Рассмотрим $I = \{ z \in A \mid za \in \mathfrak{m} \}$. Ясно, что I — левый идеал, $x \notin I$. Отображение $A/I \to A/\mathfrak{m}$, $z \mapsto za$ является вложением левых A-модулей, причем $A/I \neq 0$. Так как $A/\mathfrak{m}$ — простой A-модуль, то $A/I \cong A/\mathfrak{m}$, значит I максимален, и $x \notin \mathfrak{R}_A$. □

Лемма 1.2. *Радикал Джекобсона алгебры $B = A/\mathfrak{R}_A$ равен нулю.*

Доказательство: пусть $f : A \to B$ — проекция. Если $\mathfrak{m} \subset B$ — максимальный левый идеал в B, то $f^{-1}(\mathfrak{m})$ — максимальный идеал в A. Обратно, если $\mathfrak{m} \subset A$ — максимальный левый идеал, то $\mathfrak{R}_A \subset \mathfrak{m}$, поэтому $\mathfrak{m}/\mathfrak{R}_A \subset B$ — максимальный идеал в B. Следовательно, $\mathfrak{R}_A = f^{-1}(\mathfrak{R}_B)$. значит $\mathfrak{R}_B = f(f^{-1}(\mathfrak{R}_B)) = f(\mathfrak{R}_A) = 0$. □

Пусть теперь A — конечномерная алгебра с нулевым радикалом Джекобсона. Тогда пересечение всех левых максимальных идеалов в A равно нулю.

Лемма 1.3. *Пересечению конечного числа левых максимальных идеалов в A равно нулю.*

Доказательство: рассмотрим среди множества конечных пересечений левых максимальных идеалов идеал минимальной размерности над полем k. Ясно, что он лежит в любом левом максимальном идеале (иначе размерность пересечения уменьшилась бы), поэтому он равен нулю. □

Выберем представление $0 = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ с минимально возможным r. Пусть $L_i = \bigcap_{j \neq i} \mathfrak{m}_j$.

Лемма 1.4. *Имеем $\mathfrak{m}_i \cap L_i = 0$, $\mathfrak{m}_i + L_i = A$.*

Доказательство: $\mathfrak{m}_i \cap L_i = \bigcap_j \mathfrak{m}_j = 0$. Кроме того, $\mathfrak{m}_i \subset \mathfrak{m}_i + L_i$, поэтому либо $\mathfrak{m}_i + L_i = A$, либо $\mathfrak{m}_i + L_i = \mathfrak{m}_i$. В последнем случае $L_i \subset \mathfrak{m}_i$, значит $0 = L_i$ и r не было минимальным. □

Следствие 1.5. *Имеем изоморфизм A-модулей $L_i \cong A/\mathfrak{m}_i$.*

Доказательство: гомоморфизм $L_i \to A \to A/\mathfrak{m}_i$ инъективен и сюръективен. □

Следствие 1.6. *Идеал L_i прост.*

Лемма 1.7. *Имеем $A \cong \oplus_{i=1}^r L_i$.*

Доказательство: докажем индукией по k, что $\oplus_{i=1}^k L_i = \bigcap_{j=k+1}^r \mathfrak{m}_j$. База индукции, $k = 0$ очевидна. Пусть случай $k-1$ доказан. Тогда $(\oplus_{i=1}^{k-1} L_i) \cap L_k = (\bigcap_{j=k}^r \mathfrak{m}_j) \cap L_k \subset \mathfrak{m}_k \cap L_k = 0$, значит сумма $\sum_{i=1}^k L_i \subset A$ — прямая. Кроме того, ясно что $\oplus_{i=1}^k L_i \subset \bigcap_{j=k+1}^r \mathfrak{m}_j$, так как каждое из слагаемых в левой части содержится в каждом из пересекаемых идеалов в правой части. Рассмотрим идеал $I = \bigcap_{j=k+1}^r \mathfrak{m}_j$. Мы уже доказали, что морфизм $L_k = (\oplus_{i=1}^k L_i)/(\oplus_{i=1}^{k-1} L_i) \to I/I \cap \mathfrak{m}_k \to A/\mathfrak{m}_k$ является изоморфизмом, а при этом отображение $I/I \cap \mathfrak{m}_k \to A/\mathfrak{m}_k$ — вложение, поэтому $L_k \cong I/I \cap \mathfrak{m}_k$, следовательно $\oplus_{i=1}^k L_i = I$. □

Следствие 1.8. *Алгебра A полупроста.*

Теорема 1.9. *Конечномерная над полем k алгебра A полупроста $\iff \mathfrak{R}_A = 0$.*

Доказательство: ($\Longleftarrow$) уже доказано, докажем ($\Longrightarrow$). Если A полупроста, то A есть сумма простых левых идеалов, $A = \oplus_{i=1}^{r} L_i$. Ясно, что $\mathfrak{m}_j = \oplus_{i \neq j} L_i = \operatorname{Ker}(A \to L_j)$ является максимальным левым идеалом, и $\bigcap_{j=1}^{r} \mathfrak{m}_j = 0$, поэтому $\mathfrak{R}_A = 0$. □

Следствие 1.10. *Если конечномерная алгебра A над полем k не имеет нетривиальных двусторонних идеалов, то A проста.*

Доказательство: радикал Джекобсона является двусторонним идеалом, поэтому $\mathfrak{R}_A = 0$ и A — полупроста, то есть A есть произведение матричных алгебр над телами. Если сомножителей больше одного, то в A есть двусторонние идеалы. □

Часть 2. Простые алгебры и расширения полей

Лемма 2.1. *Если D тело, то все односторонние идеалы в $D[t]$ главные.*

Доказательство: элемент минимальной степени в иделе порождает его, так как в $D[t]$ можно делить с остатком (для левых идеалов надо делить справа, а для правых — слева). □

Лемма 2.2. *Пусть D — тело, $K = Z(D)$— его центр. Левый идеал $D[t]f(t) \subset D[t]$ является двусторонним $\Longleftrightarrow$ $f(t) = ag(t)$, где $a \in D^*$, $g(t) \in K[t]$.*

Доказательство: пусть a — старший коэффициент f, и $g(t) = a^{-1}f(t)$. Ясно, что идеал $D[t]g(t) = D[t]f(t)$ — двусторонний. Пусть $x \in D^*$. Тогда $g(t)x \in D[t]g(t)$, значит $g(t)x = yg(t)$, где $y \in D^*$. Сравнивая старшие коэффициенты, получаем $y = x$. Значит все коэффициенты многочлена $g(t)$ коммутируют с x. Так как x любое, то $g(t) \in K[t]$. □

Пусть A и B — алгебры над полем K. Рассмотрим тензорное произведение $A \otimes_K B$. Тогда отображение $(A \otimes_K B) \otimes_K (A \otimes_K B) = A \otimes_K B \otimes_K A \otimes_K B = (A \otimes_K A) \otimes_K (B \otimes_K B) \overset{m_A \otimes m_B}{\longrightarrow} A \otimes_K B$ задает на $A \otimes_K B$ структуру K-алгебры. Иначе говоря, если $e_1, \ldots, e_m$ — базис A над K, а $f_1, \ldots, f_n$ — базис B над K, то в базисе $e_i \otimes f_j$ умножение задается формулой $(e_i \otimes f_j)(e_k \otimes f_l) = (e_i e_k) \otimes (f_j f_l)$.

Примеры 2.3.

1. $\operatorname{Mat}_{m\times m}(K) \otimes_K \operatorname{Mat}_{n\times n}(K) \cong \operatorname{Mat}_{mn\times mn}(K)$;
2. $\operatorname{Mat}_{n\times n}(K) \otimes_K A \cong \operatorname{Mat}_{n\times n}(A)$;
3. $\operatorname{Mat}_{m\times m}(A) \otimes_K \operatorname{Mat}_{n\times n}(B) \cong \operatorname{Mat}_{mn\times mn}(A \otimes_K B)$.

Лемма 2.4. *Имеем $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$.*

Доказательство: пусть $x \in Z(A \otimes_K B)$. Разложим x по базису $\{e_i\}$ алгебры A: $x = \sum e_i \otimes x_i$. Для всякого $b \in B$ имеем $(1 \otimes b)x = \sum e_i \otimes (bx_i)$, $x(1 \otimes b) = \sum e_i \otimes (x_i b)$, поэтому $x_i \in Z(B)$, то есть $x \in A \otimes_K Z(B)$. Раскладывая x по базису $Z(B)$ и коммутируя с элементами вида $a \otimes 1$, $a \in A$ получаем, что $x \in Z(A) \otimes_K Z(B)$. □

Определение 2.5. Алгебра A над полем K называется центральной простой алгеброй, если она проста (то есть изоморфна матричной алгебре над полем), а ее центр совпадает с полем K.

Лемма 2.6. *Пусть D — тело, $K = Z(D)$— его центр. Если L/K — примитивное расширение полей, то $D \otimes_K L$ — центральная простая алгебра над L.*

Доказательство: Заметим, что $L \cong K[t]/K[t]f(t)$, где $f(t) = \operatorname{Irr}_\alpha^K(t)$ и $D \otimes_K L \cong D[t]/D[t]f(t)$. Обозначим через $\pi : D[t] \to D \otimes_K L$ — проекцию. Пусть $I \subset D \otimes_K L$ — двусторонний идеал. Тогда $\pi^{-1}(I) \subset D[t]$ — двусторонний идеал в $D[t]$, поэтому $\pi^{-1}(I) = D[t]g(t)$, $g(t) \in K[t]$. Так как $\pi^{-1}(I) \supset \operatorname{Ker}\pi = D[t]f(t)$, то $g(t)$ делит $f(t)$, поэтому $g(t) = 1$ или $g(t) = f(t)$, так как $f(t)$ неприводим над K. В первом случае $\pi^{-1}(I) = D[t]$, значит $I = D \otimes_K L$, а во втором случае $\pi^{-1}(I) = D[t]f(t)$, значит $I = 0$. Таким образом, в алгебре $D \otimes_K L$ нет нетривиальных двусторонних идеалов, значит она проста. Остается заметить, что $Z(D \otimes_K L) = Z(D) \otimes_K Z(L) = K \otimes_K L = L$. □

Следствие 2.7. *Если A — центральная простая алгебра над K, а L/K — примитивное расширение полей, то $A \otimes_K L$ — центральная простая алгебра над L.*

Доказательство: $A \cong \mathrm{Mat}_{n\times n}(D)$ так как A простая, и $Z(A) = Z(D) = K$, так как A центральная, поэтому $A \otimes_K L \cong \mathrm{Mat}_{n\times n}(D) \otimes_K L \cong \mathrm{Mat}_{n\times n}(K) \otimes_K D \otimes_K L \cong \mathrm{Mat}_{n\times n}(K) \otimes_K \mathrm{Mat}_{m\times m}(D') \cong \mathrm{Mat}_{nm\times nm}(D')$ и $Z(A \otimes_K L) = Z(A) \otimes_K Z(L) = K \otimes_K L = L$. □

Следствие 2.8. *Если A — центральная простая алгебра над K, а L/K — конечное расширение полей, то $A \otimes_K L$ — центральная простая алгебра над L.*

Доказательство: всякое конечное расширение представляется в виде башни примитивных расширений. □

Часть 3. Группа Брауера

Лемма 3.1. *Всякий автоморфизм алгебры $A = \mathrm{Mat}_{n\times n}(K)$ является внутренним.*

Доказательство: пусть $V = K^n$, так что $A = \mathrm{End}_K(V)$. Для всех $f \in V^*$ идеал $L_f = \{\, a \in \mathrm{End}_K(V) \mid \mathrm{Ker}\, a \subset \mathrm{Ker}\, f \,\}$ прост так как $L_f \cong V$ (изоморфизм задается отображением $a \mapsto av$ для любого $v \in V$, такого что $f(v) \neq 0$). Выберем базис $\{\, e_i \,\}$ в V, рассмотрим двойственный базис $\{\, f_i \,\}$ в V^* и пусть $L_1 = L_{f_1}$. Пусть теперь ϕ — автоморфизм A Тогда $\phi(L_1)$ — простой идеал, поэтому $\phi(L_1) = L_f$. Прокомпонировав ϕ с внутренним автоморфизмом можно считать, что $f = f_1$, то есть $\phi(L_1) = L_1$. Зафиксировав изоморфизм $L_1 \cong V$ мы видим, что ϕ индуцирует автоморфизм V. Прокомпонировав ϕ с соответсвтующим внутренним автоморфизмом можно считать, что $\phi_{|L_1} = \mathrm{Id}_{L_1}$. Покажем, что тогда $\phi = \mathrm{Id}$. Действительно, если E_{ij} — матричные единицы, то $\phi(E_{i1}) = E_{i1}$. Соотношение $E_{kj}E_{i1} = \delta_{ji}E_{k1}$ тогда показывает, что $\phi(E_{kj}) = E_{kj}$. □

Лемма 3.2. *Если A — центральная простая алгебра над K, то найдется конечное расширение полей L/K, такое что $A \otimes_K L \cong \mathrm{Mat}_{n\times n}(L)$.*

Доказательство: пусть $A = \mathrm{Mat}_{m\times m}(D)$. Достаточно проверить, что если $D \neq K$, то найдется расширение L/K, такое что $A \otimes_K L \cong \mathrm{Mat}_{m'\times m'}(D')$, и $\dim_K D' < \dim_K D$. Действительно, если $\alpha \in D$, $\alpha \notin K$, то $K(\alpha) \subset D$ — подполе, а $D \otimes K(\alpha)$ имеет делители нуля, поэтому $D \otimes_K K(\alpha) = \mathrm{Mat}_{m''\times m''}(D')$ и $m'' > 1$, поэтому $\dim_K D' < \dim_K D$. □

Расширение L/K, такое что $A \otimes_K L \cong \mathrm{Mat}_{n\times n}(L)$ называется полем разложения алгебры A.

Пусть K — совершенное поле, а L/K — поле разложения алгебры A. Тогда L/K сепарабельно, и расширив L еще немного, можно считать, что L/K — расширение Галуа. Пусть $G = \mathrm{Gal}(L/K)$. Зафиксируем изоморфизм $f_0 : A \otimes_K L \to \mathrm{Mat}_{n\times n}(L)$. Для всякого элемента $g \in G$ отображение $\phi_g = 1 \otimes g : A \otimes_K L \to A \otimes_K L$ является автоморфизмом алгебры $A \otimes_K L$ над K, который на L действует автоморфизмом g. Кроме того, изоморфизм f_0 и действие группы G на $\mathrm{Mat}_{n\times n}(L)$ индуцирует автоморфизм ϕ'_g алгебры $A \otimes_K L$ над K с тем же действием на L. Поэтому композиция $\phi_g \circ {\phi'_g}^{-1}$ является автоморфизмом алгебры $A \otimes_K L$ над L, следовательно найдется элемент $a(g) \in \mathrm{GL}_n(L)$, такой что $\phi_g \circ {\phi'_g}^{-1} = \mathrm{Ad}_{a(g)}$, то есть $\phi_g = \mathrm{Ad}_{a(g)} \circ \phi'_g$. Перемножая эти равенства для $g_1, g_2 \in G$ получаем $\phi_{g_1g_2} = \phi_{g_1} \circ \phi_{g_2} = \mathrm{Ad}_{a(g_1)} \circ \phi'_{g_1} \circ \mathrm{Ad}_{a(g_2)} \circ \phi'_{g_2} = \mathrm{Ad}_{a(g_1)} \circ \mathrm{Ad}_{g_1 a(g_2)} \circ \phi'_{g_1} \circ \phi'_{g_2} = \mathrm{Ad}_{a(g_1)\cdot g_1 a(g_2)} \circ \phi'_{g_1g_2}$, значит $\mathrm{Ad}_{a(g_1)\cdot g_1 a(g_2)} = \mathrm{Ad}_{a(g_1g_2)}$. Следовательно, найдутся элементы $\lambda(g_1, g_2) \in L^*$, такие что $a(g_1g_2) = \lambda(g_1, g_2)a(g_1)g_1a(g_2)$. Тогда $\lambda(g_1g_2, g_3) \cdot \lambda(g_1, g_2) = g_1\lambda(g_2, g_3) \cdot \lambda(g_1, g_2g_3)$, то есть λ — 2-коцикл группы G с коэфициентами в L^*. Можно показать, что произвол в выборе λ сводится к изменению λ на когранicу. Тем самым, всякой центральной простой алгебре A можно сопоставить класс когомологий $\bar\lambda \in H^2(\mathrm{Gal}(L/K), L^*)$. Обратно, если λ — 2-коцикл, представляющий такой клас когомологий, то пространство $L[G]$ с умножением $e_{g_1} * e_{g_2} = \lambda(g_1, g_2)e_{g_1g_2}$, $e_g * \lambda = g(\lambda)e_g$ является центральной простой алгеброй над K. Можно показать, что эти две конструкции взаимно обратны в следующем смысле. Назовем центральные простые K-алгебры A и B подобными, если $\mathrm{Mat}_{n\times n}(A) \cong \mathrm{Mat}_{m\times m}(B)$. Тогда $A \equiv B \Longrightarrow \bar\lambda(A) = \bar\lambda(B)$, $A_{\bar\lambda(A)} \equiv A$, $\bar\lambda(A_{\bar\lambda}) = \bar\lambda$.

