

# Алгебра. Неофициальный конспект

Лектор: Николай Александрович Вавилов

Конспектировал Леонид Данилевич

II семестр, весна 2023 г.

# Оглавление

<b>1</b>	<b>Вычислительная линейная алгебра</b>	<b>4</b>
1.1	Элементарные преобразования . . . . .	4
1.1.1	Элементарные трансвекции . . . . .	4
1.1.2	Элементарные псевдоотражения . . . . .	5
1.1.3	Действия элементарных преобразований на матрицах . . . . .	6
1.2	Матрицы перестановки . . . . .	7
1.3	Классификация линейных отображений над полем. Канонический вид линейного отображения . . . . .	8
1.4	Комбинаторная эквивалентность матриц . . . . .	9
1.4.1	Элементарная эквивалентность матриц . . . . .	10
1.4.2	Ранг матрицы над полем. Различные определения ранга над кольцом . . . . .	11
1.4.3	Системы линейных уравнений . . . . .	12
1.4.4	Векторная запись системы линейных уравнений. Теорема Кронекера — Капелли . . . . .	13
1.4.5	Решение систем линейных уравнений методом Гаусса . . . . .	13
1.4.6	Определитель по Вейерштрассу . . . . .	14
1.4.7	Знак перестановки. Определение через декремент . . . . .	14
1.4.8	Знак перестановки. Определение через инверсии . . . . .	15
1.4.9	Знакопеременное определение определителя . . . . .	16
1.4.10	Существование определителя (удовлетворяющего условиям Вейерштрасса) . . . . .	16
1.4.11	Единственность определителя (удовлетворяющего условиям Вейерштрасса) . . . . .	17
1.5	Мультипликативность определителя . . . . .	17
1.5.1	Блочные матрицы . . . . .	18
1.5.2	Определитель блочно треугольной матрицы . . . . .	18
1.5.3	Мультипликативность определителя . . . . .	19
1.5.4	Миноры, разложение по строке, определитель по Лапласу . . . . .	19
1.5.5	Формула Крамера, теорема Крамера . . . . .	20
1.6	Определители некоторых матриц . . . . .	20
1.6.1	Определитель Вандермонда . . . . .	21
1.6.2	Пфаффианы . . . . .	21
<b>2</b>	<b>Многочлены</b>	<b>22</b>
2.1	Гомоморфизм эвалюации . . . . .	22
2.2	Число корней многочлена над областью целостности . . . . .	23
2.3	Формальное и функциональное равенство многочленов . . . . .	24
2.4	Задача интерполяции с простыми узлами . . . . .	24
2.5	Локализация или кольца частных . . . . .	25
2.5.1	Мультипликативные системы . . . . .	25
2.5.2	Построение кольца частных . . . . .	26
2.5.3	Универсальное свойство кольца частных . . . . .	27
2.5.4	Кольцо частных в терминах элементов . . . . .	28
2.5.5	Примеры колец частных . . . . .	28
2.6	Поле частных факториального кольца . . . . .	28
2.7	Рациональные дроби . . . . .	29
2.8	Разложение на простейшие дроби . . . . .	30

2.9	Факториальность кольца многочленов . . . . .	31
2.9.1	Примитивные многочлены . . . . .	31
2.9.2	Теорема Гаусса . . . . .	32
2.10	Дифференцирование алгебр . . . . .	33
2.10.1	Операции над дифференцированиями . . . . .	34
2.10.2	Дифференцирование кольца многочленов, теорема Лейбница — Бернулли . . . . .	34
2.11	Алгебраические и трансцендентные элементы; минимальный многочлен . . . . .	35
2.11.1	Что можно сказать, если $A$ — область целостности? . . . . .	35
<b>3</b>	<b>Канонические формы линейных операторов</b>	<b>37</b>
3.1	Инвариантные подпространства . . . . .	37
3.2	Собственные подпространства. Собственные числа . . . . .	38
3.3	Характеристический многочлен оператора . . . . .	39
3.4	Геометрическая и алгебраическая кратности собственного числа . . . . .	39
3.5	Корневые векторы. Корневое подпространство . . . . .	40
3.6	Теорема Кэли — Гамильтона . . . . .	41
3.6.1	Алгебраическое доказательство . . . . .	41
3.6.2	Геометрическое доказательство . . . . .	42
3.7	Примарное разложение . . . . .	43
3.7.1	Минимальный многочлен вектора относительно оператора . . . . .	43
3.7.2	Ядро операторного многочлена . . . . .	43
3.7.3	Примарное разложение . . . . .	44
3.8	Теорема о жордановой форме . . . . .	44
3.8.1	Жорданов базис нильпотентного оператора . . . . .	45
3.9	Сепарабельные многочлены, совершенные поля . . . . .	46
3.10	Разложение Жордана — Шевалле . . . . .	47
3.11	Вещественные жордановы формы . . . . .	48
3.12	Циклические подпространства, фробениусовы клетки . . . . .	48
<b>4</b>	<b>Классификация модулей над PID</b>	<b>50</b>
4.1	Нормальная форма Смита . . . . .	50
4.1.1	Над евклидовым кольцом . . . . .	50
4.1.2	Над PID . . . . .	51
4.2	Подмодули кручения, модули без кручения . . . . .	52
4.3	Формулировка основных теорем о строении конечнопорождённых модулей над PID . . . . .	53
4.3.1	Вложение конечнопорождённых модулей без кручения в свободные модули . . . . .	53
4.4	Согласованный выбор базисов в свободном модуле и его подмодуле . . . . .	54
4.4.1	Частные случаи . . . . .	55
<b>5</b>	<b>Геометрия пространств со скалярным произведением</b>	<b>56</b>
5.1	Скалярные произведения . . . . .	56
5.1.1	«Классификация» билинейных скалярных произведений . . . . .	57
5.2	Матрица Грама скалярного произведения . . . . .	57
5.3	Скалярное произведение и двойственные пространства . . . . .	58
5.4	Классификация пространств со скалярным произведением . . . . .	59
5.5	Ортогональное дополнение . . . . .	60
5.5.1	Ортогональная прямая сумма . . . . .	61
5.5.2	Теорема об ортогональном дополнении . . . . .	61
5.5.3	Теорема Лагранжа о существовании ортогонального базиса в квадратичном пространстве . . . . .	63
5.6	Введение в теорию (Диксона — ) Витта. Классификация симплектических пространств . . . . .	63
5.6.1	Выделение гиперболических плоскостей . . . . .	63
5.6.2	Классификация симплектических пространств . . . . .	64
5.7	Квадратические пространства. Квадратичные формы . . . . .	64
5.7.1	Квадратичная форма в координатах . . . . .	65
5.8	Классификация квадратичных пространств . . . . .	65
5.8.1	Над квадратично замкнутым полем . . . . .	65

5.8.2	Над полем вещественных чисел (закон инерции Сильвестра)	66
5.9	Теория (Диксона — ) Витта	67
5.9.1	Ортогональные отражения	68
5.9.2	Доказательство теоремы Витта о продолжении для невырожденных подпространств	68
5.9.3	Доказательство теоремы Витта о продолжении для невырожденного пространства	69
5.10	Полуторалинейные скалярные произведения	70
5.10.1	Полулинейные отображения, инволюции	70
5.10.2	Полуторалинейные скалярные произведения	71
5.10.3	Вещественная и мнимая часть эрмитова скалярного произведения	72
<b>6</b>	<b>Теория групп</b>	<b>74</b>
6.1	Действия групп	74
6.1.1	Действия групп на множествах	74
6.1.2	Действие группы на себе. Теорема Кэли	75
6.1.3	Действие группы на однородных пространствах. Обобщённая теорема Кэли	76
6.2	Классификация $G$ -множеств	78
6.3	Конечные группы	79
6.3.1	Центр $p$ -группы, теоремы Коши	79
6.3.2	Теоремы Силова	80
6.4	Тождества с коммутаторами	82
6.5	Прямое произведение двух подгрупп	83
6.5.1	Прямое произведение нескольких подгрупп	84
6.5.2	Прямое произведение многих подгрупп	84
6.6	Полупрямое произведение	84
6.7	Группы порядка $pq$	85
6.8	Крохотный кусок комбинаторной теории групп	86
6.8.1	Свободные группы	86
6.8.2	Задание группы образующими соотношениями	89

# Глава 1

## Вычислительная линейная алгебра

### Лекция I

14 февраля 2023 г.

#### 1.1 Элементарные преобразования

Пусть  $R$  — ассоциативное кольцо с единицей. Займёмся изучением некоторых особенных видов (пока квадратных) матриц  $M(n, R)$ .

##### 1.1.1 Элементарные трансвекции

**Определение 1.1.1** (Элементарная трансвекция).  $t_{i,j}(\xi) = e + \xi \cdot e_{i,j}$  для  $i \neq j, \xi \in R$ . Иными словами, матрица вида

$$i \begin{pmatrix} & & j \\ 1 & & 0 \\ & \ddots & \xi \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

**Определение 1.1.2** (Элементарные преобразования первого типа, или трансвекции). Группа по умножению, порождённая элементарными трансвекциями.

В частности,  $t_{1,2}(\xi) = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$ ,  $t_{2,1}(\xi) = \begin{pmatrix} 1 & 0 \\ \xi & 1 \end{pmatrix}$ .

**Лемма 1.1.1** (Аддитивность трансвекций по  $\xi$ ).  $t_{i,j}(\xi) \cdot t_{i,j}(\zeta) = t_{i,j}(\xi + \zeta)$ . Иными словами,  $t_{i,j} : R \rightarrow GL(n, R)$  — гомоморфизм для любых  $1 \leq i \neq j \leq n$ .

*Доказательство.* Посчитаем  $t_{i,j}(\xi) \cdot t_{i,j}(\zeta)$ . Это можно сделать так:

$$(e + \xi e_{i,j})(e + \zeta e_{i,j}) = e + \xi e_{i,j} + \zeta e_{i,j} + \xi \zeta e_{i,j} e_{i,j}, \text{ последнее слагаемое } 0, \text{ так как } i \neq j.$$

а можно так:

$$\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \xi + \zeta \\ 0 & 1 \end{pmatrix}$$

Последняя выкладка работает и для матриц произвольного размера, так как в вычислении на самом деле используются лишь 2 различных индекса —  $i$  и  $j$ . При замене из на 1 и 2 ничего не поменяется, так как определение умножения не опирается на порядок строк или столбцов.

Такой трюк позволяет компактно записывать вычисления с большими матрицами, мало отличающимися от нейтральной  $e$ .  $\square$

**Следствие 1.1.1.**  $t_{i,j}(\xi)^{-1} = t_{i,j}(-\xi)$ , откуда  $t_{i,j}(\xi) \in GL(n, R) \stackrel{def}{=} M(n, R)^*$ .

**Лемма 1.1.2** (Коммутационная формула Шевалле). *Мультипликативный коммутатор двух трансвекций — часто трансвекция:*

$$[t_{i,j}(\xi), t_{h,k}(\zeta)] = \begin{cases} t_{i,k}(\xi\zeta), & i \neq k \wedge j = h \\ t_{h,j}(-\zeta\xi), & i = k \wedge j \neq h \\ e, & i \neq k \wedge j \neq h \\ \text{что-то}, & i = k \wedge j = h \end{cases}$$

(Мультипликативный коммутатор  $[x, y] \stackrel{def}{=} xyx^{-1}y^{-1}$ )

*Доказательство.* Можно тупо записать огромные формулы:

$$\begin{aligned} [t_{i,j}(\xi), t_{h,k}(\zeta)] &= t_{i,j}(\xi) \cdot t_{h,k}(\zeta) \cdot t_{i,j}(-\xi) \cdot t_{h,k}(-\zeta) = (e + \xi e_{i,j})(e + \zeta e_{h,k})(e - \xi e_{i,j})(e - \zeta e_{h,k}) = \\ &= \dots = e + \xi\zeta\delta_{j,h}e_{i,k} - \zeta\xi\delta_{k,i}e_{h,j} + \zeta\xi\zeta\delta_{k,i}\delta_{j,h}e_{h,k} - \xi\zeta\xi\delta_{j,h}\delta_{k,i}e_{i,j} + \xi\zeta\xi\zeta\delta_{j,h}\delta_{k,i}\delta_{j,h}e_{i,k} \end{aligned}$$

~~Какая боль это писать... И ведь никто не прочтает и не проверит...~~ Прошу прощения, был неправ.

Члены с коэффициентами вида  $\xi^2$  или  $\xi^2\zeta$ , то есть те, где есть квадрат чего-то, точно обнуляются, так как по определению трансвекции  $i \neq j, k \neq h$ . Имея записанное, проверить, что лемма говорит правду — легко.

(Ещё можно поумножать матрицы  $3 \times 3$  или  $4 \times 4$  — тут ещё разбор случаев, когда какие индексы совпадают. Кайф)  $\square$

## 1.1.2 Элементарные псевдоотражения

**Определение 1.1.3** (Элементарное псевдоотражение). Матрица вида  $d_i(\varepsilon) = e + (\varepsilon - 1)e_{i,i}$ , где  $i \neq j, \varepsilon \in R^*$ . Иными словами, матрица вида

$$d_i(\varepsilon) = \begin{pmatrix} 1 & & & 0 \\ & \varepsilon & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

**Определение 1.1.4** (Элементарные преобразования второго типа, или псевдоотражения). Группа по умножению, порождённая элементарными псевдоотражениями.

**Лемма 1.1.3** (Мультипликативность псевдоотражений по  $\varepsilon$ ).  $d_i(\varepsilon)d_i(\theta) = d_i(\varepsilon\theta)$ . Иными словами,  $d_i : R^* \rightarrow GL(n, R)$  — гомоморфизм для любого  $1 \leq i \leq n$ .

*Доказательство.* Здесь есть всего один индекс, умножим матрицы  $1 \times 1$ :  $(\varepsilon) \cdot (\theta) = (\varepsilon\theta)$ .  $\square$

**Следствие 1.1.2.**  $d_i(\varepsilon)^{-1} = d_i(\varepsilon^{-1})$ , откуда  $d_i(\varepsilon) \in GL(n, R)$ .

*Замечание.* Псевдоотражения — подгруппа обратимых элементов в диагональных матрицах

$$\text{diag}(a_1, \dots, a_n) \stackrel{def}{=} \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

Так как умножаются диагональные матрицы покомпонентно, то справедливость (лемма 1.1.3) очевидна ещё и с другой стороны.

**Лемма 1.1.4.**  $[d_i(\varepsilon), d_j(\theta)] = \begin{cases} d_i([\varepsilon, \theta]), & i = j \\ e, & i \neq j \end{cases}$  — в частности, псевдоотражения с разными индексами коммутируют, а с одинаковыми — коммутируют, если коммутируют параметры.

**Лемма 1.1.5.**  $d_i(\varepsilon)t_{j,k}(\xi)d_i(\varepsilon)^{-1} = \begin{cases} t_{j,k}(\varepsilon\xi), & i = j \\ t_{j,k}(\xi\varepsilon^{-1}), & i = k \\ t_{j,k}(\xi), & \text{иначе} \end{cases}$

*Доказательство.*

Если  $i = j = 1 \wedge k = 2$ , то

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon^{-1} & \xi \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \varepsilon\xi \\ 0 & 1 \end{pmatrix}$$

Если  $i = k = 1 \wedge j = 2$ , то

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ \xi & 1 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \varepsilon^{-1} & 0 \\ \xi\varepsilon^{-1} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \xi\varepsilon^{-1} & 1 \end{pmatrix}$$

Наконец, если  $i \neq j, k$ , то домножение на псевдоотражение справа домножит  $i$ -й столбец на  $\varepsilon^{-1}$ , слева —  $i$ -ю строчку на  $\varepsilon$ , так как единственный ненулевой элемент в них — 1 на пересечении, то  $t_{j,k}(\xi)$  останется прежней.  $\square$

### 1.1.3 Действия элементарных преобразований на матрицах

**Лемма 1.1.6.** Элементарная трансвекция действует на матрицу  $x$  слева следующим образом:

$$t_{h,k}(\xi) \cdot \begin{pmatrix} x_{1,*} \\ \vdots \\ x_{h,*} \\ \vdots \\ x_{n,*} \end{pmatrix} = \begin{pmatrix} x_{1,*} \\ \vdots \\ x_{h,*} + \xi x_{k,*} \\ \vdots \\ x_{n,*} \end{pmatrix}$$

**Лемма 1.1.7.** Элементарное псевдоотражение действует на матрицу  $x$  слева следующим образом:

$$d_h(\varepsilon) \cdot \begin{pmatrix} x_{1,*} \\ \vdots \\ x_{h,*} \\ \vdots \\ x_{n,*} \end{pmatrix} = \begin{pmatrix} x_{1,*} \\ \vdots \\ \varepsilon x_{h,*} \\ \vdots \\ x_{n,*} \end{pmatrix}$$

**Лемма 1.1.8.** Элементарная трансвекция действует на матрицу  $x$  справа следующим образом:

$$(x_{*,1} \quad \dots \quad x_{*,h} \quad \dots \quad x_{*,n}) \cdot t_{h,k}(\xi) = (x_{*,1} \quad \dots \quad x_{*,h} + x_{*,k}\xi \quad \dots \quad x_{*,n})$$

**Лемма 1.1.9.** Элементарное псевдоотражение действует на матрицу  $x$  справа следующим образом:

$$(x_{*,1} \quad \dots \quad x_{*,h} \quad \dots \quad x_{*,n}) \cdot d_h(\varepsilon) = (x_{*,1} \quad \dots \quad x_{*,h}\varepsilon \quad \dots \quad x_{*,n})$$

**Определение 1.1.5** (Элементарная подгруппа).  $E(n, R) \stackrel{\text{def}}{=} \langle t_{i,j}(\xi) | \xi \in R, 1 \leq i \neq j \leq n \rangle \leq GL(n, R)$  — подгруппа в группе обратимых матриц, состоящая из трансвекций.

Используя  $D(n, R)$  как подгруппу в  $GL(n, R)$ , состоящую из обратимых диагональных матриц, можно ввести определение:

**Определение 1.1.6** (Полная элементарная подгруппа).  $GE(n, R) \stackrel{\text{def}}{=} \langle E(n, R), D(n, R) \rangle \leq GL(n, R)$  — подгруппа в группе обратимых матриц, порождённая трансвекциями и псевдоотражениями.

**Факт 1.1.1.**  $GE(n, R) = E(n, R) \cdot D(n, R)$ .

*Доказательство.* Всякий элемент  $g \in GE(n, R)$  по определению представим в виде  $e_1 d_1 \dots e_m d_m$ , где  $e_i \in E(n, R), d_i \in D(n, R)$ . Согласно (лемма 1.1.5)  $d_i e_{i+1} d_i^{-1} \in E(n, R)$ , то есть можно постепенно перекидывать элементы из  $E(n, R)$  в начало произведения.  $\square$

## Лекция II

15 февраля 2023 г.

Положим за  $d_{i,j}(\varepsilon) \stackrel{\text{def}}{=} d_i(\varepsilon) d_j(\varepsilon^{-1})$ , где  $i \neq j, \varepsilon \in R^*$ .

**Теорема 1.1.1.**  $d_{i,j}(\varepsilon)$  является произведением 4 элементарных трансвекций.

*Доказательство.* Будем двигаться назад: чтобы получить  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  из  $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ , добавим

- первую строчку ко второй с коэффициентом  $\varepsilon^{-1}$ ,
- вторую строчку к первой с коэффициентом  $1 - \varepsilon$ ,
- первую строчку ко второй с коэффициентом  $-1$ ,
- вторую строчку к первой с коэффициентом  $1 - \varepsilon^{-1}$ .

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} \rightsquigarrow \begin{pmatrix} \varepsilon & 0 \\ 1 & \varepsilon^{-1} \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & \varepsilon^{-1} - 1 \\ 1 & \varepsilon^{-1} \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & \varepsilon^{-1} - 1 \\ 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Таким образом,  $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\varepsilon^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 + \varepsilon \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ +1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 + \varepsilon^{-1} \\ 0 & 1 \end{pmatrix}$ . (Как было правильно замечено, в формуле порядок матриц пришлось развернуть, и прибавления строчек заменить на вычитания. Поэтому знаки в матрицах противоположны заявленным) В общем случае  $d_{i,j}(\varepsilon) = t_{i,j}(-\varepsilon^{-1}) t_{j,i}(-1 + \varepsilon) t_{i,j}(1) t_{j,i}(-1 + \varepsilon^{-1})$ . Операции можно было совершать не над строками, а над столбцами: например, можно то же произведение транспозиций применить к  $e$  не слева, а справа.  $\square$

## 1.2 Матрицы перестановки

**Определение 1.2.1** (Мономиальная матрица  $x$ ). В каждой строке  $x$  и каждом столбце  $x$  единственный элемент, не равный 0 (причём он обратим).

Множество мономиальных матриц обозначают  $N(n, R)$ , и это подгруппа в  $GL(n, R)$ .

**Определение 1.2.2** (Матрица перестановки). Такая мономиальная матрица, что все её ненулевые элементы равны 1.

Множество всех матриц перестановки обозначают  $W_n$ , это тоже подгруппа  $GL(n, R)$ .

**Определение 1.2.3** (Означенная (signed) матрица перестановки). Такая мономиальная матрица, что все её ненулевые элементы равны  $\pm 1$ .

Матрица перестановки переставляет элементы базиса, изоморфны  $S_n$ , означенные матрицы перестановки переставляют означенный базис, изоморфны октаэдральной группе.

**Определение 1.2.4** (Октаэдральная группа). Положим  $X := \{-n, \dots, -1, 1, \dots, n\}$  ( $|X| = 2n$ ).

$$\text{Oct}_n \stackrel{\text{def}}{=} \{\pi \in S_X \mid \pi(-i) = -\pi(i)\} \leq S_X$$



Имеет место изоморфизм  $S_n \cong W_n$ ,  $\pi \mapsto (\pi)$ ,  $(\pi)_{i,j} = \delta_{i,\pi(j)}$ . Можно проверить, что  $(\pi)(\rho) = (\pi \cdot \rho)$ .

Так как перестановки порождаются транспозициями, то матрицы перестановки порождаются матрицами транспозиций  $w_{i,j} = e - e_{i,i} - e_{j,j} + e_{i,j} + e_{j,i}$ .

Так определённые  $w_{i,j}$  — элементарные преобразования третьего вида.

**Следствие 1.2.1.**  $W_n = \langle \{w_{i,j} | i+1 = j\} \rangle$ . Это абсолютный аналог утверждения, что симметрическая группа  $S_n$  порождена фундаментальными транспозициями.

**Лемма 1.2.1.** Умножение на  $w$  слева переставляет строки, справа — переставляет столбцы. В частности,  $w_{1,2} \cdot \begin{pmatrix} x_{1,*} \\ x_{2,*} \end{pmatrix} = \begin{pmatrix} x_{2,*} \\ x_{1,*} \end{pmatrix}$  и  $\begin{pmatrix} x_{*,1} & x_{*,2} \end{pmatrix} \cdot w_{1,2} = \begin{pmatrix} x_{2,*} & x_{1,*} \end{pmatrix}$

Преобразования третьего типа выражаются через преобразования первого и второго типа:

**Определение 1.2.5.**

$$w_{i,j}(\varepsilon) = t_{i,j}(\varepsilon)t_{j,i}(-\varepsilon^{-1})t_{i,j}(\varepsilon) \in E(n, R)$$

Проще говоря, матрица где все строчки и столбцы как у единичной матрицы  $e$  кроме тех, что с номерами  $i, j$ :

$$w_{i,j}(\varepsilon) \stackrel{def}{=} \begin{pmatrix} & i & & j \\ & 0 & & \varepsilon \\ j & -\varepsilon^{-1} & & 0 \end{pmatrix}$$

**Лемма 1.2.2.**  $w_{i,j} = w_{i,j}(1) \cdot d_i(-1) = d_j(-1)w_{i,j}(1) \in GE(n, R)$

### 1.3 Классификация линейных отображений над полем. Канонический вид линейного отображения

Модуль над полем (то есть векторное пространство) с точностью до изоморфизма определяется своей размерностью. А чем определяется (с точностью до изоморфизма, естественно) линейное отображение?

**Определение 1.3.1** (Изоморфность линейных отображений  $\phi : U \rightarrow V$  и  $\psi : W \rightarrow Z$ ). Существуют два изоморфизма  $U \cong W$  и  $V \cong Z$ , такие, что диаграмма коммутативна.

$$\begin{array}{ccc} U & \xrightarrow{\phi} & V \\ \cong \downarrow & & \downarrow \cong \\ W & \xrightarrow{\psi} & Z \end{array}$$

**Определение 1.3.2** (Ранг линейного отображения  $\phi$ ). Размерность образа:  $\text{rk}(\phi) \stackrel{def}{=} \dim(\text{Im}(\phi))$ .

**Теорема 1.3.1.**  $(U, V, \phi) \cong (W, Z, \psi) \iff \begin{cases} \dim(U) = \dim(W) \\ \dim(V) = \dim(Z) \\ \text{rk}(\phi) = \text{rk}(\psi) \end{cases}.$

*Доказательство.*

$\Rightarrow$ . Очевидно.

$\Leftarrow$ . Так как  $\phi, \psi : U \rightarrow V$  — линейные отображения, то можно считать, что они заданы, как домножения на матрицу. Получаем аналогичный вопрос: когда можно одну матрицу привести к другой при замене базиса в  $U$  и замене базиса в  $V$ , то есть при домножении на **обратимые** матрицы слева и справа?

**Теорема 1.3.2.** Для любого линейного отображения  $\phi : U \rightarrow V$  можно так выбрать базисы в  $U$  и в  $V$ , чтобы матрица отображения имела вид  $\left( \begin{array}{c|c} e & 0 \\ \hline 0 & 0 \end{array} \right)$  — *окаймлённая* единичная матрица (здесь  $e$  — квадратная единичная матрица,  $0$  — матрицы из нулей произвольного размера).

*Доказательство.* Обозначим  $n = \dim(U)$ ,  $m = \dim(V)$ .

- Выберем базис  $\text{Ker}(\phi)$ ;  $\dim(\text{Ker}(\phi)) = n - r$ . Обозначим этот базис  $u_{r+1}, \dots, u_n$ .
- Дополним до базиса  $U$ :  $u_1, \dots, u_r$  — относительный базис  $U/\text{Ker}(\phi)$ .
- Рассмотрим  $\phi(u_1), \dots, \phi(u_r)$  — базис  $\text{Im}(\phi)$ .
- Дополним этот базис до базиса  $V$ .

В данных базисах матрица линейного отображения — действительно окаймлённая матрица.

□

Таким образом, всякое линейное отображение имеет лишь 3 инварианта — параметры окаймлённой матрицы, а это и есть  $\text{rk}(\phi)$ ,  $\dim(U)$ ,  $\dim(V)$ .

□

## 1.4 Комбинаторная эквивалентность матриц

Пусть  $x \in M(m, n, K)$ , где  $K$  — поле (рассуждения также можно обобщить до случая тела).

К какому виду можно привести  $x$  элементарными преобразованиями над строками?

**Теорема 1.4.1.** Для любого  $x \in M(m, n, K)$ :  $\exists h \in GE(m, K)$ :  $hx$  имеет специальный (*строково-эшелонированный*) вид:

1. В каждой строке ведущий элемент (pivot) — первый ненулевой элемент — равен 1.
2. В каждой следующей строке ведущий элемент правее, чем в предыдущей.
3. Элементы над ведущими равны 0.
4. Последние строки состоят из нулей.

$$\left( \begin{array}{cccccc} 1 & * & 0 & * & 0 & * \\ & & 1 & * & 0 & * \\ & & & \ddots & & \vdots \\ & & & & 1 & * \\ \hline 0 & & \dots & & 0 & \\ & & \vdots & & & \\ 0 & & \dots & & 0 & \end{array} \right)$$

*Доказательство.* Рассмотрим наименьший номер ненулевого столбца  $j$ :  $a_{*,j} \neq 0$ . Перестановкой строк можно добиться того, что  $a_{1,j} \neq 0$ . Поделим строку  $a_{1,*}$  на  $a_{1,j}$ , теперь первая строчка соответствует строково-эшелонированному виду.

Вычитая эту строку из следующих с правильными коэффициентами получаем, что  $a_{*,j} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ .

Кроме того, надо занулить коэффициенты выше, буде такие найдутся (они будут в последующих шагах индукции). Таким образом, дальше (к следующим строкам матрицы) можно применить индукцию — она оборвётся либо когда закончатся строки, либо останутся только строки из нулей.

□

**Следствие 1.4.1** (Комбинаторная эквивалентность). *Всякую матрицу преобразованиями над строками и перестановкой столбцов можно привести к следующему виду (ступенчатый вид):*

$$\forall x \in M(m, n, K), \exists h \in GE(m, K), w \in W_n : h x w = \left( \begin{array}{c|c} e & * \\ \hline 0 & 0 \end{array} \right)$$

где  $e$  — квадратная матрица некоего размера  $r \times r$ , а остальные блоки — произвольного размера.

Таким образом, две матрицы комбинаторно эквивалентны, если одна может быть получена из другой элементарными преобразованиями над строками и перестановкой столбцов, или, что аналогично, они обе могут быть приведены к одному ступенчатому виду.