Теорема 3.3. *Множество классов подобия центральных простых алгебр над полем K, разлагающихся над полем L изоморфно группе $H^2(\mathrm{Gal}(L/K), L^*)$.*

Легко видеть, что в каждом класе подобия найдется ровно одно тело, поэтому множество тел над полем K, разлагающихся над полем L изоморфно группе $H^2(\mathrm{Gal}(L/K), L^*)$.

Следствие 3.4. *Множество классов изоморфизма всех центральных тел над полем K изоморфно группе $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = \bigcup\limits_{L/K} H^2(\mathrm{Gal}(L/K), L^*)$, которая называется* группой Брауэра *поля K.*

Задачи семинаров первого семестра

10 сентября 2002

1. Докажите изоморфизмы групп: a) $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$; b) $\mathbb{Q}/\mathbb{Z} \cong \mu = \bigcup_n \mu_n \subset \mathbb{C}$; c) $\mathbb{R}/\mathbb{Z} \cong \mathbf{S}^1$; d) $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$.
2. Докажите изоморфизмы групп: a) $\mathbb{R}^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}_{>0}$; b) $\mathbb{C}^* \cong \mathbf{S}^1 \times \mathbb{R}_{>0}$; c) $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$;
d) $\mathrm{Map}(\{1,2\}, G) \cong G \times G$.
3. Докажите изоморфизм колец $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, если n и m взаимно просты.
4. Найдите группы обратимых элементов в кольцах (в пунктах a)–c) K — произвольное поле):
a) $K[x]$; b) $K[[x]]$; c) $\mathrm{Mat}_{2\times 2}(K)$; d) $\mathbb{Z}/p\mathbb{Z}$, p — простое; e*) $\mathbb{Z}/n\mathbb{Z}$, n — любое.
5. Опишите все подгруппы в следующих группах: a) $\mathbb{Z}$; b) μ_n; c) $\mathbb{Q}/\mathbb{Z}$; d) $\mathfrak{S}_3$; e) $\mathfrak{S}_4$.
6. Найдите группы автоморфизм следующих групп: a) $\mathbb{Z}$; b) $\mathbb{Z}/n\mathbb{Z}$; c) $\mathfrak{S}_3$; d) $\mathfrak{S}_4$.
7. Найдите группы автоморфизмов колец: a) $\mathbb{Z}$; b) $\mathbb{Z}/n\mathbb{Z}$; c) $\mathbb{Z}[x]$; d) $\mathbb{Z}[[x]]$; e) $\mathbb{Q}[i]$.

17 сентября 2002

1. a) Докажите, что если $H \subset G$ — подгруппа, то множество G/H находится в биекции с множеством $H\backslash G$.
b) Докажите, что если $K \subset H \subset G$— подгруппы, то $(G:K) = (G:H)(H:K)$.
2. Постройте канонические гомоморфизмы групп:
a) если $K \subset H \subset G$, $K, H \triangleleft G$, то $G/H \cong (G/K)/(H/K)$; b) если $K, H \subset G$ и $H \subset N_K$, то $H/(H \cap K) \cong HK/K$;
c) если $f : G \to G'$ и $N \subset \operatorname{Ker} f$, $N \triangleleft G$, то $\bar{f} : G/N \to G'$; d) если $f : G \to G'$ и $H' \triangleleft G'$, то $G/f^{-1}(H') \to G'/H'$.
3. Докажите изоморфизмы групп: a) $\mathbf{S}^1/\mu_n \cong \mathbf{S}^1$; b) $\mathbb{R}/\mathbb{Q} \cong \mathbf{S}^1/\mu$; c) $(G_1 \times G_2)/G_1 \cong G_2$;
4. Пусть H — подгруппа в G и $(G:H) = n$. a) Докажите, что группа $G/(\bigcap_{x\in G} xHx^{-1})$ изоморфна подгруппе группы $\mathfrak{S}_n$. b) Если $(G:1) = N$, то G изоморфна подгруппе группы $\mathfrak{S}_N$. c) Если $n = 2$, то $H \triangleleft G$. d) Если $(G:1) = N$, а n — минимальный простой делитель числа N, то $H \triangleleft G$.

24 сентября 2002

1. Найдите орбиты и стабилизаторы в примерах a) 1.2.1; b) 1.2.2; c) 1.2.3; d) 1.2.5; e) 1.2.6; f) 1.2.7. Являются ли эти действия транзитивными? Свободными? Точными?
2. Докажите, что a) если $|G| = p^n$, p — простое, то $|Z_G| = p^k$, $k > 0$; b) $Z_{\mathfrak{S}_n} = \{e\}$ при $n \geqslant 3$.
3. a) Докажите, что группа симметрий тетраэдра изоморфна $\mathfrak{S}_4$. b) Постройте эпиморфизм $\mathfrak{S}_4 \to \mathfrak{S}_3$ и найдите его ядро (группа Клейна). c) Постройте эпиморфизм из группы симметрий куба в $\mathfrak{S}_4$ и найдите его ядро. d*) Постройте эпиморфизм из группы симметрий додекаэдра в A_5 и найдите его ядро.
4. Докажите, что a) $\mathrm{Inn}(G) \cong G/Z_G$; b) $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.
5. Пусть $(k_1, \ldots, k_n)$ — разбиение, соответствующее перестановке σ. Найдите a) порядок σ; b) знак σ;
c) порядок централизатора σ; d) обратную перестановку.
6. Докажите, что любая перестановка σ раскладывается в произведение a) транспозиций $(12), \ldots, (n-1, n)$;
b) перестановок (12) и $(123\ldots n)$; c) циклов длины 3, если σ — четна.
7. a) Покажите, что всякая нормальная подгруппа является объединением классов сопряженности.
b*) Докажите, что при $n \geqslant 5$ знакопеременная группа A_n не имеет нетривиальных нормальных подгрупп.

1 октября 2002

1. Докажите изоморфизмы колец: a) если K — поле и $f(x)$ — многочлен степени 1, то $K[x]/f(x)K[x] \cong K$;
b) если $f(x) \in \mathbb{R}[x]$ — многочлен степени 2, не имеющий вещественных корней, то $\mathbb{R}[x]/f(x)\mathbb{R}[x] \cong \mathbb{C}$;
c) если A — кольцо верхнетреугольных матриц размера $n \times n$ с коэффициентами в кольце R, а I — идеал строго верхнетреугольных матриц, то $A/I \cong R \times R \times \cdots \times R$ (n раз).
d) $\mathrm{End}_A(A^{\oplus n}) \cong \mathrm{Mat}_{n\times n}(A)$; $\mathrm{Hom}_A(A^{\oplus m}, A^{\oplus n}) \cong \mathrm{Mat}_{n\times m}(A)$;
2. Пусть $K = \mathbb{Z}/2\mathbb{Z}$. Докажите, что $K[x]/(x^2 + x + 1)K[x]$ — поле.

3. Докажите изоморфизмы A-модулей: a) $\mathrm{Hom}_A(A,M)\cong M$; b) $\mathrm{Hom}_A(M_1\oplus M_2,N)\cong \mathrm{Hom}_A(M_1,N)\oplus \mathrm{Hom}_A(M_2,N)$; c) $\mathrm{Hom}_A(M,N_1\oplus N_2)\cong \mathrm{Hom}_A(M,N_1)\oplus \mathrm{Hom}_A(M,N_2)$; d) $\mathrm{Map}(S,M)\cong \bigoplus_{s\in S} M$;
e) $\mathrm{Mat}_{n\times m}(B)\cong \mathrm{Mat}_{n\times 1}(B)^{\oplus m}$, если $A=\mathrm{Mat}_{n\times n}(B)$.
4. Какие модули являются свободными? Конечно порожденными? a) $A=\mathbb{Z}$, $M=\mathbb{Q}$; b) $A=\mathbb{Q}$, $M=\mathbb{R}$; c) $A=\mathbb{R}$, $M=\mathbb{C}$; d) $A=\mathrm{Mat}_{n\times n}(A)$, $M=\mathrm{Mat}_{n\times m}(A)$.
5. Найдите a) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}/m\mathbb{Z})$; b) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z},\mathbb{Z})$; c) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q},\mathbb{Z}/m\mathbb{Z})$;
6. Пусть $N_i\subset M$ — подмодули. Покажите, что a) $\sum N_i:=\{\sum n_i\}$, где почти все слагаемые равны нулю; b) $\bigcap N_i$ — подмодули в M.

8 октября 2002

1. Постройте базисы над полем K в кольцах a) матриц $n\times n$, b) верхнетреугольных матриц, c) многочленов с коэффициентами в K и запишите законы умножения в этих базисах.
2. Постройте канонические изоморфизмы a) $U+W\cong (U\oplus W)/(U\cap W)$, если $U,W\subset V$;
b) $(U+W)/U\cong W/(U\cap W)$, если $U,W\subset V$; c) $V/(U+W)\cong (V/U)/(W/(U\cap W))$, если $U,W\subset V$;
d) $(V/W)/(U/W)\cong V/U$, если $W\subset U\subset V$;
3. Постройте неканонический изоморфизм $V\cong U\oplus V/U$, если $U\subset V$.
4. Докажите, что a) $\dim(U+W)=\dim U+\dim W-\dim(U\cap W)$; b) $\dim(U\oplus W)=\dim U+\dim W$;
c) $\dim V=\dim U+\dim V/U$, если $U\subset V$; d) $\dim V-\dim U=\dim V/(\mathrm{Im}\, f)-\dim \mathrm{Ker}\, f$, если $f: U\to V$.
5. Покажите, что целочисленными элементарными преобразованиями строк и столбцов любую целочисленную матрицу можно привести к диагональному виду с числами $d_1,\dots,d_r$ на диагонали, так что $d_1|d_2|\dots|d_r$.
6. Докажите, что a) любая подгруппа в свободной конечнопорожденной абелевой группе является свободной конечнопорожденной абелевой группой; b) любая конечнопорожденная абелева группа изоморфна группе $\mathbb{Z}/d_1\mathbb{Z}\oplus\mathbb{Z}/d_2\mathbb{Z}\oplus\dots\oplus\mathbb{Z}/d_r\mathbb{Z}$, где $d_1|d_2|\dots|d_r$; c) если $\oplus_{i=1}^r\mathbb{Z}/d_i\mathbb{Z}\cong\oplus_{i=1}^s\mathbb{Z}/c_i\mathbb{Z}$, где $d_1|d_2|\dots|d_r$ и $c_1|c_2|\dots|c_s$, то $r=s$ и $\forall i\ d_i=\pm c_i$.

15 октября 2002

1. Найдите след, определитель, характеристический многочлен и ранг матриц:
a) $\begin{pmatrix} a & b & 0 & \dots & 0 & 0\\ c & a & b & \dots & 0 & 0\\ 0 & c & a & \dots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & a & b\\ 0 & 0 & 0 & \dots & c & a\end{pmatrix}$ b) $\begin{pmatrix} 1 & 1 & 1 & \dots & 1\\ x_1 & x_2 & x_3 & \dots & x_n\\ x_1^2 & x_2^2 & x_3^2 & \dots & x_n^2\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_n^{n-1}\end{pmatrix}$ c) $\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0\\ 1 & 0 & 0 & \dots & 0 & -a_1\\ 0 & 1 & 0 & \dots & 0 & -a_2\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \dots & 0 & -a_{n-2}\\ 0 & 0 & 0 & \dots & 1 & -a_{n-1}\end{pmatrix}$ d) $\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n\\ a_n & a_1 & a_2 & \dots & a_{n-2} & a_{n-1}\\ a_{n-1} & a_n & a_1 & \dots & a_{n-3} & a_{n-2}\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ a_3 & a_4 & a_5 & \dots & a_1 & a_2\\ a_2 & a_3 & a_4 & \dots & a_n & a_1\end{pmatrix}$
2. Пусть $A\in\mathrm{Mat}_{m\times n}(K)$. Докажите, что если $\forall X\in\mathrm{Mat}_{n\times m}(K)$ имеем $\mathrm{tr}(AX)=0$, то $A=0$.
3. Пусть A — матрица $n\times n$. Покажите, что
a) если $r(A)=n$, то $r(\widehat{A})=n$; b) если $r(A)=n-1$, то $r(\widehat{A})=1$; c) если $r(A)\leqslant n-2$, то $\widehat{A}=0$.
4. Покажите, что a) $r(AB)\leqslant r(A)$; b) $r(AB)\leqslant r(B)$; c) $r(A+B)\leqslant r(A)+r(B)$.
5. Покажите, что всякая матрица $A\in\mathrm{Mat}_{m\times n}(K)$ ранга r представляется в виде $A=B\cdot C$, где $B\in\mathrm{Mat}_{m\times r}(K)$ и $C\in\mathrm{Mat}_{r\times n}(K)$. Насколько однозначно такое представление?
6. Системой линейных уравнений называется изображенная справа система, записываемая кратко в виде $Ax=b$, где $A\in\mathrm{Mat}_{m\times n}(K)$, $b\in\mathrm{Mat}_{m\times 1}(K)$ и x — столбец неизвестных. Докажите, что
$\begin{cases} a_{11}x_1+\dots+a_{1n}x_n &= b_1\\ \vdots & \vdots\\ a_{m1}x_1+\dots+a_{mn}x_n &= b_m\end{cases}$
a) множество решений системы $Ax=0$ является векторным пространством размерности $n-r(A)$.
b) либо множество решений системы $Ax=b$ пусто, либо на нем свободно и транзитивно действует множество решений системы $Ax=0$.
c) множество решений системы $Ax=b$ непусто $\iff r(A)=r(A|b)$.
7. Пусть R — коммутативное кольцо, M — R-модуль и $A\in\mathrm{Mat}_{n\times n}(R)$. Докажите, что если $\forall x\in\mathrm{Mat}_{n\times 1}(M)$ имеем $Ax=0$, то $(\det A)M=0$.

22 октября 2002

1. Найдите ЖНФ операторов a) d/dt; b) $(d/dt)^k$ в $\{f(t)\in K[t]\mid \deg f\leqslant n\}$; c) t в $\mathbb{C}[t]/p(t)\mathbb{C}[t]$.
2. Пусть $D=J_n(0)\in\mathrm{Mat}_{n\times n}(K)$. Покажите, что
a) $(tE+D)^k=\sum_p \frac{k!}{(k-p)!}t^{k-p}\frac{D^p}{p!}$; b) $f(tE+D)=\sum_p f^{(p)}(t)\frac{D^p}{p!}$, где $f(t)\in K[t]$.
3. Пусть дана матрица A в ЖНФ. Найдите a) $f(A)$, где $f\in K[t]$; b) A^{-1}; c) $Z_A(\mathrm{Mat}_{n\times n}(K))$.
4. Пусть A оператор в n-мерном векторном пространстве над полем K. Докажите эквивалентность условий 1) $\chi_A(t)=t^n$; 2) $m_A(t)=t^m$; 3) A — нильпотентен; 4) $\forall k\geqslant 1\ \mathrm{tr}\,A^k=0$ (если $1/k\in K$ при $1\leqslant k\leqslant n$).
5. Пусть A и B — нильпотентны и $AB=BA$. Докажите, что a) $A+B$; b) AB — нильпотентны.

6. Пусть K — алгебраически замкнуто, $A \in \mathrm{End}_K(V)$, V_λ — корневое подпространство A. Докажите, что
a) если $AB = BA$, то $B(V_\lambda) \subset V_\lambda$; b) если $A = A_{ss} + A_n$ — разложение Жордана, то $A_{ss}(V_\lambda) \subset V_\lambda$, $A_n(V_\lambda) \subset V_\lambda$;
c) если A нильпотентен, то $A_{ss} = 0$; d) разложение Жордана единственно.
7. Пусть $A, A_1, \ldots, A_n$ — проекторы в V. Докажите, что a) $\mathrm{Id} - A$ — проектор, коммутирующий с A;
b) $\mathrm{Ker}\, A = \mathrm{Im}(\mathrm{Id} - A)$, $\mathrm{Im}\, A = \mathrm{Ker}(\mathrm{Id} - A)$; c) $V = \mathrm{Ker}\, A \oplus \mathrm{Im}\, A$; d) если $\sum A_i = \mathrm{Id}$ и $A_i A_j = A_j A_i$, то $V = \oplus \mathrm{Im}\, A_i$. e) если $V = \oplus V_i$ и $B_i = \mathrm{Id}_{V_i}$, то B_i — проекторы, $B_i B_j = B_j B_i$ и $\sum B_i = \mathrm{Id}$.
8. Опишите орбиты и стабилизаторы для действия a) $\mathrm{GL}_n(\mathbb{C})$ на $\mathrm{Mat}_{n\times n}(\mathbb{C})$, $(g, A) \mapsto gAg^{-1}$;
b) $\mathrm{GL}_n(K) \times \mathrm{GL}_m(K)$ на $\mathrm{Mat}_{n\times m}(K)$, $(g_1, g_2, A) \mapsto g_1 A g_2^{-1}$.

29 октября 2002

1. Пусть $\mathfrak{a}_i \subset A$ — идеалы. Докажите, что a) $\mathfrak{a}_1 + \mathfrak{a}_2$ — идеал; b) $\mathfrak{a}_1\mathfrak{a}_2 := \{ \sum_{i=1}^n x_i y_i \mid x_i \in \mathfrak{a}_1,\ y_i \in \mathfrak{a}_2 \}$ — идеал; c) $\bigcap_{i\in I} \mathfrak{a}_i$ — идеал; d) $\mathfrak{a}_1(\mathfrak{a}_2\mathfrak{a}_3) = (\mathfrak{a}_1\mathfrak{a}_2)\mathfrak{a}_3$; e) $\mathfrak{a}_1(\mathfrak{a}_2 + \mathfrak{a}_3) = \mathfrak{a}_1\mathfrak{a}_2 + \mathfrak{a}_1\mathfrak{a}_3$.
2. Пусть $f : A \to B$ — гомоморфизм колец. Докажите, что прообраз $f^{-1}(\mathfrak{p}) \subset A$ простого идеала $\mathfrak{p} \subset B$ является простым идеалом. Покажите, что прообраз максимального идеала может не быть максимальным.
3. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset A$ — идеалы, такие что $\forall i \neq j$ имеем $\mathfrak{a}_i + \mathfrak{a}_j = A$. Докажите, что
a) $\forall x_1, \ldots, x_n \in A\ \exists x \in A$ такой что $\forall i\ x \equiv x_i \pmod{\mathfrak{a}_i}$; b) $\prod_{i=1}^n A/\mathfrak{a}_i \cong A/\bigcap_{i=1}^n \mathfrak{a}_i$.
4. Пусть A — целостное кольцо. a) Докажите, что кольца $A[x]$ и $A[[x]]$ — целостные.
b) Опишите их поля частных.
5. Докажите, что кольцо $K[[x]]$ a) нётерово; b) факториально. c) Перечислите в нем простые идеалы.
6. Докажите, что в факториальном кольце A элемент p неприводим $\iff$ идеал $pA \subset A$ — прост.
7. Докажите, что кольцо $\mathbb{Z}[i] = \{ a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z} \}$ a) целостное; b) факториальное.
8. Перечислите в кольце $\mathbb{Z}[i]$ все a) единицы; b*) неприводимые элементы;
9. Пусть A — факториальное кольцо с полем частных K, а $p \in A$ — неприводимый элемент. Докажите, что
a) существует единственное отображение $\mathrm{ord}_p : A \to \mathbb{Z} \cup \infty$, такое что $\mathrm{ord}_p(p) = 1$, $\mathrm{ord}_p(0) = \infty$, $\mathrm{ord}_p(a) = 0$ $\iff (a, p) = 1$ и $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$. b) Отображение ord_p однозначно продолжается на поле K с сохранением свойств. c) Функция $\rho(x, y) = C^{-\mathrm{ord}_p(x-y)}$, где $C \in \mathbb{R}$, $C > 1$ является метрикой на поле K.
d) $A_p := \{ x \in K \mid \rho(x, 0) \leqslant 1 \}$ — подкольцо в K. e) $\mathfrak{m}_p := \{ x \in K \mid \rho(x, 0) < 1 \}$ — максимальный идеал в A_p.

5 ноября 2002

1. a) (Теорема Безу) Докажите, что если $f(x) \in K[x]$ и $f(\alpha) = 0$, где $\alpha \in K$, то $(x - \alpha) | f(x)$.
b) Покажите, что если $f(x) \in K[x]$, $\deg f(x) = n$, то f имеет не больше чем n различных корней.
c) Пусть $\mu_n(K) = \{ x \in K \mid x^n = 1 \}$. Покажите, что $|\mu_n(K)| \leqslant n$.
d) Пусть $G \subset K^*$ — конечная подгруппа мультипликативной группы поля. Докажите, что G — циклична (воспользуйтесь классификацией конечных абелевых групп).
2. Докажите, что если $[L : K] = 2$, то $L = K[\sqrt{a}]$, $a \in K$.
3. Найдите $[K(\alpha) : K]$ и $\mathrm{Irr}_\alpha^K(x)$, если a) $K = \mathbb{Q}$, $\alpha = \sqrt{2} + \sqrt{3}$; b) $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\alpha = 1 + \sqrt{2}$;
c) $K = \mathbb{F}_p$, α — образующая группы $\mu_n(\overline{\mathbb{F}}_p)$.
4. Для расширений из предыдущей задачи найдите все поля L, такие что $K \subset L \subset K(\alpha)$.
5. Докажите, что 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{10}$, $\sqrt{15}$ и $\sqrt{30}$ линейно независимы над $\mathbb{Q}$.
6. Найдите группу $\mu(K) = \bigcup_{n=1}^{\infty} \mu_n(K)$ для полей a) $\mathbb{Q}(i)$; b) $\mathbb{Q}(\sqrt{-2})$; c) $\mathbb{Q}(\sqrt{2})$; d) $\mathbb{Q}(\sqrt{-3})$; e) $\mathbb{Q}(\sqrt{3})$; f) $\mathbb{Q}(\sqrt{-5})$.
7. a) Докажите, что поля $\overline{\mathbb{Q}}$ и $\overline{\mathbb{F}}_p$ счетны. b) Покажите, что поля $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}}_p$, $\mathbb{C}$ попарно не изоморфны.
c) Проверьте, что $\overline{\mathbb{R}} \cong \mathbb{C}$.

12 ноября 2002

1. Докажите, что a) поле $\mathbb{F}_q$ вкладывается в поле $\mathbb{F}_r \iff r = q^n$;
b) $\forall n$ поле $\mathbb{F}_q$ имеет единственное расширение степени n; c) $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.
2. Опишите все автоморфизмы a) поля $\mathbb{C}$ над $\mathbb{R}$; b) поля $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$;
3. Докажите, что a) если $F \subset K \subset L$ и L/F нормально, то L/K нормально;
b) если $K \subset L$ и $[L : K] = 2$, то L/K нормально; c) $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ не нормально.
d) Приведите пример башни полей $F \subset K \subset L$, в которой K/F и L/K нормальны, но L/F не нормально.
4. Найдите $[L : \mathbb{Q}]$, где L — поле разложения многочлена a) $x^4 - 2$; b) $x^p - a$, p — простое.
5. Пусть $\zeta \in \mathbb{C}$ — образующая группы $\mu_n(\mathbb{C})$.
a) Найдите $[\mathbb{Q}(\zeta) : \mathbb{Q}]$. b) Покажите, что $\mathbb{Q}(\zeta)/\mathbb{Q}$ — нормально. c) Найдите $\mathrm{Aut}(\mathbb{Q}(\zeta))$.

6. Пусть $f(x) = x^p - x - a$, $a \in K$, $\operatorname{char} K = p$. Докажите, что a) $f(x+1) = f(x)$; b) $f(x)$ либо неприводим, либо раскладывается на линейные множители; c) если $L = K[x]/f(x)K[x]$, то $\operatorname{Aut}(L/K) = \mathbb{Z}/p\mathbb{Z}$.
7. Пусть $L = K(\alpha)$, $[L:K] = n$. Покажите, что
a) если $K \subset F \subset L$, $\operatorname{Irr}_\alpha^F = x^k + a_1 x^{k-1} + \cdots + a_k$, то $F = K(a_1, \ldots, a_k)$; b) $|\{\, F \mid K \subset F \subset L \,\}| \leqslant 2^n$.
8. a) Если $K \subset L$, $\alpha, \beta \in L$ и $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$, $c_1, c_2 \in K$, то $K(\alpha, \beta) = K(\alpha + c_1\beta)$.
b) Если $r = q^n$, то $\exists \alpha$ т.ч. $\mathbb{F}_r = \mathbb{F}_q(\alpha)$. c) Если $[L:K] < \infty$, и $|\{\, F \mid K \subset F \subset L \,\}| < \infty$, то $\exists \alpha$ т.ч. $L = K(\alpha)$.

19 ноября 2002

1. Пусть $f(x), g(x) \in K[x]$ и $h(x) = \operatorname{res}_{\overline{K}[x]}(f(x), g(x))$. Покажите, что $h(x) \in K[x]$.
2. Покажите, что если L/K одновременно сепарабельно и чисто несепарабельно, то $L = K$.
3. Покажите, что если L/K нормально, то L^{sep}/K нормально.
4. Докажите, что любое конечное поле совершенно.
5. Докажите, что a) расширение $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p, y^p)$ чисто несепарабельно; b) $[\mathbb{F}_p(x,y) : \mathbb{F}_p(x^p, y^p)] = p^2$;
c) существует бесконечное число полей K, таких что $\mathbb{F}_p(x^p, y^p) \subset K \subset \mathbb{F}_p(x,y)$.
6. Пусть K — бесконечное поле, $K(\alpha,\beta)/K$ — сепарабельно, $[K(\alpha,\beta) : K] = n$ и $G = \operatorname{Aut}(K(\alpha,\beta)/K)$. Докажите, что a) $\exists c \in K$ т.ч. $|G(\alpha + c\beta)| = n$, где $G(\alpha + c\beta)$ — орбита $\alpha + c\beta$ относительно группы G;
b) если $|G(\alpha + c\beta)| = n$, то $[K(\alpha + c\beta) : K]_s \geqslant n$; c) если $|G(\alpha + c\beta)| = n$, то $K(\alpha + c\beta) = K(\alpha, \beta)$.
d) Если L/K — конечно и сепарабельно, то $L = K(\alpha)$.

26 ноября 2002

1. Найдите группу $\operatorname{Gal}(\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q})$ и опишите все промежуточные подполя.
2. Найдите группу Галуа многочленов a) $x^2 + ax + b$; b) $x^3 + ax + b$; c) $x^p - a$.
3. Докажите, что группа Галуа многочлена степени n является подгруппой группы $\mathfrak{S}_n$.
4. Докажите, что группа Галуа многочлена $p(x) \in K[x]$ степени n является подгруппой группы $\mathrm{A}_n \iff \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j) \in K$, где α_i — корни $p(x)$ в $\overline{K}$.
5. Пусть $\operatorname{char} K = p > 0$, $p(x) = x^p - x - a \in K[x]$ — неприводим, θ — корень $p(x)$ в $\overline{K}$ и $L = K(\theta)$.
a) Докажите, что L/K — расширение Галуа. b) Найдите группу $\operatorname{Gal}(L/K)$ и опишите ее действие.
c) Докажите, что любое расширение Галуа степени p имеет такой вид.

Задачи семинаров второго семестра

11 февраля 2003 г.

1. Докажите, что a) любое уравнение степени $\leqslant 4$ разрешимо в радикалах; b) общее уравнение степени $\geqslant 5$ неразрешимо в радикалах.
2. Докажите, что все группы порядка $\leqslant 10$ разрешимы.
3. Сформулируйте и докажите теорему о разрешимости в радикалах над полем положительной характеристики a) в сепарабельном случае; b) в общем случае.
4. Пусть L/K — сепарабельное расширение, а $\sigma_1, \ldots, \sigma_n$ — все различные вложения $L \to \overline{K}$. Определим норму и след выражениями $\mathrm{N}_{L/K}(\beta) = \prod_{k=1}^{n} \sigma_k(\beta)$, $\mathrm{Tr}_{L/K}(\beta) = \sum_{k=1}^{n} \sigma_k(\beta)$. a) Докажите, что норма и след являются гомоморфизмами групп $\mathrm{N}_{L/K} : L^* \to K^*$, $\mathrm{Tr}_{L/K} : L \to K$. b) Если L/K сепарабельно, $[L : K] = n$, и $a \in K$, то $\mathrm{N}_{L/K}(a) = a^n$, $\mathrm{Tr}_{L/K}(a) = na$. c) Если $F \subset K \subset L$ — башня сепарабельных расширений, то $\mathrm{N}_{L/F} = \mathrm{N}_{K/F} \circ \mathrm{N}_{L/K}$, $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K}$. d) Вычислите $\mathrm{N}_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha)$, если L/K — сепарабельно, $\mathrm{Irr}_{\alpha}^{K}(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ и $[L : K(\alpha)] = m$. e) Если определить $\mathrm{N}_{L/K}(\beta) = \left(\prod_{k=1}^{r} \sigma_k(\beta)\right)^{[L:K]_i}$, $\mathrm{Tr}_{L/K}(\beta) = [L : K]_i \sum_{k=1}^{r} \sigma_k(\beta)$, то свойства a), b), c), d) будут выполняться также и для несепарабельных расширений.
5. (Построения циркулем и линейкой) На плоскости заданы оси координат и точка с координатами $(1, 0)$; разрешается выполнять следующие действия: (1) проводить прямую через две отмеченные точки; (2) проводить через отмеченную точку окружность с центром в отмеченной точке; (3) отмечать точку пересечения двух линий. a) Докажите, что можно построить любую точку с рациональными координатами. b) Пусть фиксирована некотрая последовательность построений. Обозначим через K_s поле, порожденное над $\mathbb{Q}$ координатами всех точек, отмеченных после s шагов. Докажите, что $[K_s : K_{s-1}] \leqslant 2$. c) Докажите, что для того, чтобы точку с координатами (x, y) можно было построить необходимо условие $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^n$, а если расширение $\mathbb{Q}(x, y)/\mathbb{Q}$ нормально, то оно и достаточно. d) Докажите невозможность трисекции угла и удвоения куба. e) Докажите, что правильный n-угольник можно построить т.т.т.к $n = 2^k p_1 p_2 \ldots p_m$, где $2 < p_1 < p_2 < \cdots < p_m$ — простые числа вида $p_i = 2^{k_i} + 1$.

18 февраля 2003 г.