## Лекция III

21 февраля 2023 г.

### 1.4.1 Элементарная эквивалентность матриц

В этом параграфе  $K$  опять-таки поле.

**Теорема 1.4.2.**  $x \in M(m, n, K) \Rightarrow \exists g \in GE(m, K), h \in GE(n, K) : g x h = \left( \begin{array}{c|c} e & 0 \\ \hline 0 & 0 \end{array} \right)$  — окаймлённая единичная матрица размера  $r \times r$ .

*Доказательство.* В предыдущем вопросе мы доказали, что можно подобрать такие  $g, w : g x w$  — окаймлённая единичная матрица, у которой справа сверху мусор. Этот мусор можно вынести, поочерёдно вычитая столбцы слева (в которых все элементы равны 0, кроме одного — 1), домноженные на правильный коэффициент.  $\square$

Две матрицы элементарно эквивалентны, если ни могут быть приведены к одному окаймлённому виду.

Две матрицы  $x, y \in M(m, n, K)$  строго элементарно эквивалентны, если  $\exists g \in E(m, K), h \in E(n, K) : y = g x h$ , то есть разрешены только элементарные трансвекции первого рода.

**Теорема 1.4.3.**  $x \in M(m, n, K) \Rightarrow \exists g \in E(m, K), h \in E(n, K) : g x h$  — либо окаймлённая единичная матрица  $r \times r$ , либо  $d_m(\varepsilon)$  (в случае  $m = n = r$ ):

$$g x h = \left[ \begin{array}{c} \left( \begin{array}{c|c} e & 0 \\ \hline 0 & 0 \end{array} \right) \\ d_m(\varepsilon) \end{array} \right]$$

*Замечание.* Такой  $\varepsilon$  равен определителю (определителю Дьёдоне) матрицы  $x$ ,  $\det(x)$  (либо если матрица не строго эквивалентна псевдоотражению, то  $\det(x) = 0$ ). К сожалению, такой способ определить определитель не обобщается даже на кольца (даже коммутативные).

*Доказательство.* Вспомним доказательство предыдущей теоремы о комбинаторной эквивалентности матриц, и применим к нему лемму о  $d_i(\varepsilon) d_j(\varepsilon^{-1}) \in E(n, K)$ . Таким образом можно всякий раз кроме последней строки применять эту лемму, и обойтись преобразованиями первого типа, чтобы выставить все, кроме быть может одной, единицы в главной диагонали.  $\square$

*Замечание.* Всё вышеописанное применимо к телу. Для тела определитель Дьёдоне лежит в  $\{0\} \cup T^*/[T^*, T^*]$ .

## 1.4.2 Ранг матрицы над полем. Различные определения ранга над кольцом

### Тензорный и скелетный ранги

Рассмотрим матрицу над полем  $x \in M(m, n, K)$ .

Для коммутативного кольца  $R$  определим

**Определение 1.4.1** (Внешнее произведение, outer tensor). Матрица  $uv$ , где  $u \in R^m, v \in {}^n R$ .

Внешнее произведение — это матрица ранга 1.

**Определение 1.4.2** (Ранг матрицы  $x \in M(m, n, K)$ ). Наименьшее  $r$ , такое что существуют  $r$  матриц ранга 1, таких, что  $x$  равен их сумме. Обозначают  $rk(x)$ , иногда для определённости называют *тензорным* рангом.

**Теорема 1.4.4.** Ранг матрицы  $x \in M(n, m, R)$  равен наименьшему числу  $r$ , такому, что  $\exists y \in M(n, r, R)$  и  $z \in M(r, m, R)$ , такие, что

$$x = yz$$

Иногда такое  $r$  называют *скелетным* рангом, но скелетный ранг всегда равен тензорному рангу.

*Доказательство.*

$\Rightarrow$ . Если  $x = u_1 v_1 + \dots + u_r v_r$ , то

$$x = \begin{pmatrix} u_1 & \dots & u_r \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix}$$

$$\Leftarrow. x = yz = y e^2 z = (y(e_{1,1} + \dots + e_{r,r})) \cdot ((e_{1,1} + \dots + e_{r,r})z) = y_{*,1} z_{1,*} + \dots + y_{*,r} z_{r,*}. \quad \square$$

### Строчный и столбцовый ранги

**Определение 1.4.3** (Строчный ранг матрицы,  $\text{rk}(x)$ ). Ранг модуля, порождённого строками  $x$ , если этот модуль **свободен**.

**Определение 1.4.4** (Столбцовый ранг матрицы,  $\text{crk}(x)$ ). Ранг модуля, порождённого столбцами  $x$ , если этот модуль **свободен**.

*Замечание.* Строчный ранг и столбцовый не обязаны существовать. Для коммутативного кольца если оба существуют, то они равны. В таком случае их общее значение называют *внешним* рангом,  $\text{ork}(x)$ .

*Интересный факт.* Внешний ранг всегда не меньше тензорного ранга.

**Теорема 1.4.5.** Если  $K$  — поле, то тензорный ранг матрицы совпадает с её строчными и столбцовыми рангами, а ещё равен  $r$  из теоремы о комбинаторной эквивалентности матриц (следствие 1.4.1).

*Доказательство.* Переходя  $x \rightsquigarrow gx$ , где  $g \in GE(m, K)$  — элементарная матрица, мы переходим к пространству строк, содержащемуся в пространстве строк  $x$ .

Так как  $g$  обратимо, то пространства строк совпадают. Аналогично для столбцов,  $\text{crk}(x) = \text{crk}(xh)$ , и пространства столбцов совпадают.

Заметим, что преобразований над строками достаточно, чтобы получить эшелонированную матрицу с единичным блоком  $r \times r$ , то есть  $r$  линейно независимых строк. Применив далее преобразования над столбцами, приведём матрицу к каноническому виду — окаймлённой единичной, причём ранг её будет тот же  $r$ .

Если же аналогичные действия проделать сначала над столбцами, то получится столбцово-эшелонированная матрица с единичным блоком  $\tilde{r} \times \tilde{r}$ . Так как канонический вид матрицы единственен (теорема 1.3.1), то  $r = \tilde{r}$ .

Отсюда получается, что  $r = \text{crk}(x) = \text{grk}(x) = \text{rk}(x)$ , где последнее — ранг линейного отображения. Кроме того, отсюда вытекают факты, что строчный ранг не меняется при столбцовых преобразованиях, а столбцовый — при строчных.  $\square$

*Замечание.* Без использования понятия о ранге линейного отображения можно так доказать то, что элементарные преобразования над строчками не меняют и столбцовый ранг тоже: если какое-то подмножество столбцов было линейно зависимо:  $\lambda_1 u_1 + \dots + \lambda_s u_s = 0$ , то и после применения элементарного преобразования эта комбинация осталась нулевой:

$$\lambda_1(u_1 g) + \dots + \lambda_s(u_s g) = 0$$

**Определение 1.4.5** (Ранг по минору,  $\text{mrk}(x)$ ). Наибольший размер минора, имеющего ненулевой определитель.

*Интересный факт.*  $\text{mrk}(x) \leq \text{rk}(x)$ .

*Интересный факт* (Теорема о базисном миноре). Над полем  $\text{mrk}(x) = \text{rk}(x)$ .

### 1.4.3 Системы линейных уравнений

Пусть мы всё ещё работаем над полем.

Рассмотрим линейное отображение  $\phi : K^n \rightarrow K^m$ . Пусть  $u \in K^m$ .

**Определение 1.4.6** (Система линейных уравнений). Уравнение  $\phi(x) = u$ , где неизвестный  $x \in K^n$ .

Уравнение называется системой уравнений, потому что традиционно, выбрав базисы, можно запи-

сать  $\phi(x) = ax$ , где  $a \in M(m, n, K)$ ,  $u = \begin{pmatrix} u_1 \\ \vdots \\ u_m \end{pmatrix}$ , и система уравнений приобретает вид  $ax = u$ .

Но людям раньше нравилось много писать, поэтому они записывали

$$\begin{cases} a_{1,1}x_1 + \dots + a_{1,n}x_n = u_1 \\ a_{2,1}x_1 + \dots + a_{2,n}x_n = u_2 \\ \dots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n = u_m \end{cases}$$

## Лекция IV

22 февраля 2023 г.

**Теорема 1.4.6.** Если  $x_0$  — какое-то (частное) решение уравнения  $\phi(x) = u$ , то множество всех решений — это  $x_0 + \text{Ker}(\phi)$ .

*Доказательство.* Любое (общее) решение  $x$  удовлетворяет  $\phi(x) = u$ , откуда  $\phi(x - x_0) = 0$ , и  $x \in x_0 + \text{Ker}(\phi)$ .  $\square$

Система  $\phi(x) = 0$  называется *однородной*.

Ядро, разумеется, является подпространством; при работе над полем оно свободно, то есть

$$\text{Ker}(\phi) = \langle v_1, \dots, v_d \rangle$$

**Факт 1.4.1.**  $d = n - r$ .

Этот базис  $v_1, \dots, v_d$  называется *фундаментальной системой решений*.

**Следствие 1.4.2.** Любое решение  $x$  имеет вид  $x_0 + v_1 \lambda_1 + \dots + v_d \lambda_d$ .

### 1.4.4 Векторная запись системы линейных уравнений. Теорема Кронекера — Капелли

На самом деле теорема Кронекера — Капелли — очевидный факт, который Капелли, записывая, назвал *теорема Кронекера*, что потом при ссылках преобразовалось в текущее название.

$$a = (a_{*,1} \quad \dots \quad a_{*,n}) \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Векторная запись системы линейных уравнений  $a_{*,1}x_1 + \dots + a_{*,n}x_n = u$ .

Является ли вектор  $u$  линейной комбинацией векторов  $a_{*,1}, \dots, a_{*,n}$ ?

**Теорема 1.4.7** (Кронекер — Капелли). Ответ на этот вопрос известен: когда  $u \in \langle a_{*,1}, \dots, a_{*,n} \rangle \iff \langle a_{*,1}, \dots, a_{*,n} \rangle = \langle a_{*,1}, \dots, a_{*,n}, u \rangle$ .

Иначе говоря, система  $ax = u$  совместна  $\iff \text{rk}(a) = \text{rk}(a|u)$ .

**Факт 1.4.2** (Дополнение к теореме Кронекера — Капелли). Система  $ax = u$  имеет единственное решение  $\iff \text{rk}(a) = \text{rk}(a|u) = n$ .

*Доказательство.* В этом случае  $\dim \text{Ker}(a) = \dim K^n - \dim \text{Im } a = 0$  и ядро нулевое.  $\square$

### 1.4.5 Решение систем линейных уравнений методом Гаусса

Гаусс, может, этим методом и не решал системы, ну да ладно.

$$ax = u \quad a \in M(m, n, K) \quad x \in K^n \quad u \in K^m$$

Для любого  $g \in GL(m, K) = GE(m, K)$  умножение на матрицу слева приводит к эквивалентной системе  $gax = gu$ . Также можно перенумеровать неизвестные:

$$(gaw)(w^{-1}x) = gu, \quad w \in W_n$$

Раньше было доказано (следствие 1.4.1), что можно подобрать такие  $g \in GE(m, K), w \in W_n$ , что  $gaw$  имеет ступенчатый вид:  $(gaw|gu) = \left( \begin{array}{cc|c} e & * & * \\ 0 & 0 & \delta \end{array} \right), \delta \in \{0, 1\}^{m-r}$ . Система совместна  $\iff \delta = 0$ . Таким образом, неизвестные разбились на 2 группы: *главные*  $x_1, \dots, x_r$  и *свободные*  $x_{r+1}, \dots, x_n$ .

Систему можно переписать в виде

$$\begin{cases} x_1 + & c_{1,r+1}x_{r+1} + \dots + c_{1,n}x_n = d_1 \\ \dots & \\ x_r + & c_{r,r+1}x_{r+1} + \dots + c_{r,n}x_n = d_r \end{cases}$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \begin{pmatrix} d_1 \\ \vdots \\ d_r \end{pmatrix} - \begin{pmatrix} c_{1,r+1} \\ \vdots \\ c_{r,r+1} \end{pmatrix} x_{r+1} - \dots - \begin{pmatrix} c_{1,n} \\ \vdots \\ c_{r,n} \end{pmatrix} x_{r+1}$$

В качестве частного решения можно взять решение при занулённых свободных переменных, а в качестве базиса ядра — решения, принимая каждую свободную переменную по очереди единицей:

$$\begin{pmatrix} d_1 - c_{1,r+1}x_{r+1} - \dots - c_{1,n}x_n \\ \vdots \\ d_r - c_{r,r+1}x_{r+1} - \dots - c_{r,n}x_n \\ \hline x_{r+1} \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} d_1 \\ \vdots \\ d_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} -c_{1,r+1} \\ \vdots \\ -c_{r,r+1} \\ 1 \\ \vdots \\ 0 \end{pmatrix} x_{r+1} + \dots + \begin{pmatrix} -c_{1,n} \\ \vdots \\ -c_{r,n} \\ 0 \\ \vdots \\ 1 \end{pmatrix} x_n$$

### 1.4.6 Определитель по Вейерштрассу

Пусть  $x \in M(n, R)$  — матрица над коммутативным кольцом.

В определении по Вейерштрассу матрица фигурирует, как строка столбцов  $x = (x_{*,1}, \dots, x_{*,n})$ .

**Определение 1.4.7** (Определитель по Вейерштрассу).  $\text{Det} : \underbrace{R^n \times \dots \times R^n}_n \rightarrow R$  со следующими свойствами.

1. Полилинейность:  $\text{Det}$  линейно по каждому аргументу при фиксированных остальных.
2. Антисимметричность: если два столбца совпали, то определитель — нуль.
3. Нормированность:  $\text{Det}(e_1, \dots, e_n) = \text{Det}(e) = 1$ .

Существует ли такой определитель? (Да, например, определитель Лейбница (определение 1.4.13))

Единственен ли он? (Да: (теорема 1.4.13))

**Лемма 1.4.1.** *Определитель не меняется при элементарных преобразованиях над столбцами.*

*Доказательство.*

$$\begin{aligned} \text{Det}(x \cdot t_{r,s}(\xi)) &= \text{Det}(x_{*,1}, \dots, x_{*,r}, \dots, x_{*,s} + x_{*,r}\xi, \dots, x_{*,n}) = \\ &= \text{Det}(x_{*,1}, \dots, x_{*,r}, \dots, x_{*,s}, \dots, x_{*,n}) + \underbrace{\text{Det}(x_{*,1}, \dots, x_{*,r}, \dots, x_{*,r}, \dots, x_{*,n})}_0 \xi \end{aligned} \quad \square$$

**Лемма 1.4.2** (Кососимметричность определителя). *При перестановке двух столбцов местами определитель меняет знак.*

*Доказательство.* Обозначим  $F(u_r, u_s) := \text{Det}(u_1, \dots, u_r, \dots, u_s, \dots, u_n)$ .

$$\begin{aligned} \text{В силу линейности определителя, } 0 = F(u_r + u_s, u_r + u_s) &= \underbrace{F(u_r, u_r)}_0 + F(u_r, u_s) + F(u_s, u_r) + \\ &+ \underbrace{F(u_s, u_s)}_0. \end{aligned} \quad \square$$

*Замечание.* Кососимметричность следует из антисимметричности, а обратное верно только если 2 — не делитель 0 (и  $2 \neq 0$ ).

**Лемма 1.4.3.** *Если один из столбцов является линейной комбинацией остальных, то определитель равен 0.*

### 1.4.7 Знак перестановки. Определение через декремент

**Определение 1.4.8** (Декремент). Любая перестановка представима в виде произведения независимых циклов (включая тривиальные).

$$\forall \pi \in S_n : \quad \pi = \rho_1 \cdot \dots \cdot \rho_m$$

**Определение 1.4.9** (Орбита перестановки). Множество  $\{k, \pi(k), \pi(\pi(k)), \dots\} = \{\pi^l(k) | l \in \mathbb{Z}\}$  Так как перестановка обратима (является биекцией), то любые две различные орбиты не пересекаются.

*Замечание.* Количество независимых циклов  $\pi$  — количество орбит  $\pi$ .

**Определение 1.4.10** (Декремент  $\pi$ ).  $\text{decr}(\pi) \stackrel{\text{def}}{=} n - m$ , где  $\pi \in S_n$ , а  $m$  — количество независимых циклов (или орбит)  $\pi$ .

Если  $\{1, \dots, n\} = X_1 \sqcup \dots \sqcup X_m$ , где  $X_1, \dots, X_m$  — орбиты перестановки, то декремент — это сумма  $\sum_{i=1}^m (|X_i| - 1)$ .

**Определение 1.4.11** (Знак перестановки).  $\text{sgn}(\pi) = (-1)^{\text{decr}(\pi)}$

**Теорема 1.4.8.**  $\text{decr}(\pi)$  — наименьшее количество транспозиций, произведение которых в некотором порядке равно  $\pi$ .

*Доказательство.* Давайте следить за длиной конкретного разложения перестановки по системе образующих транспозиций.

База:  $\text{decr}(\text{id}) = n - n = 0$ .

Переход: Всякое применение транспозиции меняет декремент на 1 (если она меняет местами элементы одного цикла  $\pi$ , то декремент увеличивается, а если из разных — то уменьшается).

В самом деле, если элементы из одного цикла меняются местами, то цикл разлагается на 2: для  $p < q$ :  $(i_p i_q)(i_1 i_2 \dots i_r) = (i_1 \dots i_{p-1} i_q \dots i_r) \cdot (i_p i_{p+1} \dots i_{q-1})$ .

Если же местами меняются элементы разных циклов, то это вычисление получается домножением равенства выше на  $(i_p i_q)$  слева:  $(i_1 i_2 \dots i_r) = (i_p i_q)(i_1 \dots i_{p-1} i_q \dots i_r) \cdot (i_p i_{p+1} \dots i_{q-1})$ .



□

## 1.4.8 Знак перестановки. Определение через инверсии

Вспользуемся тем, что  $S_n = \langle (ij), i + 1 = j \rangle$ .

**Определение 1.4.12** ( $i < j$  образуют инверсию в перестановке  $\pi \in S_n$ ).  $\pi_i > \pi_j$ .

Обозначим за  $\text{inv}(\pi)$  количество инверсий в перестановке  $\pi$ .

**Теорема 1.4.9.**  $\text{sgn}(\pi) = (-1)^{\text{inv}(\pi)} = \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}$ .

Ещё можно сказать, что количество инверсий равняется минимальному количеству фундаментальных транспозиций, произведение которых в некотором порядке даёт  $\pi$ .

*Доказательство.* Несложно проверить, что всякая фундаментальная транспозиция, после домножения на перестановку (неважно, слева или справа), меняет количество инверсий в ней на  $\pm 1$ .

А именно, при домножении  $\pi$  на транспозицию  $(ij)$  слева происходит смена  $\pi(i)$  и  $\pi(j)$ , пара индексов  $i$  и  $j$  либо перестаёт, либо начинает образовывать инверсию. Кроме того, все инверсии  $i, k$  меняются на инверсии  $j, k$  и наоборот, так как относительное положение индекса  $k$  относительно  $i$  или  $j$  не поменялось (транспозиция фундаментальная, поэтому  $|i - j| = 1$ ).

При домножении  $\pi$  на транспозицию  $(xy)$  справа происходит смена  $\pi(i)$  и  $\pi(j)$  где  $\pi(i) = x, \pi(j) = y$ , пара индексов  $i$  и  $j$  либо перестаёт, либо начинает образовывать инверсию. Остальные инверсии остаются прежними, так как  $|x - y| = 1$ . □

Без доказательства существования знак ещё можно определить следующим образом:

**Теорема 1.4.10.** Для  $n \geq 2$  существуют ровно два гомоморфизма  $\phi : S_n \rightarrow \{\pm 1\}$ . Это тождественный 1 и  $\text{sgn}$ .



*Доказательство.*  $\{\pm 1\}$  — абелева группа. Пусть  $\pi \sim \sigma \in S_n \iff \phi(\pi) = \phi(\sigma)$ .

При сопряжении аргумента  $\phi(\pi)$  не меняется:  $\phi(\sigma\pi\sigma^{-1}) = \phi(\sigma)\phi(\pi)\phi(\sigma)^{-1} = \phi(\pi)$ .

Так как все транспозиции сопряжены, то  $\phi(\tau) = \text{const}$  для всех транспозиций  $\tau$ .

Если  $\phi(\tau) = 1$ , то гомоморфизм — тождественная единица, иначе  $\phi(\tau) = -1$ , и  $\phi \equiv \text{sgn}$ .  $\square$

### 1.4.9 Знакопеременное определение определителя

Пусть  $x \in M(n, R)$ , где  $R$  — коммутативное кольцо.

**Определение 1.4.13** (Определитель по Лейбницу).  $\det(x) = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{j=1}^n x_{j, \pi(j)}$ .

**Лемма 1.4.4** (Общее правило знаков). *Слагаемое  $x_{\pi(1), \rho(1)} \cdot \dots \cdot x_{\pi(n), \rho(n)}$  входит в сумму со знаком  $\text{sgn}(\pi) \cdot \text{sgn}(\rho)$ .*

*Доказательство.* В коммутативном кольце  $x_{\pi(1), \rho(1)} \cdot \dots \cdot x_{\pi(n), \rho(n)} = x_{1, \rho(\pi^{-1}(1))} \cdot \dots \cdot x_{n, \rho(\pi^{-1}(n))}$ .  $\square$

Свойства транспонирования:

1.  $x^{tt} = x$
2.  $(x + y)^t = x^t + y^t$
3.  $(xy)^t = y^t \cdot x^t$ .

Данному набору свойств удовлетворяет  $(x^t)_{j,i} \stackrel{\text{def}}{=} x_{i,j}$ . Транспонирование  $^t : M(n, R) \rightarrow M(n, R^o)$ .

**Теорема 1.4.11.**  $\det(x^t) = \det(x)$ .

*Доказательство.* Согласно правилу знаков  $\det(x^t) = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{j=1}^n x_{\pi(j), j} = \det(x)$ .  $\square$

Для некоммутативного кольца  $R$  это неверно:

*Пример.* Определим алгебру Вейля  $W_1(K) = K\langle x, d \rangle / ([d, x] = 1)$  — алгебра над полем  $K$ , где  $d, x$  не коммутируют, и взят фактор по отношению  $[d, x] = 1$ . Алгебра дифференциальных операторов некоммутативна.

Говорят, в квантовой механике активно используется  $W_n(K)$ .

Если посчитать  $\text{row det} \begin{pmatrix} d & d \\ x & x \end{pmatrix} = dx - xd = 1$ .

В другую сторону:  $\text{col det} \begin{pmatrix} d & d \\ x & x \end{pmatrix} = dx - dx = 0$ .

В самом деле, столбцы линейно зависимы, а строки — нет.

## Лекция V

1 марта 2023 г.

### 1.4.10 Существование определителя (удовлетворяющего условиям Вейерштрасса)

**Теорема 1.4.12.** Определитель по Лейбницу удовлетворяет условиям Вейерштрасса

*Доказательство.*

- Линейность по столбцам. Пусть  $x_{*,r} = u + v$ . Тогда

$$\det(x) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) x_{\pi(1),1} \cdot \dots \cdot \underset{\substack{\parallel \\ (u+v)_{\pi(r)}}}{x_{\pi(r),r}} \cdot \dots \cdot x_{\pi(n),n}$$

В силу дистрибутивности кольца можно раскрыть скобки  $(a(b+c)d = (ab+ac)d = abd + acd)$ :

$$\det(x) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) x_{\pi(1),1} \cdot \dots \cdot u_{\pi(r)} \cdot \dots \cdot x_{\pi(n),n} + \sum_{\pi \in S_n} \operatorname{sgn}(\pi) x_{\pi(1),1} \cdot \dots \cdot v_{\pi(r)} \cdot \dots \cdot x_{\pi(n),n}$$

Аналогично можно выносить константу, домноженную на произвольный столбец.

- Если два столбца, пусть  $x_{*,r}$  и  $x_{*,s}$ , совпадают, то определитель равен 0:

$$\det(x) = \sum_{\pi \in A_n} x_{\pi(1),1} \cdot \dots \cdot x_{\pi(r),r} \cdot \dots \cdot x_{\pi(s),s} \cdot \dots \cdot x_{\pi(n),n} - \sum_{\substack{\pi \in (rs) \cdot A_n \\ \parallel \\ S_n \setminus A_n}} x_{\pi(1),1} \cdot \dots \cdot x_{\pi(r),r} \cdot \dots \cdot x_{\pi(s),s} \cdot \dots \cdot x_{\pi(n),n}$$

В силу равенства столбцов  $x_{*,r}$  и  $x_{*,s}$  в левой сумме все слагаемые совпадают со слагаемыми в правой сумме.

- Нормированность определителя:  $\det(e) = 1$ . Несложно видеть даже большее: определитель треугольной матрицы равен произведению диагональных элементов

$$\det \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} = a_1 \cdot \dots \cdot a_n$$

□

#### 1.4.11 Единственность определителя (удовлетворяющего условиям Вейерштрасса)

**Теорема 1.4.13.** Никакое другое отображение, кроме определителя Лейбница, не удовлетворяет условиям определителя Вейерштрасса.

*Доказательство.* Всякий столбец раскладывается по столбцовому базису  $\{e_i\}_{i=1..n}$ :

$$u_j = e_1 x_{1,j} + \dots + e_n x_{n,j}$$

Рассмотрим произвольный определитель Вейерштрасса  $\operatorname{Det}$ , и разложим его аргументы по столбцовому базису:

$$\begin{aligned} \operatorname{Det}(u_1, \dots, u_n) &= \operatorname{Det}((e_1 x_{1,1} + \dots + e_n x_{n,1}), \dots, (e_1 x_{1,n} + \dots + e_n x_{n,n})) = \\ &= \sum_{i_1, \dots, i_n=1}^n \operatorname{Det}(e_{i_1}, \dots, e_{i_n}) \cdot x_{i_1,1} \cdot \dots \cdot x_{i_n,n} = \\ &= \sum_{\pi \in S_n} \operatorname{Det}(e_{\pi(1)}, \dots, e_{\pi(n)}) \cdot x_{\pi(1),1} \cdot \dots \cdot x_{\pi(n),n} \end{aligned}$$

Таким образом, мы видим, что получили определение определителя по Лейбницу. В самом деле,  $\operatorname{Det}(e_{\pi(1)}, \dots, e_{\pi(n)})$  равен знаку перестановки, так как из антисимметричности следует кососимметричность, и  $\operatorname{Det}(e_{\pi(1)}, \dots, e_{\pi(n)})$  равен с точностью до знака  $\det(e)$ , а знак определителя — чётность декремента  $\pi$ . □

### 1.5 Мультипликативность определителя

$$\det(xy) = \det(x) \det(y)$$

### 1.5.1 Блочные матрицы

Рассмотрим матрицу из  $M(m, n, R)$ .

Пусть  $\mu = (m_1, \dots, m_r)$  — разбиение числа  $m$ , то есть  $m_1 + \dots + m_r = m$ , и  $\nu = (n_1, \dots, n_s)$  — разбиение  $n$ .

Разобьём элементы матрицы в соответствии с разбиением:

$$\begin{matrix} m_1 \\ \vdots \\ m_r \end{matrix} \left( \begin{array}{c|c|c} n_1 & \dots & n_s \\ \hline & & \\ \hline & & \\ \hline & & \\ \hline \end{array} \right)$$

Подматрицу  $x^{i,j} \in M(m_i, n_j, R)$  называют *блок матрицы*  $x$  в позиции  $(i, j)$  для  $i \in [1, r], j \in [1, s]$ .

#### Операции над блочными матрицами

1. Сложение.

Рассмотрим две матрицы  $x, y$  с одинаковым разбиением на блоки.

Тогда сумма определяется поблочно  $(x + y)^{i,j} = x^{i,j} + y^{i,j}$ .

2. Умножение. Пусть  $x \in M(l, m, R), y \in M(m, n, R), \lambda = (l_1, \dots, l_q)$  — разбиение  $l$ .

Рассмотрим  $(\lambda, \mu)$  разбиение  $x$  и  $(\mu, \nu)$  разбиение  $y$ .

Тогда произведение определяется поблочно:

$$(x \cdot y)^{i,k} = \sum_{j=1}^r x^{i,j} \cdot y^{j,k}$$

Важнейший частный случай — разбиения на равные слагаемые. Так, квадратную матрицу из  $M(m \cdot n, R)$  можно разбить на  $m \times m$  блоков размера  $n \times n$ :  $M(m \cdot n, R) = M(m, M(n, R))$ .

### 1.5.2 Определитель блочно треугольной матрицы

**Теорема 1.5.1.** Рассмотрим матрицу  $x = \left( \begin{array}{c|c} y & * \\ \hline 0 & z \end{array} \right) \in M(n, R)$ . Для определённости можно положить  $y \in M(m, R), z \in M(n - m, R)$ .

Утверждается, что  $\det(x) = \det(y) \det(z)$ .

*Доказательство.* Определим подгруппы Юнга в  $S_n$ . Пусть  $\mu = (m_1, \dots, m_r)$  — разбиение  $m$ . Тогда  $\pi$  лежит в подгруппе Юнга, соответствующей разбиению  $\mu$ , если  $\forall k = 1..r : \pi(i) \in m_k \iff i \in m_k$ . Здесь запись  $i \in m_k$  означает, что  $\sum_{j=1}^{k-1} m_j < i \leq \sum_{j=1}^k m_j$ .