1. Докажите, что a) в категории множеств декартово произведение является произведением, а несвязное объединение — копроизведением; b) в категориях групп, абелевых групп, колец, A-модулей существуют произведения; c) в категории абелевых групп копроизведение совпадает с произведением; d) в категории групп существуют копроизведения.
2. Дайте категорное определение произведения и копроизведения произвольного семейства объектов, и покажите, что в категории абелевых групп бесконечные копроизведения и произведения не изоморфны.
3. Докажите, что a) если $S = S_1 \sqcup S_2$, то $F_S \cong F_{S_1} \sqcup F_{S_2}$, где F_S — свободный объект, порожденный множеством S; b) свободная абелева группа (соотв. A-модуль), порожденная множеством S, изоморфна $\oplus_{s \in S} \mathbb{Z}$ (соотв. $\oplus_{s \in S} A$); c) свободное коммутативное кольцо, порожденное множеством S, изоморфно кольцу многочленов с целыми коэффициентами от переменных, занумерованных элементами множества S.
4. Пусть G — группа. Докажите, что a) найдется подмножество образующих $S \subset G$, такое что канонический гомоморфизм $f : F_S \to G$ сюръективен; b) найдется подмножество порождающих соотношений $R \subset \mathrm{Ker}\, f \subset F_S$, такое что гомоморфизм $g : F_R \to \mathrm{Ker}\, f$ сюръективен.
5. Пусть $G_{S,R}$ — группа с образующими S и соотношениями R. Докажите, что a) если $S = \{\, \sigma \,\}$, $R = \{\, \sigma^n \,\}$, то $G_{S,R} \cong \mathbb{Z}/n\mathbb{Z}$; b) если $S = \{\, \sigma, \tau \,\}$, $R = \{\, \sigma^n, \tau^2, (\tau\sigma)^2 \,\}$, то $G_{S,R}$ есть группа симметрий правильного n-угольника; c) если $S = \{\, \sigma_1, \ldots, \sigma_n \,\}$, $R = \{\, \sigma_i^2 \,\}_{i=1}^{n} \cup \{\, (\sigma_i \sigma_{i+1})^3 \,\}_{i=1}^{n-1} \cup \{\, (\sigma_i \sigma_j)^2 \,\}_{1 \leqslant i,j \leqslant n \ |i-j| \geqslant 2}$, то $G_{S,R} \cong \mathfrak{S}_{n+1}$.
6. Пусть G' — коммутант группы G, то есть подгруппа группы G, порожденная всеми элементами вида $[g, h] := ghg^{-1}h^{-1}$. Докажите, что a) $G' \lhd G$; b) G/G' — абелева; c) проекция $G \to G/G'$ — универсальный объект, в категории пар (f, A), где $A \in \mathcal{A}b$ и $f \in \mathrm{Hom}_{\mathcal{G}r}(G, A)$; d) сопоставление $G \mapsto G/G'$ продолжается до

функтора $C : \mathcal{G}r \to \mathcal{A}b$; e) если $I : \mathcal{A}b \to \mathcal{G}r$ — вкладывающий функтор, то $\mathrm{Hom}_{\mathcal{G}r}(G, I(A)) \cong \mathrm{Hom}_{\mathcal{A}b}(C(G), A)$ — функториальный изоморфизм; f) существуют морфизмы функторов $\mathrm{Id}_{\mathcal{G}r} \to I \circ C$, $C \circ I \cong \mathrm{Id}_{\mathcal{A}b}$,
7. Докажите эквивалентности категорий a) Vect_K^n всех n-мерных K-векторных пространств, и категории с одним объектом K^n и $\mathrm{Hom}(K^n, K^n) = \mathrm{Mat}_{n\times n}(K)$; b) если A — коммутативное кольцо, то A-Mod $\cong$ Mod-A; c) $\{\,(V, A) \mid V \in \mathrm{Vect}_K,\ A \in \mathrm{End}(A)\,\} \cong K[x]$-Mod. d) Эквивалентны ли категории $\mathrm{Vect}_{\mathbb{F}_2}$ и $\mathrm{Vect}_{\mathbb{F}_3}$?
8. Докажите, что функтор $F : \mathcal{C} \to \mathcal{C}'$ является эквивалентностью категорий $\iff$ F строго полон и сюръективен на множестве классов изоморфизма.
9. Докажите, что a) все функторы $\mathcal{C} \to \mathcal{D}$ образуют категорию $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$; b) всякий колчан Q можно рассматривать как категорию, так что категория $\mathcal{C}^Q$ эквивалентна категории $\mathrm{Fun}(Q, \mathcal{C})$; c) если G — группа, то $\mathrm{Fun}(G, \mathcal{C}) \cong \mathcal{C}^G$.

25 февраля 2003 г.

1. Докажите, что a) если отображение $f : U \to V$ задается матрицей A, то отображение f^* в двойственных базисах задается транспонированной матрицей A^T; b) если заменить базис в V матрицей C, то матрица перехода для двойственных базисов равна $C^{-T} := (C^T)^{-1}$.
2. Докажите, что тензорное произведение над полем a) ассоциативно; b) коммутативно.
3. Докажите, что a) $V \otimes_A A \cong V \cong A \otimes_A V$; b) $A^* \cong A$; c) $\mathrm{Hom}(A, V) \cong V$; d) $V \otimes_A 0 \cong 0 \cong 0 \otimes_A V$.
4. Докажите, что a) если $\dim_K U = n$, то всякий тензор в $U \otimes_K V$ имеет ранг не больше чем n, то есть его можно представить в виде суммы не более чем n разложимых тензоров; b) ранг тензора в $U^* \otimes V$ равен рангу соответствующего морфизма в $\mathrm{Hom}(U, V)$; c) образ канонического отображения $U^* \otimes V \to \mathrm{Hom}(U, V)$ состоит из гомоморфизмов конечного ранга.
5. Пусть A — коммутативное кольцо, а V — свободный A-модуль конечного ранга. Докажите, что
a) $\mathrm{Hom}_A(U, V \otimes W) \cong \mathrm{Hom}_A(U \otimes V^*, W)$; b) $\mathrm{Hom}_A(U \otimes V, W) \cong \mathrm{Hom}_A(U, V^* \otimes W)$; c) $(U \otimes V)^* \cong V^* \otimes U^*$.
6. Постройте канонический гомоморфизм a) $\mathrm{ev} : V^* \otimes V \to K$; b) $\mathrm{ev}^* : K \to V^* \otimes V$ при $\dim V < \infty$. Докажите, что c) $\mathrm{ev} \circ \mathrm{ev}^* = \dim V$; d) при отождествлении $V^* \otimes V \cong \mathrm{Hom}(V, V)$ имеем $\mathrm{ev} = \mathrm{Tr}$, $\mathrm{ev}^* = \mathrm{Id}_V$.
7. Пусть A и B — коммутативные кольца. Введите на $A \otimes_{\mathbb{Z}} B$ структуру кольца, и покажите, что полученное кольцо является копроизведением колец A и B в категории коммутативных колец.
8. Вычислите в категории $\mathbb{Z}$-модулей a) $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$; b) $(\mathbb{Z}/n\mathbb{Z})^*$; c) $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$.

4 марта 2003 г.

1. Найдите размерности пространств a) симметрических форм; b) кососимметрических форм ($\mathrm{char} \neq 2$);
c) эрмитовых форм; d) косоэрмитовых форм.
2. Пусть g — невырожденная форма на V, $\dim V = n$. Докажите, что $\{\,e_1, \ldots, e_n\,\}$ — базис $\iff$ матрица $\big(g(e_i, e_j)\big)_{i,j=1}^n$ — невырождена.
3. Докажите, что если $\mathrm{char} \neq 2$, то всякая симметрическая билинейная форма $g : V \otimes V \to K$ однозначно определяется ассоциированной квадратичной формой $q(v) := g(v, v)$.
4. Если g — билинейная форма на V, т.ч. $g(v, v') = 0 \iff g(v', v) = 0$, то g либо симметрическая, либо знакопеременная.
5. Опишите орбиты действия группы $\mathrm{Aut}(V)$ на множестве всех симметрических и знакопеременных форм на n-мерном векторном пространстве V над полем a) $\mathbb{C}$; b) $\mathbb{R}$; c) $\mathbb{F}_q$.
6. Пусть g — невырожденная $\mathbb{Z}$-билинейная кососимметрическая форма на свободном $\mathbb{Z}$-модуле. Докажите, что g приводится к блочнодиагональному виду $\mathrm{diag}(a_1 I_2, \ldots, a_n I_2)$, где $0 < a_1 | a_2 | \ldots | a_n \neq 0$.
7. Определим категорию $\mathcal{B}il_K$ K-билинейных форм: $\mathrm{Ob}(\mathcal{B}il_K) = \{\,(V, g) \mid V \in \mathrm{Vect}_K,\ g \in \mathrm{Hom}(V \otimes V, K)\,\}$, $\mathrm{Hom}_{\mathcal{B}il_K}((V, g), (W, h)) = \{\,\phi \in \mathrm{Hom}_K(V, W) \mid h \circ (\phi \otimes \phi) = g\,\}$. Докажите, что a) $(V, g) \mapsto (V, g_L^{-1} g_R)$ — функтор из полной подкатегории $\mathcal{B}il_K^{\mathrm{nd}}$ невырожденных форм в категорию представлений одного эндоморфизма;
b) если $(V, g) \in \mathcal{B}il_K^{\mathrm{nd}}$, то всякий морфизм $(V, g) \to (W, h)$ в категории $\mathcal{B}il_K$ — вложение.
8. Пусть $\mathcal{B}il_K^{\pm}$ — категория симметрических (кососимметрических) форм ($\mathrm{char}\, K \neq 2$). Докажите, что
a) если $(V, g) \subset (W, h) \in \mathcal{B}il_K^{\pm}$ и g — невырождена, то $(W, h) \cong (V, g) \perp (V', g')$ (ортогональная прямая сумма);
b) если $U = \mathrm{Ker}\, g \subset V$, то $(V, g) \cong (U, 0) \perp (V', g')$, где g' — невырождена; c) объекты (V', g') в пунктах (a) и (b) определены однозначно с точностью до канонического изоморфизма.

11 марта 2003 г.

1. (Критерий Сильвестра) Пусть G — матрица Грама симметрической билинейной формы g. Пусть Δ_k — ее минор на первых k строках и столбцах. Докажите, что a) если $\Delta_1, \ldots, \Delta_n \neq 0$, то r_- равно количеству перемен знака в последовательности $1 = \Delta_0, \Delta_1, \ldots, \Delta_n$; b) g положительно определена $\iff$ $\Delta_1, \ldots, \Delta_n > 0$.

2. Рассмотрим пространство $\mathbb{R}[x]$ с базисом $1, x, x^2, x^3, \dots$ и применим к нему процесс ортогонализации Грама–Шмидта. Докажите, что получатся (с точностью до константы) следующие базисы
a) (многочлены Лежандра) $P_n(x) = \frac{d^n}{dx^n}[(1-x^2)^n]$, если $P \cdot Q = \int_{-1}^{1} P(x)Q(x)\,dx$;
b) (многочлены Чебышева) $_n(x) = \cos(n \arccos x)$, если $P \cdot Q = \int_{-1}^{1} P(x)Q(x)\frac{dx}{\sqrt{1-x^2}}$;
c) (многочлены Лаггера) $P_n(x) = e^x \frac{d^n}{dx^n}[e^{-x}x^n]$, если $P \cdot Q = \int_0^\infty P(x)Q(x)e^{-x}\,dx$;
d) (многочлены Эрмита) $P_n(x) = e^{x^2}\frac{d^n}{dx^n}[e^{-x^2}]$, если $P \cdot Q = \int_{-\infty}^{\infty} P(x)Q(x)e^{-x^2}\,dx$.
3. (Неравенства Коши–Буняковского) a) $\sum x_i y_i \leqslant \sqrt{\sum x_i^2}\sqrt{\sum y_i^2}$; b) $\sum a_i x_i y_i \leqslant \sqrt{\sum a_i x_i^2}\sqrt{\sum a_i y_i^2}$, $a_i > 0$;
c) $\int f(x)g(x)\,dx \leqslant \sqrt{\int f(x)^2\,dx}\sqrt{\int g(x)^2\,dx}$. d) $\int f(x)g(x)p(x)\,dx \leqslant \sqrt{\int f(x)^2 p(x)\,dx}\sqrt{\int g(x)^2 p(x)\,dx}$, $p(x) > 0$.
4. Рассмотрим на пространстве $\mathrm{Mat}_{n\times n}(\mathbb{R})$ форму $\mathrm{Tr}(AB)$. Найдите ее сигнатуру на подпространствах
a) матриц со следом нуль; b) симметрических матриц; c) кососимметрических матриц; d) (строго) верхнетреугольных матриц и вычислите ортогонал к этим подпространствам.
5. Докажите положительную определенность формы a) $\mathrm{Tr}(AB^T)$ на $\mathrm{Mat}_{n\times n}(\mathbb{R})$; b) $\mathrm{Tr}(A\bar{B}^T)$ на $\mathrm{Mat}_{n\times n}(\mathbb{C})$.
6. Докажите a) $\mathrm{SO}(2;\mathbb{R}) \cong \mathrm{U}(1) \cong \mathbf{S}^1$; b) $\mathrm{SO}(1,1;\mathbb{R}) \cong \mathbb{R}\times\{\pm 1\}$; c) $\mathrm{O}(n;\mathbb{R})/\mathrm{SO}(n;\mathbb{R}) \cong \{\pm 1\}$;
d) $\mathrm{U}(n)/\mathrm{SU}(n) \cong \mathbf{S}^1$; e) $\mathrm{SU}(2)/\{\pm 1\} \cong \mathrm{SO}(3;\mathbb{R})$; f) $\mathrm{SU}(2) \cong \mathbf{S}^3$.
7. Докажите, что a) $\mathrm{O}(n) \cong \{A \mid A^T A = E\}$, $\mathrm{U}(n) \cong \{A \mid \bar{A}^T A = E\}$; b) группа $\mathrm{O}(V,g;\mathbb{R})$ (соотв. $\mathrm{U}(V,h)$) компактна $\iff$ форма g (соотв. h) положительно или отрицательно определена.

18 марта 2003 г.

1. Докажите, что a) $(\mathrm{Ker}\,A)^\perp = \mathrm{Im}\,A^T$; b) если $A(U) \subset U$, то $A^T(U^\perp) \subset U^\perp$.
2. Проверьте, что a) $\mathrm{Tr}(A^T) = \mathrm{Tr}(A)$; b) $\det(A^T) = \det(A)$; c) $\chi_{A^T} = \chi_A$; d) $m_{A^T} = m_A$.
3. Пусть $V = \mathbb{R}[x]$, $(P,Q) = \int_{-\infty}^{\infty} P(x)Q(x)e^{-x^2}dx$. Найдите A^T, если a) $A = d/dx$; b) $A = f(x)$.
4. Пусть $V = \mathbb{R}[x]$, $(P,Q) = \int_0^1 P(x)Q(x)\,dx$ и $K(x,y) \in \mathbb{R}[x,y]$. Положим $A_K(f)(x) = \int_0^1 K(x,y)f(y)\,dy$. Найдите A_K^T.
5. Оператор называется нормальным, если $A^T A = AA^T$ (в эрмитовом случае $A^\dagger A = AA^\dagger$). Докажите, что A — нормален $\iff$ a) $|Av| = |A^T v|$ $\forall v \in V$; b) $(A + A^T)/2$ и $(A - A^T)/2$ коммутируют; c) существует ортонормированный базис, в котором A диагонален (в эрмитовом случае); d) существует ортонормированный базис, в котором A блочно-диагонален с блоками вида $\left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right)$ и (c) на диагонали (в билинейном случае).
6. Докажите, что a) самосопряженные, антисамосопряженные и ортогональные операторы нормальны.
b) всякий ортогональный оператор в некотором ортонормированном базисе блочно-диагонален с блоками вида $\left(\begin{smallmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi\end{smallmatrix}\right)$, и (± 1) на диагонали.
7. Докажите, что a) вырожденные операторы допускают полярное разложение; b) всякая матрица представляется в виде $A = N_1 S N_2$, где S — диагональна и неотрицательна, а N_1, N_2 — ортогональны. c) Насколько неоднозначно такое представление?
8. Пусть L/K — конечное расширение Галуа, $\mathrm{Gal}(L/K) = G$. a) Докажите, что $V \mapsto V_L := V \otimes_K L$ — строгий функтор $\mathrm{Vect}_K \to \mathrm{Vect}_L$. b) Пусть $W \in \mathrm{Vect}_L$ и $B : G \to \mathrm{GL}(W;K)$ гомоморфизм групп, такой что $\forall \lambda \in L, \sigma \in G, w \in W$ имеем $B(\sigma)(\lambda w) = \sigma(\lambda)B(\sigma)(w)$ (K-структура на W). Докажите, что $V = W^G := \{w \in W \mid \forall \sigma \in G\ B(\sigma)(w) = w\}$ — K-подпространство, такое что $W = V_L$. c) Докажите, что $V \mapsto V_L$ и $W \mapsto W^G$ — эквивалентности категории Vect_K и категории пар (W,B) (L-векторное пространство с K-структурой).

25 марта 2003 г.