Иными словами, подгруппы Юнга не перемешивают элементы вне разбиения.

Такая подгруппа Юнга изоморфна  $S_{m_1} \times \dots \times S_{m_k}$ .

Для удобства будем рассматривать подгруппы Юнга размера 2: для разбиения  $n = (m, n - m)$ . Здесь определение упрощается до  $i \leq m \iff \pi(i) \leq m$ .

Итак, посчитаем определитель  $x$ . Заметим, что в формуле

$$\sum_{\pi \in S_n} \text{sgn}(\pi) x_{1, \pi(1)} \cdot \dots \cdot x_{n, \pi(n)}$$

суммирование можно проводить только по перестановкам из подгруппы Юнга для  $(m, n - m)$ .

В самом деле, по принципу Дирихле, если какая-то из первых  $m$  строчек попала не в первый из  $m$  столбцов, то тогда какой-то из них остался свободен, и в него попадёт что-то из следующих строчек, то есть конкретное произведение даст 0. В соответствии с этим, будем суммировать по не  $\pi \in S_n$ , а по  $(\rho, \sigma) \in S_m \times S_{n-m}$ .

$$\sum_{(\rho, \sigma) \in S_m \times S_{n-m}} \operatorname{sgn}(\rho) x_{1, \rho(1)} \cdots x_{m, \rho(m)} \cdot \operatorname{sgn}(\sigma) x_{m+1, m+\sigma(1)} \cdots x_{m+(n-m), m+\sigma(n-m)} = \det(y) \det(z)$$

□

**Следствие 1.5.1.** Для любого квадратного разбиения матрицы на блоки  $(r = s)$ , такого, что элементы ниже главной диагонали — нуль-матрицы, определитель равен произведению блочных подматриц на главной диагонали.

### 1.5.3 Мультипликативность определителя

Пусть  $x, y \in M(n, R)$ .

**Теорема 1.5.2.**  $\det(xy) = \det(x) \det(y)$

*Доказательство.* Рассмотрим блочную матрицу  $\begin{pmatrix} y & e \\ 0 & x \end{pmatrix}$ , и домножим её слева на  $\begin{pmatrix} e & 0 \\ -x & e \end{pmatrix}$  (это трансвекция, прибавляющая ко второй строчке первую, домноженную на  $-x$ ):

$$\begin{pmatrix} e & 0 \\ -x & e \end{pmatrix} \cdot \begin{pmatrix} y & e \\ 0 & x \end{pmatrix} = \begin{pmatrix} y & e \\ -xy & 0 \end{pmatrix}$$

Так как это элементарное преобразование, то определитель не поменялся. Сделаем ещё пару пассов руками:

$$\begin{pmatrix} y & e \\ -xy & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -e \\ e & 0 \end{pmatrix} = \begin{pmatrix} e & -y \\ 0 & xy \end{pmatrix}$$

Это тоже произведение парочки элементарных преобразований первого типа, значит,  $\det(y) \det(x) = \det(xy)$ , и из коммутативности кольца  $R$ , в котором мы считаем определитель, доказательство завершено. □

## Лекция VI

7 марта 2023 г.

### 1.5.4 Миноры, разложение по строке, определитель по Лапласу

$R$  — коммутативное кольцо,  $x \in M(m, n, R)$ . Выберем  $I \subset \underline{m} = \{1, \dots, m\}$ ;  $J \subset \underline{n} = \{1, \dots, n\}$  так, что  $|I| = |J| = d$ . Рассмотрим сужение матрицы  $x$  на  $I \times J$ , как матрицу из  $M(d, R)$ .

**Определение 1.5.1** (Минор  $M_{I,J}(x)$ ). Определитель матрицы  $(x_{i,j})_{i \in I, j \in J}$ .

Если же  $m - |I| = n - |J|$ , то  $\det(x_{i,j})_{i \notin I, j \notin J}$  — *дополнительный минор*, обозначается  $\overline{M}_{I,J}$ .

Особенно важен случай  $m = n$ . Здесь определён дополнительный минор

$$\overline{M}_{i,j} = \det(\text{вычеркнули из } x \text{ строку } i \text{ и столбец } j)$$

**Определение 1.5.2** (Алгебраическое дополнение к элементу  $x_{i,j}$ ).  $A_{i,j}(x) \stackrel{\text{def}}{=} (-1)^{i+j} \overline{M}_{i,j}(x)$ . Можно также сказать, что это определитель матрицы, где  $x_{*,j}$  и  $x_{i,*}$  заменили на нули, но  $x_{i,j}$  — на единицу.

**Теорема 1.5.3** (Разложение по строке). Для матрицы  $x \in M(n, R)$ :

$$\forall i_1, i_2 \in [1, n] : \sum_{j=1}^n x_{i_1, j} A_{i_2, j} = \begin{cases} \det(x), & i_1 = i_2 \\ 0, & i_1 \neq i_2 \end{cases}$$

*Доказательство.* Рассмотрим  $i_1$ -ю строку матрицы  $x$ . Разложим её по строчному базису  $x_{i_1,*} = x_{i_1,1}f_1 + \dots + x_{i_1,n}f_n$ .

Разложим определитель в сумму  $n$  слагаемых, где  $i_1$ -я строка разложена по строчному базису.

Дальше мы можем переставлять строчки по одной, получив форму разложения по строке для  $i_1 = i_2$ .

Если же  $i_1 \neq i_2$ , то мы посчитали определитель матрицы, у которой на место строки  $i_2$  поставили строку  $i_1$ , то есть определитель матрицы с равными строками — 0.  $\square$

**Определение 1.5.3** (Определитель по Лапласу (индуктивно)).  $\det(x) = x_{1,1}A_{1,1}(x) + \dots + x_{1,n}A_{1,n}(x)$ .

*Замечание.* Вместо строк можно раскладывать по столбцам.

*Интересный факт* (Лаплас). Можно раскладывать не по одной строке, а по нескольким (по  $k$  строкам). Минор определяется выбором  $k$  столбцов.

$$\det(x) = \sum_{1 \leq j_1 < \dots < j_k \leq n} (-1)^{i_1 + \dots + i_k + j_1 + \dots + j_k} M_{\{i_1, \dots, i_k\} \times \{j_1, \dots, j_k\}} \cdot \overline{M}_{\{i_1, \dots, i_k\} \times \{j_1, \dots, j_k\}}$$

## 1.5.5 Формула Крамера, теорема Крамера

Формула Крамера получает по матрице её обратную.

Пусть  $x \in M(n, R)$ . Когда  $x$  обратима?

**Определение 1.5.4** (Присоединённая матрица).  $\text{adj}(x) \stackrel{\text{def}}{=} (A_{i,j}(x))_{1 \leq i, j \leq n}^t = (A_{j,i}(x))_{1 \leq i, j \leq n}$

**Лемма 1.5.1.**  $x \cdot \text{adj}(x) = \text{adj}(x) \cdot x = \det(x) \cdot e$ .

*Доказательство.* Раскрыть произведение матриц в сумму и применить теорему Лапласа.  $\square$

**Теорема 1.5.4** (формула Крамера). Матрица  $g$  обратима, если и только если  $\det(g) \in R^*$ . Если  $\det(g) \in R^*$ , то  $g^{-1} = \frac{1}{\det(g)} \text{adj}(g)$ .

*Доказательство.* Если  $g$  обратима, то  $\exists g^{-1} \in M(n, R)$ , откуда  $1 = \det(e) = \det(gg^{-1}) = \det(g) \cdot \det(g^{-1})$ , получается,  $\det(g)$  обратим.

Если  $\det(g) \in R^*$ , то  $\exists g^{-1} = \frac{1}{\det(g)} \text{adj}(g)$ .  $\square$

**Теорема 1.5.5** (Крамер). В поле  $K$  система  $ax = u$  ( $a \in M(n, K)$ ,  $u \in K^n$ ) имеет единственное решение  $\iff \det(a) \neq 0$ . Если  $\det(a) \neq 0$ , то это решение задаётся формулой  $x = a^{-1}u$ .

*Доказательство.* Если  $\det(a) \neq 0$ , то условия эквивалентны:  $ax = u \iff x = a^{-1}u$ .

Если в поле  $\det(a) = 0$ , то  $\text{rk}(a) < n$ . Тогда либо  $\text{rk}(a|u) = \text{rk}(a)$ , откуда по теореме Кронекера — Капелли  $ax = u$  совместна, но не определена, либо  $\text{rk}(a|u) > \text{rk}(a)$ , откуда система несовместна.  $\square$

## 1.6 Определители некоторых матриц

Даны  $n$  функций  $f_1, \dots, f_n : R \rightarrow R$  и  $n$  аргументов  $x_1, \dots, x_n$ .

Чаше всего полезны определители вида  $\det \begin{pmatrix} f_1(x_1) & \dots & f_n(x_1) \\ \vdots & \ddots & \vdots \\ f_1(x_n) & \dots & f_n(x_n) \end{pmatrix}$  — *альтернанты*.

Иногда также случаются определители вида  $\det \begin{pmatrix} f(x_1, x_1) & \dots & f(x_1, x_n) \\ \vdots & \ddots & \vdots \\ f(x_n, x_1) & \dots & f(x_n, x_n) \end{pmatrix}$

### 1.6.1 Определитель Вандермонда

**Определение 1.6.1** (Матрица Вандермонда). Альтернант для  $f_i : x \mapsto x^{i-1}$

$$V(x_1, \dots, x_n) = \begin{pmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-1} \end{pmatrix}$$

**Теорема 1.6.1.**  $\det(V(x_1, \dots, x_n)) = \prod_{i>j} (x_i - x_j)$ .

*Доказательство.*

- $\det(V(x_1, \dots, x_n))$  — многочлен от переменных  $x_1, \dots, x_n$ .
- Его степень  $0 + 1 + \dots + (n-1) = \frac{n(n-1)}{2}$ .
- Профакторизуем по отношению  $(x_i - x_j)$ , отображая кольцо многочленов от  $n$  переменных в кольцо многочленов от  $n-1$  переменных. Строчки  $x_{i,*}$  и  $x_{j,*}$  стали равны, значит,  $(x_i - x_j) \mid \det(V(x_1, \dots, x_n))$ .
- Все многочлены вида  $x_i - x_j$  для  $i > j$  взаимно просты, значит,  $\prod_{i>j} (x_i - x_j) \mid \det(V(x_1, \dots, x_n))$ .  
Степень произведения тоже равна  $\frac{n(n-1)}{2}$ .
- Проверим, что константа ассоциированности между ними равна 1. Рассмотрим диагональное произведение  $1 \cdot x_2 \cdot x_3^2 \cdot \dots \cdot x_n^{n-1}$ . Входит в оба выражения со знаком  $+1$ .  $\square$

### 1.6.2 Пфаффианы

Пусть  $x \in M(n, K)$ .

**Определение 1.6.2** (Кососимметричная матрица). Матрица  $x$ , такая, что  $x^t = -x$ .

**Определение 1.6.3** (Антисимметричная матрица). Кососимметричная матрица  $x$ , такая, что  $\forall i \in [1, n] : x_{i,i} = 0$ .

*Пример.*

$$\begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix}$$

*Интересный факт.* Пусть  $x \in M(n, R)$  — антисимметричная матрица. Если  $n \equiv 1 \pmod{2}$ , то  $\det(x) = 0$ . Иначе  $n \equiv 0 \pmod{2}$ , тогда  $\det(x) \in R^2$ .

*Замечание.* Пфаффиан можно определить с точностью до знака, как корень из определителя.

**Определение 1.6.4** (Пфаффиан).  $\text{pf}(x)$  определён для антисимметричных матриц и удовлетворяет следующим свойствам:

1.  $\text{pf}(y \cdot x \cdot y^t) = \text{pf}(x) \cdot \det(y)$
2.  $\text{pf}(x \oplus y) = \text{pf}(x) \cdot \text{pf}(y)$ , где  $x \oplus y = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ .
3.  $\text{pf} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = +1$ .

*Интересный факт.*  $\det(x) = \text{pf} \begin{pmatrix} 0 & x \\ -x^t & 0 \end{pmatrix}$ .

*Интересный факт.* Если  $x$  — порядка  $2n$ , то

$$\text{pf}(x) = \sum_{\pi \in S_{2n}} \text{sgn}(\pi) x_{\pi(1), \pi(2)} \cdot \dots \cdot x_{\pi(2n-1), \pi(2n)}$$

где сумма берётся по всем таким  $\pi$ , что  $\pi(2i-1) < \pi(2i)$ .

## Глава 2

# Многочлены

## Лекция VII

14 марта 2023 г.

В доказательстве вычисления определителя Вандермонда были два пробела, надо бы их восполнить (теорема 2.2.1).

### 2.1 Гомоморфизм эвалюации

Говоря простыми словами, подстановка элемента алгебры в многочлен.

Пусть  $R$  — коммутативное кольцо.

**Определение 2.1.1** ( $A$  — алгебра над  $R$ ). Кольцо  $A$  (часто ассоциативное, с  $1_A$ ), необязательно коммутативное, являющееся  $R$ -модулем, а ещё  $\forall x, y \in A, \lambda \in R$ : выполняется аксиома алгебры

$$\lambda(xy) = (\lambda x)y = x(\lambda y)$$

Несложно заметить вложение  $R \hookrightarrow A$ ;  $\lambda \mapsto \lambda \cdot 1_A$ . Оно вкладывает  $R$  в центр  $A$ :  $R \cdot 1_A \leq \text{Cent}(A)$ .

*Замечание.* Некоммутативность алгебры позднее будет крайне существенной, так как мы будем рассматривать  $A = M(m, R) = \text{End}_R(V)$ .

*Пример.* Рассмотрим цепочку вложений  $\mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$ .  $\mathbb{C}$  и  $\mathbb{H}$  — алгебры над  $\mathbb{R}$ , но  $\mathbb{H}$  — **не**  $\mathbb{C}$ -алгебра,  $i \cdot j \neq j \cdot i$ .

Пусть  $f \in R[x]$ , обозначим  $f = a_n x^n + \dots + a_1 x + a_0$ .

**Определение 2.1.2** (Значение  $f$  в точке  $c \in A$ ). Обозначим  $f(c) = a_n c^n + \dots + a_1 c + a_0 \cdot 1_A$ .

*Замечание.* Интересно заметить, что мы пользовались более слабым условием, чем ассоциативность  $A$ : мы пользовались тем, что  $A$  — алгебра с ассоциативными степенями:

$$c^{i+j} = c^i \cdot c^j, \quad \text{что не зависит от разложения } i+j \text{ в сумму}$$

Зафиксируем  $f \in R[x]$ .

**Определение 2.1.3** (Полиномиальное отображение).

$$\tilde{f}: A \rightarrow A \quad c \mapsto f(c)$$

Зафиксируем  $c \in A$ .

**Определение 2.1.4** (Гомоморфизм эвалюации).

$$\text{ev}_c : R[x] \rightarrow A \quad f \mapsto f(c)$$

**Предложение 2.1.1.** Гомоморфизм эвалюации — гомоморфизм, то есть  $(f + g)(c) = f(c) + g(c)$  и  $(f \cdot g)(c) = f(c) \cdot g(c)$ .

*Замечание.* Коммутативность  $R$  действительно важна:

$$\begin{aligned} c^2 - ac - bc + ab &= \text{ev}_c(x^2 - (a + b)x + ab) = \\ &= \text{ev}_c((x - a)(x - b)) = \\ &= \text{ev}_c(x - a) \cdot \text{ev}_c(x - b) = (c - a)(c - b) = c^2 - ac - cb + ab \end{aligned}$$

Видим, что равенство выполняется, если и только если  $c$  коммутирует с  $b$ , где  $c \in A, b \in R$  — любые элементы.

**Определение 2.1.5** (Гомоморфизм  $R$ -алгебр). Отображение  $\phi : A \rightarrow B$ , такое, что  $\forall x, y \in A, \lambda \in R$ :

1.  $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ .
  2.  $\phi(x + y) = \phi(x) + \phi(y)$ .
  3.  $\phi(1_A) = 1_B$ .
  4.  $\phi(\lambda x) = \lambda \phi(x)$ .
- } Унитарный гомоморфизм колец

Пусть  $\{*\}$  — произвольное одноэлементное множество, *синглетон*.

$$\begin{array}{ccc} \{*\} & \xrightarrow{* \mapsto x} & R[x] \\ & \searrow * \mapsto c & \swarrow \text{ev}_c \\ & A & \end{array}$$

**Теорема 2.1.1.** Кольцо многочленов  $R[x]$  обладает **универсальным свойством**: существует и единственен гомоморфизм  $R$ -алгебр  $R[x] \rightarrow A$ , делающий диаграмму выше коммутативной.

Это гомоморфизм эвалюации  $\text{ev}_c$ .

*Доказательство.* Существование уже доказано, единственность следует из определения гомоморфизма алгебр.  $\square$

Эту теорему можно принять за определение кольца многочленов от одной переменной: кольцо многочленов — такая  $R$ -алгебра, что, вложив  $R$  в произвольную  $R$ -алгебру  $A$ , останется ровно один способ ввести гомоморфизм из кольца многочленов в алгебру.

Тем не менее, это не совсем правда — само кольцо  $R$ , разумеется, является  $R$ -алгеброй с данным свойством. Точной формулировки я не нашёл.

## 2.2 Число корней многочлена над областью целостности

Пусть  $f \in R[x]$ , где  $R$  — область целостности.

**Определение 2.2.1** (Корень / нуль  $f$ ). Такой элемент  $c \in R$ , что  $f(c) = 0$ .

**Определение 2.2.2** (Кратность корня  $c$  многочлена  $f$ ). Число  $m \in \mathbb{N}_0$ , такое, что  $(x - c)^m \parallel f$ .

**Теорема 2.2.1** (Безу).  $f(c)$  — остаток от деления  $f$  на  $x - c$ .

$$f = (x - c)g + f(c) \quad \Rightarrow \quad f(c) = 0 \iff x - c \mid f$$

**Следствие 2.2.1.**  $c$  — корень  $f$  кратности  $m \iff f = (x - c)^m g$ , где  $g(c) \neq 0$ .



**Следствие 2.2.2** (Обобщённая теорема Безу). Для  $R$ , являющейся областью целостности:

Пусть  $c_1, \dots, c_s$  — различные корни  $f$  кратностей  $m_1, \dots, m_s$  соответственно. Тогда  $f = (x - c_1)^{m_1} \dots (x - c_s)^{m_s} \cdot g$ , где  $g(c_1), \dots, g(c_s) \neq 0$ .

*Доказательство.* Индукция по количеству различных корней, использующая при переходе теорему Безу.  $\square$

**Следствие 2.2.3.** У любого многочлена  $f \in R[x]$ , где  $R$  — область целостности — количество корней с учётом кратности не превосходит  $n$ .

*Контрпримеры* (Существование области целостности).

- $x^2 - 5x \in (\mathbb{Z}/6\mathbb{Z})[x]$  имеет корни  $\bar{0}, \bar{2}, \bar{3}, \bar{5}$ .
- В булевом кольце  $R = (2^X, \triangle, \cap)$  все элементы — идемпотенты, все — корни  $x^2 - x$ .
- $R = M(2, R)$ . У многочлена  $x^2$  есть корень  $0$  кратности 2, есть корень  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ .
- $R = \mathbb{H}$  — над телом кватернионов у многочлена  $x^2 + 1$  даже не 6 корней  $(\pm i, \pm j, \pm k)$ , а целая сфера, континуум корней. Здесь проблема не в делителях нуля, а в отсутствии коммутативности.

## 2.3 Формальное и функциональное равенство многочленов

Пусть  $f, g \in R[x]$ . *Формальное равенство* многочленов  $f = g$  — равенство всех коэффициентов — равенство элементов кольца многочленов.

Всякий многочлен определяет полиномиальную функцию вычисления значения.

**Определение 2.3.1** (Функциональное равенство многочленов).  $\tilde{f} = \tilde{g} \stackrel{def}{\iff} \forall c \in R : f(c) = g(c)$ .

**Теорема 2.3.1.** Для бесконечной области целостности  $R$ :

$$f = g \iff \tilde{f} = \tilde{g}$$

*Доказательство.*

$\Rightarrow$ . Очевидно.

$\Leftarrow$ . Если  $\max(\deg f, \deg g) \leq n$ , и  $c_0, \dots, c_n \in R$  — попарно различные точки, то равенство  $\forall i : f(c_i) = g(c_i)$  влечёт равенство  $f = g$ .

В самом деле, разность  $f - g$  имеет степень не больше  $\max(\deg f, \deg g)$ , и обнуляется в  $n + 1$  точке.  $\square$

## 2.4 Задача интерполяции с простыми узлами

Пусть  $K$  — поле,  $c_0, \dots, c_n \in K$  — попарно различные элементы,  $b_0, \dots, b_n \in K$  — произвольные элементы.

**Теорема 2.4.1** (Задача Лагранжа). Существует и единственен многочлен степени не выше  $n + 1$ , решающий интерполяционную задачу с простыми узлами.

$$\begin{array}{c|cccc} x & c_0 & c_1 & \dots & c_n \\ \hline f(x) & b_0 & b_1 & \dots & b_n \end{array}$$

*Доказательство Ньютона — Грегори.* Индукция по  $n$ .  $\square$

*Доказательство Вандермонда.* Запишем систему уравнений относительно  $a_0, \dots, a_n$ .

$$\begin{aligned} f(c_0) &= a_n c_0^n + \dots + a_1 c_0 + a_0 = b_0 \\ &\dots \\ f(c_n) &= a_n c_n^n + \dots + a_1 c_n + a_0 = b_n \end{aligned}$$

Заметим, что так как все  $c_i$  различны, то определитель матрицы данной системы — определитель Вандермонда  $V(c_0, \dots, c_n)$ .

$\prod_{i>j} (c_i - c_j) \neq 0 \Rightarrow$  система имеет единственное решение.  $\square$

*Доказательство.* Решим задачу попроще:

$$\begin{array}{c|ccccc} x & c_0 & \dots & c_i & \dots & c_n \\ \hline f(x) & 0 & \dots & 1 & \dots & 0 \end{array}$$

Её решением будет многочлен

$$f_i = \frac{(x - c_0) \cdot \dots \cdot \widehat{(x - c_i)} \cdot \dots \cdot (x - c_n)}{(c_i - c_0) \cdot \dots \cdot \widehat{(c_i - c_i)} \cdot \dots \cdot (c_i - c_n)}$$

Теперь можно просто взять линейную комбинацию:  $f = \sum_{i=0}^n b_i \cdot f_i$ .  $\square$

## Лекция VIII

15 марта 2023 г.

### 2.5 Локализация или кольца частных

Пусть  $K$  — поле.

Хотим вложить кольцо многочленов  $K[x]$  в какое-то поле  $K(x)$ .

Возьмём любое кольцо  $R$ , построим по нему поле частных  $Q(R)$ . Если  $R$  — область целостности, то всё тривиально, а если есть делители нуля, то чуть сложнее.

#### 2.5.1 Мультипликативные системы

Пусть  $R$  — произвольное коммутативное кольцо с единицей. Строить кольцо частных некоммутативного кольца можно, но намного сложнее.

Рассмотрим произвольное подмножество  $S \subset R$ .

**Определение 2.5.1** ( $S$  — мультипликативная система).

- Аксиома полугруппы:  $S$  замкнуто относительно умножения,  $\forall u, v \in S : uv \in S$ .
- Аксиома моноида:  $1 \in S$ .
- Аксиома нетривиальности:  $0 \notin S$ .

Мы собираемся сопоставить паре  $(R, S)$  кольцо, в котором элементы  $S$  обратимы — кольцо  $S^{-1}R$ .

*Примеры* (Мультипликативные системы).

- $S \leq R^*$  — тривиальная мультипликативная система.
- $S = \text{Reg}(R)$  — множество элементов, на которые можно сокращать. В частности, если  $R$  — область целостности, то  $\text{Reg}(R) = R \setminus \{0\}$ .

- Пусть  $\mathfrak{p} \in \text{Spec}(R)$  — простой идеал:  $\forall xy \in \mathfrak{p} : (x \in \mathfrak{p} \vee y \in \mathfrak{p})$ . Тогда  $R \setminus \mathfrak{p}$  является мультипликативной системой.

В кольце  $(R \setminus \mathfrak{p})^{-1}R$  остался всего один максимальный идеал —  $\mathfrak{p}$ .

- Главная мультипликативная система. Рассмотрим  $s \in R \setminus \text{Nil}(R)$ . Где  $\text{Nil}(R) = \bigcap_{\mathfrak{p} \in \text{Spec}(R)} \mathfrak{p}$   
 $(\text{Nil}(R) = \{x \in R \mid \exists m \in \mathbb{N} : x^m = 0\})$

В качестве множества  $S$  рассмотрим  $\langle 1, s, s^2, \dots \rangle$ . Это аналогично построению кольца десятичных дробей  $\mathbb{Z}[\frac{1}{10}] = \mathbb{Z}[\frac{1}{2}, \frac{1}{5}]$ . Вообще, обращение двух (конечного числа) элементов  $s, t \in R$  равносильно обращению их произведения  $st$ .

## 2.5.2 Построение кольца частных

Обратимся к истокам: как строить дроби из множества  $\mathbb{Q}$ ? Это такие  $\frac{m}{n}$ , что  $n \neq 0$ .  $\frac{m_1}{n_1} = \frac{m_2}{n_2} \iff m_1 n_2 = m_2 n_1$ .

Рассмотрим произведение  $R \times S = \{(u, v) \mid u \in R, v \in S\}$ , где  $S$  — мультипликативная система.

Введём отношение эквивалентности  $(x, u) \sim (y, v)$ , если  $\exists w \in S : (xv - yu)w = 0$ . Напрашивающееся решение  $xv - yu = 0$  не соблюдает корректность: если  $(xv - yu)$  в новом кольце — не 0, то  $w$  нельзя обратить.

**Лемма 2.5.1.**  $\sim$  — отношение эквивалентности.

*Доказательство.* «Всё очевидно, кроме транзитивности. Но транзитивность тоже очевидна»

Пусть  $(x, u) \sim (y, v) \sim (z, w)$ . Тогда  $\exists s, t \in S$ :

$$\left. \begin{array}{l} (xv - yu)s = 0 \\ (yw - zv)t = 0 \end{array} \right\} \begin{array}{l} | \cdot wt \\ | \cdot us \end{array} + \\ (xw - zu)vst = 0$$

□

**Определение 2.5.2** (Кольцо частных  $R$  относительно мультипликативной системы  $S$ ). Так построенное  $S^{-1}R \stackrel{\text{def}}{=} R \times S / \sim$  с операциями, определёнными ниже. Запись  $S^{-1}R$  здесь следует понимать, как неделимый символ.

Пара  $(x, u)$  содержится в классе эквивалентности, обозначаемом  $\frac{x}{u}$ .

Операции определены следующим образом:

- $\frac{x}{u} + \frac{y}{v} = \frac{xv + yu}{uv}$ .
- $\frac{x}{u} \cdot \frac{y}{v} = \frac{xy}{uv}$ .
- $1_{S^{-1}R} = \frac{1}{1}$ .

**Лемма 2.5.2.** Операции определены корректно.

*Доказательство.* Пусть  $\frac{x}{u} = \frac{x'}{u'}$ . Тогда  $\frac{x}{u} + \frac{y}{v} = \frac{x'}{u'} + \frac{y}{v}$ , так как

$$\begin{aligned} \frac{xv + yu}{uv} &= \frac{x'v + yu'}{u'v} \\ (xv + yu) \cdot (u'v) &= (x'v + yu') \cdot (uv) \\ \exists w = (xu' - x'u)w &= 0, \text{ так как } \frac{x}{u} = \frac{x'}{u'} \\ ((xv + yu)u'v - (x'v + yu')uv)w &= 0 \\ (xu' - x'u)v^2w &= 0 \text{ — сошлось} \end{aligned}$$

□

**Теорема 2.5.1.** Эти операции превращают  $S^{-1}R$  в коммутативное кольцо с единицей, и отображение  $\phi_S : R \rightarrow S^{-1}R$ ;  $x \mapsto \frac{x}{1}$  является гомоморфизмом колец. При этом  $\phi_S(S) \subset (S^{-1}R)^*$ .

Гомоморфизм  $\phi_S$  называется *гомоморфизм локализации*.

*Доказательство.* Проверка всех свойств — утомительное занятие, которое приведено не будет.

Если  $x \in S$ , то элемент  $\frac{x}{1}$  действительно обратим, так как  $\frac{x}{1} \cdot \frac{1}{x} = 1_{R^{-1}S}$ . □

### 2.5.3 Универсальное свойство кольца частных

Пусть  $S \subset R$  — мультипликативная система. Определим  $S^{-1}R$ .

Например, найдём гомоморфизм  $\psi : R \rightarrow A$ , где  $A$  — другое коммутативное кольцо с единицей. Если  $\psi(S) \leq A^*$ , то подходящее кольцо частных нашлось.

**Определение 2.5.3** (Кольцо  $S^{-1}R$ ). Коммутативное кольцо с единицей и гомоморфизмом  $\phi_S : R \rightarrow S^{-1}R$ , таким, что  $\phi_S(S) \subset (S^{-1}R)^*$ , обладающее универсальным свойством:  $\forall A$  — коммутативное кольцо с единицей,  $\forall \psi : R \rightarrow A$  — гомоморфизм, такой, что  $\psi(S) \subset A^*$ ,  $\exists!$  гомоморфизм  $\eta : S^{-1}R \rightarrow A$ , делающий диаграмму коммутативной.

$$\begin{array}{ccc} R & \xrightarrow{\phi_S} & S^{-1}R \\ & \searrow \psi & \swarrow \eta \\ & A & \end{array}$$

Таким образом, всякий гомоморфизм  $\psi : R \rightarrow A$  пропускается через кольцо частных.

**Теорема 2.5.2.** Построенное в предыдущем параграфе кольцо дробей действительно обладает универсальным свойством.

*Доказательство.*  $S^{-1}R = \left\{ \frac{x}{u} \mid x \in R, u \in S \right\}$ . Определим гомоморфизм  $\eta : S^{-1}R \rightarrow A$  как  $\eta\left(\frac{x}{u}\right) = \psi(x)\psi(u)^{-1}$ .

Проверим, что он определён корректно:

$$\frac{x}{u} = \frac{y}{v} \iff \exists w \in S : (xv - yu)w = 0 \Rightarrow (\psi(x)\psi(v) - \psi(y)\psi(u))\psi(w) = 0$$

На  $\psi(w)$  можно сократить, получаем что надо:

$$\psi(x)\psi(y)^{-1} = \psi(u)\psi(v)^{-1}$$

Проверим, что  $\eta$  — гомоморфизм.

$$\begin{aligned} \eta\left(\frac{x}{u} + \frac{y}{v}\right) &= \eta\left(\frac{xv + yu}{uv}\right) = \\ &= (\psi(x)\psi(v) + \psi(y)\psi(u))\psi(u)^{-1}\psi(v)^{-1} = \psi(x)\psi(u)^{-1} + \psi(y)\psi(v)^{-1} = \eta\left(\frac{x}{u}\right) + \eta\left(\frac{y}{v}\right) \end{aligned}$$

Осталось проверить единственность: возьмём любой гомоморфизм  $\eta'$ , делающий диаграмму коммутативной. Почему он равен  $\eta$ ?

Так как диаграмма коммутативна, то  $\eta'(\psi_S(x)) = \psi(x)$ , то есть  $\eta'\left(\frac{x}{1}\right) = \psi(x)$ .

Проверим совпадение  $\eta = \eta'$  для дроби  $\frac{x}{u}$ . Так как  $\psi(u) \in A^*$ , то  $\psi(x) = \eta'\left(\frac{x}{1}\right) = \eta'\left(\frac{x}{u}\right) \cdot \eta'\left(\frac{u}{1}\right) = \eta'\left(\frac{x}{u}\right)\psi(u)$ . Сократив на  $\psi(u)$  (оно обратимо в  $A$ ), действительно получаем  $\eta'\left(\frac{x}{u}\right) = \psi(x)\psi(u)^{-1}$ . Значит,  $\eta'$  действительно совпадает с  $\eta$ . □

*Замечание.* Воспользовавшись универсальным свойством, нетривиально (но можно, переходя к пределам в теории категорий) доказать, что кольцо частных существует. Но мы уже его построили в предыдущем параграфе, поэтому оно несомненно существует.

## 2.5.4 Кольцо частных в терминах элементов

**Определение 2.5.4** (Кольцо  $S^{-1}R$ ).  $S^{-1}R$  — кольцо вместе с гомоморфизмом  $\phi_S : R \rightarrow S^{-1}R$ , таким, что

1.  $\phi_S(S) \subset (S^{-1}R)^*$ .
2.  $\forall y \in S^{-1}R$  представим в виде  $y = \phi_S(x)\phi_S(u)^{-1}$ , где  $x \in R, u \in S$ .
3. Если  $\phi_S(x) = 0$ , то  $\exists u \in S : xu = 0$ .

**Теорема 2.5.3.** Построенное кольцо  $S^{-1}R$  (определение 2.5.2) обладает этими свойствами. Любое кольцо  $A$  с гомоморфизмом  $\psi : R \rightarrow A$ , обладающее этими свойствами, изоморфно  $S^{-1}R$ :

1.  $\psi(S) \leq A^*$
2.  $\forall y \in A, y = \psi(x)\psi(u)^{-1}$
3.  $\psi(x) = 0 \iff \exists u \in S : xu = 0$ .

## 2.5.5 Примеры колец частных

*Примеры.*

- $S \leq R^*$  — тривиальная мультипликативная система.  $S^{-1}R = R$ .
- $S = \text{Reg}(R)$ . В таком случае  $S^{-1}R = Q(R)$  — полное кольцо частных. Здесь выполнено вложение  $R \hookrightarrow Q(R)$ . Если  $R$  — область целостности, то  $\text{Reg}(R) = R \setminus \{0\}$ , тогда  $Q(R)$  — поле, *поле частных*.

Примеры полей частных:  $Q(\mathbb{Z}) = \mathbb{Q}$ ,  $Q(\mathbb{Z}[i]) = \mathbb{Q}[i]$ ,  $Q(K[x]) = K(x)$ ,  $Q(K[[x]]) = K((x))$ .

# Лекция IX

18 марта 2023 г.

Любое конечное число главных локализаций представимо в виде одной локализации — по их произведению: Если Любая локализация — предел главных локализаций. Здесь должно быть больше информации на эту тему.

## 2.6 Поле частных факториального кольца

$R$  — UFD,  $K = Q(R) = \left\{ \frac{x}{y} \mid x, y \in R, y \neq 0 \right\}$ .

**Теорема 2.6.1.** Всякий элемент  $Q(R)$  допускает представление в виде

$$up_1^{m_1} \cdot \dots \cdot p_s^{m_s}, \quad m_i \in \mathbb{Z}$$

в единственном виде, где  $p_i$  — попарно неассоциированные неприводимые элементы.

*Доказательство.*  $v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y)$ . □

$p$ -адические показатели обладают обычными свойствами:

1.  $v_p\left(\frac{x}{y} \cdot \frac{z}{w}\right) = v_p\left(\frac{x}{y}\right) + v_p\left(\frac{z}{w}\right)$ .
2.  $v_p\left(\frac{x}{y} + \frac{z}{w}\right) \geq \min\left(v_p\left(\frac{x}{y}\right) + v_p\left(\frac{z}{w}\right)\right)$ .

Любопытно заметить, что  $R = \{x \in Q(R) \mid \forall p \in \text{Irr}(R) : v_p(x) \geq 0\}$ .

---

Пусть  $R \hookrightarrow A$ .

**Определение 2.6.1** ( $x \in A$  — целое над  $R$ ).  $x$  — корень многочлена  $f \in \mathbb{R}[t]$ , такого, что старший коэффициент  $\text{lc}(f) = 1$ . Наименьшая степень  $f$ , имеющего своим корнем  $x$ , называется *степенью*  $x$ .

*Интересный факт.* Множество целых над  $R$  образует кольцо.

Есть доказательство через тензорное произведение (сумму), есть — через симметрические многочлены и кронекеровское произведение (сумму).

В частности,  $\mathbb{A}$  — целые алгебраические числа над  $\mathbb{Z}$  (а просто алгебраические числа можно обозначить  $\overline{\mathbb{Q}}$ ).

**Определение 2.6.2** (Целозамкнутое кольцо  $R$ ). Любой элемент  $x \in Q(R)$ , являющийся целым над  $R$ , принадлежит  $R$ .

**Лемма 2.6.1** (Лемма Гаусса).  $R$  —  $UFD \Rightarrow R$  — целозамкнуто. В частности, кольцо  $\mathbb{Z}$  целозамкнуто, то есть  $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$ .

*Доказательство.* Пусть  $\frac{x}{y}$  — корень  $f \in R[t]$ . Можно считать, что  $x$  и  $y$  взаимно просты — иначе на общий множитель можно сократить.

$$\left(\frac{x}{y}\right)^n + a_{n-1} \left(\frac{x}{y}\right)^{n-1} + \dots + a_1 \left(\frac{x}{y}\right) + a_0 = 0$$

Умножив на  $y^n$ , получим равенство в  $R$ :

$$x^n + a_{n-1}x^{n-1}y + \dots + a_1xy^{n-1} + a_0y^n = 0$$

Рассмотрим любой неприводимый  $p \mid y$ . Он делит все слагаемые, кроме первого, значит, делит первое слагаемое тоже (типичное рассуждение).

Значит,  $y \in R^*$ , значит,  $\frac{x}{y} \in R$ . □

## 2.7 Рациональные дроби

Рассмотрим кольцо многочленов над полем  $K$ .

Оно является областью целостности ( $\deg(f \cdot g) = \deg f + \deg g$ ), значит, определено  $Q(K[t]) = K(t)$  — *поле рациональных дробей* над  $K$ . Часто его также называют полем рациональных функций. Тем не менее, элементы,  $K(t)$  вообще говоря, функциями не являются, например, потому что многие нетривиальные функции не определены на  $K$ .

А именно,  $f \in K[t] \rightsquigarrow (\tilde{f} : K \rightarrow K)$ . Это единственный гомоморфизм из  $K[t]$  в  $K$ , и согласованно определить аналогичный гомоморфизм на  $K(t)$  не представляется возможным. При сложении двух функций  $\frac{f}{g} \in K(t) \rightsquigarrow \left(\tilde{\frac{f}{g}} : c \mapsto \frac{f(c)}{g(c)}\right)$  их области определения пересекаются. Решением матанализа является рассматривать рациональные функции, как частичные — определённые не везде.

Ещё проблемой является вопрос — равны ли рациональные «функции»  $\frac{1}{t}$  и  $\frac{t-1}{t(t-1)}$ ? Можно говорить о равенстве в любой окрестности, которая может быть открыта как в стандартном смысле, так и в топологии Зарисского. В таком случае разные рациональные функции (например,  $\frac{1}{t}$  и  $\frac{t-1}{t(t-1)}$ ) объединяются в классы эквивалентности — *ростки функций*.

Ещё можно определить функции на одноточечной компактификации  $K$ , в народе называющейся

сферой Римана — проективной прямой  $\mathbb{P}^1(K) = K \cup \{\infty\}$ . В таком случае  $\frac{f}{g}(\infty) = \begin{cases} 0, & \deg(f) < \deg(g) \\ \infty, & \deg(f) > \deg(g) \\ \frac{\text{lc}(f)}{\text{lc}(g)}, & \deg(f) = \deg(g) \end{cases}$ .

В точках же  $c \in K$ , таких, что  $(x - c)^{m_1} \parallel f, (x - c)^{m_2} \parallel g$  и  $m_2 > m_1$ ,  $\frac{f}{g}(c) = \infty$  по определению.

**Определение 2.7.1** (Степень рациональной функции).  $\deg\left(\frac{f}{g}\right) = \deg f - \deg g$ .

**Определение 2.7.2** (Полуправильная дробь  $\frac{f}{g} \in K(t)$ ).  $\deg\left(\frac{f}{g}\right) \leq 0$ .

**Определение 2.7.3** (Правильная дробь  $\frac{f}{g} \in K(t)$ ).  $\deg\left(\frac{f}{g}\right) < 0$ .

**Лемма 2.7.1.** Степень удовлетворяет обычным условиям:  $\forall \alpha, \beta \in K(t)$ :

- $\deg(\alpha \cdot \beta) = \deg(\alpha) + \deg(\beta)$ .
- $\deg(\alpha + \beta) \leq \max(\deg(\alpha), \deg(\beta))$ .

**Следствие 2.7.1.** Правильные и полуправильные дроби образуют подкольцо (правильные — кольцо без единицы).

**Теорема 2.7.1.** Пусть  $\alpha \in K(t)$ . Для любого представления  $\alpha = \frac{f}{g}$  допускается единственное представление в виде  $\frac{f}{g} = q + \frac{r}{g}$ , где  $q \in K[t]$ ,  $\frac{r}{g}$  — правильная рациональная дробь.

Более того, для любого такого представления многочлен  $r$  один и тот же.

*Доказательство.* Запись эквивалентна  $f = qg + r$  ( $q, r \in K[t]$ ,  $\deg r < \deg g$ ), а такое представление единственно, так как деление с остатком в  $K[t]$  даёт единственный результат.

Единственность  $r$  следует от противного:  $\frac{f_1}{g_1} + r_1 = \frac{f_2}{g_2} \Rightarrow \underbrace{\frac{f_1}{g_1} - \frac{f_2}{g_2}}_{\text{правильная дробь}} = \underbrace{r_2 - r_1}_{\text{многочлен}}$ . Равенство

наступает только если  $r_1 - r_2 = 0$  □

**Определение 2.7.4** (Запись  $\frac{f}{g}$  несократима).  $f \perp g$ .

## 2.8 Разложение на простейшие дроби

Предположим, что мы в XVIII веке ищем интеграл  $\int \frac{f(x)}{g(x)} dx$ .

**Определение 2.8.1** (Примарная дробь  $\frac{f}{g} \in K(t)$ ).  $g = p^m$  для  $p \in \text{Irr}(K[t])$  и  $\deg f < \deg g$ .

**Определение 2.8.2** (Простейшая дробь  $\frac{f}{g} \in K(t)$ ). Примарная дробь, такая, что  $\deg f < \deg p$ .

В частности, простейшими дробями являются  $\frac{x^i}{p^m}$  для  $0 \leq i < \deg p$ .

**Теорема 2.8.1.** Любая рациональная дробь допускает единственное представление в виде суммы многочлена и простейших дробей с различными знаменателями.

*Доказательство.*

- Выделим целую (полиномиальную) часть. Отныне считаем, что  $\frac{f}{g}$  — правильная.
- Если  $g \perp h$  и  $\deg gh > \deg f$  то  $\frac{f}{gh}$  представима, как сумма правильных дробей  $\frac{f_1}{g} + \frac{f_2}{h}$ :

Так как  $K[t]$  — PID, то  $g$  и  $h$  — комаксимальны:  $gK[t] + hK[t] = K[t]$ , то есть  $\exists u, v \in K[t] : gu + hv = 1$ . Получаем

$$\frac{f}{gh} = \frac{fgu}{gh} + \frac{fhv}{gh} = \frac{fu}{h} + \frac{fv}{g}$$

Поделим  $fv$  на  $g$  с остатком:  $fv = qg + r$ . Равенство переписывается в виде  $\frac{f}{gh} = \left(\frac{fu}{h} + q\right) + \frac{r}{g}$ . В скобках стоит правильная дробь, как разность двух правильных дробей.

Получили разложение на правильные дроби.

Применив для  $g = p_1^{m_1} \cdot \dots \cdot p_s^{m_s}$ , получаем разложение на примарные дроби.

- Покажем, что примарная дробь есть сумма простейших:

Рассмотрим примарную дробь  $\frac{f}{p^m}$ . Поделим  $f$  на  $p$  с остатком:  $f = qp + r$ .

$$\frac{f}{p^m} = \frac{qp + r}{p^m} = \frac{q}{p^{m-1}} + \frac{r}{p^m}$$

Первая дробь по индукции разложима на простейшие, вторая — уже простейшая.

- Единственность разложения: если представление не единственно, то существует нетривиальная линейная зависимость:

$$\sum_{i,j} \frac{f_{i,j}}{p_i^j} = 0$$

где  $\deg(f_{i,j}) < \deg(p_i)$ ,  $p_i$  — неприводимые многочлены.

Сконцентрируемся на  $p_n$ . Пусть суммирование для  $i = n$  идёт по  $j = 1..m$ . Разобьём сумму:

$$- \sum_{i \neq n, j} \frac{f_{i,j}}{p_i^j} - \sum_{j < m} \frac{f_{n,j}}{p_n^j} = \frac{f_{n,m}}{p_n^m}$$

Посчитаем  $p_n$ -адический показатель обеих частей, получим противоречие:  $\geq m_1 + 1 / = m_1$ .  $\square$

**Следствие 2.8.1.** Базис кольца многочленов счётен —  $1, t, t^2, \dots$ .

Базис кольца рациональных дробей  $K(t)$  счётен только если  $K$  не более, чем счётно. А именно, это  $\{t^i \mid i \in \mathbb{N}_0\} \cup \left\{ \frac{t^i}{p^m} \mid 0 \leq i < \deg p, p - \text{нормированный} \right\}$ .

С аксиомой выбора это эквивалентно тому, что базис  $K(t)$  равномошен  $K$  для бесконечного  $K$ .

*Пример.* Над  $\mathbb{C}$  любой неприводимый нормированный многочлен — это  $x - c$  для  $c \in \mathbb{C}$ . Базис правильных дробей получается  $\left\{ \frac{1}{(x-c)^m} \mid m \in \mathbb{N} \right\}$ .

## 2.9 Факториальность кольца многочленов

**Теорема 2.9.2** (Теорема Гаусса).  $R - \text{UFD} \Rightarrow R[t] - \text{UFD}$ .

### 2.9.1 Примитивные многочлены

Пусть  $f \in R[t]$ ,  $f = a_n x^n + \dots + a_1 x + a_0$ .

**Определение 2.9.1** (Содержание многочлена  $f$ ).  $\text{Cont}(f) \stackrel{\text{def}}{=} \gcd(a_n, \dots, a_0)$ .

**Определение 2.9.2** (Примитивный многочлен  $f$ ).  $\text{Cont}(f) = 1$ .

**Определение 2.9.3** (Сильно примитивный многочлен  $f$ ).  $a_0, a_1, \dots, a_n$  — комаксимальны (возможно,  $a_1, \dots, a_n$  комаксимальны, я не справился узнать, где правда).

**Лемма 2.9.1.** Всякий многочлен представим в виде произведения его содержания и примитивного многочлена.

**Лемма 2.9.2.** Если  $af \sim bg$ , где  $a, b \in R \setminus \{0\}$ ,  $f, g \in R[t]$  — примитивные многочлены, то  $a \sim b, f \sim g$ .

*Доказательство.*  $af \cdot u = bg$ , где  $u \in (R[t])^* = R^*$ . Отсюда степени многочленов равны. Пусть  $f = a_n x^n + \dots + a_0$ ;  $g = b_n x^n + \dots + b_0$ .

$$a \gcd(a_n, \dots, a_0) = \gcd(aa_n, \dots, aa_0) = \gcd(bb_n, \dots, bb_0) = b \gcd(b_n, \dots, b_0)$$

откуда  $a \sim b$ . Отсюда  $f \sim g$ .  $\square$



**Лемма 2.9.3** (Лемма Гаусса). Если  $f, g \in R[t]$  — примитивные многочлены, то  $f \sim g$  в  $R[t] \iff f \sim g$  в  $K[t]$ .

*Доказательство.*  $f \sim g$  в  $K[t] \Rightarrow (\frac{a}{b})f = g \Rightarrow af = bg$ . По предыдущей лемме  $f \sim g$ .  $\square$

**Лемма 2.9.4** (Лемма Гаусса).  $\forall f, g \in R[t] : \forall p \in \text{Irr}(R) : v_p(fg) = v_p(f) + v_p(g)$  где  $v_p(f) = \min(v_p(a_0), \dots, v_p(a_n))$ .

В частности,  $\text{Cont}(f \cdot g) = \text{Cont}(f) \cdot \text{Cont}(g)$ .

В частности, примитивные многочлены образуют мультипликативную систему.

*Доказательство.* Введём  $r$  — наименьший номер, такой, что  $p^{v_p(f)+1} \nmid a_r$  и  $s$  — наименьший номер, такой, что  $p^{v_p(g)+1} \nmid b_s$ .

Рассмотрим  $f \cdot g$ , а именно, его коэффициент при  $t^{r+s}$ . Это

$$\underbrace{a_{r+s}b_0 + \dots + a_r b_s}_{\vdots p^{v_p(f)+v_p(g)+1}} + \underbrace{\dots + a_0 b_{r+s}}_{\vdots p^{v_p(f)+v_p(g)+1}}$$

Но средний коэффициент делится **точно** на  $p^{v_p(f)+v_p(g)}$ , значит,  $v_p(f \cdot g) \leq v_p(f) + v_p(g)$ . (Оценка снизу очевидна)  $\square$

Пусть  $R$  — UFD,  $K = Q(R)$ .

**Теорема 2.9.1** (Теорема Гаусса). Для всякого  $f \in R[t] : f \in \text{Irr}(R[t]) \Rightarrow f \in \text{Irr}(K[t])$ .

*Доказательство.* Пусть  $f = gh$  в  $K[t]$ . Запишем

$$g = \frac{a_m}{b_m} t^m + \dots + \frac{a_0}{b_0}; \quad h = \frac{c_n}{d_n} t^n + \dots + \frac{c_0}{d_0}$$

где  $a_i, c_i \in R; b_i, d_i \in R \setminus \{0\}$ . Обозначим  $B = \prod b_i, D = \prod d_i$ . Получаем

$$BD \cdot f = Bg \cdot Dh = \text{Cont}(Bg) \cdot \text{Cont}(Dh) \cdot \tilde{g} \cdot \tilde{h}, \quad \text{где} \begin{cases} \tilde{g} = Bg/\text{Cont}(Bg) \\ \tilde{h} = Dh/\text{Cont}(Dh) \end{cases}$$

Согласно предыдущей лемме  $\tilde{g} \cdot \tilde{h}$  тоже неприводимый, а ещё тогда  $f \sim \tilde{g} \cdot \tilde{h}$  в  $R[t]$  ( $f$  неприводим по условию теоремы). Так как  $f$  неприводим, то  $\deg g = 0$  или  $\deg h = 0$ , то есть  $f$  неприводим и в  $K[t]$ .  $\square$

**Следствие 2.9.1.** Для всякого примитивного  $f \in R[t] : f \in \text{Irr}(R[t]) \iff f \in \text{Irr}(K[t])$ .

*Замечание.* Обратное следствие неверно для не примитивных многочленов:  $2x - 2 \in \mathbb{Z}[x]$  не является неприводимым, но  $2x - 2 \in \mathbb{Q}[t]$  — неприводимый элемент.

## 2.9.2 Теорема Гаусса

**Теорема 2.9.2** (Теорема Гаусса).  $R$  — UFD  $\Rightarrow R[t]$  — UFD.

*Доказательство.* Воспользуемся тем, что и  $R$  факториально, и  $K[t]$  факториально, где  $K = Q(R)$ .

$f = \text{Cont}(f) \cdot \tilde{f}$ . Разложим  $\text{Cont}(f)$  внутри UFD  $R$ .

Если  $\tilde{f}$  разложим над  $K[t]$ , то он разложим и над  $R[t]$  (теорема 2.9.1).

Так как кольцо  $K[t]$  нётерово, то процесс оборвётся, значит получили разложение  $f = up_1 \cdot \dots \cdot p_r q_1 \cdot \dots \cdot q_s$ , где  $u \in R^*, p_i \in \text{Irr}(R), q_j \in \text{Irr}(R[t])$ .

Единственность доказывается следующим образом:

$$\begin{aligned} up_1 \cdot \dots \cdot p_r q_1 \cdot \dots \cdot q_s &\sim u'p'_1 \cdot \dots \cdot p'_r q'_1 \cdot \dots \cdot q'_s \\ &\Downarrow \\ up_1 \cdot \dots \cdot p_r &\sim u'p'_1 \cdot \dots \cdot p'_r \\ q_1 \cdot \dots \cdot q_s &\sim q'_1 \cdot \dots \cdot q'_s \end{aligned}$$

$R$  факториально, поэтому первые разложения совпадают. Вторые разложения — разложения и в  $K[t]$ , поэтому они ассоциированы в  $K$  ( $K[t]$  UFD, так как это евклидово кольцо, то есть PID). Но согласно лемме Гаусса они ассоциированы и в  $R$ .  $\square$

**Следствие 2.9.2.**

- $K[t_1, \dots, t_n] — UFD$
- $\mathbb{Z}[t_1, \dots, t_n] — UFD$

## Лекция X

28 марта 2023 г.

### 2.10 Дифференцирование алгебр

Пусть  $R$  — коммутативное кольцо с единицей,  $A$  — алгебра над  $R$ .

**Определение 2.10.1** (Дифференцирование). Отображение  $D : A \rightarrow A$ , являющееся аддитивным, и удовлетворяющее *тождеству Лейбница*

$$D(xy) = Dx \cdot y + x \cdot Dy$$

$D$  называется  *$R$ -дифференцированием*, если, кроме того, оно согласовано с умножением на элемент  $R$ :  $D(\lambda x) = \lambda Dx$ .

Множество всех дифференцирований алгебры  $A$  обозначается  $\text{Der}(A)$ , множество  $R$ -дифференцирований —  $\text{Der}_R(A)$ .

**Определение 2.10.2** (Константа дифференцирования  $D$ ). Элемент  $x \in A : Dx = 0$ .

*Замечание.* Аксиома  $R$ -дифференцирования — о согласованности с домножением на элемент  $R$  — утверждает, что все элементы  $R$  — константы при вложении в  $A$ .

**Лемма 2.10.1.** Константы дифференцирования образуют подкольцо с единицей в  $R$ .

*Доказательство.* Замкнутость относительно сложения и умножения;  $D(1 \cdot 1) = D(1) \cdot 1 + 1 \cdot D(1) \Rightarrow D(1) = 0$   $\square$

**Факт 2.10.1.** Любое дифференцирование полностью определяется своими значениями на какой-то системе образующих  $x_1, \dots, x_n$  алгебры  $A$  над  $R$ .

*Доказательство.* Пусть  $\forall x_i : D_1(x_i) = D_2(x_i)$ . Введём  $D := D_1 - D_2$ .  $D(x_i) = 0$ , так как  $x_i$  — система образующих, то  $\text{Ker } D = A$ .  $\square$

*Примеры.*

$\infty$ .  $C^{(\infty)}(\mathbb{R})$  — множество бесконечно дифференцируемых функций.  $\frac{d}{dx}$  — дифференцирование.

- Внутреннее дифференцирование: для какого-то  $a \in A$ :

$$d_a : A \rightarrow A; \quad x \mapsto [a, x] = ax - xa$$

## 2.10.1 Операции над дифференцированиями

1. Сумма:  $D_1 + D_2$  является дифференцированием.
2. Домножение на скаляр:  $\forall \lambda \in R : \lambda D$  является дифференцированием.
- 1. Произведение дифференцирований дифференцированием, вообще говоря не является: квадрат дифференцирования, например, не удовлетворяет тождеству Лейбница:  $(fg)'' = f''g + 2f'g' + fg'' \neq f'g + fg'$ . Вторая производная является дифференцированием только в кольце характеристики 2.
3. Коммутирование:  $D_1, D_2 \in \text{Der}_R(A) \mapsto D_1D_2 - D_2D_1 = [D_1, D_2] \in \text{Der}_R(A)$ .

*Доказательство.*

$$\begin{aligned} [D_1, D_2](xy) &= D_1(D_2(xy)) - D_2(D_1(xy)) = \\ &= D_1(D_2x \cdot y + x \cdot D_2y) - D_2(D_1x \cdot y + x \cdot D_1y) = \\ &= [D_1, D_2]x \cdot y + x \cdot [D_1, D_2]y \end{aligned}$$

□

**Теорема 2.10.1.** Для любой (не предполагается ассоциативность) алгебры  $A$ :  $\text{Der}_R(A)$  является алгеброй Ли над  $R$  относительно суммы и коммутирования.

Тождества алгебры Ли  $(+, [\cdot, \cdot])$ :

1.  $[x_1 + x_2, y] = [x_1, y] + [x_2, y]$ .
2.  $[x, y_1 + y_2] = [x, y_1] + [x, y_2]$ .
3.  $[\lambda x, y] = \lambda[x, y] = [x, \lambda y]$ .
4.  $[x, x] = 0$  — тождество антикоммутативности.
5.  $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$  — тождество Якоби.

## 2.10.2 Дифференцирование кольца многочленов, теорема Лейбница — Бернулли

Рассматриваем  $R$ -алгебру  $R[x]$ .

**Определение 2.10.3** (Формальная производная многочлена). Для многочлена  $f = a_n x^n + \dots + a_1 x + a_0$  ( $a_i \in R$ ) это многочлен  $f' = na_n x^{n-1} + \dots + a_1$ .

Операция взятия производной часто обозначается  $\frac{d}{dx} : R[x] \rightarrow R[x], f \mapsto f'$ .

**Теорема 2.10.2** (Лейбниц — Бернулли).  $\text{Der}_R(R[x]) = R[x] \cdot \frac{d}{dx}$ . Иными словами, для любого дифференцирования  $D$  существует многочлен  $h \in R[x]$ , такой, что  $D \equiv h \cdot \frac{d}{dx}$ .

*Доказательство.*

- Эта формула задаёт дифференцирование:

В силу  $R$ -линейности достаточно проверять на стандартных мономах.

$$\begin{aligned} D(x^m \cdot x^n) &= D(x^{m+n}) = h(x) \cdot (m+n)x^{m+n-1} \\ D(x^m \cdot x^n) &= D(x^m)x^n + x^m D(x^n) = h(x)mx^{m-1} + x^m h(x)nx^{n-1} = h(x) \cdot (m+n)x^{m+n-1} \end{aligned}$$

- Пусть  $D \in \text{Der}_R(R[x])$ . Тогда  $D$  полностью определяется значением на какой-то системе образующих алгебры, например, на элементе  $x$ . Пусть  $Dx = h, h \in R[x]$ . В силу линейности достаточно доказать, что  $D = h \cdot \frac{d}{dx}$  только на стандартных мономах.