1. Докажите, что a) $S^n(U\oplus V) = \bigoplus_{p+q=n} S^pU \otimes S^qV$; b) $\Lambda^n(U\oplus V) = \bigoplus_{p+q=n} \Lambda^pU \otimes \Lambda^qV$;
c) $\det(U\oplus V) = \det U \otimes \det V$; d) $(S^nV)^* \cong S^nV^*$, $(\Lambda^nV)^* \cong \Lambda^nV^*$; e) $\Lambda^nV \otimes \det V^* \cong \Lambda^{N-n}V^*$, где $N = \dim V$.
2. Докажите a) $S^\bullet U \otimes S^\bullet V \cong S^\bullet(U\oplus V)$; b) $\Lambda^\bullet U \otimes \Lambda^\bullet V \cong \Lambda^\bullet(U\oplus V)$; c) если $\dim V = n$, то $S^\bullet V^* \cong K[x_1,\dots,x_n]$.
3. Докажите существование S^n и Λ^n для модулей над произвольным a) полем; b) коммутативным кольцом.
c) Докажите, что $\mathrm{Sym} : T^n \to S^n$ и $\mathrm{Alt} : T^n \to \Lambda^n$ — морфизмы функторов.
4. Пусть $\dim U = \dim V = n$. Рассмотрим пространство $U^*\otimes V^*$ билинейных форм на $U\times V$. Докажите, что a) отображение $(U^*\otimes V^*)\times\dots\times(U^*\otimes V^*) \to \det U^* \otimes \det V^*$, $(u^1\otimes v^1,\dots,u^n\otimes v^n) \mapsto (u^1\wedge\dots\wedge u^n)\otimes(v^1\wedge\dots\wedge v^n)$ полилинейно и симметрично; b) если выбрать базисы в U и V и представить билинейную форму матрицей Грама, то индуцированное отображение $S^n(U^*\otimes V^*) \to K$ равняется определителю матрицы Грама.
5. Докажите, что присоединенная матрица $\widehat{A}$ к матрице оператора $A : V \to V$ равна матрице оператора $(\Lambda^{N-1}A)^* : \Lambda^{N-1}V^* \to \Lambda^{N-1}V^*$ с учетом изомофризма $\Lambda^{N-1}V^* \cong V \otimes \det V^*$, где $N = \dim V$.
6. Пусть A — $\mathbb{C}$-алгебра. Докажите, что a) если $\dim_{\mathbb{C}} A = 1$, то $A \cong \mathbb{C}$; b) если $\dim_{\mathbb{C}} A = 2$, то $A \cong \mathbb{C}\times\mathbb{C}$ или $A \cong \mathbb{C}[t]/t^2$. c) Опишите все классы изоморфизма алгебр A, таких что $\dim_{\mathbb{C}} A = 3$.

7. Пусть Q — колчан. Путем в колчане Q называется такая последовательность стрелок, что начало следующей совпадает с концом предыдущей. Произведение путей — это их объединение (если оно является путем), или ноль. Докажите, что a) векторное пространство $K[Q]$ всех линейных комбинаций путей в Q является K-алгеброй (алгеброй путей колчана); b) если Q состоит из одной вершины и n стрелок, то $K[Q] \cong T^\bullet(K^n)$; c) если Q состоит из n вершин без стрелок, то $K[Q] \cong K^n$; d) $\mathrm{Vect}_K^Q \cong \mathrm{Mod}\text{-}K[Q]$ эквивалентность категорий.
8. Алгеброй Клиффорда $C(g)$ формы $g \in S^2V^*$ называется фактор алгебры $T^\bullet(V)$ по идеалу, порожденному подпространством $\{\, u \otimes v + v \otimes u - 2g(u,v) \cdot 1 \mid u, v \in V \,\} \subset K \oplus V^{\otimes 2} \subset T^\bullet(V)$. Докажите, что
a) $C(g)$ конечномерна; b) если $\dim V = 2$, $K = \mathbb{C}$, а g — невырождена, то $C(g) \cong \mathrm{Mat}_{2\times 2}(\mathbb{C})$;
c) если $\dim V = 3$, $K = \mathbb{C}$, а g — невырождена, то $C(g) \cong \mathrm{Mat}_{2\times 2}(\mathbb{C}) \times \mathrm{Mat}_{2\times 2}(\mathbb{C})$.

01 апреля 2003 г.

1. Пусть $\dim V = 2n$. Рассмотрим пространство $\Lambda^2 V^*$ билинейных кососимметрических форм на V. Докажите, что a) отображение $(\Lambda^2 V^*) \times \cdots \times (\Lambda^2 V^*) \to \det V^*$, $(w^1, \ldots, w^n) \mapsto (w^1 \wedge \cdots \wedge w^n)$ полилинейно и симметрично. b) если выбрать базис в V и представить билинейную форму матрицей Грама, то индуцированное отображение $S^n(\Lambda^2 V^*) \to K$ задается многочленом степени n от коэффициентов матрицы Грама; c) этот многочлен равен пфаффиану;
2. Докажите, что $\mathrm{Pf}(C^T A C) = \mathrm{Pf}(A)\det(C)$.
3. Пусть A — кососимметрическая матрица размера $(2n+1)\times(2n+1)$. Пусть $\mathrm{Pf}_i(A)$ — пфаффиан матрицы, полученной вычеркиванием i-ой строки и i-ого столбца. Докажите, что $\widehat{A} = (\mathrm{Pf}_i(A)\,\mathrm{Pf}_j(A))$.
4. Пусть D — базисный элемент в $\det V$, а D^* — двойственный базисный элемент в $\det V^*$. Докажите, что отображения $w \mapsto w \vdash D^*$ и $\xi \mapsto D \vdash \xi$ являются взаимно обратными изоморфизмами $\Lambda^k V \rightleftarrows \Lambda^{n-k} V^*$.
5. Выпишите явно уравнения Плюккера для множества всех разложимых 2-векторов a) в $\Lambda^2 K^4$; b) в $\Lambda^2 K^5$.

08 апреля 2003 г.

1. Разложите над полем $\mathbb{C}$ в сумму неприводимых регулярное представление группы a) $\mathbb{Z}/n\mathbb{Z}$; b) $\mathfrak{S}_3$.
2. Вычислите действие функторов $\otimes$ и $*$ на неприводимых представлениях группы a) $\mathbb{Z}/n\mathbb{Z}$; b) $\mathfrak{S}_3$.
3. Докажите, что a) $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}] \cong \mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}$; b) $\mathbb{Q}[\mathbb{Z}/p\mathbb{Z}] \cong \mathbb{Q} \times \mathbb{Q}(\sqrt[p]{1})$; c) $\mathbb{C}[\mathfrak{S}_3] \cong \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_{2\times 2}(\mathbb{C})$.
4. Докажите эквивалентность категорий $\mathrm{Rep}_G(K) \cong \prod_\rho \mathrm{Vect}_K$ (произведение по классам изоморфизма неприводимых представлений), если $\bar{K} = K$, $\mathrm{char}\, K = 0$, а G — конечная группа.
5. Пусть V — представление конечной группы G над полем $\mathbb{R}$ или $\mathbb{C}$. a) Докажите, что на V существует G-инвариантное положительно определенное скалярное (эрмитово) произведение; b) Выведите из этого полную приводимость V.
6. Пусть группа G действует на множестве X, а $K[X]$ — пространство K-значных функций на X.
a) Постройте в $K[X]$ структуру G-модуля. b) Докажите, что $K[G]$ — регулярное представление;
c) $X \mapsto K[X]$ — контравариантный функтор $\mathcal{S}ets^G \to \mathrm{Rep}_G(K)$; d) $K[X \times Y] \cong K[X] \otimes K[Y]$.
7. Докажите, что a) $\otimes$ в категории $\mathrm{Rep}_G(K)$ коммутативно и ассоциативно; b) $\mathrm{Hom}(1_G, V) \cong V$, $1_G \otimes V \cong V$, $1_G^* \cong 1_G$; c) $\mathrm{Hom}(\varepsilon, \varepsilon) \cong 1_{\mathfrak{S}_n}$, $\varepsilon \otimes \varepsilon \cong 1_{\mathfrak{S}_n}$, $\varepsilon^* \cong \varepsilon$; d) $V \otimes K[G] \cong K[G]^{\oplus \dim V}$, $K[G]^* \cong K[G]$.
8. Докажите, что функториальные морфизмы $\mathrm{ev} : V^* \otimes V \to 1_G$, $\mathrm{ev}^* : 1_G \to V^* \otimes V$, $V \to V^{**}$, $U^* \otimes V \to \mathrm{Hom}(U, V)$, $\mathrm{Hom}(U, \mathrm{Hom}(V, W)) \to \mathrm{Hom}(U \otimes V, W)$ — G-эквивариантны.
9. Определим коинварианты представления V как факторпредставление $V_G := V/\langle v - gv \rangle_{v\in V, g\in G}$.
Докажите, что a) $\mathrm{Hom}_G(U, V) \cong \mathrm{Hom}(U, V)^G$; b) $U \otimes_G V := U \otimes_{K[G]} V = (U \otimes V)_G$; c) $(V^*)^G \cong (V_G)^*$;
d) если U вполне приводимо, то канонический морфизм $V^G \to V_G$ — изоморфизм.
10. a) Пусть G — конечная подгруппа в группе $\mathrm{SO}(3;\mathbb{R})$. Докажите, что G совпадает с одной из следующих групп: (1) $\mathbb{Z}/n\mathbb{Z}$; (2) группа симметрий правильного n-угольника (группа диэдра); (3) группа вращений тетраэдра; (4) группа вращений куба (октаэдра); (5) группа вращений икосаэдра (додекаэдра). b) Опишите все конечные подгруппы в $SU(2)$; c) $\mathrm{SL}(3;\mathbb{R})$; d) $\mathrm{SL}(2;\mathbb{C})$.

15 апреля 2003 г.

1. Составьте таблицу характеров (над $\mathbb{C}$) для групп a) $\mathbb{Z}/n\mathbb{Z}$; b) $\mathfrak{S}_3$; c) $H = \{\, \pm 1, \pm i, \pm j, \pm k \,\} \subset \mathbb{H}$; d) диэдра.
2. Опишите структуру кольца Гротендика для групп из предыдущей задачи.
3. Вычислите характер стандартного представления группы $\mathfrak{S}_n$.
4. Найдите кратности неприводимых представлений в стандартном представлении групп a) $\mathfrak{S}_3$; b) $\mathfrak{S}_4$.
5. Пусть ρ — неприводимое представление, $e_\rho = \frac{1}{|G|}\sum_{g\in G} \chi_\rho(g^{-1}) g \in K[G]$, и $\overline{K} = K$. Докажите, что
a) $e_\rho \in Z(K[G])$; b) e_ρ — проектор на изотипическую компоненту представления ρ.

6. Пусть V – представление группы G. a) Покажите, что $\Lambda^p V$ и $S^p V$ — подпредставления в $V^{\otimes p}$. Докажите, что b) $\chi_{S^2V}(g) = (\chi_V(g)^2 + \chi_V(g^2))/2$, $\chi_{\Lambda^2 V}(g) = (\chi_V(g)^2 - \chi_V(g^2))/2$; c) если $n_1(\sigma), \dots, n_p(\sigma)$ — длины независимых циклов, из которых состоит σ, то $\chi_{\Lambda^p V}(g) = \frac{1}{p!}\sum_{\sigma\in\mathfrak{S}_p} \varepsilon(\sigma)\chi_V(g^{n_1(\sigma)})\dots\chi_V(g^{n_p(\sigma)})$.
7. Пусть V — неприводимое комплексное представление группы G.
a) Докажите, что на V существует ненулевая G-инвариантная билинейная форма $\iff \overline{\chi}_V = \chi_V$.
Пусть теперь B такая форма. Докажите, что b) $V \cong V^*$; c) B невырождена; d) B единственна с точностью до константы; e) B либо симметрична, либо кососимметрична; f) B симметрична $\iff \sum_{g\in G}\chi_V(g^2) = |G|$; g) B кососимметрична $\iff \sum_{g\in G}\chi_V(g^2) = -|G|$.
8. Докажите, что a) V — представление над $\mathbb{R} \Longrightarrow V^* \cong V$; b) V — представление над $\mathbb{C} \Longrightarrow V^* \cong \overline{V}$.
9. Докажите, что a) если U — представление группы G над $\mathbb{R}$, то $V = U_{\mathbb{C}}$ — представление группы G над $\mathbb{C}$, причем $V \cong V^* \cong \overline{V}$; b) неприводимое комплексное представление V группы G изоморфно представлению вида $U_{\mathbb{C}} \iff$ на V существует ненулевая G-инвариантная симметрическая форма.
10[1]. Пусть U — неприводимое представление группы G над $\mathbb{R}$. Докажите, что
a) если $\mathrm{End}_G(U) = \mathbb{R}$, то $U_{\mathbb{C}} = V$ неприводимо над $\mathbb{C}$ и $\chi_U = \chi_V$;
b) если $\mathrm{End}_G(U) = \mathbb{C}$, то $U_{\mathbb{C}} \cong V \oplus V^*$, $V \ncong V^*$ неприводимо над $\mathbb{C}$ и $\chi_U = \chi_V + \overline{\chi}_V$;
c) если $\mathrm{End}_G(U) = \mathbb{H}$, то $U_{\mathbb{C}} \cong V \oplus V$, V неприводимо над $\mathbb{C}$ и $\chi_U = 2\chi_V$.
11. Пусть V — неприводимое представление группы G над $\mathbb{C}$. Докажите, что
a) если $\overline{\chi}_V = \chi_V$ и $\sum_{g\in G}\chi_V(g^2) = |G|$, то $V \cong U_{\mathbb{C}}$, U — неприводимо над $\mathbb{R}$ и $\chi_U = \chi_V$;
b) если $\overline{\chi}_V \neq \chi_V$, то $V \oplus V^* \cong U_{\mathbb{C}}$, U — неприводимо над $\mathbb{R}$ и $\chi_U = \chi_V + \overline{\chi}_V$;
c) если $\overline{\chi}_V = \chi_V$ и $\sum_{g\in G}\chi_V(g^2) = -|G|$, то $V \oplus V \cong U_{\mathbb{C}}$, U — неприводимо над $\mathbb{R}$ и $\chi_U = 2\chi_V$.
12. Опишите неприводимые представления над $\mathbb{R}$ групп a) $\mathbb{Z}/n\mathbb{Z}$; b) $\mathfrak{S}_3$; c) $H = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}$.
13. Если G — абелева группа, то группа $\widehat{G} := \mathrm{Hom}(G, \mathbf{S}^1)$ называется двойственной по Понтрягину к G. Постройте канонические изоморфизмы a) $\widehat{G\times H} \cong \widehat{G}\times\widehat{H}$; b) $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mu_n(\mathbb{C})$, $\widehat{\mu_n(\mathbb{C})} \cong \mathbb{Z}/n\mathbb{Z}$; c) $\widehat{\widehat{G}} \cong G$; d) $\widehat{\mathbb{Z}} \cong \mathbf{S}^1$, $\widehat{\mathbf{S}^1} \cong \mathbb{Z}$. e) Докажите, что всякая $\mathbb{C}$-значная функция на G является линейной комбинацией элементов из $\widehat{G}$ и выпишите явную формулу для коэффициентов (преобразование Фурье).
14. (Соответствие Маккея) Пусть G — конечная подгруппа в $\mathrm{SL}(2;\mathbb{C})$, $V_1, \dots, V_n$ — все ее неприводимые представления, а L — ее тавтологическое двумерное представление. Пусть $a_{ij} = \mathrm{mult}_{V_i}(V_j \otimes L)$. Предположим, что G — циклическая группа или группа диэдра. Докажите, что a) матрица $C = (2\delta_{ij} - a_{ij})$ симметрична; b) билинейная форма с матрицей Грама C положительно полуопределена; c) вектор с координатами $x_i = \dim V_i$ порождает ядро формы C; d) Нарисуйте граф с n вершинами и a_{ij} ребрами между i-ой и j-ой вершиной. e) Сотрите вершину, соответствующую тривиальному представлению, и все ребра, выходящие из нее. f*) Проделайте те же действия для бинарных групп тетраэдра, куба и октаэдра.
Графы, возникающие в пунктах (d), (e) и (f) очень часто встречаются в математике в задачах классификации. Они называются диаграммами Дынкина.

22 апреля 2003 г.