Это верно, так как для  $f_1, \dots, f_n : D(f_1 \cdot \dots \cdot f_n) = D(f_1)f_2 \cdot \dots \cdot f_n + \dots + f_1 \cdot \dots \cdot f_{n-1}D(f_n)$ . В частности, для коммутирующих  $f$  и  $Df$ :  $D(f^n) = n f^{n-1} \cdot Df$ . □

*Свойства* (Свойства производной).

- $D(f \circ g) = (Df \circ g) \cdot D(g)$ .
- Тожество для дифференцирований высших порядков:  $f'' = (f')'$ ,  $f''' = (f'')'$ ,  $(f \cdot g)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(k)} g^{(n-k)}$ .
- Формула Фаа ди Бруно:

$$D^n(f \circ g) = \sum \frac{n!}{m_1! 1!^{m_1} \cdot \dots \cdot m_n! n!^{m_n}} D^{(m_1 + \dots + m_n)}(f \circ g) \cdot \prod_{j=1}^n (D^j g)^{m_j}$$

где сумма берётся по всем таким  $m_1, \dots, m_n$ , что  $m_1 \cdot 1 + \dots + m_n \cdot n = n$ .

- $D(g^{-1}) = -g^{-1} \cdot Dg \cdot g^{-1}$ . Для коммутативного кольца, например,  $K(x) : \left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$ .

**Теорема 2.10.3.** Константы дифференцирования  $K[x]$  у  $\frac{d}{dx}$  — это  $K[x^p]$ , где  $p = \text{char}(K)$ .

## 2.11 Алгебраические и трансцендентные элементы; минимальный многочлен

Пусть  $K$  — поле,  $A$  — необязательно коммутативная  $K$ -алгебра.

Гомоморфизм эвалюации определён  $\forall c \in A : \text{ev}_c : K[x] \rightarrow A, f \mapsto f(c)$ .

У гомоморфизма есть ядро  $\text{Ker}(\text{ev}_c) \trianglelefteq K[x]$ .

- Либо  $\text{Ker}(\text{ev}_c) = \{0\}$ . В таком случае  $c \in A$  — *трансцендентный* над  $K$  элемент.
- Либо  $\text{Ker}(\text{ev}_c) \neq \{0\}$ . В таком случае  $c \in A$  — *алгебраический* над  $K$  элемент.

**Определение 2.11.1** (Минимальный многочлен для  $c \in A$ ). Многочлен  $\theta_c$ , порождающий  $\text{Ker}(\text{ev}_c)$

Все многочлены из ядра  $\text{Ker}(\text{ev}_c)$  называются *аннулирующими*. Так как  $K[x]$  — PID, то минимальный многочлен существует (и все аннулирующие многочлены делятся на минимальный).

**Определение 2.11.2** (Степень элемента  $c$  над  $K$ ). Степень  $\deg \theta_c$ .

**Теорема 2.11.1.**

- Если  $c$  — трансцендентный над  $K$ , то  $K[c] \cong K[x]$ .
- Если  $c$  — алгебраический над  $K$ , то  $K[c] \cong K[x]/(K[x]\theta_c)$  — векторное пространство над  $K$  размерности  $n := \deg \theta_c$ .

$$K[c] = \{a_0 + a_1c + \dots + a_{n-1}c^{n-1} + K[x]\theta_c \mid a_i \in K\}$$

*Доказательство.* Теорема о ядре и образе для  $\text{ev}_c$ . □

*Замечание.*  $K[c]$  — наименьшая  $K$ -подалгебра, содержащая  $c$ .

### 2.11.1 Что можно сказать, если $A$ — область целостности?

$\text{ev}_c : K[x] \rightarrow A$  — область целостности. Если  $c$  — алгебраическое, то  $K[x]/K[x]\theta_c \cong K[c] \trianglelefteq A$ .

Таким образом,  $\theta_c$  неприводим в  $K[x]$ : если  $\theta_c = \phi \cdot \psi$ , то  $\bar{\phi}$ , равно как и  $\bar{\psi}$  — делители нуля в  $K[x]/K[x]\theta_c$ .

Обозначим поле частных  $K[c]$  как  $K(c) \stackrel{\text{def}}{=} Q(K[c]) \leq Q(A)$ .

**Теорема 2.11.2.** Если  $c$  трансцендентно, то  $K(c) \cong K(x)$ . Если  $c$  алгебраическое, то  $K(c) = K[c]$ .

*Доказательство.*

- Часть про трансцендентность очевидна, так как  $K[c] \cong K[x]$ .
- Необходимо проверить, что  $K[c]$  — поле. Это верно, так как  $K[x]$  — PID, значит, идеал, порождённый неприводимым многочленом, максимален.  $\square$

## Глава 3

# Канонические формы линейных операторов

1. Конечные задачи: Рассмотрим линейное отображение  $\phi : U \rightarrow V$  из первой главы. Его канонической формой является матрица  $\left( \begin{array}{c|c} e & 0 \\ \hline 0 & 0 \end{array} \right)$  при правильном выборе базиса в  $U$  и в  $V$ . Все инварианты, возникавшие здесь, имели дискретную природу — размерность и ранг.
2. Ручные задачи: Сейчас мы рассмотрим более сложную задачу: каноническая форма линейного оператора  $\phi : U \rightarrow U$ . Трудность состоит в том, что матрицу хочется выбрать так, чтобы базисы в  $U$  слева и справа совпадали. Здесь будут возникать непрерывные инварианты.
3. Дикие задачи: классификация пар линейных операторов  $\phi, \psi : U \rightarrow U$ . Ответ на ту задачу не найден, и, по-видимому, не будет получен, так как он позволяет классифицировать слишком много всего.

### 3.1 Инвариантные подпространства

Рассмотрим линейный оператор над полем  $K$ :  $\phi : V \rightarrow V$  ( $\phi \in \text{End}_K(V)$ ).

**Определение 3.1.1** ( $\phi$ -инвариантное подпространство  $U \leq V$ ). Такое подпространство, что  $\phi(U) \subset U$ .

$\phi$  можно ограничить на любом  $\phi$ -инвариантном подпространстве  $U$ .

*Примеры.*

- Тривиальное ( $\{0\}$ ) и несобственное ( $V$ ) подпространства инвариантны для любого оператора.
- Движение пространства  $\mathbb{R}^3$  с неподвижной точкой  $0$  — поворот (и, возможно, отражение). Ось вращения и ортогональная ей плоскость поворота инвариантны.
- $K[x]_{\leq n}$  для любого  $n \in \mathbb{N}$  инвариантно для оператора дифференцирования  $\frac{d}{dx}$ .
- Оператор сдвига бесконечномерного пространства: пусть базис пронумерован целыми числами  $\dots, u_{-1}, u_0, u_1, \dots$ . Тогда оператор сдвига определён на базисе  $\phi(u_i) = u_{i+1}$ . У него нет инвариантных подпространств, а если бы было  $\phi(u_i) = u_{i+2}$ , то были бы только бесконечномерные.

Пусть  $\dim V < \infty$ ,  $\phi \in \text{End}_K(V)$ ,  $\phi(U) \subset U$ .

**Теорема 3.1.1.** В подходящем базисе  $\phi$  имеет матрицу  $\left( \begin{array}{c|c} [\phi|_U] & * \\ \hline 0 & [\phi|_{V/U}] \end{array} \right)$

*Доказательство.*  $\phi|_{V/U} : V/U \rightarrow V/U$  определено корректно:  $\phi(v + U) = \phi(v) + U$ .

Выберем в качестве базиса произвольный базис  $U = (v_1, \dots, v_m)$ , а потом дополним его до базиса всего пространства  $(v_{m+1}, \dots, v_n)$ .

В этом базисе матрица действительно имеет такой вид.  $v_{m+1} + U, \dots, v_n + U$  — базис  $V/U$ .  $\square$

**Определение 3.1.2** (Инвариантное дополнение  $\phi$ -инвариантного пространства  $U \leq V$ ). Такое подпространство  $W \leq V$ , что оно тоже  $\phi$ -инвариантно, причём  $V = U \oplus W$ .

**Теорема 3.1.2** (Случай полной приводимости). Если  $U$  имеет инвариантное дополнение  $W$ , то в подходящем базисе  $[\phi] = \left( \begin{array}{c|c} [\phi|_U] & 0 \\ \hline 0 & [\phi|_W] \end{array} \right)$ .

*Доказательство.* Выберем в качестве базисов объединение базисов  $U$  и  $W$ .  $\square$

## 3.2 Собственные подпространства. Собственные числа

Собственные подпространства инвариантны, но, к сожалению, инвариантно не дополняемы.

Считаем, что  $K$  — поле,  $\dim_K(V) < \infty$ .

**Определение 3.2.1** (Собственный вектор оператора  $\phi$ ). Такой вектор  $v \in V$ , что  $\langle v \rangle = vK$  инвариантно относительно  $\phi$ . Иными словами,  $\phi(v) = v\lambda$  для некоего  $\lambda \in K$ .

**Определение 3.2.2** (Собственное число оператора  $\phi$ ). Такое число  $\lambda \in K$ , что существует  $v \in V$ , такой, что  $\phi(v) = v\lambda$ .

*Примеры.*

- Если  $[\phi] = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$  в некотором базисе  $(v_1, \dots, v_n)$ , то  $v_1, \dots, v_n$  — собственные векторы с соответственно собственными числами  $\lambda_1, \dots, \lambda_n$ . Оператор простой структуры или диагонализуемый оператор.
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  имеет собственные числа 1 и  $-1$  — для векторов  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  и  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  соответственно.
- $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$  не имеет собственных чисел, как оператор над полем  $\mathbb{R}$ . Как оператор над полем  $\mathbb{C}$ , оператор имеет собственные числа  $i$  и  $-i$  — для векторов  $\begin{pmatrix} 1 \\ i \end{pmatrix}$  и  $\begin{pmatrix} 1 \\ -i \end{pmatrix}$  соответственно.

Оператор диагонализуем над  $\mathbb{C}$ , но не над  $\mathbb{R}$ .

**Лемма 3.2.1** (Частный случай леммы Дедекинда — Артина о линейной независимости характеров). Пусть  $v_1, \dots, v_m \in V$  — ненулевые собственные векторы, отвечающие **попарно различным** собственным числам  $\lambda_1, \dots, \lambda_m \in K$ .

Тогда  $v_1, \dots, v_m$  линейно независимы.

*Доказательство.* Пусть  $v_1\mu_1 + \dots + v_m\mu_m = 0$  — самая короткая линейная зависимость (наименьшее  $t$ , такое, что все  $\mu_i \neq 0$ ).

При  $t = 1$  теорема верна, так как  $v_1 \neq 0$ .

При  $t \geq 2$ : запишем два равенства

$$\begin{aligned} 0 &= 0 \cdot \lambda_m = (v_1\mu_1 + \dots + v_m\mu_m)\lambda_m \\ 0 &= \phi(0) = v_1\mu_1\lambda_1 + \dots + v_m\mu_m\lambda_m \end{aligned}$$

Вычитая равенства, получаем линейную зависимость длины ровно  $t - 1$ :

$$0 = v_1 \cdot \mu_1(\lambda_1 - \lambda_m) + \dots + v_{m-1} \cdot \mu_{m-1}(\lambda_{m-1} - \lambda_m) \quad \square$$

**Теорема 3.2.1.** Если оператор  $\phi \in \text{End}_K(V)$  имеет  $n := \dim V$  различных собственных чисел, то он диагонализуется.

*Доказательство.* По определению существуют ненулевые  $v_1, \dots, v_n$  — собственные векторы для данных собственных чисел.

По лемме они линейно независимы, значит, образуют базис. В этом базисе  $[\phi] = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$  □

### 3.3 Характеристический многочлен оператора

Пусть  $\phi \in \text{End}_K(V)$ .

**Определение 3.3.1** (Характеристический многочлен  $\chi_\phi(t)$ ). Многочлен, равный  $\det([\phi] - te)$ , где  $[\phi]$  — матрица  $\phi$  в каком-то базисе,  $e$  — единичная матрица,  $t$  — свободная переменная в многочлене.

**Лемма 3.3.1.**  $\chi_\phi$  не зависит от выбора базиса.

*Доказательство.* Любые две матрицы  $\phi$  в разных базисах,  $[\phi]_u$  и  $[\phi]_v$  сопряжены: для  $g = (u \rightsquigarrow v)$  выполняется  $g[\phi]_u g^{-1} = [\phi]_v$ .

Тогда  $\det([\phi]_v - te) = \det(g) \det([\phi]_u - te) \det(g^{-1}) = \det(g[\phi]_u g^{-1} - tge g^{-1}) = \det([\phi]_u - te)$ . □

**Определение 3.3.2** (Сингулярные собственные числа). Корни  $\chi_\phi$ . Не путать с сингулярными числами (пусть они и не определялись).

Множество  $\lambda$ , для которых  $\phi - \lambda e$  не является обратимым, называется *спектром* оператора  $\phi$ .

**Теорема 3.3.1.** Для конечномерного пространства  $V$  над полем  $K$  сингулярные собственные числа  $\phi$  совпадают с собственными числами  $\phi$ .

*Доказательство.* Зафиксируем базис и отождествим  $V = K^n$ . Также отождествим  $\phi$  и  $[\phi]$ .

Для собственного числа  $\lambda \in K$  найдётся собственный вектор  $v \in V$ , такой, что  $\phi v = v\lambda \iff (\phi - \lambda \text{id})v = 0$ .

По теореме Крамера  $\exists v \neq 0 : (\phi - \lambda \text{id})v = 0 \iff \chi_\phi(\lambda) = \det(\phi - \lambda \text{id}) = 0$ . □

*Замечание.* Выше определённые собственные числа — *правые*. Можно определить левые собственные числа:  ${}^n K \rightarrow {}^n K; u \mapsto (u)\phi$ . Всякий элемент  $\lambda \in K$ , такой, что  $(u)\phi = \lambda u$  является *левым собственным числом*. Для поля левые собственные числа и правые собственные числа совпадают с сингулярными собственными числами, то есть это всё одно и то же.

### 3.4 Геометрическая и алгебраическая кратности собственного числа

**Определение 3.4.1** (Собственное подпространство оператора  $\phi$ , отвечающее собственному числу  $\lambda$ ).  $V(\lambda) = \{v \in V \mid \phi(v) = v\lambda\}$ .

Очевидно, что  $V(\lambda)$  — это подпространство, причём его размерность равна числу различных линейно независимых векторов с собственным числом  $\lambda$ .

**Определение 3.4.2** (Геометрическая кратность собственного числа  $\lambda$ ). Размерность  $V(\lambda)$ .

**Определение 3.4.3** (Алгебраическая кратность собственного числа  $\lambda$ ). Кратность  $\lambda$  как корня  $\chi_\phi$ .

**Лемма 3.4.1.** Геометрическая кратность  $\lambda$  не превосходит алгебраической кратности.



*Доказательство.* Пусть  $m$  — геометрическая кратность  $\lambda$ . Значит,  $\exists v_1, \dots, v_m$  — линейно независимые собственные векторы для собственного числа  $\lambda$ .

Выберем базис  $V$ , дополнив  $(v_1, \dots, v_m)$ . Теперь матрица  $\phi$  имеет вид  $[\phi] = \left( \begin{array}{ccc|c} \lambda & & 0 & * \\ & \ddots & & \\ 0 & & \lambda & * \\ \hline & & 0 & * \end{array} \right)$ .

Очевидно, характеристический многочлен делится на  $(t - \lambda)^m$ .  $\square$

*Замечание.* Если алгебраическая кратность собственного числа равна 1, то она равна геометрической кратности.

*Примеры.*

- Рассмотрим элементарную трансвекцию в каком-то базисе  $[\phi] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ .

С одной стороны,  $\chi_\phi(t) = (t - 1)^2$ .

С другой стороны,  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a+b \\ b \end{pmatrix} \lambda$  выполняется для произвольного  $\lambda$  только если  $b = 0$ , то есть геометрическая размерность единицы как собственного числа — 1, что меньше алгебраической кратности 2.

В частности, видим, что пространство не порождается собственными векторами, матрица не диагонализуема.

- Рассмотрим пространство  $K[t]_{\leq n}$  с оператором  $\phi = \frac{d}{dt}$ . В стандартном базисе:  $[\phi] = \begin{pmatrix} 0 & 1 & & \dots & 0 \\ & 0 & 2 & & \\ \vdots & & \ddots & \ddots & \\ & & & 0 & n \\ 0 & \dots & & & 0 \end{pmatrix}$ .

Здесь  $\chi_\phi(t) = (-t)^{n+1}$ . Алгебраическая кратность  $n + 1$ , геометрическая — 1.

- Жорданова клетка  $J(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}_n$ . Геометрическая кратность собственного числа  $\lambda$  этой клетки равна 1, алгебраическая —  $n$ .

### 3.5 Корневые векторы. Корневое подпространство

По-прежнему  $\phi \in \text{End}_K(V)$ .

**Определение 3.5.1** (Корневой вектор  $v \in V$  оператора  $\phi$ , отвечающий собственному числу  $\lambda$ ). Существует  $m \in \mathbb{N} : (\phi - \lambda \text{id})^m(v) = 0$ . Такое наименьшее  $m$  называется высотой корневого вектора.

В частности, собственный вектор — корневой вектор высоты 1.

**Определение 3.5.2** (Подпространство корневых векторов высоты, не превосходящей  $m$ ).  $V_m(\lambda) = \{v \in V | (\phi - \lambda \text{id})^m(v) = 0\}$ .

Очевидна цепочка вложений  $(V(\lambda) =) V_1(\lambda) \leq V_2(\lambda) \leq V_3(\lambda) \leq \dots$

Пространство конечномерно, цепочка стабилизируется. Можно заметить, что как только  $V_m(\lambda) = V_{m+1}(\lambda)$ , так сразу  $\forall k > m : V_k(\lambda) = V_m(\lambda)$ .

**Теорема 3.5.1.** Над алгебраически замкнутым полем всё пространство раскладывается в прямую сумму корневых подпространств, отвечающих собственному числу  $\lambda$ .

Доказательство. См. (теорема 3.7.3). □

*Пример* (Основной пример корневых векторов).

**Определение 3.5.3** (Экспоненциальные многочлены). Конечная линейная комбинация мономов  $t^m e^{\lambda t}$ , где  $m \in \mathbb{N}_0$ ,  $\lambda \in \mathbb{R}$ ,  $e$  — основание натурального логарифма.

Все мономы формально независимы и образуют кольцо экспоненциальных многочленов  $\text{Exp}_{\mathbb{R}}$  с умножением, определённым как обычно:

$$t^m e^{\lambda t} \cdot t^n e^{\mu t} = t^{m+n} e^{(\lambda+\mu)t}$$

Также в данном кольце определено дифференцирование  $\frac{d}{dt} (t^m e^{\lambda t}) = m t^{m-1} e^{\lambda t} + \lambda t^m e^{\lambda t}$ .

Заметим, что

$$\begin{aligned} \left( \frac{d}{dt} - \lambda \text{id} \right) (t^m e^{\lambda t}) &= m t^{m-1} e^{\lambda t} \\ \left( \frac{d}{dt} - \lambda \text{id} \right)^2 (t^m e^{\lambda t}) &= m(m-1) t^{m-2} e^{\lambda t} \\ \left( \frac{d}{dt} - \lambda \text{id} \right)^m (t^m e^{\lambda t}) &= m! \cdot e^{\lambda t} \\ \left( \frac{d}{dt} - \lambda \text{id} \right)^{m+1} (t^m e^{\lambda t}) &= 0 \end{aligned}$$

Таким образом,  $t^m e^{\lambda t}$  — корневой вектор, отвечающий собственному числу  $\lambda$ , высоты  $m+1$ .

## 3.6 Теорема Кэли — Гамильтона

Отождествим эндоморфизм  $\phi$  с его матрицей  $[\phi]$ .

Заметим, что  $\chi_{\phi}(\phi) = 0$ , то есть

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - (a+d) \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

Для матриц  $2 \times 2$  это заметил Гамильтон, для матриц  $3 \times 3$  — Кэли, Фробениус обобщил.

### 3.6.1 Алгебраическое доказательство

Формально, пусть  $R$  — произвольное коммутативное кольцо,  $x \in M(n, R)$ .

**Теорема 3.6.1** (Кэли — Гамильтон).  $\chi_x(x) = \text{ev}_x(\det(x - te)) = 0$ .

*Алгебраическое доказательство.* По теореме Крамера  $x^{\#} \cdot x = x \cdot x^{\#} = \det(x)e$ , где  $x^{\#} = \text{adj}(x)$ . Запишем

$$(x - te)^{\#}(x - te) = \chi_x(t)e$$

Это равенство в кольце  $M(n, R[t]) \cong M(n, R)[t]$

$$\left[ \text{изоморфизм состоит в вынесении } t \text{ за матрицы: } \begin{pmatrix} 1-t & 0 \\ 0 & 1-t \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} t \right]$$

В равенство хочется подставить  $t \leftarrow x$ . Если получится ноль, то значит действительно  $\chi_x(x) = 0$ .

При рассмотрении данного равенства, как равенства в  $M(n, R[t])$  подстановка ничего интересного, по-видимому, не даст: мы хотим, чтобы  $x - te$  стало нулём, а подстановка даст матрицу из  $M(n, R[x])$ , где  $R[x]$  — многочлены от данной матрицы, факторкольцо кольца многочленов.

$$\left( \begin{pmatrix} x_{1,1} - t & \dots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{n,1} & \dots & x_{n,n} - t \end{pmatrix} \right) \Big|_{t \leftarrow x} = \begin{pmatrix} x_{1,1}e - x & \dots & x_{1,n}e \\ \vdots & \ddots & \vdots \\ x_{n,1}e & \dots & x_{n,n}e - x \end{pmatrix}$$

Если же рассматривать данное равенство, как равенство в  $M(n, R)[t]$ , то априори подставлять  $t \leftarrow x$  нельзя, так как можно утверждать о сохранении равенства при эвалюации только если коэффициенты коммутируют с элементом алгебры, который планируется подставить.

Пусть  $(x - te)^\# = b_{n-1}t^{n-1} + b_{n-2}t^{n-2} + \dots + b_0$ , где  $b_i \in M(n, R)$ .

Пусть  $\chi_x(t) = c_nt^n + \dots + c_0$ , где  $c_i \in R$ .

В этих терминах равенство переписывается в  $M(n, R)[t]$  следующим образом

$$(b_{n-1}t^{n-1} + b_{n-2}t^{n-2} + \dots + b_0) \cdot (x - te) = (c_nt^n + \dots + c_0)e$$

**Лемма 3.6.1.** *Утверждается, что  $x$  коммутирует со всеми  $b_i$  (поэтому его можно подставить в данное равенство).*

*Доказательство леммы.*

Докажем, что матрица  $b_{n-i}$  является многочленом от  $x$  степени  $i - 1$ . Это доказывать мы будем по индукции, причём пользоваться будем написанным выше равенством в  $M(n, R)[t]$ .

Записав равенство коэффициентов при  $t^{n-i}$ , получаем

$$b_{n-i}x - b_{n-1-i}e = c_{n-i}e \text{ для } 0 \leq i < n \text{ (здесь формально } b_n = 0)$$

Сразу получаем  $b_{n-1} = -c_ne$ ;  $b_{n-1-i} = -c_{n-i}e + b_{n-i}x$ . □

Таким образом, эвалюация данного равенства  $t \leftarrow x$  сохранит его справедливость, а левая часть очевидным образом обратится в нуль. □

### 3.6.2 Геометрическое доказательство

**Определение 3.6.1** (Алгебраическое замыкание). Такое поле  $\overline{K}$ , что оно алгебраически замкнуто и все элементы  $\overline{K}$  алгебраичны над  $K$ .

*Интересный факт* (Теорема Штейница). Для любого  $K$  существует (и единственно с точностью до изоморфизма) алгебраическое замыкание  $\overline{K}$ .

*Геометрическое доказательство теоремы Кэли — Гамильтона.* Здесь будем рассматривать  $x$  как матрицу некоего  $\phi \in \text{End}_K(V)$ .

Рассмотрим многочлен  $\chi_\phi(t)$  с коэффициентами в некотором расширении  $K$  — конкретно, в алгебраическом замыкании. Будем считать  $K = \overline{K}$  — если в  $\overline{K} : \chi_\phi(\phi) = 0$ , то это же верно и в  $K$ .

У  $\chi_\phi$  есть корень, назовём его  $\lambda$ .

$$\chi_\phi(t) = (t - \lambda)f(t), \lambda \in K, f \in K[t], \deg f \leq n - 1.$$

Собственному числу  $\lambda$  соответствует вектор  $\underset{\neq 0}{v} \in V$ , такой, что  $\phi(v) = v\lambda$ . Разложим  $V$  в прямую сумму  $V = vK \oplus U$ .

$$[\phi] = \left( \begin{array}{c|c} \lambda & * \\ \hline 0 & [\phi|_{U/vK}] \end{array} \right)$$

$$\phi|_{U/vK} =: \psi \in \text{End}_K(U).$$

Дальше будем действовать по индукции по  $n$ . Индукционное предположение звучит так:  $\forall u \in U : f(\phi)(u) \in vK$ , то есть матрица  $f(\phi)$  выглядит следующим образом:

$$[f(\phi)] = \left( \begin{array}{c|c} \lambda & * \\ \hline 0 & 0 \end{array} \right)$$

Теперь  $\chi_\phi(\phi) = (\phi - \lambda \text{id})f(\phi)$  и  $\forall w \in V : (\phi - \lambda \text{id}) \cdot \underbrace{f(\phi)(v)}_{v\mu} = (\phi - \lambda \text{id})v\mu = 0$ . □

# Лекция XI

7 апреля 2023 г.

## 3.7 Примарное разложение

Самым сложным случаем оказывается тот, когда минимальный многочлен (или характеристический) имеют примарный вид — степень неприводимого.

### 3.7.1 Минимальный многочлен вектора относительно оператора

$\phi \in \text{End}(V)$ , причём  $\dim_K V < \infty$ . Рассмотрим  $v \in V, f \in K[t]$ .

**Определение 3.7.1** (Многочлен  $f$  аннулирует  $v$  относительно  $\phi$ ).  $f(\phi)(v) = 0$ , то есть  $v \in \text{Ker}(f(\phi))$ .

Теперь рассмотрим аннулятор  $\text{Ann}(\phi, v) \stackrel{\text{def}}{=} \{f \in K[t] \mid f(\phi)(v) = 0\}$ . Напомним, что просто аннулятор  $\text{Ann}(\phi) \stackrel{\text{def}}{=} \{f \in K[t] \mid f(\phi) = 0\}$ .

**Лемма 3.7.1.**  $\text{Ann}(\phi, v) \leq K[t]$ .

**Определение 3.7.2** (Минимальный многочлен вектора  $v$  относительно  $\phi$ ). Нормированный многочлен  $\theta_{\phi, v}$ , порождающий  $\text{Ann}(\phi, v)$ , как идеал.

**Лемма 3.7.2.**  $\text{Ann}(\phi) = \bigcap_{v \in V} \text{Ann}(\phi, v)$

**Следствие 3.7.1.** Для любого  $v \in V$  минимальный многочлен  $\theta_{\phi, v}$  делит минимальный многочлен  $\theta_\phi$ .

Ещё можно заметить, что так как  $\theta_\phi \mid \chi_\phi$ , то  $\theta_{\phi, v} \mid \chi_\phi$ .

**Следствие 3.7.2.** Делителей многочлена конечное число, значит,  $\{\theta_{\phi, v}\}_{v \in V}$  конечно.

### 3.7.2 Ядро операторного многочлена

Рассмотрим оператор  $\phi \in \text{End}_K(V)$ ; зафиксируем многочлен  $f \in K[t]$ . Какие векторы он аннулирует?

**Лемма 3.7.3.** Если  $f, g \in K[t]$ , то  $\text{Ker}(f(\phi))$  инвариантно относительно  $g(\phi)$ .

*Доказательство.* Рассмотрим  $v \in \text{Ker}(f(\phi))$ . Покажем  $g(\phi)(v) \in \text{Ker}(f(\phi))$ :

$$f(\phi)(g(\phi)(v)) = (f(\phi) \cdot g(\phi))(v) = (g(\phi) \cdot f(\phi))(v) = g(\phi)(\underbrace{f(\phi)(v)}_0) = 0 \quad \square$$

**Лемма 3.7.4.** Если  $f, g \in K[t], f \mid g$ , то  $\text{Ker}(f(\phi)) \leq \text{Ker}(g(\phi))$ .

*Доказательство.* Пусть  $g = hf$ . Тогда если  $f(\phi)(v) = 0$ , то  $g(\phi)(v) = (hf)(\phi)(v) = h(0) = 0$ .  $\square$

**Теорема 3.7.1.** Пусть  $f, g, h \in K[t]; f = gh$ , где  $g \perp h$  — взаимно просты.

Тогда  $\forall \phi \in \text{End}_K(V) : \text{Ker}(f(\phi)) = \text{Ker}(g(\phi)) \oplus \text{Ker}(h(\phi))$ .

*Доказательство.*

- Так как  $K[t]$  — PID, то есть кольцо Безу, то  $\exists p, q \in K[t] : pg + qh = 1$ .

Эвалюация в  $\phi$ :

$$p(\phi)g(\phi) + q(\phi)h(\phi) = \text{id}$$

Применим к произвольному вектору  $v \in V$ :

$$v = p(\phi)(g(\phi)(v)) + q(\phi)(h(\phi)(v))$$

- Покажем  $\text{Ker}(g(\phi)) \cap \text{Ker}(h(\phi)) = \{0\}$ .

В самом деле, если  $v \in \text{Ker}(g(\phi)) \cap \text{Ker}(h(\phi))$ , то  $v = 0 + 0$ .

- Покажем  $\text{Ker}(g(\phi)) + \text{Ker}(h(\phi)) = \text{Ker}(f(\phi))$ .

Пусть  $v \in \text{Ker}(f(\phi))$ . Опять же, запишем

$$v = p(\phi)(g(\phi)(v)) + q(\phi)(h(\phi)(v))$$

Первое слагаемое лежит в  $\text{Ker}(h(\phi))$ , второе — в  $\text{Ker}(g(\phi))$ .

Согласно лемме, применение  $p(\phi)$  ничего не меняет —  $p(\phi)(g(\phi)(v))$  тоже лежит в ядре  $\text{Ker}(h(\phi))$ .  $\square$

### 3.7.3 Примарное разложение

$\phi \in \text{End}_K(V)$ , рассмотрим  $\chi_\phi = (-1)^n p_1^{m_1} \cdot \dots \cdot p_s^{m_s}$ , где  $p_i \in K[t]$  — неприводимые, нормированные многочлены.

**Определение 3.7.3** (Примарное подпространство).  $V^{p_i} = \text{Ker}(p_i^{m_i}(\phi))$  — аналог корневого подпространства.

**Теорема 3.7.2** (О примарном разложении).  $V = V^{p_1} \oplus \dots \oplus V^{p_s}$ .

*Доказательство.* Теорема Гамильтона — Кэли (теорема 3.6.1) + (теорема 3.7.1) + индукция по  $s$ .  $\square$

#### Случай алгебраически замкнутого поля

Все неприводимые многочлены имеют степень 1. В таком случае  $\chi_\phi(t) = (\lambda_1 - t)^{m_1} \cdot \dots \cdot (\lambda_s - t)^{m_s}$ .

$V^{t-\lambda}$  — в точности корневое подпространство, отвечающее собственному числу  $\lambda$ .

**Теорема 3.7.3** (О корневом разложении). Если  $\chi_\phi$  разложим на линейные множители, как выше (в частности, если  $K$  — алгебраически замкнутое поле), то  $V = V^{\lambda_1} \oplus \dots \oplus V^{\lambda_s}$ .

Для приведения оператора к каноническому виду достаточно привести его, ограниченного на корневые подпространства.

## 3.8 Теорема о жордановой форме

Ограничим  $\psi := \phi|_{V^{\lambda_i}}$ .

Ограниченный оператор имеет единственное собственное число;  $\chi_\psi = (\lambda - t)^n$ .

Чтобы было ещё удобнее, будем считать, что  $\lambda = 0$  — вместо  $\psi$  рассмотрим  $\psi - \lambda \text{id}_{V^\lambda}$ .

Теперь  $\chi_\psi(t) = (-t)^n$ , то есть  $\psi^n = 0$  или  $\psi$  — нильпотентен.

Как выглядит нильпотентный оператор? Например, так:

$$\begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$$

Рассмотрим ещё более специфичный случай

$$J_n(0) = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}; \text{ прибавим } \lambda \text{id} \text{ обратно: } J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$$

Оказывается, над полем ничего другого не бывает.

**Определение 3.8.1** (Жорданова клетка (жорданов блок) степени  $n$  с собственным числом  $\lambda$ ). Выше изображённая матрица  $J_n(\lambda)$ .

**Теорема 3.8.1.** Если  $\phi$  — оператор, такой, что его характеристический многочлен разложим над  $K$  на линейные множители:  $\chi_\phi = \prod_{i=1}^s (t - \lambda_i)^{n_i}$ , то в пространстве  $V$  существует базис, в котором матрица  $\phi$  имеет вид

$$J_{m_1}(\mu_1) \oplus \cdots \oplus J_{m_t}(\mu_t) = \begin{pmatrix} J_{m_1}(\mu_1) & & 0 \\ & \ddots & \\ 0 & & J_{m_t}(\mu_t) \end{pmatrix}$$

где  $m_1 + \cdots + m_t = n = \dim_K(V)$ , а  $\mu_i \in \{\lambda_i\}$ . Быть может,  $\mu_i = \mu_j$ , но типы жордановых клеток — пары  $(m_i, \mu_i)$  — определены однозначно.

**Определение 3.8.2** (Жорданов базис). Базис, в котором  $\phi$  имеет вышеописанный вид.

Если многочлен не разложим на линейные множители, то возникнут Фробениусовы клетки в разложении в прямую сумму. Впрочем, возникает трудный вопрос о единственности.

## Лекция XII

11 апреля 2023 г.

### 3.8.1 Жорданов базис нильпотентного оператора

Пусть  $\phi \in \text{End}(V)$  над произвольным полем, нильпотентен:  $\exists m : \phi^m = 0$ .

Обозначим за  $m$  *степень нильпотентности*  $\phi$  — наименьшее  $m$ , такое, что  $\phi^m = 0$ . По определению,  $\text{Ker}(\phi^{m-1}) \subsetneq \text{Ker}(\phi^m) = V$ .

**Лемма 3.8.1.** Если  $v_1, \dots, v_s \in \text{Ker}(\phi^{k+1})$  и линейно независимы относительно  $\text{Ker}(\phi^k)$ , то  $\phi(v_1), \dots, \phi(v_s) \in \text{Ker}(\phi^k)$  (очевидно) и линейно независимы относительно  $\text{Ker}(\phi^{k-1})$ .

*Доказательство.* Пусть  $\phi(v_1)\lambda_1 + \cdots + \phi(v_s)\lambda_s \in \text{Ker}(\phi^{k-1})$ .

Тогда  $\phi(v_1\lambda_1 + \cdots + v_s\lambda_s) \in \text{Ker}(\phi^{k-1})$ , и  $v_1\lambda_1 + \cdots + v_s\lambda_s \in \text{Ker}(\phi^k)$ , откуда  $\lambda_1 = \cdots = \lambda_s = 0$ .  $\square$

Рассмотрим цепочку  $\{0\} \subsetneq \text{Ker}(\phi) \subsetneq \text{Ker}(\phi^2) \cdots \subsetneq \text{Ker}(\phi^m) = V$ .

$m$ . Пусть  $v_1^m, \dots, v_{n_1}^m$  — базис  $V$  относительно  $\text{Ker}(\phi^{m-1})$ .

$m-1$ . Рассмотрим  $\phi(v_1^m), \dots, \phi(v_{n_1}^m)$  — линейно независимые векторы  $\text{Ker}(\phi^{m-1})$  относительно  $\text{Ker}(\phi^{m-2})$ .  
Дополним их до базиса  $\text{Ker}(\phi^{m-1})$  относительно  $\text{Ker}(\phi^{m-2})$ , добавив векторы  $v_1^{m-1}, \dots, v_{n_2}^{m-1}$ .

$m-2$ . Ко всем векторам на предыдущем уровне ещё раз применим  $\phi$ :

$$\phi^2(v_1^m), \dots, \phi^2(v_{n_1}^m), \phi(v_1^{m-1}), \dots, \phi(v_{n_2}^{m-1})$$

Дополним их до базиса  $\text{Ker}(\phi^{m-2})$  относительно  $\text{Ker}(\phi^{m-3})$ , добавив векторы  $v_1^{m-2}, \dots, v_{n_3}^{m-2}$ .

$\leq m-3$ . И так далее.

1. На данном шаге получается набор векторов  $\phi^{m-1}(v_1^m), \dots, \phi^{m-1}(v_{n_1}^m), \phi^{m-2}(v_1^{m-1}), \dots, \phi^{m-2}(v_{n_2}^{m-1}), \dots$ , независимых в  $V$  относительно  $\{0\}$ .

Дополним их до абсолютного базиса  $\text{Ker}(\phi)$ , он же — относительный базис  $\text{Ker}(\phi)$  относительно  $\{0\}$ .

**Теорема 3.8.2.** Полученные векторы  $\phi^i(v_j^k)$  — базис  $V$ .

*Доказательство.* Очевидно из того, что (для  $U \leq V$ ) объединение базиса  $U$  и базиса  $V$  относительно  $U$  — базис  $V$ .  $\square$

Получили жордановы башенки следующего вида:



где цепочек высоты  $k$  будет  $n_{m-k}$ . Башне высоты  $k$  соответствует жорданова клетка  $J_k(0) = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$ . Клеток  $J_k(0)$  будет  $n_{m-k}$ , а  $\phi = \underbrace{J_m(0) \oplus \dots \oplus J_m(0)}_{n_1} \oplus \dots$

Осталось доказать единственность в некотором смысле.

Это видно из следующей выкладки:

$$\begin{aligned} n_1 &= \text{codim}(\text{Ker}(\phi^{m-1}), V) \\ n_2 &= \text{codim}(\text{Ker}(\phi^{m-2}), \text{Ker}(\phi^{m-1})) - n_1 \\ n_3 &= \text{codim}(\text{Ker}(\phi^{m-3}), \text{Ker}(\phi^{m-2})) - n_1 - n_2 \end{aligned}$$

Таким образом, количество жордановых клеток данного размера зависит только от коразмерностей ядер, не зависят от выбора базиса.

*Замечание.* Для разложения оператора  $\phi$  с характеристическим многочленом  $(t - \lambda)^n$  надо рассмотреть оператор  $\phi - \lambda \text{id}$ , после чего прибавить  $\lambda \text{id}$  обратно.

### 3.9 Сепарабельные многочлены, совершенные поля

Пусть  $f \in K[t]$ .

**Определение 3.9.1** ( $f$  — сепарабельный).  $f \perp f'$ . Так как  $K[t]$  — PID, то  $K[t]f + K[t]f' = K[t]$ .

*Пример.* Допустим,  $f(x) = (x - c)^2 g(x)$ . Тогда  $f'(x) = 2(x - c)g(x) + (x - c)^2 \cdot g'(x)$ . Это же можно записать для  $f = p^2 g$  — все многочлены такого вида не сепарабельны.

Таким образом, сепарабельный многочлен не имеет кратных корней (ни в одном расширении поля  $K$ ).

Обратно, если  $f = p_1 \cdot \dots \cdot p_m$ , где  $p_i \in K[t]$ , различны (с точностью до ассоциированности) и неприводимы **и все  $p_i$  сепарабельны**, то  $f$  сепарабелен.

**Определение 3.9.2** (Совершенное поле  $K$ ). Все неприводимые многочлены над  $K[t]$  сепарабельны.

*Примеры* (Совершенные поля).

- Любое поле характеристики 0.
- Алгебраически замкнутое поле. (Все неприводимые многочлены —  $(x - c)$ , они сепарабельны по определению).
- Все конечные поля.

*Контрпример* (Не все поля совершенны).

Пусть  $\text{char}(K) = p > 0$ . Поле  $K(x)$  несовершенно:

Рассмотрим  $y := x^{1/p}$  — элемент какого-то расширения  $K(x)$ . Он является корнем своего минимального многочлена  $\theta_y(t) := t^p - x \in K(x)[t]$ .

$\theta'_y = 0$ , значит,  $\gcd(\theta_y, \theta'_y) = \theta_y$ , откуда  $\theta_y$  не является сепарабельным.

Многочлен  $\theta_y$  неприводим ( $x^{1/p}$  не является рациональной функцией), но в расширении поля, где есть  $y$ , многочлен  $\theta_y$  разложим на линейные множители:  $\theta_y(t) = (t - y)^p$ .

К счастью, этот пример является единственным в некотором роде.

*Интересный факт.* Все совершенные поля — поля, для которых эндоморфизм Фробениуса ( $\text{Frob}_p : K \rightarrow K, \text{Frob}_p(x) = x^p$ ) сюръективен.

## 3.10 Разложение Жордана — Шевалле

Пусть  $K$  — совершенное поле.

Рассмотрим  $x \in M(n, K)$ .

**Определение 3.10.1** (Полупростая матрица). Диагонализуемая над каким-то расширением матрица. Над совершенным полем достаточно взять алгебраическое замыкание.

**Определение 3.10.2** (Унипотентная матрица). Такая матрица  $x$ , что  $x - e$  — нильпотентна, то есть все собственные числа  $x - e$  равны 0.

*Интересный факт* (Аддитивное разложение Жордана — Шевалле).  $\forall x \in M(n, K) : \exists! x_s, x_n \in M(n, K)$ , такие, что

1.  $x_s$  — полупростая.
2.  $x_n$  — нильпотентна.
3.  $x = x_s + x_n$ .
4.  $x_s x_n = x_n x_s$ .

Утверждается, что, более того, такие матрицы  $x_s$  и  $x_n$  являются многочленами от  $x$ .

*Доказательство.* Перейдём к алгебраическому замыканию  $K$ , разложим  $J_n(\lambda) = \lambda \text{id} + J_n(0)$ . Доказательство единственности сложнее.  $\square$

*Интересный факт* (Мультипликативное разложение Жордана — Шевалле).  $\forall x \in GL(n, K) : \exists! x_s, x_u \in M(n, K)$ , такие, что

1.  $x_s$  — полупростая.
2.  $x_u$  — унипотентна.
3.  $x = x_s x_u$ .
4.  $x_s x_u = x_u x_s$ .

Утверждается, что, более того, такие матрицы  $x_s$  и  $x_u$  являются многочленами от  $x$ .

## Лекция XIII

12 апреля 2023 г.



### 3.11 Вещественные жордановы формы

Пусть  $V$  — векторное пространство над  $\mathbb{R}$ .

Рассмотрим  $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$ . Что такое это в общем случае — непонятно, но здесь это значит, что для базиса  $V$   $(e_1, \dots, e_n)$  над  $\mathbb{R}$  у пространства  $V_{\mathbb{C}}$  базис —  $(e_1, \dots, e_n)$  над  $\mathbb{C}$ .

Это называется *комплексификация*  $V$ . Вещественный базис комплексификации —  $(e_1, e_1 i, \dots, e_n, e_n i)$ , где  $i$  — мнимая единица. Можно сказать, что комплексификация имеет двойную размерность.

Всякому оператору  $\phi : V \rightarrow V$  сопоставляется *комплексификация оператора*  $\phi : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$ . Воспользовавшись тем, что мы зафиксировали базис, мы определим комплексификацию, как оператор с той же матрицей:  $M(n, \mathbb{R}) \hookrightarrow M(n, \mathbb{C})$ .

Можно привести матрицу  $\phi$  к жордановому виду над  $\mathbb{C}$ . Вспомнив, что  $\phi$  — вещественный оператор, получаем  $\chi_{\phi}(t) \in \mathbb{R}[t]$ . Таким образом, его корни — либо вещественные числа, либо пары сопряжённых комплексных.

**Лемма 3.11.1.** Если  $u$  — корневой вектор  $\phi$ , отвечающий собственному числу  $\lambda \in \mathbb{C} \setminus \mathbb{R}$  высоты  $m$ , то  $\bar{u}$  — корневой вектор той же высоты и собственного числа  $\bar{\lambda}$ .

*Доказательство.*  $(\phi - \lambda \text{id})^m(u) = 0 \Rightarrow (\overline{\phi - \lambda \text{id}})^m(\bar{u}) = 0$  — пользуемся тем, что комплексное сопряжение — автоморфизм.  $\square$

**Следствие 3.11.1.** Жордановы клетки комплексно сопряжённых пар тоже бьются на пары одной размерности.

Значит, для приведения комплексной жордановой формы к какой-то хорошей вещественной, надо преобразовать  $J_m(\lambda) \oplus J_m(\bar{\lambda})$ .

Вспомним, что  $\begin{pmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{pmatrix} \sim \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$  для  $\lambda = a + bi$ .

$$\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix} \oplus \begin{pmatrix} \bar{\lambda} & & 0 \\ & \ddots & \\ 0 & & \bar{\lambda} \end{pmatrix} = \left( \begin{array}{cc|cc|cc} a & b & 1 & 0 & & 0 \\ -b & a & 0 & 1 & & 0 \\ \hline & & & & 1 & 0 \\ & & & & 0 & 1 \\ \hline & & & & a & b \\ & & & & -b & a \end{array} \right)$$

Эти матрицы тоже сопряжены:

*Доказательство.* Если  $J_m(\lambda)$  отвечает базису  $u_1, \dots, u_m$ , то  $J_m(\bar{\lambda})$  отвечает базису  $\bar{u}_1, \dots, \bar{u}_m$ .

Тогда матрица из  $M(2m, \mathbb{R})$  отвечает базису  $(\frac{u_1 + \bar{u}_1}{2}, \frac{u_1 - \bar{u}_1}{2i}, \dots) = (\Re(u_1), \Im(u_1), \dots)$ .  $\square$

Зафиксируем результат.

**Теорема 3.11.1.** Матрица любого оператора  $\phi \in \text{End}_{\mathbb{R}}(V)$  приводится к виду прямой суммы клеток двух типов —  $J_m(\lambda)$  для  $\lambda \in \mathbb{R}$  и клеток  $J_m(a, b) : a, b \in \mathbb{R}, b \neq 0$ .

При этом числа и размеры клеток определены однозначно.

### 3.12 Циклические подпространства, фробениусовы клетки

Пусть  $\phi \in \text{End}_K(V)$ ,  $v \in V$ .

**Определение 3.12.1** (Циклическое подпространство оператора  $\phi$ , порождённое вектором  $v$ ). Наименьшее  $\phi$ -инвариантное подпространство в  $V$ , содержащее  $v$ .

**Лемма 3.12.1.** Циклическое подпространство, порождённое  $v$  — это  $\langle v, \phi(v), \phi^2(v), \dots \rangle$ .

Если  $n = \dim V$ , то  $v, \phi(v), \dots, \phi^n(v)$  линейно зависимы. Возьмём наибольшее  $m \in \mathbb{N} : \phi^0(v), \dots, \phi^{m-1}(v)$  линейно независимы:

Значит,  $\phi^m(v) \in \langle \phi^0(v), \dots, \phi^{m-1}(v) \rangle$ :

$$\phi^m(v) = \phi^0(v)\alpha_0 + \dots + \phi^{m-1}(v)\alpha_{m-1}$$

откуда циклическое подпространство —  $\langle \phi^0(v), \dots, \phi^{m-1}(v) \rangle$ .

**Лемма 3.12.2.**  $\phi|_{\langle \phi^0(v), \dots, \phi^{m-1}(v) \rangle}$  в этом базисе имеет матрицу

$$B(f) \stackrel{\text{def}}{=} \begin{pmatrix} 0 & & 0 & \alpha_0 \\ 1 & & & \alpha_1 \\ & \ddots & & \vdots \\ 0 & & 1 & \alpha_{m-1} \end{pmatrix}$$

(сопровождающая матрица многочлена  $f$ , фробениусова клетка)

где  $f = t^m - \alpha_{m-1}t^{m-1} - \dots - \alpha_1t - \alpha_0$ .

*Замечание.*  $\chi_{B(f)} = (-1)^m f$ .

Разложим характеристический многочлен  $\phi$  на произведение примарных множителей  $p_1^{m_1} \cdot \dots \cdot p_s^{m_s}$ . Пространство разложится в сумму примарных подпространств  $V = V^{p_1} \oplus \dots \oplus V^{p_s}$ , на которых  $\chi_{\phi|_{V^{p_i}}} = \pm p_i^{m_i}$ .

*Интересный факт.* Любое примарное пространство раскладывается в прямую сумму циклических.

Любой оператор приводится к прямой сумме фробениусовых клеток, отвечающих примарным многочленам.

## Глава 4

# Классификация модулей над PID

### 4.1 Нормальная форма Смита

Доказана Смитом над  $\mathbb{Z}$ , над произвольным PID — Фробениусом.

#### 4.1.1 Над евклидовым кольцом

$x \in M(m, n, R)$ , где  $R$  — евклидово кольцо с нормой  $\delta : R \rightarrow \mathbb{N}_0 \cup \{-\infty\}$ .

Если бы вместо кольца было поле, то матрицу можно было бы привести к окаймлённому виду

$$\left( \begin{array}{c|c} e & 0 \\ \hline 0 & 0 \end{array} \right)$$

**Теорема 4.1.1.** Если  $R$  евклидово, то  $\forall x \in M(m, n, R) : \exists h \in E(m, R), g \in E(n, R)$ , такие, что

$$h x g = \left( \begin{array}{ccc|c} \varepsilon_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & \varepsilon_k & \\ \hline & 0 & & 0 \end{array} \right), \text{ где } \varepsilon_1 \mid \varepsilon_2 \mid \dots \mid \varepsilon_k, \text{ причём } \varepsilon_i \text{ определены однозначно с точностью}$$

до ассоциированности.

*Доказательство.* Рассмотрим множество

$$\mathcal{M} := \{h x g \mid h \in E(m, R), g \in E(n, R)\}$$

и множество элементов матриц из  $\mathcal{M}$

$$\mathcal{D} := \{m_{i,j} \mid m \in \mathcal{M}, 1 \leq i \leq n, 1 \leq j \leq m\}$$

- Либо  $x = 0$ , тогда она уже приведена к необходимому виду.
- Либо в множестве  $\mathcal{D}$  есть элементы кроме 0. Выберем среди них элемент с минимальной нормой  $\delta$ . Так как перестановки содержатся в  $E(n, R)$  и в  $E(m, R)$ , то можно считать, что для неких  $h, g$  этот элемент —  $(h x g)_{1,1}$ .

Заменим для удобства  $x$  на эту матрицу, теперь  $x_{1,1}$  имеет минимальную норму в  $\mathcal{D}$ .

$$\left( \begin{array}{c|ccc} x_{1,1} & x_{1,2} & \dots & x_{1,n} \\ \hline x_{2,1} & & & \\ \vdots & & * & \\ x_{m,1} & & & \end{array} \right)$$

Заметим, что  $x_{1,1}$  делит все остальные  $x_{1,j}$  и  $x_{i,1}$ , так как иначе можно было бы получить элемент меньшей нормы, чем  $\delta(x_{1,1})$  с помощью одного шага алгоритма Евклида ( $y = x_{1,1}q + r$ , где  $\delta(r) < \delta(x_{1,1})$ , значит, с помощью трансвекции получаем  $r = y - x_{1,1}q$ ).

Применим элементарные преобразования, получим

$$\left( \begin{array}{c|ccc} x_{1,1} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array} \right)$$

Дальше по индукции ненулевые числа останутся только на некоем префиксе главной диагонали.

Тот факт, что  $x_{1,1} \mid x_{2,2}$  можно видеть, если прибавить вторую строчку к первой — в противном случае опять можно было бы получить элемент в  $\mathcal{D}$  меньшей нормы, чем  $x_{1,1}$ .

Единственность разложения следует из того, что результирующие  $x_{i,i}$  можно найти из формул:

$$x_{1,1} = \gcd(\mathcal{D}) = \gcd(x_{i,j}, 1 \leq i \leq n, 1 \leq j \leq m) = \gcd(\text{миноры первого порядка})$$

$$x_{2,2} = \frac{\gcd(\text{миноры второго порядка})}{x_{1,1}}$$

$$x_{3,3} = \frac{\gcd(\text{миноры третьего порядка})}{x_{1,1} \cdot x_{2,2}}$$

Эти инварианты не меняются (с точностью до ассоциированности) при домножении на элементы  $E(n, R)$  или  $E(m, R)$ , а ещё однозначно задают нормальную форму.  $\square$

**Следствие 4.1.1.** *Над евклидовым кольцом*

$SL(n, R) = E(n, R)$  — матрицы с единичным определителем и группа, порождённая элементарными трансвекциями.

$GL(n, R) = GE(n, R)$  — обратимые матрицы и матрицы, порождённые элементарными трансвекциями и псевдоотражениями.

*Контрпример (Хитрая PID).* Возьмём локализацию  $\mathbb{Z}[t]$  относительно мультипликативной системы  $S := \langle \Phi_n \mid n \in \mathbb{N} \rangle$ , где  $\Phi_n$  — круговой многочлен номера  $n$ , то есть минимальный многочлен над  $\mathbb{Q}$ , делящий  $x - \omega_n$ , ( $\omega_n^n = 1$ ).

В данном кольце главных идеалов  $E(n, R) \neq SL(n, R)$ .

## 4.1.2 Над PID

Пусть  $R$  — PID.

**Теорема 4.1.2.** Для матрицы  $x \in M(m, n, R)$  существует  $h \in SL(m, R), g \in SL(n, R)$ , такие, что

$$hxg = \left( \begin{array}{ccc|c} \varepsilon_1 & & 0 & 0 \\ & \ddots & & \\ 0 & & \varepsilon_k & \\ \hline & & 0 & 0 \end{array} \right) \text{ где } \varepsilon_1 \mid \varepsilon_2 \mid \dots \mid \varepsilon_k, \text{ причём } \varepsilon_i \text{ определены однозначно с точностью до ассоциированности.}$$

**Лемма 4.1.1.** *Любая унимодулярная строчка (строка с комаксимальными элементами) длины 2 дополняется до матрицы с определителем 1.*

*Доказательство леммы.*

$$aR + bR = R \Rightarrow \exists u, v \in R : au + bv = 1. \text{ Матрица } \begin{pmatrix} a & b \\ -v & u \end{pmatrix} \text{ искомая: } \begin{vmatrix} a & b \\ -v & u \end{vmatrix} = 1 \quad \square$$

**Лемма 4.1.2.** *Если  $R$  — PID, то  $a \perp b \Rightarrow aR + bR = R$ .  $\exists g \in SL(2, R) : \begin{pmatrix} a & b \end{pmatrix} g = \begin{pmatrix} d & 0 \end{pmatrix}$  где  $d = \gcd(a, b)$ .*

Доказательство леммы.

Строчку  $(a/d \quad b/d)$  надо достроить до  $SL(2, R)$ : пусть  $\begin{vmatrix} a/d & b/d \\ -u & v \end{vmatrix} = 1$ . Тогда

$$\begin{pmatrix} a & b \\ u & v \end{pmatrix} \cdot \begin{pmatrix} v & -b/d \\ u & a/d \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}, \text{ причём } \begin{pmatrix} v & -b/d \\ u & a/d \end{pmatrix} \in SL(2, R) \quad \square$$

## Лекция XIV

18 апреля 2023 г.

Доказательство формы Смита для PID. По индукции.

Пусть  $\left( \begin{array}{c|ccc} x_{1,1} & \cdots & x_{1,n} \\ \vdots & & * \\ x_{n,1} & & \end{array} \right) = x \in M(m, n, R).$

Умножая справа, её можно привести к виду  $\left( \begin{array}{c|ccc} d & \cdots & 0 \\ \vdots & & * \\ y_{n,1} & & \end{array} \right)$ , где  $d = \gcd(x_{1,1}, \dots, x_{1,n})$ .

Дальше, умножив слева, мы приводим все к виду  $\left( \begin{array}{c|ccc} d' & \cdots & z_{1,n} \\ \vdots & & * \\ 0 & & \end{array} \right)$ , где  $d' = \gcd(d, y_{2,1}, \dots, y_{n,1})$ .

Так, умножая то справа, то слева, мы (так как PID  $\Rightarrow$  нётерово кольцо, и всякий раз идеал растёт), мы в какой-то момент придём к матрице  $\left( \begin{array}{c|ccc} \varepsilon_1 & \cdots & 0 \\ \vdots & & * \\ 0 & & \end{array} \right).$

Дальше по индукции, приводим оставшуюся матрицу к диагональной.

$\begin{pmatrix} \varepsilon_1 & 0 \\ 0 & \varepsilon_2 \end{pmatrix} \sim \begin{pmatrix} \varepsilon_1 & \varepsilon_2 \\ 0 & \varepsilon_2 \end{pmatrix} \sim \begin{pmatrix} \gcd(\varepsilon_1, \varepsilon_2) & 0 \\ * & * \end{pmatrix} \sim \begin{pmatrix} \gcd(\varepsilon_1, \varepsilon_2) & 0 \\ 0 & \text{lcm}(\varepsilon_1, \varepsilon_2) \end{pmatrix}$ , все преобразования были с определителем 1, поэтому после приведения нижнего правого прямоугольника к хорошему виду можно добиться преобразования, такие, что  $\varepsilon_1 \mid \varepsilon_2$ .  $\square$

## 4.2 Подмодули кручения, модули без кручения

Пусть  $M$  — модуль над коммутативным кольцом  $R$ .

Обычно будем предполагать, что  $R$  — область целостности.

**Определение 4.2.1** (Элемент кручения  $x \in M$ ).  $\exists \lambda \in \text{Reg } R$  — не делитель 0 — такой, что  $\lambda x = 0$ . Также такой элемент называют *периодическим*.

Обозначим  $T(M) \stackrel{\text{def}}{=} \{x \in M \mid \exists \lambda \in \text{Reg } R : \lambda x = 0\}$  — множество элементов кручения.