1. Найдите размерности неприводимых над полем $\mathbb{C}$ представлений группы a) $\mathfrak{S}_4$; b) $\mathfrak{S}_5$.
2. Пусть C — центр группы G, $H = \{(x_1, \dots, x_n) \in C^n \mid x_1 \cdot \ldots \cdot x_n = 1\} \subset C^n \subset G^n$, а V — неприводимое представление G. Докажите, что
a) $V^{\otimes n}$ — неприводимое представление группы G^n/H; b) $(\dim V)^n | (|G|^n/|C|^{n-1})$; c) $\dim V | (G : C)$.
3. Пусть $K/\mathbb{Q}$ — конечное расширение, а $R \subset K$ — подкольцо целых. Докажите, что
a) если $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$, то $\sigma(R) = R$; b) $R \cong \mathbb{Z}^{[K:\mathbb{Q}]}$; c) $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$.
4. Найдите кольца целых в полях a) $\mathbb{Q}(i)$; b) $\mathbb{Q}(\sqrt[3]{1})$.
5. Опишите действие функторов Res и Ind на неприводимые представления групп $V_4 \subset A_4 \subset \mathfrak{S}_4$.
6. Пусть $G_2 \subset G_1 \subset G$. Докажите, что a) $\mathrm{Res}^G_{G_2} = \mathrm{Res}^{G_1}_{G_2} \circ \mathrm{Res}^G_{G_1}$; b) $\mathrm{Ind}^G_{G_2} = \mathrm{Ind}^G_{G_1} \circ \mathrm{Ind}^{G_1}_{G_2}$.
7. Пусть $\varphi : H \to G$ — гомоморфизм групп. Определите функторы ограничения $\mathrm{Rep}_G \to \mathrm{Rep}_H$ и индукции $\mathrm{Rep}_H \to \mathrm{Rep}_G$, так чтобы выполнялось условие сопряженности и утверждения предыдущей задачи.
8. Докажите, что a) $\mathrm{Res}(U \oplus V) = \mathrm{Res}\, U \oplus \mathrm{Res}\, V$, $\mathrm{Ind}(U \oplus V) = \mathrm{Ind}\, U \oplus \mathrm{Ind}\, V$; b) $\mathrm{Res}(U \otimes V) = \mathrm{Res}\, U \otimes \mathrm{Res}\, V$; c) $\mathrm{Res}(V^*) = (\mathrm{Res}\, V)^*$; d) (формула проекции) $\mathrm{Ind}^G_H(U \otimes \mathrm{Res}^G_H V) = (\mathrm{Ind}^G_H U) \otimes V$.
9. Докажите, что a) $\mathrm{Ind}^G_H U = \{f : G \to U \mid f(hx) = hf(x)\}$ с действием G, заданным формулой $gf(x) = f(xg)$; b) $\mathrm{Ind}^G_H V = V \otimes_{K[H]} K[G]$.

[1] По теореме Фробениуса (если L — тело над $\mathbb{R}$, то или $L = \mathbb{R}$, или $L = \mathbb{C}$, или $L = \mathbb{H}$) и лемме Шура все возможности для алгебры $\mathrm{End}_G(U)$ исчерпываются приведенными в задаче случаями

10. Пусть V — представление группы G, $V = \oplus_i V_i$ (сумма подпространств), причем группа G транзитивно переставляет слагаемые. Докажите, что $V = \operatorname{Ind}_H^G V_{i_0}$, где $H = \{\, g \in G \mid g(V_{i_0}) \subset V_{i_0} \,\}$.
11. Пусть H и K подгруппы в G, а ρ — представление G. Докажите, что $\operatorname{Res}_K^G \operatorname{Ind}_H^G \rho = \bigoplus_{s \in K\backslash G/H} \operatorname{Ind}_{H_s}^K \rho_s$, где $H_s = sHs^{-1} \cap K$, а представление ρ_s группы H_s задается формулой $\rho_s(x) = \rho(s^{-1}xs)$.
12. (Критерий Макки.) Докажите, что
a) $\operatorname{Ind}_H^G \rho$ — неприводимо $\iff$ ρ — неприводимо, и $\forall s \in G - H$ имеем $\langle \chi_{\rho_s}, \chi_{\operatorname{Res}^H_{H_s} \rho} \rangle = 0$, где $H_s = sHs^{-1} \cap H$;
b) если H — нормальна, то $\operatorname{Ind}_H^G \rho$ — неприводимо $\iff$ ρ — неприводимо, и $\forall s \in G - H$ имеем $s^{-1}\rho s \not\cong \rho$.
13. Над полем $\mathbb{R}$ разложите в сумму неприводимых над $G_1 \times G_2$ представление $V_1 \otimes V_2$, если
a) $G_i = \mathbb{Z}/n_i\mathbb{Z}$, $(n_1, n_2) = 1$, а V_i — неприводимы; b) $G_1 = G_2 = H$, $V_1 = V_2 = \mathbb{H}$.
14. Докажите, что $\operatorname{Ind}_{G_1}^{G_1 \times G_2} V = V \otimes K[G_2]$.

Задачи семинаров третьего семестра

08 сентября 2003 г.

1. Сформулируйте и докажите теорему Жордана–Гельдера в категории модулей над кольцом.
2. Пусть p и q простые. Докажите, что a) нильпотентная группа разрешима; b) всякая p-группа разрешима; c) всякая группа порядка $p^n q$, где $p > q$ разрешима.
3. Пусть G — группа порядка p^n. Докажите, что a) $\forall k \leqslant n$ найдется подгруппа $H \subset G$ порядка p^k; b) любая подгруппа порядка p^{n-1} в G нормальна.
4. Докажите, что все группы порядка < 60 разрешимы.
5. Пусть p и q простые. a) Докажите, что любая группа порядка p^2 абелева. Опишите все группы порядка b) pq; c) p^3.
6. Докажите, что если $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ — центральный ряд, то a) $Z_s G \subset G_s \subset Z^{m-s} G$; b) верхний и нижний центральные ряды обрываются и их длины не превосходят m; c) длины верхнего и нижнего центральных рядов совпадают.
7. Докажите, что следующие условия эквивалентны: (i) группа G нильпотентна; (ii) верхний центральный ряд группы G обрывается; (iii) нижний центральный ряд группы G обрывается.
8. Опишите все силовские 2-подгруппы в группе $\mathfrak{S}_4$.

10 ноября 2003 г.

1. Пусть алгебра A конечномерна. Докажите, что
a) $x \in \mathfrak{R}_A \iff x$ действует нулем во всех простых левых A-модулях;
b) $x \in \mathfrak{R}_A \iff x$ действует нулем во всех простых правых A-модулях;
c) $\mathfrak{R}_A$ равен пересечению всех правых максимальных идеалов.
2. Пусть K'/K — алгебраическое расширение полей. Докажите, что $K' \otimes_K L$ — полупростая алгебра для всех $L \iff$ расширение K'/K сепарабельно.
3. Пусть D — тело над K, а B — K-алгебра. Докажите, что
a) двусторонние идеалы в алгебре $D \otimes_K B$ порождаются двусторонними идеалами в алгебре $Z(D) \otimes_K B$;
b) если $Z(D) = K$, а B — простая, то $D \otimes_K B$ — простая.
4. Докажите, что тензорное произведение центральных простых алгебр над полем K является центральной простой алгеброй над полем K.
5. Докажите, что $A^{\mathrm{op}} \otimes_K A$ — матричная алгебра над полем K.
6. Докажите, что
a) множество классов подобия центральных простых алгебр над полем K с операцией $\otimes$ образуют группу;
b) эта группа изоморфна группе Брауэра поля K.
7. Вычислите группу Брауэра поля a) $\mathbb{R}$; b) $\mathbb{F}_q$.
8. Найдите все центральные тела над полем a) $\mathbb{R}$; b) $\mathbb{F}_q$.
9. Докажите, что a) $H^0(\mathrm{Gal}(L/K), L^*) = K^*$; b) $H^1(\mathrm{Gal}(L/K), L^*) = 0$ (теорема Гильберта-90).

15 сентября 2003 г.

1. Если (f_A, f_B, f_C) — — морфизм точных троек, то точна последовательность $0 \to \operatorname{Ker} f_A \to \operatorname{Ker} f_B \to \operatorname{Ker} f_C \to A'/\operatorname{Im} f_A \to B'/\operatorname{Im} f_B \to C'/\operatorname{Im} f_C \to 0$.

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \downarrow f_A & & \downarrow f_B & & \downarrow f_C & & \\ 0 & \to & A' & \to & B' & \to & C' & \to & 0 \end{array}$$

2. Если в коммутативной диаграмме строки точны, f_1 — эпиморфизм, f_5 — мономорфизм, а f_2 и f_4 — изоморфизмы, то f_3 — изоморфизм.

$$\begin{array}{ccccccccccc} X_1 & \to & X_2 & \to & X_3 & \to & X_4 & \to & X_5 \\ \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \downarrow f_4 & & \downarrow f_5 \\ Y_1 & \to & Y_2 & \to & Y_3 & \to & Y_4 & \to & Y_5 \end{array}$$

3. Пусть $\mathcal{A} = \operatorname{Mod} -A$ — категория модулей над кольцом A. Докажите, что a) комплексы в $\mathcal{A}$ и морфизмы комплексов образуют категорию $\mathsf{Com}\mathcal{A}$; b) $H^i : \mathsf{Com}\mathcal{A} \to \mathcal{A}$ — функтор; c) в категории $\mathsf{Com}\mathcal{A}$ существуют ядра и образы; d) постройте функтор свертки $\operatorname{Tot} : \mathsf{Bicom}\mathcal{A} := \mathsf{Com}\mathsf{Com}\mathcal{A} \to \mathsf{Com}\mathcal{A}$.
4. Морфизмы комплексов $f, f' : E^\bullet \to F^\bullet$ называются гомотопными, если найдется набор морфизмов $h^i : E^i \to F^{i-1}$, такой что $f'^i - f^i = h^{i+1}d_E^i + d_F^{i-1}h^i$. Докажите, что a) гомотопия — отношение эквивалентности; b) если $f \sim f'$, то $H^\bullet f = H^\bullet f'$; c) если $\operatorname{Id}_{E^\bullet} \sim 0$, то $E^\bullet$ — ацикличен; d) множество морфизмов гомотопных нулю — идеал в кольце $\operatorname{Hom}_{\mathsf{Com}\mathcal{A}}(E^\bullet, E^\bullet)$; e) если $\operatorname{Ob}(\mathsf{Hot}\mathcal{A}) = \operatorname{Ob}(\mathsf{Com}\mathcal{A})$, $\operatorname{Hom}_{\mathsf{Hot}\mathcal{A}}(E^\bullet, F^\bullet) = \operatorname{Hom}_{\mathsf{Com}\mathcal{A}}(E^\bullet, F^\bullet)/\sim$, то Hot — категория (гомотопическая категория); f) функтор когомологий $\mathsf{Com}\mathcal{A} \to \mathcal{A}$ пропускается через $\mathsf{Hot}\mathcal{A}$.
5. Пусть $E^\bullet$ и $F^\bullet$ — комплексы. Пусть $\operatorname{RHom}^k(E^\bullet, F^\bullet) := \oplus_{i\in\mathbb{Z}} \operatorname{Hom}(E^i, F^{i+k})$ и рассмотрим отображения $D^k : \operatorname{RHom}^k \to \operatorname{RHom}^{k+1}$, $(f_i) \mapsto (d_F^{i+k} \circ f^i - (-1)^k f^{i+1} \circ d_E^i)$. Докажите, что a) $(\operatorname{RHom}^\bullet, D^\bullet)$ — комплекс;
b) $Z^0 = \{$ морфизмы комплексов $\}$, c) $B^0 = \{$ морфизмы, гомотопные нулю $\}$; d) $H^0 = \operatorname{Hom}_{\mathsf{Hot}}(E^\bullet, F^\bullet)$.
6. Пусть X — топологическое пространство, а F — конечно-порожденная абелева группа. Постройте точные последовательности a) $0 \to \mathbb{Z}^{\oplus a} \to \mathbb{Z}^{\oplus b} \to F \to 0$; b) $0 \to C_\bullet(X)^{\oplus a} \to C_\bullet(X)^{\oplus b} \to C_\bullet(X) \otimes_{\mathbb{Z}} F \to 0$; c) (формула универсальных коэффициентов) $0 \to H_i(X,\mathbb{Z}) \otimes_{\mathbb{Z}} F \to H_i(X,F) \to \operatorname{Tor}_1(H_{i-1}(X,\mathbb{Z}),F) \to 0$, где $\operatorname{Tor}_1(H_{i-1}(X,\mathbb{Z}),F) := \operatorname{Ker}(H_{i-1}(X,\mathbb{Z})^{\oplus a} \to H_{i-1}(X,\mathbb{Z})^{\oplus b})$; d) $H_i(X,\mathbb{Q}) = H_i(X,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$.
7. Докажите, что $H_1(G,\mathbb{Z}) \cong G/[G,G]$.

22 сентября 2003 г.

1. Докажите, что $H^1(G,\mathbb{Z}) = (G/[G,G])^*$.
2. Пусть $0 \to M \to P^0 \to P^1 \to \dots$ — точная последовательность, в которых $H^i(G,P^n) = 0$ при $i > 0$ и всех n (ацикличная резольвента). Докажите, что $H^i(G,M) \cong H^i(P^{\bullet G})$.
3. Пусть $G = \mathbb{Z}/m\mathbb{Z}$, а M — G-модуль. Докажите, что a) $H^i(G,M[G]) = 0$ при $i > 0$ и $H^0(G,M[G]) = M$;
b) $0 \to M \to M[G] \xrightarrow{1-t} M[G] \xrightarrow{N} M[G] \xrightarrow{1-t} \dots$ — ацикличная резольвента. c) Вычислите $H^i(G,M)$.
4. Пусть p, q — простые и $p < q$. Вычислите a) $H^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z})$; b) $H^2(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$.
5. Докажите, что расширение групп $1 \to N \to E \to G \to 1$ расщепимо $\iff E = N \leftthreetimes G$.
6. Докажите, что множество всех классов расщеплений расширения $1 \to N \to N \leftthreetimes G \to G \to 1$ по модулю сопряжения элементами из N, изоморфно группе $H^1(G,N)$.
7. Пусть $\xi : G_1 \times G_2 \to N$ — 2-коцикл. Докажите, что
a) операция $(n_1,g_1)\cdot(n_2,g_2) = (n_1 + g_1n_2 + \xi(g_1,g_2), g_1g_2)$ на множестве $N \times G$ ассоциативна;
b) элемент $(-\xi(1,1),1)$ является единицей;
c) элемент $(-g^{-1}(\xi(1,1) + \xi(g,g^{-1}) + n), g^{-1})$ — обратный к (n,g);
d) отображения $n \mapsto (n - \xi(1,1),1)$ и $(n,g) \mapsto g$ дают расширение групп;
e) если ξ — кограница, то полученное расширение расщепимо.
8. Расширение называется центральным, если $N \subset Z(E)$. Докажите, что множество центральных расширение G с помощью N изоморфно группе $H^2(G,N)$, где N — тривиальный G-модуль.
9. Пусть $1 \to N \xrightarrow{i_1} E_1 \xrightarrow{f_1} G \to 1$ и $1 \to N \xrightarrow{i_2} E_2 \xrightarrow{f_2} G \to 1$ — абелевы расширения групп. Докажите, что
a) расслоенное произведение $E_1 \times_G E_2 := \{ (x_1,x_2) \mid f_1(x_1) = f_2(x_2) \}$ является подгруппой в $E_1 \times E_2$;
b) если действия $\overline{\mathrm{Ad}}_1$ и $\overline{\mathrm{Ad}}_2$ совпадают, то $i : N \to E_1 \times_G E_2$, $n \mapsto (i_1(n), i_2(n^{-1}))$ — нормальное вложение;
c) последовательность $1 \to N \xrightarrow{i_1} \dfrac{E_1 \times_G E_2}{i(N)} \xrightarrow{f_1} G \to 1$ — абелево расширение групп;
d) построенная операция вводит на множестве абелевых расширений, индуцирующих данное действие, структуру абелевой группы, совпадающую со структурой группы $H^2(G,N)$.
10. Пусть G, N — группы и $\bar{A} : G \to \operatorname{Out}(N)$ — гомоморфизм. Выберем его теоретико-множественное поднятие $\tilde{A} : G \to \operatorname{Aut}(N)$. Докажите, что
a) найдется отображение $\xi : G \times G \to N$, такое что $\tilde{A}(g_1) \circ \tilde{A}(g_2) = \operatorname{Ad}_{\xi(g_1,g_2)} \circ \tilde{A}(g_1g_2)$;
b) $\operatorname{Ad}_{\xi(g_1,g_2)} \circ \operatorname{Ad}_{\xi(g_1g_2,g_3)} = \operatorname{Ad}_{\tilde{A}(g_1)\xi(g_2,g_3)} \circ \operatorname{Ad}_{\xi(g_1,g_2g_3)}$;
c) найдется отображение $\zeta : G \times G \times G \to Z(N)$, т.ч. $\zeta(g_1,g_2,g_3)\xi(g_1,g_2)\xi(g_1g_2,g_3) = (\tilde{A}(g_1)\xi(g_2,g_3))\xi(g_1,g_2g_3)$;
d) ζ — 3-коцикл группы G со значениями в $Z(N)$;
e) $\bar{\zeta} \in H^3(G,Z(N))$ не зависит от выборов $\tilde{A}$, ξ и ζ;
f) если $\bar{\zeta} = 0$, то ξ можно выбрать так, что $\xi(g_1,g_2)\xi(g_1g_2,g_3) = (\tilde{A}(g_1)\xi(g_2,g_3))\xi(g_1,g_2g_3)$;
g) два таких выбора различаются на 2-коцикл группы G со значениями в $Z(N)$;
h) всякому такому ξ можно сопоставить расширение G с помощью N;
i) если $\bar{\zeta} = 0$, то множество расширений G с помощью N, таких что $\overline{\mathrm{Ad}} = \bar{A}$, изоморфно $H^2(G,Z(N))$, а если $\bar{\zeta} \neq 0$, то оно пусто.