**Лемма 4.2.1.**  $T(M) \leq M$  — подмодуль.  $T(M/T(M)) = \{0\}$ , то есть  $M/T(M)$  — модуль без кручения.

Доказательство.

- Пусть  $x, y \in T(M)$ .  $\exists \lambda, \mu \in \text{Reg } R : \lambda x = \mu y = 0$ . Тогда  $\lambda \mu (x + y) = 0$ , но  $\lambda \mu \in \text{Reg } R$ .  
Теперь покажем, что  $x \in T(M) \Rightarrow \mu x \in T(M) : \lambda(\mu x) = \mu(\lambda x) = 0$ .
- От противного: пусть  $\exists x \notin T(M), \exists \lambda \in \text{Reg } R : \lambda x \in T(M)$ . Значит,  $\exists \mu \in \text{Reg } R : \mu \lambda x = 0$ . Тогда  $x \in T(M)$  с множителем  $\mu \lambda$ .  $\square$

**Определение 4.2.2** (Модуль  $M$  без кручения).  $T(M) = \{0\}$

**Определение 4.2.3** (Модуль кручения, периодический модуль).  $T(M) = M$ .

### 4.3 Формулировка основных теорем о строении конечнопорождённых модулей над PID

Пусть  $R$  — PID,  $M$  — свободный модуль.

**Теорема 4.3.1.**

1. Подмодуль  $N$  свободного модуля свободен и  $\text{rk } N \leq \text{rk } M$ .
2. Конечнопорождённый модуль без кручения свободен.
3. Если  $M$  — конечнопорождён, то  $M \cong R^n \oplus T(M)$ .

*Доказательство.* (теорема 4.3.4) и ниже. □

**Определение 4.3.1** (Циклический модуль  $M$ ).  $M$  порождён одним элементом:  $M = Rx$ .

Посмотрим на отображение  $\phi : R \rightarrow M : \lambda \mapsto \lambda x$ . У гомоморфизма есть ядро  $\text{Ann}_R(x) \stackrel{\text{def}}{=} \text{Ker}(\phi)$  — аннулятор  $x$ .

По теореме о гомоморфизме  $M \cong R / \text{Ann}_R(x)$ .

- Если  $\text{Ann}_R(x) = \{0\}$ , то модуль свободен и изоморфен  $R$ .
- Если  $\text{Ann}_R(x) \neq \{0\}$ , то  $M$  — модуль кручения. Так как  $R$  — PID, то  $\text{Ann}_R(x) = R\lambda$  для некоего  $\lambda \in R$  — для порождающего  $\text{Ann}_R(x)$ .

**Теорема 4.3.2.** Любой конечнопорождённый периодический модуль является прямой суммой циклических подмодулей.

**Следствие 4.3.1.** Любой конечнопорождённый периодический модуль является прямой суммой примарных циклических подмодулей. Примарный циклический модуль — модуль вида  $R/p_1^{m_1} R$ .

*Доказательство.* Китайская теорема об остатках:

$$R/(p_1^{m_1} \cdots p_s^{m_s})R \cong (R/p_1^{m_1} R) \oplus \cdots \oplus (R/p_s^{m_s} R) \quad \square$$

**Теорема 4.3.3** (О существовании согласованных базисов для подмодулей свободного модуля). Пусть  $N \leq M \cong R^n$ . Тогда  $\exists(e_1, \dots, e_n)$  — базис в  $M$ ,  $\exists \lambda_1, \dots, \lambda_m \in R : \lambda_1 \mid \cdots \mid \lambda_m$ , причём  $N = \langle \lambda_1 e_1, \dots, \lambda_m e_m \rangle \cong R^m$ .

*Доказательство.* См. (теорема 4.4.1). □

#### 4.3.1 Вложение конечнопорождённых модулей без кручения в свободные модули

**Теорема 4.3.4.** Пусть  $R$  — область целостности,  $M$  — конечнопорождённый модуль без кручения. Тогда для некоего  $n$ :  $M$  можно вложить в  $R^n$  так, чтобы он имел ненулевое пересечение со всеми координатными осями.

*Доказательство.*  $M$  порождено элементами  $\langle x_1, \dots, x_m \rangle$ . Пусть  $y_1, \dots, y_n \in M$  — максимальная линейно независимая система. Построим  $R^n$  на системе образующих  $\langle e_1, \dots, e_n \rangle$ .

Рассмотрим подмодуль в  $M \geq \langle y_1, \dots, y_n \rangle =: N$ . Построим вложение  $M \xrightarrow{\phi} N$ .  $N \cong R^n$  — просто переводим базис  $\{y_i\}$  в базис  $\{e_i\}$  — поэтому данное вложение изоморфно искомому  $M \rightarrow R^n$ .

$\forall x_i : (x_i, y_1, \dots, y_n)$  — линейно зависима система. Тогда  $\exists \lambda_i \neq 0 : \lambda_i x_i \in N$ .

Устроим вложение следующим образом: для  $\lambda = \lambda_1 \cdot \dots \cdot \lambda_m \neq 0$  положим

$$\phi : M \rightarrow N; \quad x \mapsto \lambda x$$

Оно инъективно, так как модуль  $M$  — без кручения.  $\phi(M) \cap Ry_i \neq \{0\}$ , так как там есть  $\lambda y_i$ .  $\square$

**Следствие 4.3.2.** 1. в (теорема 4.3.1). Если  $R$  — PID,  $M$  — свободный модуль конечного ранга, то  $\forall N \leq M$ :  $N$  свободен, причём  $\text{rk } N \leq \text{rk } M$ .

*Доказательство.* Индукция по рангу  $M$ .

База:  $\text{rk } M = 1$ ,  $M \cong R$ . Все подмодули имеют ранг 0 или 1 — это идеалы в кольце.

Переход:  $M \cong R^n$ . Построим проекцию  $\pi : R^n \rightarrow R^{n-1}$ ,  $\begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}$ .

$N \leq M \Rightarrow \pi(N) \leq R^{n-1}$ ,  $\text{Ker}(\pi|_N) \leq \text{Ker } \pi \cong R$ . Подмодули в  $R$  мы знаем,  $\text{Ker}(\pi|_N) = \{0\}$ , либо  $\text{Ker}(\pi|_N) \cong R$ .

Воспользовавшись индукционным предположением, получаем, что  $\pi(N) \cong R^l$ , где  $l \leq n-1$ . Если  $\text{Ker}(\pi|_N) = \{0\}$ , то  $N \cong R^l$ . Иначе  $\text{Ker}(\pi) \cong R$ , тогда  $N \cong R^{l+1}$ .  $\square$

**Следствие 4.3.3.** Конечнопорождённый модуль без кручения над PID свободен.

**Теорема 4.3.5.** Если  $M$  — конечнопорождённый, то  $M = R^n \oplus T(M)$ .

*Доказательство.*  $M/T(M)$  — модуль без кручения, причём тоже конечнопорождён. Значит,  $M/T(M) \cong R^n$  для некоего  $n \in \mathbb{N}$ , то есть  $M \cong T(M) \oplus R^n$ .  $\square$

Таким образом, (теорема 4.3.1) полностью доказана.

## 4.4 Согласованный выбор базисов в свободном модуле и его подмодуле

**Теорема 4.4.1.** Пусть  $N \leq M \cong R^n$ . Тогда  $\exists(e_1, \dots, e_n)$  — базис в  $M$ ,  $\exists \lambda_1, \dots, \lambda_m \in R : \lambda_1 \mid \dots \mid \lambda_m$ , причём  $N = \langle \lambda_1 e_1, \dots, \lambda_m e_m \rangle \cong R^m$ .

*Доказательство.* Пусть  $u_1, \dots, u_n$  — базис в  $M$ ,  $v_1, \dots, v_m$  — базис в  $N$ . Разложим  $v$  по базису  $u$ :

$$\begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = x \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

где  $x \in M(m, n, R)$ . При замене базиса векторы  $v, u$  домножаются слева на матрицы из  $h \in SL(m, R)$  и  $g \in SL(n, R)$  соответственно.

При этом над  $x$  будут совершаться преобразования  $x \rightsquigarrow h^{-1}xg$ , то есть  $x$  можно привести к нормальной форме Смита:

$$\begin{pmatrix} \lambda_1 e_1 \\ \vdots \\ \lambda_m e_m \end{pmatrix} = \left( \begin{array}{ccc|c} \lambda_1 & & 0 & \\ & \ddots & & \\ 0 & & \lambda_n & \\ \hline & & & 0 \end{array} \right) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}, \quad \lambda_1 \mid \dots \mid \lambda_m$$

$\square$

# Лекция XV

19 апреля 2023 г.

**Теорема 4.4.2.** Любой конечнопорождённый модуль  $M = \langle u_1, \dots, u_n \rangle$  над PID является прямой суммой циклических.

*Доказательство.* Рассмотрим сюръекцию  $\phi : R^n \rightarrow M, e_i \mapsto u_i$ . Положим  $N := \text{Ker}(\phi)$ .

$N$  — подмодуль свободного модуля, он свободен. Пусть  $(v_1, \dots, v_m)$  — базис  $N$ .

Выразим базисы через матрицу перехода:  $\begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = x \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}, x \in M(m, n, R)$ . Воспользовавшись

для  $x$  канонической формой Смита, можно выбрать согласованные базисы, так, что  $\forall i = 1..m : v_i = e_i \lambda_i$ , причём  $\lambda_1 \mid \dots \mid \lambda_m$ .

Таким образом,  $M \cong R^{n-m} \oplus (R/\lambda_1 R) \oplus \dots \oplus (R/\lambda_m R)$ .

По китайской теореме об остатках получаем, что любой модуль является прямой суммой свободных и примарных модулей.  $\square$

## 4.4.1 Частные случаи

1.  $R = \mathbb{Z}$  — конечнопорождённые абелевы группы.

Согласно ранее доказанной теореме, любая абелева группа

$$G \cong \mathbb{Z}^m \oplus \underbrace{\mathbb{Z}/p_1^{m_1} \mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p_s^{m_s} \mathbb{Z}}_{c_{p_1} m_1}$$

где  $p_i \in \mathbb{P}, m_i \in \mathbb{N}, p_i$  могут повторяться, но пары  $(p_i, m_i)$  определены однозначно.

Такие группы, соответствующие примарным числам, называются *элементарными абелевыми группами*.

К сожалению, классифицировать что-то более сложное, даже метабелевы группы (группы, содержащие абелеву подгруппу, фактор по которой абелев) — задача несоизмеримо большей сложности. Классификация метабелевых групп влечёт классификацию пары матриц над полем, а это — дикая задача.

2.  $R = K[t]$  — форма Фробениуса. Пусть  $V$  — конечномерное векторное пространство над  $K$ ,  $\phi \in \text{End}_K(V)$ .

$(V, \phi)$  имеет структуру  $K[t]$  модуля:  $t \cdot v = \phi(v)$ . Модуль, очевидно — модуль кручения (например, по теореме Кэли — Гамильтона).

Значит,  $V \cong \bigoplus K[t]/(p^m K[t])$ , на каждом подпространстве  $\phi$  имеет примарный характеристический многочлен.

Значит, любой оператор имеет базис, в котором его матрица — прямая сумма фробениусовых клеток.



## Глава 5

# Геометрия пространств со скалярным произведением

### 5.1 Скалярные произведения

$K$  — поле,  $V$  — векторное пространство над  $K$  ( $\dim V < \infty$ ).

**Определение 5.1.1** (Скалярное произведение). Отображение  $B : V \times V \rightarrow K$ , удовлетворяющее следующим свойствам:

1. Билинейность.
2. Рефлексивность  $B(u, v) = 0 \iff B(v, u) = 0$ .

**Определение 5.1.2** (Ортогональные векторы).  $u \perp v \iff B(u, v) = 0$ .

**Определение 5.1.3** (Симметрическое скалярное произведение).  $\forall u, v \in V : B(u, v) = B(v, u)$ .

**Определение 5.1.4** (Кососимметрическое скалярное произведение).  $\forall u, v \in V : B(u, v) = -B(v, u)$ .

*Замечание.* Если характеристика 2, то кососимметрическое скалярное произведение — симметрическое.

**Определение 5.1.5** (Симплектическое скалярное произведение). Любой вектор *изотропен*:  $\forall u \in V : B(u, u) = 0$ .

*Замечание.* В эрмитовом скалярном произведении  $B(u, v) = \overline{B(v, u)}$ , например, в гильбертовом пространстве над  $\mathbb{C}$ .

**Факт 5.1.1.** Симплектическое и кососимметрические произведения связаны:

*симплектическое всегда кососимметрическое, обратное верно не в характеристике 2.*

$$\begin{aligned} 0 &= B(u + v, u + v) = B(u, u) + B(u, v) + B(v, u) + B(v, u) = B(u, v) + B(v, u) \\ &B(u, u) = -B(u, u) \Rightarrow 2B(u, u) = 0 \end{aligned}$$

**Определение 5.1.6** (Невырожденное скалярное произведение).  $\forall u \in V : u \neq 0 \Rightarrow \exists v : B(u, v) \neq 0$ .

*Примеры.*

- $(K^n, B)$ , где  $B \left( \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right) = u_1 v_1 + \dots + u_n v_n = u^t v$ .

Если  $K = \mathbb{R}$ , то это евклидово скалярное произведение, обладающее свойствами

- Анизотропность:  $B(u, u) \neq 0$  для  $u \neq 0$ .
- Положительная определённость:  $B(u, u) \geq 0$ , причём  $B(u, u) = 0 \iff u = 0$ .

- Можно выбрать базис и  $r$ , в котором скалярное произведение имеет вид:

$$B(u, v) = u_1 v_1 + \dots + u_r v_r - u_{r+1} v_{r+1} - \dots - u_n v_n$$

Такое скалярное произведение пишут в пространстве  $\mathbb{R}^{r,s}$  ( $r + s = n$ ), самое известное — пространство Минковского  $\mathbb{R}^{3,1}$ .

- $B(u, v) = u_1 v_n + u_2 v_{n-1} + \dots + u_n v_1$  — расщепимое скалярное произведение.
- Пусть  $n = 2m$ .

$$B(u, v) = (u_1 v_2 - u_2 v_1) + \dots + (u_{2m-1} v_{2m} - u_{2m} v_{2m-1})$$

Это пример симплектического скалярного произведения.

- $V = M(n, K)$ . Здесь можно выбрать  $B(x, y) = \text{tr}(x^t y)$

### 5.1.1 «Классификация» билинейных скалярных произведений

**Теорема 5.1.1.** Любое билинейное рефлексивное  $B : V \times V \rightarrow K$  — симметрическое или симплектическое (в характеристике 2 может выполняться одновременно и то, и то).

*Доказательство.* Рассмотрим  $u, v, w \in V$ , вычислим

$$B(u, vB(u, w) - wB(u, v)) = B(u, v)B(u, w) - B(u, w)B(u, v) = 0$$

Из рефлексивности в другом порядке тоже 0:

$$0 = B(vB(u, w) - wB(u, v), u) = B(v, u)B(u, w) - B(w, u)B(u, v) \quad (5.1)$$

Подставим  $w = u$ :

$$B(u, u)(B(u, v) - B(v, u)) = 0 \quad (5.2)$$

Таким образом, если  $B(u, u) \neq 0$ , то  $\forall v : B(u, v) = B(v, u)$ , а если  $B(u, v) \neq B(v, u)$ , то  $B(u, u) = B(v, v) = 0$ .

Докажем, что если найдутся такие  $u, v \in V : B(u, v) - B(v, u) \neq 0$ , то все векторы изотропны. Пусть нашлись. Тогда выберем  $w \in V$ , предположим, что  $B(w, w) \neq 0$ .

Посчитаем

$$\begin{aligned} B(v, u + w) &= B(v, u) + B(v, w) \\ B(u + w, v) &= B(u, v) + B(w, v) \end{aligned}$$

Первые слагаемые неравны по предположению, вторые — равны, так как  $B(w, w) \neq 0$  (5.2). Значит,  $B(v, u + w) \neq B(u + w, v)$ , откуда (5.2)  $B(u + w, u + w) = 0$ .

Кроме того, из (5.1) видим, что так как  $B(u, v) \neq B(v, u)$ , но  $B(u, w) = B(w, u)$ , то  $B(u, w) = B(w, u) = 0$ . Отсюда, раскрыв скобки в  $B(u + w, u + w) = 0$  действительно получаем, что  $B(w, w) = 0$ .  $\square$

## 5.2 Матрица Грама скалярного произведения

$V, (e_1, \dots, e_n)$  — пространство и базис.

**Определение 5.2.1** (Симплектическое пространство). Пара  $(V, B)$  «пространство — скалярное произведение», если  $B$  — симплектическое.

**Определение 5.2.2** (Квадратическое пространство). Пара  $(V, B)$  «пространство — скалярное произведение», если  $B$  — симметрическое.

*Замечание.* Термин *симметрическое пространство* уже зарезервирован под что-то другое, а в связи с симметрическим скалярным произведением будут возникать квадратичные формы, поэтому термин таков.

**Определение 5.2.3** (Матрица Грама).  $G_e(B) = (B(e_i, e_j))_{1 \leq i, j \leq n}$ .

**Лемма 5.2.1.** Записав векторы столбцами координат в данном базисе, получаем  $B(u, v) = u^t G_e(B) v$ .

*Доказательство.*

$$B(u, v) = B(u_1 e_1 + \dots + u_n e_n, v_1 e_1 + \dots + v_n e_n) = \sum_{i, j} u_i B(e_i, e_j) v_j = u^t G_e(B) v \quad \square$$

**Лемма 5.2.2.**  $B$  — симметрическое  $\iff G_e(B)$  симметрическая ( $G_e(B) = G_e(B)^t$ ).

$B$  — симплектическая  $\iff G_e(B)$  антисимметрическая ( $G_e(B)^t = -G_e(B) \wedge G_e(B)_{i,i} = 0$ ).

**Лемма 5.2.3.** Скалярное произведение  $B$  невырождено  $\iff G_e(B)$  невырождена.

*Доказательство.*  $B$  вырождено  $\iff \exists v \neq 0 : \forall u : B(u, v) = 0 \iff \forall u : u^t G_e(B) v = 0 \iff G_e(B) v = 0 \iff G_e(B)$  вырождена.  $\square$

## Лекция XVI

24 апреля 2023 г.

**Лемма 5.2.4.** При замене базиса матрица Грама преобразуется по формуле  $G_{e'}(B) = g^t G_e(B) g$ , где  $g$  — матрица перехода.

*Доказательство.* Пусть  $g$  — матрица перехода от базиса  $(e_i)_{i=1}^n$  к базису  $(e'_i)_{i=1}^n$ :

$$(e_1 \quad \dots \quad e_n) g = (e'_1 \quad \dots \quad e'_n)$$

Тогда координаты преобразуются контравариантно:  $g^{-1} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} u'_1 \\ \vdots \\ u'_n \end{pmatrix}; \quad \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = g \begin{pmatrix} u'_1 \\ \vdots \\ u'_n \end{pmatrix}.$

Получаем, что  $(gu')^t \cdot G_e(B) \cdot (gv') = (u')^t \cdot g^t G_e(B) g \cdot v'.$   $\square$

*Замечание.* Если матрица  $x$  симметрическая ( $x^t = x$ ), то  $g^t x g$  — тоже симметрическая:

$$(g^t x g)^t = g^t x^t g^{tt} = g^t x g$$

*Замечание.* Задача поиска канонической формы матриц  $x$  относительно преобразований  $g^t x g$  не решена, хотя, казалось бы, должна быть того же уровня сложности, что и каноническая форма относительно поиска базиса — сопряжения  $g^{-1} x g$ .

Это связано с тем, что идейно матрица Грама — не матрица; она имеет два индекса, оба описывающие столбцы (или оба строки). Отсюда и появляется транспонирование первого вектора.

### 5.3 Скалярное произведение и двойственные пространства

$V^* = \text{Hom}_K(V, K)$  — множество ковекторов (линейных функционалов).

Базису  $(e_1, \dots, e_n)$  сопоставляется двойственный базис  $(e_1^*, \dots, e_n^*)$ , такой, что  $e_i^*(e_j) = \delta_{i,j}$ .

Рассмотрим пространство всех билинейных отображений  $L(V, V; K) = \{B : V \times V \rightarrow K \mid B \text{ — билинейно}\}$ . Оказывается, есть канонический изоморфизм между  $L(V, V; K)$  и  $\text{Hom}(V, V^*)$ .

Пусть  $B : V \times V \rightarrow K$  — билинейно. Сопоставим ему парциальные отображения

$${}_u B \stackrel{\text{def}}{=} B(u, \cdot) : V \rightarrow K; \quad B_v \stackrel{\text{def}}{=} B(\cdot, v) : V \rightarrow K$$

Полученные парциальные отображения линейны.

Значит, отображение  $\tilde{B} : u \mapsto {}_u B$  бьёт из  $V$  в  $V^*$ . Более того, оно само линейно, и задаёт биекцию, не зависящую от выбора базисов.

**Теорема 5.3.1.**  $L(V, V; K) \rightarrow \text{Hom}(V, V^*)$ ;  $B \mapsto \tilde{B}$  задаёт канонический изоморфизм  $L(V, V; K) \cong \text{Hom}(V, V^*)$ .

*Доказательство.* Проверим, что отображение — гомоморфизм:  $\widetilde{B_1 + B_2} = \tilde{B}_1 + \tilde{B}_2$  и  $\widetilde{\lambda B} = \lambda \tilde{B}$ .

Проверим, что  $B \mapsto \tilde{B}$  обратимо:  $B(u, v) = \tilde{B}(u)(v)$ . Отсюда получаем инъективность, а сюръективность следует из теоремы о размерности ядра и образа — мы работаем с конечномерными пространствами.

$$\dim(L(V, V; K)) = \dim(V) \cdot \dim(V) = \dim(V) \cdot \dim(V^*) = \dim(\text{Hom}(V, V^*)). \quad \square$$

**Теорема 5.3.2.**  $B : V \times V \rightarrow K$  невырождено  $\iff \tilde{B} : V \rightarrow V^*$  — изоморфизм.

*Доказательство.*

$$\forall u \neq 0 : \exists v \in V : B(u, v) \neq 0$$

$$\Updownarrow$$

$$\forall u \neq 0 : B(u, \cdot) \neq 0 \quad \square$$

*Замечание.* Получается, всякий раз, когда пишут транспонирование, задают изоморфизм  $V \cong V^*$ , который никак не является каноническим. Это уже не линейная алгебра, а евклидова геометрия. Транспонированию не место в канонической линейной алгебре!

*Замечание.* Если билинейная форма симметрическая, то  $\forall u \in V : B(u, \cdot) = B(\cdot, u)$ , то есть изоморфизмы фиксирования первого и второго аргумента одинаковы.

Если билинейная форма симплектическая, то  $\forall u \in V : B(u, \cdot) = -B(\cdot, u)$ .

## 5.4 Классификация пространств со скалярным произведением

Первый шаг классификации: скалярное произведение бывает симметрическим или симплектическим.

Пусть  $(U, B_U)$  и  $(V, B_V)$  — два пространства со скалярными произведениями.

**Определение 5.4.1** (Изометрия пространств). Изоморфизм векторных пространств  $\phi : U \rightarrow V$ , сохраняющий скалярное произведение:  $B_U(u, v) = B_V(\phi(u), \phi(v))$ .

**Задача 5.4.1.** Когда  $(U, B_U) \cong (V, B_V)$ ?

Очевидные инварианты:

1. Размерность  $n = \dim U = \dim V$  — если равенства нет, то нет изоморфизма.
2. Ранг  $r := \text{rk } U \stackrel{\text{def}}{=} \text{rk}(G(B_U))$  — не зависит от выбора базиса, замена базиса — обратимая матрица.

Можно также заметить, что  $\text{rk}(G(B_U)) = \text{rk}(\tilde{B}_U)$ .

3. **Определение 5.4.2** (Дискриминант).  $\text{disc}(V) = (\det(G(B_V))) \cdot (K^*)^2$  — элемент  $K/(K^*)^2$ .

В частности,  $\mathbb{R}^*/\mathbb{R}^{*2} \cong \{\pm 1\}$ ;  $\mathbb{F}_q^*/\mathbb{F}_q^{*2} \cong \{\pm 1\}$  для  $q \in \mathbb{P}_{\geq 3}$ .

**Определение 5.4.3** (Радикал  $V$ ).  $\text{Rad}(V) = \{u \in V \mid \forall v \in V : B(u, v) = 0\}$ . Иначе говоря,  $V^\perp$ .

Пусть  $V = \text{Rad}(V) \oplus U$ , где  $U$  — произвольное прямое слагаемое. Заметим, что  $\text{Rad}(U) = \{0\}$ , иначе  $\text{Rad}(V)$  больше, чем предполагался.

Значит, классификацию подпространств можно свести к классификации невырожденных подпространств.

**Теорема 5.4.1** (О классификации симплектических пространств).  $U \cong V \iff \begin{cases} \dim U = \dim V \\ \operatorname{rk} U = \operatorname{rk} V \end{cases}$ .

*Доказательство.* См. (теорема 5.6.2)  $\square$

**Следствие 5.4.1.** Для любой чётной размерности существует единственное невырожденное симплектическое пространство. Примерами матриц Грама для этих изоморфных пространств являются следующие матрицы

$$\left( \begin{array}{ccc|ccc} & & & 1 & & 0 \\ & 0 & & & \ddots & \\ -1 & & 0 & 0 & & 1 \\ & \ddots & & & & \\ 0 & & -1 & & 0 & \end{array} \right) \quad \left( \begin{array}{cc|cc|cc} 0 & 1 & & & & 0 \\ -1 & 0 & & & & \\ \hline & & & \ddots & & \\ 0 & & & & 0 & 1 \\ & & & & -1 & 0 \end{array} \right) \quad \left( \begin{array}{ccc|ccc} & & & 0 & & 1 \\ & 0 & & & \ddots & \\ 0 & & -1 & 1 & & 0 \\ & \ddots & & & & \\ -1 & & 0 & & 0 & \end{array} \right)$$

так пишут физики так пишут топологи так пишут алгебраисты

**Определение 5.4.4** (Квадратически замкнутое поле  $K$ ). Такое поле, что  $(K^*)^2 = K^*$ , то есть  $\forall x \in K : \exists y \in K : y^2 = x$ .

**Теорема 5.4.2.** Если  $K$  квадратически замкнуто и  $\operatorname{char}(K) \neq 2$ , то квадратические пространства  $U \cong V \iff \begin{cases} \dim(U) = \dim(V) \\ \operatorname{rk}(U) = \operatorname{rk}(V) \end{cases}$ .

*Доказательство.* См. (теорема 5.8.1).  $\square$

**Следствие 5.4.2.** В частности, над квадратически замкнутым полем в любой размерности существует единственное невырожденное квадратическое пространство.

*Интересный факт.* Над конечными полями — ровно два пространства, с дискриминантом, являющимся и не являющимся полным квадратом.

**Теорема 5.4.3** (Закон инерции Сильвестра). Над  $\mathbb{R}$  поля со скалярным произведением определяются тремя инвариантами

1.  $\dim(V) = n$ .
2.  $\operatorname{rk}(V) = r = r^+ + r^-$ .
3. Сигнатура  $s = r^+ - r^-$ .

Здесь  $r^+$  и  $r^-$  — количества положительных и отрицательных квадратов.

В матрице Грама на главной диагонали стоит  $r^+$  единиц,  $r^-$  минус единиц, остальные — нули.

*Доказательство.* См. (теорема 5.8.4)  $\square$

## Лекция XVII

25 апреля 2023 г.

### 5.5 Ортогональное дополнение

$U \leq V$  — подпространство,  $B : V \times V \rightarrow K$  — скалярное произведение.

**Определение 5.5.1** (Ортогональное дополнение).  $U^\perp \stackrel{\text{def}}{=} \{v \in V \mid \forall u \in U : B(u, v) = 0\}$ .

*Замечание.* Рефлексивность скалярного произведения влечёт, что можно не различать  $U^\perp$  и  ${}^\perp U$ .

*Предостережение.* Ортогональное дополнение не является дополнением: совсем не факт, что  $U \oplus U^\perp = V$ .

*Свойства.*

- $\forall U \leq V : U \cap U^\perp = \text{Rad}(U) \stackrel{\text{def}}{=} \{u \in U \mid \forall u' \in U : B(u, u') = 0\}$ .
- $\text{Rad}(V) = V^\perp; \{0\}^\perp = V$ .
- $U^\perp \leq V$ .
- $U \leq U^{\perp\perp}$  (равенство в случае невырожденного  $V$ : следствие (лемма 5.5.3)).
- $U \rightsquigarrow U^\perp$  обращает включения:  $U \leq W \Rightarrow W^\perp \leq U^\perp$ .
- $(U + W)^\perp = U^\perp \cap W^\perp$ .
- $(U \cap W)^\perp \geq U^\perp + W^\perp$  (равенство в случае невырожденного  $V$ : следствие (лемма 5.5.3)).

### 5.5.1 Ортогональная прямая сумма

$(U, B_U), (V, B_V)$  — два произвольных пространства (но либо оба симметрические, либо оба симплектические).