29 сентября 2003 г.

1. Докажите, что
a) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$, если $\mathfrak{a} \supset \mathfrak{b}$ или $\mathfrak{a} \supset \mathfrak{c}$ (модулярность);
b) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{ab}$;
c) $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, если $\mathfrak{a} + \mathfrak{b} = A$.
2. Докажите, что если $\mathfrak{a}_i + \mathfrak{a}_j = A$ для всех $1 \leqslant i < j \leqslant n$, то $A/\bigcap_{i=1}^n \mathfrak{a}_i \cong \prod_{i=1}^n (A/\mathfrak{a}_i)$.
3. Докажите, что
a) если $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ — простые и $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, то $\mathfrak{a} \subset \mathfrak{p}_i$ для некоторого i;
b) если $\mathfrak{p}$ — простой и $\bigcap_{i=1}^n \mathfrak{a}_i \subset \mathfrak{p}$, то $\mathfrak{a}_i \subset \mathfrak{p}$ для некоторого i;
c) если $\mathfrak{p}$ — простой и $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$, то $\mathfrak{a}_i = \mathfrak{p}$ для некоторого i.
4. Частным идеалов $\mathfrak{a}$ и $\mathfrak{b}$ называется идеал $(\mathfrak{a} : \mathfrak{b}) = \{\, x \in A \mid x\mathfrak{b} \subset \mathfrak{a} \,\}$. Докажите, что
a) $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$; b) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$; c) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{bc}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$;
d) $(\bigcap \mathfrak{a}_i : \mathfrak{b}) = \bigcap (\mathfrak{a}_i : \mathfrak{b})$; e) $(\mathfrak{a} : \sum \mathfrak{b}_i) = \bigcap (\mathfrak{a} : \mathfrak{b}_i)$.
5. Докажите, что
a) $\mathfrak{r}(\mathfrak{ab}) = \mathfrak{r}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{r}(\mathfrak{a}) \cap \mathfrak{r}(\mathfrak{b})$; b) $\mathfrak{r}(\mathfrak{a}) = A \iff \mathfrak{a} = A$;
c) $\mathfrak{r}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{r}(\mathfrak{r}(\mathfrak{a}) + \mathfrak{r}(\mathfrak{b}))$; d) $\mathfrak{r}(\mathfrak{p}^n) = \mathfrak{p}$.
6. Аннулятором идеала $\mathfrak{a}$ называется идеал $\operatorname{Ann}(\mathfrak{a}) := (0 : \mathfrak{a}) = \{\, x \in A \mid x\mathfrak{a} = 0 \,\}$. Докажите, что множество делителей нуля совпадает с множеством a) $\bigcup_{x \neq 0} \operatorname{Ann}((x))$; b) $\bigcup_{x \neq 0} \mathfrak{r}(\operatorname{Ann}((x)))$.
7. Вычислите в кольце $\mathbb{Z}$ сумму, произведение, пересечение, частное и радикал идеалов.
8. Докажите, что множество простых идеалов имеет минимальные по включению элементы.
9. Радикалом Джекобсона $\mathfrak{R}$ кольца A называется пересечение всех максимальных идеалов в A. Докажите, что a) $x \in \mathfrak{R} \iff 1 - xy$ обратим при всех $y \in A$; b) $\mathfrak{N} \subset \mathfrak{R}$.
10. Пусть X — аффинное алгебраическое многообразие. Докажите, что
a) на X существует единственная топология на X, в которой замкнутыми подмножествами являются подмногообразия (топология Зарисского);
b) X — неприводимо $\iff$ всякое непустое открытое подмножество в X всюду плотно;
c) замыкание неприводимого множества неприводимо.
11. Спектром кольца A называется топологическое пространство $\operatorname{Spec} A$, точки которого — это простые идеалы в A, а замкнутые подмножества — подмножества вида $V(\mathfrak{a}) = \{\, \mathfrak{p} \subset A \mid \mathfrak{a} \subset \mathfrak{p} \,\}$.
a) Нарисуйте $\operatorname{Spec}\mathbb{Z}$, $\operatorname{Spec}\mathbb{R}$, $\operatorname{Spec}\mathbb{C}[x]$, $\operatorname{Spec}\mathbb{Z}[x]$.
Пусть $\mathfrak{p}_x$— простой идеал в A, соответствующий точке $x \in \operatorname{Spec} A$. Докажите, что
b) точка $x \in \operatorname{Spec} A$ замкнута $\iff$ идеал $\mathfrak{p}_x$ максимален;
c) $\{\, \bar{x} \,\} = V(\mathfrak{p}_x)$;
d) $y \in \{\, \bar{x} \,\} \iff \mathfrak{p}_x \subset \mathfrak{p}_y$.
12. Докажите, что
a) множества $U_f = \operatorname{Spec} A \setminus V((f))$ образуют базис открытых множеств в топологии Зарисского;
b) $U_f \cap U_g = U_{fg}$;
c) $U_f = \emptyset \iff f$ — нильпотент;
d) $U_f = \operatorname{Spec} A \iff f$ обратим;
e) $U_f = U_g \iff \mathfrak{r}((f)) = \mathfrak{r}((g))$.
13. Пусть $\phi : A \to B$ — гомоморфизм колец. Пусть $\phi^* : \operatorname{Spec} B \to \operatorname{Spec} A$, $\mathfrak{q} \mapsto \phi^{-1}(\mathfrak{q})$. Докажите, что
a) $\phi^{*-1}(U_f) = U_{\phi(f)}$;
b) ϕ^* — непрерывно;
c) если ϕ сюръективен, то $\phi^* : \operatorname{Spec} B \to V(\operatorname{Ker}\phi) \subset \operatorname{Spec} A$ — гомеоморфизм;
d) $\operatorname{Spec} A \cong \operatorname{Spec}(A/\mathfrak{N})$;
e) если ϕ инъективен, то $\phi^*(\operatorname{Spec} B)$ плотно в $\operatorname{Spec} A$;
f) $A \mapsto \operatorname{Spec} A$, $\phi \mapsto \phi^*$ — контравариантный функтор $\mathcal{C}omm \to \mathcal{T}op$.
14. Докажите, что a) $\operatorname{Spec}(A \times B) = \operatorname{Spec} A \bigsqcup \operatorname{Spec} B$; b) $\operatorname{Spec}(A \otimes_{\mathsf{k}} B) = \operatorname{Spec} A \times \operatorname{Spec} B$.

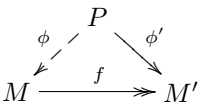
06 октября 2003 г.

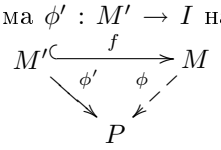
1. Пусть Σ — частично упорядоченное множество. Докажите эквивалентность условий (i) всякая возрастающая цепочка стабилизируется; (ii) любое непустое подмножество в Σ содержит максимальный элемент.
2. Модуль M над кольцом A называется артиновым, если всякая убывающая цепочка подмодулей в M стабилизируется. Проверьте, являются ли следующие $\mathbb{Z}$-модули нетеровыми и артиновыми:
a) конечная абелева группа; b) $\mathbb{Z}$; c) $\mathbb{Q}/\mathbb{Z}$; d) $\{\, m/p^n \in \mathbb{Q} \,\} \subset \mathbb{Q}$.

3. Докажите, что a) если $0 \to M' \to M \to M'' \to 0$ — точная тройка, то M артинов $\iff$ M' и M'' артиновы; b) если M_i — артиновы A-модули, то $\oplus_{i=1}^n M_i$ — артинов.
4. Кольцо A называется артиновым, если A является артиновым A-модулем. Проверьте, являются ли следующие кольца нетеровыми и артиновыми: a) k; b) $\mathbb{Z}/n\mathbb{Z}$; c) $\mathbb{Z}$; d) $\mathsf{k}[x]/f(x)\mathsf{k}[x]$; e) $\mathsf{k}[x_1, \dots, x_n]$; f) $\mathsf{k}[x_1, \dots, x_n, \dots]$.
5. Докажите, что a) прямое произведение нетеровых колец нетерово; b) прямое произведение артиновых колец артиново. c) факторкольцо артинова кольца артиново; d) кольцо $\mathsf{k}[x_1, \dots, x_n]/(x_1^{k_1} \cdots x_n^{k_n})_{k_1+\dots+k_n=m}$ артиново; e) если $X \subset \mathbb{A}^n$ — конечный набор точек и $I_X^m \subset I \subset I_X$, то $\mathsf{k}[x_1, \dots, x_n]/I$ — артиново кольцо.
6. Докажите, что конечно порожденный модуль над артиновым кольцом артинов.
7. Ненулевой модуль M называется простым, если у него нет нетривиальных подмодулей. Модуль M называется модулем конечной длины, если существует цепочка $0 = M_0 \subset M_1 \subset \dots \subset M_n = M$, в которой все факторы M_i/M_{i-1} просты. Такая цепочка называется композиционным рядом модуля M. Докажите, что
a) $0 = M_0 \subset M_1 \cdots \subset M_n = M$ — к.р. и $N \subset M$, то $0 = N \cap M_0 \subset N \cap M_1 \cdots \subset N \cap M_n = N$ — к.р.;
b) если $\ell(M)$ — длина минимального к.р. M, то $N \subset M \Longrightarrow \ell(N) \leqslant \ell(M)$, причем $\ell(N) = \ell(M) \Longrightarrow N = M$;
c) всякая цепочка подмодулей в M без повторений имеет длину не больше $\ell(M)$;
d) длины всех к.р. модуля M равны;
e) последовательности фактормодулей в двух к.р. модуля M совпадают.
8. Докажите, что a) M — модуль конечной длины $\iff$ M артинов и нетеров;
b) если $0 \to M' \to M \to M'' \to 0$ — точная тройка, то M — модуль конечной длины $\iff$ M' и M'' — модули конечной длины, причем $\ell(M) = \ell(M') + \ell(M'')$;
c) если M_i — модули конечной длины, то $\oplus_{i=1}^n M_i$ — модуль конечной длины, причем $\ell(\oplus_{i=1}^n M_i) = \sum_{i=1}^n \ell(M_i)$.
9. Докажите, что a) если M — простой $\mathbb{C}[x]$-модуль, то $M \cong \mathbb{C}[x]/(x-\lambda)\mathbb{C}[x]$; b) если M — $\mathbb{C}[x]$-модуль конечной длины, то $M \cong \mathbb{C}[x]/f(x)\mathbb{C}[x]$; c) категория $\mathbb{C}[x]$-модулей конечной длины эквивалентна категории конечномерных векторных пространств с эндоморфизмом; d) категория $\mathbb{C}[x, y]$-модулей конечной длины эквивалентна категории конечномерных векторных пространств с парой коммутирующих эндоморфизмов.
10. Пусть M — A-модуль, а $u : M \to M$ — эндоморфизм. Докажите, что
a) если M нетеров, а u сюръективен, то u — изоморфизм (рассмотрите цепочку подмодулей $\operatorname{Ker} u^n$);
b) если M артинов, а u инъективен, то u — изоморфизм (рассмотрите цепочку подмодулей $\operatorname{Im} u^n$).
11. Докажите, что если A — нетерово кольцо, то кольцо $A[[x]]$ тоже нетерово.
12. Пусть A — артиново кольцо. Докажите, что
a) если A целостное, то A поле (рассмотрите цепочку идеалов (x^n));
b) всякий простой идеал в A максимален;
c) $\mathfrak{N}_A = \mathfrak{R}_A$;
d) множество максимальных идеалов в A конечно;
e*) существует целое число n, такое что $\mathfrak{N}_A^n = 0$;
f*) кольцо A нетерово.
g*) кольцо A имеет вид кольца из задачи 5e.
(Иначе говоря, артиновы кольца соответствуют нульмерным многообразиям.)

13 октября 2003 г.

1. A-модуль P называется проективным, если для всякого эпиморфизма $f : M \to M'$ и всякого морфизма $\phi' : P \to M'$ найдется морфизм $\phi : P \to M$, такой что $\phi' = f \circ \phi$. A-модуль I называется инъективным, если для всякого мономорфизма $f : M' \to M$ и всякого морфизма $\phi' : M' \to I$ найдется морфизм $\phi : M \to I$, такой что $\phi' = \phi \circ f$.





Докажите, что a) функтор $\operatorname{Hom}_A(P, -)$ точен $\iff$ P — проективный A-модуль;
b) функтор $\operatorname{Hom}_A(-, I)$ точен $\iff$ I — инъективный A-модуль.
2. Докажите, что a) P проективен $\iff$ любая точная тройка $0 \to M \to N \to P \to 0$ расщепляется;
b) модуль P проективен $\iff$ найдется P', так что $P \oplus P'$ свободен;
c) функтор $\operatorname{Ext}(M, -)$ можно вычислять с помощью проективной резольвенты модуля M.
3. Пусть A — коммутативная k-алгебра. Пусть $M^\vee := \operatorname{Hom}_{\mathsf{k}}(M, \mathsf{k})$. Докажите, что
a) $M^\vee$ обладает естественной структурой A-модуля;
b) отображение $M \to M^{\vee\vee}$ — мономорфизм A-модулей;
c) $\operatorname{Hom}_A(M, N) \cong M^\vee \otimes_A N$;

d) если A — k-алгебра, а P — проективный A-модуль, то модуль $P^\vee$ инъективен;
e) всякий A-модуль вкладывается в инъективный A-модуль;
f) всякий A-модуль имеет правую инъективную резольвенту;
g) I инъективен $\iff$ любая точная тройка $0 \to I \to M \to N \to 0$ расщепляется;
h) функтор $\mathrm{Ext}(-, N)$ можно вычислять с помощью инъективной резольвенты модуля N.

4. (Цилиндр морфизма.) Пусть $f : K^\bullet \to L^\bullet$ — морфизм комплексов. Докажите, что
a) $\mathrm{Cyl}(f)^i = L^i \oplus K^i \oplus K^{i+1}$, $d^i_{\mathrm{Cyl}(f)}(l^i, k^i, k^{i+1}) = (d^i_L(l_i) + f^{i+1}(k^{i+1}), d^i_K(k^i) - k^{i+1}, -d^{i+1}_K(k^{i+1}))$ — комплекс;
b) отображение $\bar f : K^\bullet \to \mathrm{Cyl}(f)^i$, $k^i \mapsto (0, k^i, 0)$ — морфизм комплексов;
c) отображение $\alpha : L^\bullet \to \mathrm{Cyl}(f)^\bullet$, $l^i \mapsto (l^i, 0, 0)$ — морфизм комплексов;
d) отображение $\beta : \mathrm{Cyl}(f)^\bullet \to L^\bullet$, $(l^i, k^i, k^{i+1}) \mapsto l^i + f(k^i)$ — морфизм комплексов;
e) $\beta \circ \alpha = \mathrm{Id}_{L^\bullet}$;
f) $\alpha \circ \beta \sim \mathrm{Id}_{\mathrm{Cyl}(f)^\bullet}$, где $h^i(l^i, k^i, k^{i+1}) = (0, 0, k^i)$;
g) морфизмы α и β индуцируют изоморфизм когомологий;
h) $\beta \circ \bar f = f$.

5. (Конус морфизма.) Пусть $f : K^\bullet \to L^\bullet$ — морфизм комплексов. Докажите, что
a) $\mathrm{C}(f)^i = L^i \oplus K^{i+1}$, $d^i_{\mathrm{C}(f)}(l^i, k^{i+1}) = (d^i_L(l_i) + f^{i+1}(k^{i+1}), -d^{i+1}_K(k^{i+1}))$ — комплекс;
b) отображение $\pi f : \mathrm{Cyl}(f)^\bullet \to \mathrm{C}(f)^i$, $(l^i, k^i, k^{i+1}) \mapsto (l^i, k^{i+1})$ — морфизм комплексов;
c) отображение $\bar\pi : L^\bullet \to \mathrm{C}(f)^\bullet$, $l^i \mapsto (l^i, 0)$ — морфизм комплексов;
d) отображение $\delta : \mathrm{C}(f)^\bullet \to K^{\bullet+1}$, $(l^i, k^{i+1}) \mapsto k^{i+1}$ — морфизм комплексов;
e) $0 \to K^\bullet \xrightarrow{\bar f} \mathrm{Cyl}(f)^\bullet \xrightarrow{\pi} \mathrm{C}(f)^\bullet \to 0$ — точная последовательность комплексов;
f) $0 \to L^\bullet \xrightarrow{\bar\pi} \mathrm{C}(f)^\bullet \xrightarrow{\delta} K^{\bullet+1} \to 0$ — точная последовательность комплексов;
g) $\pi \circ \alpha = \bar\pi$.

6. Пусть $0 \to K^\bullet \xrightarrow{f} L^\bullet \xrightarrow{g} M^\bullet \to 0$ — точная тройка комплексов. Докажите, что
a) отображение $\gamma : \mathrm{C}(f)^\bullet \to M^\bullet$, $(l^i, k^{i+1}) \mapsto g(l^i)$ — морфизм комплексов;
b) $\gamma \circ \pi = g \circ \beta$;
c) $\mathrm{Ker}\,\gamma = \mathrm{Cyl}(0)$;
d) γ индуцируют изоморфизм когомологий;
e) δ индуцирует связывающий гомоморфизм в точной последовательности когомологий исходного комплекса.

7. Пусть $0 \to N \xrightarrow{i_1} E_1 \xrightarrow{\pi_1} M \to 0$ и $0 \to N \xrightarrow{i_2} E_2 \xrightarrow{\pi_2} M \to 0$ — расширения A-модулей. Докажите, что
a) расслоенное произведение $E_1 \times_M E_2 := \{\, (x_1, x_2) \mid \pi_1(x_1) = \pi_2(x_2) \,\}$ является подмодулем в $E_1 \oplus E_2$;
b) отображение $i : N \to E_1 \times_M E_2$, $n \mapsto (i_1(n), -i_2(n))$ — мономорфизм A-модулей;
c) последовательность $0 \to N \xrightarrow{i_1} (E_1 \times_M E_2)/i(N) \xrightarrow{\pi_1} M \to 0$ — расширение A-модулей;
d) построенная операция вводит на множестве классов эквивалентности расширений A-модулей структуру абелевой группы, совпадающую со структурой группы $\mathrm{Ext}^1_A(M, N)$.

8. Пусть $P_\bullet \to L$, $Q_\bullet \to M$ — проективные резольвенты. Докажите, что
a) если $f : P_s \to M$ представляет элемент $\mathrm{Ext}^s(L, M)$, то существует $f_\bullet : P_{s+\bullet} \to Q_\bullet$, такой что $f = d^Q_0 \circ f_0$;
b) если $g : Q_T \to N$ представляет элемент $\mathrm{Ext}^t(M, N)$, то $g \circ f_t : P_{s+t} \to N$ представляет элемент $\mathrm{Ext}^{s+t}(L, N)$;
c) построенное отображение $\mu_{s,t} : \mathrm{Ext}^s(L, M) \times \mathrm{Ext}^t(M, N) \to \mathrm{Ext}^{s+t}(L, N)$ корректно определено;
d) построенное отображение $\mu_{s,t} : \mathrm{Ext}^s(L, M) \times \mathrm{Ext}^t(M, N) \to \mathrm{Ext}^{s+t}(L, N)$ A-билинейно;
e) $\mu_{0,0} : \mathrm{Hom}(L, M) \otimes \mathrm{Hom}(M, N) \to \mathrm{Hom}(L, N)$ совпадает с отображением композиции;
f) $(\mathrm{Ext}^\bullet(M, M), \mu)$— градуированная A-алгебра.

9. (Расширения по Ионеда.) Расширением длины k A-модуля M с помощью A-модуля N называется точная последовательность A-модулей вида $0 \to N \xrightarrow{i} E_k \xrightarrow{f_k} \dots \xrightarrow{f_2} E_1 \xrightarrow{\pi} M \to 0$. Докажите, что
a) всякому расширению длины k соответствует элемент в $\mathrm{Ext}^k(M, N)$;
b) при замене $E'_i = E_i \oplus E$, $E'_{i+1} = E_{i+1} \oplus E$, $f'_{i+1} = f_{i+1} \oplus \mathrm{Id}_E$, где $1 \leqslant i \leqslant k-1$, класс расширения не меняется;
c) классы изоморфных расширений равны;
d) классы расширений равны $\iff$ они соединяются цепочкой замен вида (b) и обратных к ним;
e) всякий элемент из $\mathrm{Ext}^k(M, N)$ представляется расширением длины k;
f) если $0 \to M \xrightarrow{j} F_l \xrightarrow{g_l} \dots \xrightarrow{g_2} F_1 \xrightarrow{\rho} L \to 0$ — другое расширение, то их произведением является расширение $0 \to N \xrightarrow{i} E_k \xrightarrow{f_k} \dots \xrightarrow{f_2} E_1 \xrightarrow{j\circ\pi} F_l \xrightarrow{g_l} \dots \xrightarrow{g_2} F_1 \xrightarrow{\rho} L \to 0$.

10. A-модуль N называется плоским, если функтор $- \otimes_A N$ точен. Докажите, что
a) N плоский $\iff$ для всякого вложения $M' \xrightarrow{f} M$ морфизм $f \otimes 1_N : M' \otimes_A N \to M \otimes_A N$ — вложение;
b) предыдущее условие достаточно проверять только для конечно порожденных A-модулей;

c) N плоский $\Longleftrightarrow$ для всякого идеала $\mathfrak{a} \subset A$ морфизм $\mathfrak{a} \otimes_A N \to A \otimes_A N = N$ — вложение;
d) всякий проективный модуль является плоским;
e) всякий модуль обладает левой плоской резольвентой.
11. Пусть $P_\bullet \to M \to 0$ — проективная резольвента. Определим $\operatorname{Tor}_i^A(M,N) = H_i(P_\bullet \otimes_A N)$. Докажите, что
a) группы $\operatorname{Tor}_i^A(M,N)$ определены однозначно с точностью до канонического изоморфизма;
b) $\operatorname{Tor}_i^A(M,N)$ является функтором как по первому, так и по второму аргументу;
c) $\operatorname{Tor}_i^A(M,N)$ коммутирует с прямыми суммами;
d) $\operatorname{Tor}_0^A(M,N) = M \otimes_A N$;
e) если N плоский, то $\operatorname{Tor}_i^A(M,N) = 0$ при $i > 0$;
f) всякой точной тройке $0 \to M' \to M \to M'' \to 0$ соответствуют функториальные точные последовательности

$$\cdots \to \operatorname{Tor}_1(M'',N) \xrightarrow{\delta} \operatorname{Tor}_1(M',N) \to \operatorname{Tor}_1(M,N) \to \operatorname{Tor}_1(M'',N) \xrightarrow{\delta} M' \otimes_A N \to M \otimes_A N \to M'' \otimes_A N \to 0$$

$$\cdots \to \operatorname{Tor}_1(N,M'') \xrightarrow{\delta} \operatorname{Tor}_1(N,M') \to \operatorname{Tor}_1(N,M) \to \operatorname{Tor}_1(N,M'') \xrightarrow{\delta} N \otimes_A M' \to N \otimes_A M \to N \otimes_A M'' \to 0$$

g) $\operatorname{Tor}_i^A(M,N) \cong \operatorname{Tor}_i^A(N,M)$ — канонический изоморфизм.
12. Докажите, что $H_i(G,M) = \operatorname{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z},M)$.
13. Вычислите Ext и Tor в категориях a) $\mathbb{Z}$-модулей; b) $\mathbb{C}[x]$-модулей.
14. Опишите все a) проективные; b) инъективные; c) плоские $\mathbb{Z}$-модули.
15. Докажите формулы универсальных коэффициентов:
a) $0 \to H_i(X,\mathbb{Z}) \otimes_{\mathbb{Z}} F \to H_i(X,F) \to \operatorname{Tor}_1^{\mathbb{Z}}(H_{i-1}(X,\mathbb{Z}),F) \to 0$;
b) $0 \to H^i(X,\mathbb{Z}) \otimes_{\mathbb{Z}} F \to H^i(X,F) \to \operatorname{Tor}_1^{\mathbb{Z}}(H^{i+1}(X,\mathbb{Z}),F) \to 0$;
c) $0 \to \operatorname{Ext}_{\mathbb{Z}}^1(H_{i-1}(X,\mathbb{Z}),F) \to H^i(X,F) \to H_i(X,\mathbb{Z})^* \to 0$;
d) $H^i(X,\mathsf{k}) = H_i(X,\mathsf{k})^*$.

20 октября 2003 г.

1. Докажите, что если $\mathsf{k} \subset K \subset L$ — башня полей, то $\operatorname{degtr} L/\mathsf{k} = \operatorname{degtr} L/K + \operatorname{degtr} K/\mathsf{k}$.
2. Докажите, что факториальное кольцо целозамкнуто.
3. Пусть $A \subset B$ — целое расширение колец. Докажите, что
a) $x \in A$ обратим в $B \Longrightarrow x$ обратим в A;
b) $\mathfrak{R}_A = \mathfrak{R}_B \cap A$.
4. Докажите, что если $B_1, \ldots, B_n$ целы над A, то $\prod_{i=1}^n B_i$ цело над A.
5. Пусть G конечная группа автоморфизмов кольца A и $A^G \subset A$ — подкольцо инвариантов. Докажите, что $A^G \subset A$ — целое расширение колец.
6. Пусть K — поле частных целозамкнутого кольца A, L/K — конечное расширение Галуа, а $B \subset L$ — целое замыкание A в L. Докажите, что
a) L является полем частных кольца B;
b) $A = B^{\operatorname{Gal}(L/K)}$.
7. Докажите лемму Нетера о нормализации для конечных полей.
8. Найдите целое замыкание кольца $\mathbb{Z}$ в поле a) $\mathbb{Q}(\sqrt{2})$; b) $\mathbb{Q}(\sqrt{5})$.
9. Существует ли подполе в $\mathbb{C}$ изоморфное $\mathbb{R}$, но отличное от $\mathbb{R}$?
10. Пусть $f : X \to Y$ — сюръективный морфизм, такой что расширение координатных алгебр $A_Y \to A_X$ — целое. Докажите, что f — замкнутое отображение.
11. Приведите пример многообразия X и конечного взаимно однозначного морфизма $f : X \to X$, не являющегося изоморфизмом.

27 октября 2003 г.

1. Найдите фактормногообразия
a) $\mathbb{A}^1/\!/\mu_n$; b) $\mathbb{A}^2/\!/\mu_2$, $(x,y) \longmapsto (-x,-y)$; c) $\mathbb{A}^4/\!/\mathfrak{S}_2$, $(x_1,x_2,y_1,y_2) \longmapsto (x_2,x_1,y_2,y_1)$.
2. Категорным фактором многообразия X по действию группы G называется универсальный отталкивающий объект в категории пар (Y,f), где Y — многообразие, $f : X \to Y$ — морфизм многообразий, такой что $f \circ g = f$для всех $g \in G$, а $\operatorname{Hom}((Y,f),(Y'f')) = \{\, \phi : Y \to Y' \mid \phi \circ f = f' \,\}$. Докажите, что для любой группы G, если алгебра инвариантов A_X^G конечно порождена, то категорный фактор Y существует и $A_Y = A_X^G$.
3. Найдите категорный фактор
a) $\mathbb{A}^n/\!/\mathsf{k}^*$, где $z(x_1,\ldots,x_n) = (zx_1,\ldots,zx_n)$;
b) $\mathbb{A}^2/\!/\mathsf{k}^*$, где $z(x,y) = (z^a x, z^b y)$, $a,b \in \mathbb{Z}$.

4. Докажите, что элементарные симметрические многочлены порождают $\mathbb{Z}[x_1,\dots,x_n]^{\mathfrak{S}_n}$ над $\mathbb{Z}$.
5. Докажите, что симметрические многочлены Ньютона $t_k = x_1^k + \dots + x_n^k$
a) алгебраически независимы и порождают $\mathsf{k}[x_1,\dots,x_n]^{\mathfrak{S}_n}$ над k, если $\operatorname{char}\mathsf{k} > n$;
b) не порождают $\mathbb{Z}[x_1,\dots,x_n]^{\mathfrak{S}_n}$ над $\mathbb{Z}$.
6. Многочлен $f(x_1,\dots,x_n)$ называется кососимметрическим, если $f(x_{\sigma(1)},\dots,x_{\sigma(n)}) = \varepsilon(\sigma)f(x_1,\dots,x_n)$ для всех перестановок $\sigma \in \mathfrak{S}_n$. Докажите, что
a) кососимметрические многочлены являются модулем над $\mathsf{k}[x_1,\dots,x_n]^{\mathfrak{S}_n}$;
b) это свободный модуль ранга 1 с образующей $\delta(x_1,\dots,x_n) = \prod_{i<j}(x_i - x_j)$.
7. Пусть $f(x) = a_0\prod_{i=1}^n(x-\alpha_i)$. Докажите, что
a) результант $R(f,f')$ делится на $\delta(\alpha_1,\dots,\alpha_n)$;
b) частное $R(f,f')/\delta(\alpha_1,\dots,\alpha_n)$ является кососимметрическим многочленом от $\alpha_1,\dots,\alpha_n$;
c) $R(f,f')$ делится на $\delta(\alpha_1,\dots,\alpha_n)^2$;
d) $R(f,f') = (-1)^{\frac{n(n-1)}{2}}a_0D(f)$.

03 ноября 2003 г.

1. Пусть D — тело. Введем новое умножение на D формулой $x \star y = y \cdot x$. Докажите, что $(D,+,\star)$ — тело (оно обозначается D^{op}).
2. Пусть D — тело и L — одномерный левый D-модуль. Докажите, что $\operatorname{End}_D(L) = D^{\mathrm{op}}$, $\operatorname{End}_{D^{\mathrm{op}}}(L) = D$.
3. Докажите теорему Жордана–Гельдера для модулей над некоммутативными кольцами.
4. Докажите, что если M — прямая сумма конечного числа простых модулей, то количество простых слагаемых, изоморфных данному простому модулю не зависит от выбора разложения.
5. Пусть M — полупростой A-модуль, $B = \operatorname{End}_A(M)$, $f \in \operatorname{End}_B(M)$. Докажите, что для любого $x \in M$
a) существует проектор $\pi : M \to Ax$, коммутирующий с действием A;
b) $f(x) = \pi(f(x))$;
c) найдется $a \in A$, так что $f(x) = ax$;
d) для любых $x_1,\dots,x_n \in M$ найдется $a \in A$, так что $f(x_i) = ax_i$ (Указание: рассмотрите $f^{\oplus n} \in \operatorname{End}_B(M^{\oplus n})$).
6. Докажите, что если $A \subset \operatorname{Mat}_{n\times n}(\mathsf{k})$ — подалгебра, такая что k^n — простой A-модуль, и k — алгебраически замкнуто, то $A = \operatorname{Mat}_{n\times n}(\mathsf{k})$.
7. Докажите, что над полупростым кольцом существует только конечное множество классов изоморфизма простых модулей.
8. Докажите, что артинова алгебра с нулевым радикалом Джекобсона полупроста.
9. Докажите, что конечномерная коммутативная алгебра без нильпотентов полупроста.

10 ноября 2003 г.

1. Пусть алгебра A конечномерна. Докажите, что
a) $x \in \mathfrak{R}_A \iff x$ действует нулем во всех простых левых A-модулях;
b) $x \in \mathfrak{R}_A \iff x$ действует нулем во всех простых правых A-модулях;
c) $\mathfrak{R}_A$ равен пересечению всех правых максимальных идеалов.
2. Пусть K'/K — алгебраическое расширение полей. Докажите, что $K' \otimes_K L$ — полупростая алгебра для всех $L \iff$ расширение K'/K сепарабельно.
3. Пусть D — тело над K, а B — K-алгебра. Докажите, что
a) двусторонние идеалы в алгебре $D \otimes_K B$ порождаются двусторонними идеалами в алгебре $Z(D) \otimes_K B$;
b) если $Z(D) = K$, а B — простая, то $D \otimes_K B$ — простая.
4. Докажите, что тензорное произведение центральных простых алгебр над полем K является центральной простой алгеброй над полем K.
5. Докажите, что $A^{\mathrm{op}} \otimes_K A$ — матричная алгебра над полем K.
6. Докажите, что
a) множество классов подобия центральных простых алгебр над полем K с операцией $\otimes$ образуют группу;
b) эта группа изоморфна группе Брауэра поля K.
7. Вычислите группу Брауэра поля a) $\mathbb{R}$; b) $\mathbb{F}_q$.
8. Найдите все центральные тела над полем a) $\mathbb{R}$; b) $\mathbb{F}_q$.
9. Докажите, что a) $H^0(\mathrm{Gal}(L/K), L^*) = K^*$; b) $H^1(\mathrm{Gal}(L/K), L^*) = 0$ (теорема Гильберта-90).