Определим скалярное произведение на  $U \oplus V$  следующим образом:

$$B_{U \oplus V} : (U \oplus V) \times (U \oplus V) \rightarrow K; \quad (u_1, v_1), (u_2, v_2) \mapsto B_U(u_1, u_2) + B_V(v_1, v_2)$$

Так как  $B((u, 0), (0, v)) = 0$  в данном определении, то  $(U \oplus V, B_{U \oplus V})$  — ортогональная прямая сумма.

**Лемма 5.5.1.** *Определённая выше  $B_{U \oplus V}$  — скалярное произведение на  $U \oplus V$ .*

Будем обозначать ортогональную прямую сумму  $U \boxplus V \stackrel{\text{def}}{=} (U \oplus V, B_{U \oplus V})$ .

Если  $U, W \leq V$  — лежат в одном объёмлющем пространстве, то прямая сумма  $U \boxplus W$  — внутренняя ортогональная прямая сумма — существует если

1.  $U \cap W = \{0\}$
2.  $U \perp W$  здесь эквивалентно  $U \leq W^\perp$  здесь эквивалентно  $W \leq U^\perp$ .

**Лемма 5.5.2.** *Пусть  $U$  — любое дополнение к  $\text{Rad}(V)$  :  $U \oplus \text{Rad}(V) = V$ .*

*Тогда  $V = U \boxplus \text{Rad}(V)$ , причём  $B_U$  невырождено.*

*Доказательство.* Докажем лишь часть про невырожденность, первое очевидно.

Если  $\exists u \in U, u \neq 0 : \forall v \in U : B(u, v) = 0$ , то  $\forall v \in V : v \in U + \text{Rad}(V) \Rightarrow B(u, v) = 0$  по линейности  $B$ , противоречие —  $B_U$  невырождено.  $\square$

### 5.5.2 Теорема об ортогональном дополнении

**Лемма 5.5.3.** *Если  $U$  невырождено, либо  $V$  невырождено, то имеет место  $\dim(U) + \dim(U^\perp) = \dim(V)$ .*

*Доказательство.* Вложению  $U \xhookrightarrow{i} V$  отвечает  $V^* \xrightarrow{i^*} U^*$  — двойственное линейное отображение.

Воспользуемся отображением  $\tilde{B} : V \rightarrow V^*$ . Найдём  $\text{Ker}(V \xrightarrow{\tilde{B}} V^* \xrightarrow{i^*} U^*) = \left\{ v \in V \mid \left( \begin{matrix} u \\ \in U \end{matrix} \mapsto B(v, u) \right) = 0 \right\}$ .

Это  $U^\perp$  по определению.

Кроме того,  $V \xrightarrow{\tilde{B}} V^* \xrightarrow{i^*} U^*$  сюръективно:

- Если  $U$  невырождено, то даже  $U \xrightarrow{i} V \xrightarrow{\tilde{B}} V^* \xrightarrow{i^*} U^*$  сюръективно —  $B_U$  невырождено.

• Иначе это верно, так как  $V$  невырождено и  $V \xrightarrow{\tilde{B}} V^*$  — сюръекция ( $i^*$  — просто сужение).  
Используя теорему о размерности ядра и образа получаем, что  $\dim(U) + \dim(U^\perp) = \dim(V)$ .  $\square$

*Предостережение.* Если  $U \leq V$ ,  $V$  невырождено, то совсем необязательно  $U$  невырождено. Например,  $\dim(V) = 2$ ,  $G(B) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . Оба пространства размерности 1, натянутые на базисные векторы, вырождены.

**Теорема 5.5.1.** Если  $U \leq V$ ,  $B_U$  невырождено, то  $V = U \boxplus U^\perp$ .

*Доказательство.*

- $U \cap U^\perp = \text{Rad}(U) = \{0\}$ .
- По определению  $U \perp U^\perp$ .
- $\dim(U) + \dim(U^\perp) = \dim(V)$  согласно (лемма 5.5.3).  $\square$

*Замечание.* Может быть, что скалярное произведение на  $U$  невырождено, но на  $U^\perp$  — вырождено. Тем не менее,

**Теорема 5.5.2.** Если  $V$  невырождено, то  $\forall U \leq V : U = U^{\perp\perp}$ .

*Доказательство.* Согласно (лемма 5.5.3) получаем  $\dim(U) = \dim(U^{\perp\perp})$ .  $\square$

**Теорема 5.5.3.** Если из пространств  $V, U, U^\perp$  два невырождены, то и третье тоже, в этом случае разложения  $V = U \boxplus U^\perp = U^\perp \boxplus U^{\perp\perp}$  симметричны по  $U$  и  $U^\perp$ .

*Доказательство.*

- Если  $V$  невырождено, то (тривиально)  $U^{\perp\perp} \geq U$ , но согласно (лемма 5.5.3) наблюдается равенство.

Если  $U^\perp$  невырождено, то заменим  $\begin{cases} U^\perp \rightsquigarrow U^{\perp\perp} \\ U \rightsquigarrow U^\perp \end{cases}$ , в дальнейшем доказательстве невырождено  $U$ .

Таким образом,  $\forall u \in U^\perp : \exists v \in U^\perp : B(u, v) \neq 0$  (иначе данный  $u$  лежит в  $U^{\perp\perp}$ ). Но это по определению невырожденность  $U^\perp$ .

- Если  $U^\perp, U$  невырождены, то  $\dim(U) + \dim(U^\perp) = \dim(V)$ . Из невырожденности их пересечение пусто, откуда  $V = U \oplus U^\perp$ .

$$\forall v \in V : \exists u \in U, u' \in U^\perp : v = u + u' \Rightarrow B(v, \cdot) = B(u, \cdot) + B(u', \cdot)$$

Так как  $U$  невырождено, то найдётся  $w \in U : B(u, w) \neq 0$ .  $B(u', w) = 0 \Rightarrow B(v, w) \neq 0$ .  $\square$

**Следствие 5.5.1.** Если в  $V$  нашлось невырожденное подпространство, то можно взять к нему ортогональное дополнение, матрица Грама разложится на блоки в базисах  $U$  и  $U^\perp$ :

$$G(B) = \left( \begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array} \right)$$

Дальше можно пытаться раскладывать пространство по индукции в прямую сумму одномерных.

### 5.5.3 Теорема Лагранжа о существовании ортогонального базиса в квадратичном пространстве

**Определение 5.5.2** (Ортогональный базис). Базис  $(e_1, \dots, e_n)$  пространства  $V$ , такой что  $i \neq j \Rightarrow B(e_i, e_j) = 0$ .

В ортогональном базисе матрица Грама диагональна:  $G(B) = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}, a_i \in K$ .

**Теорема 5.5.4** (Лагранж).  $B : V \times V \rightarrow K$  — симметрическая форма. Если  $\text{char}(K) \neq 2$ , то в любом пространстве над  $K$  существует ортогональный базис.

*Доказательство.*

**Лемма 5.5.4.** Если  $\text{char}(K) \neq 2$ , то в пространстве с ненулевым симметрическим скалярным произведением найдётся неизотропный вектор  $v : B(v, v) \neq 0$ .

*Доказательство леммы.*

Пусть  $B(u, v) \neq 0$ . Тогда среди векторов  $u, v, u + v$  хотя бы один неизотропен:  $B(u, v) = \frac{1}{2}(B(u+v, u+v) - B(u, u) - B(v, v))$  и здесь существенно, что характеристика — не 2.  $\square$

Если  $B = 0$ , то всякий базис ортогонален, доказывать нечего.

Если  $B \neq 0$ , то проведём индукцию по размерности.

База: В одномерном пространстве любой базис ортогонален.

Переход: Найдётся неизотропный  $e_1 \in V$ , тогда согласно (теорема 5.5.3)  $V = e_1 K \oplus (e_1 K)^\perp$ , по индукционному предположению  $V = \langle e_1 \rangle \oplus \dots \oplus \langle e_{n-1} \rangle$ .  $\square$

## 5.6 Введение в теорию (Диксона — ) Витта. Классификация симплектических пространств

Теория опубликована Виттом примерно в 1936 году, но Диксон показал примерно то же в 1905, в год рождения Витта. К сожалению, работа Диксона осталась незамеченной.

### 5.6.1 Выделение гиперболических плоскостей

$B : V \times V \rightarrow K$  — произвольное скалярное произведение.

Пусть  $u \in V$  — изотропный вектор.

**Определение 5.6.1** (Анизотропное скалярное произведение).  $\forall u \in V, u \neq 0 \Rightarrow B(u, u) \neq 0$ .

*Замечание.* Анизотропные скалярные произведения изучаются в матанализе, и там хорошо, что они положительно определены. А в алгебре — это, наоборот, мешает.

**Определение 5.6.2** (Гиперболическая плоскость  $H$ ). Двумерное пространство над  $K$  с матрицей Грама  $G(B_H) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  или  $G(B_H) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ .

**Лемма 5.6.1.** Пусть  $B$  невырождено, нашёлся  $u \in V, u \neq 0, B(u, u) = 0$ . Если  $B$  симметрическое, то дополнительно предположим, что  $\text{char}(K) \neq 2$ .

Тогда и можно вложить в гиперболическую плоскость, то есть  $\exists v \in V : B(u, v) = 1, B(v, v) = 0$ .

*Доказательство.* В силу невырожденности  $\exists w \in V : B(u, w) \neq 0$ . Домножением  $w$  на скаляр можно добиться того, что  $B(u, w) = 1$ .



Так как  $B(u, u) = 0 \neq B(u, w)$ , то  $\langle u, w \rangle$  — пространство размерности 2. Матрица Грама данного пространства в базисе  $(u, w)$  — это  $\begin{pmatrix} 0 & 1 \\ \pm 1 & * \end{pmatrix}$ .

Если пространство симплектическое, то матрица уже имеет искомый вид.

Иначе ( $B$  симметрическое) элементарным преобразованием получаем, что искомая гиперболическая плоскость натянута на векторы  $u, w + \alpha u$ , где  $\alpha$  подобрано таким образом, что

$$B(w + \alpha u, w + \alpha u) = 0 \Rightarrow B(w, w) + 2\alpha B(u, w) = 0 \Rightarrow \alpha = -\frac{1}{2} \frac{B(w, w)}{B(u, w)}$$

□

*Замечание.* Условие невырожденности  $B$  можно ослабить до  $u \notin \text{Rad}(V)$ .

## Лекция XVIII

26 апреля 2023 г.

**Теорема 5.6.1.** Пусть  $u \in V \setminus \text{Rad}(V)$  — изотропный вектор, причём если  $V$  квадратично, то дополнительно предполагаем, что  $\text{char}(K) \neq 2$ .

Тогда  $u$  можно включить в гиперплоскость  $H \leq V$ , такую, что  $H \oplus H^\perp = V$ .

*Доказательство.* По лемме  $H$  существует;  $H$  невырождена, значит достаточно сослаться на (лемма 5.6.1). □

### 5.6.2 Классификация симплектических пространств

Пусть  $K$  — произвольное поле,  $V$  — симплектическое пространство над  $K$ . Тогда  $V = \underbrace{H \oplus \dots \oplus H}_t \oplus \text{Rad}(V)$ .

**Теорема 5.6.2.** Два симплектических пространства  $U \cong V \iff \dim(U) = \dim(V)$  и  $\text{rk}(U) = \text{rk}(V)$ .

*Доказательство.* Количество гиперплоскостей — это  $\frac{1}{2} \text{rk}$ . Размерность радикала — это  $\dim - \text{rk}$ , причём все радикалы одной размерности изометричны. □

**Следствие 5.6.1.** Ранг симплектического пространства чётен.

**Следствие 5.6.2.** Невырожденные симплектические пространства существуют только в чётных размерностях.

## 5.7 Квадратические пространства. Квадратичные формы

$V$  — векторное пространство над  $K$ . Будем предполагать, что  $\text{char}(K) \neq 2$ , иначе всё намного сложнее.

**Определение 5.7.1** (Квадратичная форма). Отображение  $Q : V \rightarrow K$ , такое, что

1.  $Q$  — однородно степени 2:  $Q(v\lambda) = Q(v)\lambda^2$ .
2. Поляризация формы  $Q$  — билинейное (симметрическое автоматически) скалярное произведение.

**Определение 5.7.2** (Поляризация квадратичной формы  $Q$ ). Скалярное произведение

$$B(u, v) \stackrel{\text{def}}{=} \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$$

**Факт 5.7.1.** Квадратичная форма — скалярный квадрат:  $Q(v) = B(v, v)$ .

**Теорема 5.7.1.** Существует биективное соответствие между квадратичными формами и симметрическими скалярными произведениями.

*Доказательство.* В одну сторону — поляризация, в другую — скалярный квадрат.  $\square$

### 5.7.1 Квадратичная форма в координатах

Пусть  $V \ni x = x_1 e_1 + \dots + x_n e_n$ . Тогда квадратичная форма — однородный многочлен степени 2:

$$Q(x) = B(x, x) = x^t G(B) x = \sum_{i,j=1}^n a_{i,j} x_i x_j = \sum_{i < j} 2a_{i,j} x_i x_j + \sum_{i=1}^n a_{i,i} x_i^2$$

**Теорема 5.7.2** (Лагранж). Пусть  $\text{char}(K) \neq 2$ . Любая квадратичная форма  $Q : V \rightarrow K$  линейно невырожденной заменой переменных приводится к сумме квадратов:

$$Q(x) = a_1 x_1^2 + \dots + a_n x_n^2, \quad a_i \in K$$

*Доказательство.* Есть ортогональный базис: (теорема 5.5.4)  $\square$

## 5.8 Классификация квадратичных пространств

### 5.8.1 Над квадратично замкнутым полем

$K^* = (K^*)^2$ ,  $\text{char}(K) \neq 2$ .

**Определение 5.8.1** (Ортонормированный базис  $V$ ). Ортогональный базис  $V$ , такой, что  $B(e_i, e_i) \in \{0, 1\}$ .

**Теорема 5.8.1.** В любом квадратичном пространстве над квадратично замкнутым полем характеристики не 2 выполнимы следующие условия:

1. Существует ортонормированный базис.
2. У квадратичных пространств ровно 2 инварианта: размерность и ранг.
3. Любая квадратичная форма приводима к виду

$$Q(x_1, \dots, x_n) = x_1^2 + \dots + x_r^2, \quad r \leq n$$

4. Всякое пространство приводимо к виду

$$V = H \boxplus \dots \boxplus H \boxplus \text{Rad}(V) \boxplus \underbrace{\langle 1 \rangle}_{\text{если } \text{rk } V \text{ нечётен}}$$

*Доказательство.* Согласно теореме Лагранжа (теорема 5.5.4) найдётся ортогональный базис  $(e_1, \dots, e_n)$ . Переупорядочим базисные векторы так, что первые  $r$  имеют ненулевой скалярный квадрат, остальные — нулевой.

После этого заменим  $e_i \rightsquigarrow \frac{e_i}{\sqrt{B(e_i, e_i)}}$ ,  $i \leq r$ .

Пункт 4 следует из того, что над таким полем (например,  $K = \mathbb{C}$ ):  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

А именно рассмотрим сначала матрицу  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ :

$$\begin{cases} B(e, e) = 1 \\ B(f, f) = -1 \\ B(e, f) = 0 \end{cases}$$

Выберем новый базис  $\left(\frac{e+f}{\sqrt{2}}, \frac{e-f}{\sqrt{2}}\right)$ . Для него

$$\begin{cases} B\left(\frac{e+f}{\sqrt{2}}, \frac{e+f}{\sqrt{2}}\right) = 0 \\ B\left(\frac{e+f}{\sqrt{2}}, \frac{e-f}{\sqrt{2}}\right) = 1 \\ B\left(\frac{e-f}{\sqrt{2}}, \frac{e-f}{\sqrt{2}}\right) = 0 \end{cases}$$

Таким образом, например, над полем  $\mathbb{R} : \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Над квадратичным полем можно заменить вектор  $v \rightsquigarrow \sqrt{-1} \cdot v$ , получается, над  $K : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .  $\square$

### 5.8.2 Над полем вещественных чисел (закон инерции Сильвестра)

Пусть  $V$  — пространство над  $\mathbb{R}$  с симметрическим скалярным произведением.

*Замечание.* Доказать также можно доказать для формально вещественных полей — числа бывают отрицательные и положительные, а множество квадратов — множество положительных чисел.

**Определение 5.8.2** (Ортонормированный базис  $(e_1, \dots, e_n)$ ). Ортогональный базис, такой, что  $B(e_i, e_i) \in \{+1, -1, 0\}$ .

**Теорема 5.8.2.** В  $V$  существует ортонормированный базис.

*Доказательство.* Согласно теореме Лагранжа (теорема 5.5.4) найдётся ортогональный базис  $(e_1, \dots, e_n)$ . Переупорядочим базисные векторы так, что первые  $r$  имеют ненулевой скалярный квадрат, остальные — нулевой.

После этого заменим  $e_i \rightsquigarrow \frac{e_i}{\sqrt{|B(e_i, e_i)|}}$ ,  $i \leq r$ .  $\square$

Таким образом, ортонормированный базис есть, характеризуется тремя числами —  $r^+, r^-, n$ . Являются ли они инвариантами?

Ограничимся невырожденными пространствами:

$$V_1 = U_1 \oplus \text{Rad}(V_1) \cong U_2 \oplus \text{Rad}(V_2) = V_2 \Rightarrow U_1 \cong U_2$$

(из-за единственности ранга  $\dim \text{Rad}(V_1) = \dim \text{Rad}(V_2)$ ; разные прямые слагаемые к одному радикалу изометричны, так как в них можно выбрать базисы, где соответствующие векторы различаются на вектор из радикала).

**Теорема 5.8.3** (Сильвестр). Обозначим  $\mathbb{R}^{p,q}$  как пространство с матрицей Грама

$$\left( \begin{array}{cc|cc} 1 & & & 0 \\ & \ddots & & \\ 0 & & 1 & \\ \hline & & & -1 & 0 \\ 0 & & & & \ddots & \\ & & & 0 & & -1 \end{array} \right)$$

где размеры блоков  $p$  и  $q$  соответственно.

Пространства  $\mathbb{R}^{p,q} \cong \mathbb{R}^{s,t}$  изометричны  $\iff (p, q) = (s, t)$ .

*Доказательство.* Обозначим за  $U^+, U^-, V^+, V^-$  пространства, натянутые на соответствующие базисные векторы.

Предположим, что  $p > s$ . Рассмотрим отображение  $U^+ \hookrightarrow U \cong V \xrightarrow{\text{pr}} V^+$ , где  $\text{pr}$  — проекция на  $V^+$  вдоль (параллельно)  $V^-$ .

Пусть  $\phi : U \cong V$ , тогда  $\phi(U^+) \leq V$ , но так как  $s < p$ , то проекция  $\text{pr}(\phi(U^+))$  имеет ненулевое ядро.

$\text{Ker}(\text{pr}) = V^-$ , значит,  $\text{Ker}(\text{pr}|_{\phi(U^+)}) \leq V^-$ . Значит, нашёлся вектор из  $U^+$ , который при изометрии попал в  $V^-$ . Но так не бывает при изометрии — значит, ядро на самом деле нулевое, противоречие.  $\square$

**Теорема 5.8.4** (Закон инерции Сильвестра). Любое квадратичное пространство над  $\mathbb{R}$  изометрично ровно одному пространству вида

$$\underbrace{\langle 1, \dots, 1 \rangle}_{r^+} \underbrace{\langle -1, \dots, -1 \rangle}_{r^-} \underbrace{\langle 0, \dots, 0 \rangle}_{n-r^+-r^-} \stackrel{\text{def}}{=} \underbrace{\langle 1 \rangle \boxplus \langle 1 \rangle}_{r^+} \boxplus \underbrace{\langle -1 \rangle \boxplus \langle -1 \rangle}_{r^-} \boxplus \underbrace{\langle 0 \rangle \boxplus \langle 0 \rangle}_{n-r^+-r^-}$$

Заметим, что пространства  $\langle 1, \dots, 1 \rangle$  и  $\langle -1, \dots, -1 \rangle$  — евклидово и антиевклидово соответственно, значит, они анизотропны.

## Лекция XIX

2 мая 2023 г.

Положим  $m = \min(r^+, r^-)$ . Получается, всякое квадратичное пространство над  $\mathbb{R}$  изометрично ровно одному пространству вида

$$\underbrace{H \boxplus \dots \boxplus H}_m \boxplus \begin{matrix} \langle 1, \dots, 1 \rangle \\ \text{или} \\ \langle -1, \dots, -1 \rangle \end{matrix} \boxplus \text{Rad}(V)$$

### 5.9 Теория (Диксона — ) Витта

**Теорема 5.9.1** (Витт о разложении). Пусть  $V$  — пространство над  $K$ ,  $\text{char}(K) \neq 2$ . Тогда

$$V = \underbrace{H \boxplus \dots \boxplus H}_s \boxplus V_0 \boxplus \text{Rad}(V)$$

причём  $s$  определено однозначно,  $V_0$  — анизотропно и определено однозначно с точностью до изометрии.

*Доказательство.* См. (теорема 5.9.7)  $\square$

**Теорема 5.9.2** (Витт о продолжении). Пусть  $V$  — пространство над  $K$ ,  $\text{char}(K) \neq 2$ , пусть  $U, W \leq V$ . Если  $\psi : U \cong W$  — изометрия, то  $\exists \phi \in \text{Isom}(V) : \phi|_U = \psi$ . Дополнительно потребуем невырожденности либо  $U$  (тогда и  $W$ ), либо  $V$ .

*Доказательство.* См. (теорема 5.9.4 and ??).  $\square$

Если всё невырождено, то эта теорема эквивалентна следующей:

**Теорема 5.9.3** (Витт о сокращении). Пусть  $U, W, V$  — невырожденные пространства над  $K$ ,  $\text{char}(K) \neq 2$ . Если  $U \boxplus V \cong W \boxplus V$ , то  $U \cong W$ .

*Доказательство.* Пусть  $\phi : U \boxplus V \cong W \boxplus V$ ; согласно теореме Витта о продолжении можно считать, что  $\phi$  оставляет  $V$  на месте ( $V \cong \phi(V)$ ). Тогда  $U \cong W$ , как ортогональные дополнения  $V$  в одном и том же пространстве.  $\square$

### 5.9.1 Ортогональные отражения

Пусть  $V$  — квадратичное пространство,  $\text{char}(K) \neq 2$ . Дополнительно предположим, что  $B \neq 0$ , выберем  $v \in V : B(v, v) \neq 0$  (такой есть, так как  $\text{char}(K) \neq 2$ ).

**Определение 5.9.1** (Ортогональное отражение относительно  $v$ ).  $w_v : V \rightarrow V$ ,  $w_v(x) = x - 2\frac{B(x, v)}{B(v, v)}v$ .

Обозначим  $L_v = \langle v \rangle^\perp$  — *зеркало отражения*. Так как  $V = \langle v \rangle \boxplus L_v$  —  $v$  анизотропен — то ортогональное отражение переводит  $v \mapsto -v$ , а каждая точка ортогональной гиперплоскости остаётся на месте.

**Лемма 5.9.1.** Пусть  $\text{char}(K) \neq 2$ ,  $B(u, u) = B(v, v) \neq 0$ . Тогда  $\exists \phi \in \text{Isom}(V) : \phi(u) = v$ .

*Доказательство.*  $u + v, u - v \in \langle u, v \rangle$ . Один из этих двух векторов анизотропен:

$$B(u + v, u - v) = B(u, u) - B(v, v) = 0$$

откуда

$$0 \neq 4B(u, u) = B((u + v) + (u - v), (u + v) + (u - v)) = B(u + v, u + v) + B(u - v, u - v)$$

Если  $u - v$  анизотропен, то  $w_{u-v}(u) = v$ . Иначе  $u + v$  анизотропен, тогда  $w_{u+v}(u) = -v$ , домножив преобразование на  $-1$  получим необходимое. Можно написать выкладку, а можно посмотреть на картинку:



*Предостережение.* Если  $B(u, u) = B(v, v) = 0$ , то необязательно  $\exists \phi \in \text{Isom}(V) : \phi(u) = v$ . Это верно только если пространство невырождено.

*Контрпример.* Пусть  $u \in V \setminus \text{Rad}(V), v \in \text{Rad}(V)$ .  $v$  ортогонален всему,  $u$  — не всему, нет изометрии, переводящей один в другой.

**Лемма 5.9.2.** Если  $V$  невырождено, то для любых ненулевых изотропных векторов  $u, v \in V : \exists \phi \in \text{Isom}(V) : \phi(u) = v$ .

### 5.9.2 Доказательство теоремы Витта о продолжении для невырожденных подпространств

**Теорема 5.9.4.** Если  $U, W \leq V, \psi : U \cong W$ , причём  $U, W$  невырождены ( $B$  симметрическое,  $\text{char}(K) \neq 2$ ). Тогда  $\exists \phi : V \cong V : \phi|_U = \psi$ .

*Доказательство.* Индукция по  $\dim(U) = \dim(W)$ .

База: (лемма 5.9.1).

Переход: Согласно (лемма 5.5.4), в  $U$  найдётся неизотропный вектор  $u \in U$ . Положим  $v = \psi(u) \in W$ .

Выберем  $\theta \in \text{Isom}(V)$ ,  $\theta(u) = v$  — такая есть согласно (лемма 5.9.1).

Заменим  $W$  на  $\theta^{-1}(W)$ , а  $\psi$  — на  $\theta^{-1}\psi$ . Достаточно доказать теорему после замены, изначально искомого  $\phi$  получится домножением полученного на  $\theta$  слева. После замены  $u = \psi(u)$ .

Применим трижды теорему об ортогональном разложении (теорема 5.5.1):

$$\begin{aligned} U &= \langle u \rangle \boxplus \langle u \rangle_U^\perp \\ W &= \langle u \rangle \boxplus \langle u \rangle_W^\perp \\ V &= \langle u \rangle \boxplus \langle u \rangle_V^\perp \end{aligned}$$

Понятно, что  $\langle u \rangle_U^\perp, \langle u \rangle_W^\perp \leq \langle u \rangle_V^\perp$ .

Ограничение  $\psi|_{\langle u \rangle_V^\perp} : \langle u \rangle_V^\perp \rightarrow \langle u \rangle_W^\perp$  — изометрия. По индукционному предположению  $\exists \eta \in \text{Isom}(\langle u \rangle_V^\perp)$ , такая, что  $\eta|_{\langle u \rangle_V^\perp} = \psi|_{\langle u \rangle_V^\perp}$ .

Тогда  $\phi = \text{id}_{\langle u \rangle} \oplus \eta$  подойдёт.  $\square$

### 5.9.3 Доказательство теоремы Витта о продолжении для невырожденного пространства

**Теорема 5.9.5.** Пусть  $U, W \leq V, \psi : U \cong W$ , причём  $V$  невырождено ( $B$  симметрическое,  $\text{char}(K) \neq 2$ ). Тогда  $\exists \phi : V \cong V : \phi|_U = \psi$ .

*Доказательство.* Сначала докажем следующее:

**Теорема 5.9.6.** Пусть  $V$  невырождено,  $U \leq V$ ,  $U = U_0 \boxplus \text{Rad}(U)$  ( $U_0$  невырождено). Тогда  $\exists$  невырожденное  $\bar{U} : U \leq \bar{U} \leq V$ , такое, что

$$\bar{U} = U_0 \boxplus \underbrace{H \boxplus \dots \boxplus H}_{d(U) := \dim(\text{Rad}(U))}$$

*Доказательство.* Индукция по  $d(U)$  — дефекту  $U$ .

Пусть  $e_1, \dots, e_s$  — базис  $\text{Rad}(U)$ . Из невырожденности  $V$  следует  $\dim(U) + \dim(U^\perp) = \dim(V)$ .

Назовём  $W = U_0 \boxplus \langle e_1, \dots, e_{s-1} \rangle \leq U$ .  $\dim(W) = \dim(U) - 1$ ,  $\dim(W^\perp) = \dim(U^\perp) + 1$ .

Значит,  $\exists v \in W^\perp \setminus U^\perp$ . Тогда  $B(e_s, v) \neq 0$ . Согласно (лемма 5.6.1) (подпространство  $\langle e_s, v \rangle$  невырождено, так как  $B(e_s, v) \neq 0$ , но  $e_s$  изотропен) найдётся  $e_{-s} \in \langle e_s, v \rangle : B(e_{-s}, e_{-s}) = 0, B(e_s, e_{-s}) = 1$ .

Получили равенство  $U \oplus \langle e_{-s} \rangle = W \boxplus H$ , дальше действуем по индукции.  $\square$

Согласно доказанной теореме найдутся  $\bar{U}, \bar{W}$ :

$$\begin{aligned} U &\leq \bar{U} \leq V & \dim(\bar{U}) &= \dim(U) + d(U) \\ W &\leq \bar{W} \leq V & \dim(\bar{W}) &= \dim(W) + d(W) \end{aligned}$$

Пространства изоморфны, значит, их дефекты равны, то есть  $\dim(\bar{U}) = \dim(\bar{W})$ . С другой стороны,

$$U = U_0 + \text{Rad}(U) \quad W = W_0 + \text{Rad}(W)$$

Заметим, что ограничение  $\psi$  — тоже изометрия:  $\psi|_{U_0} : U_0 \cong W_0$ . Построим эту изометрию до  $\bar{\psi} : \bar{U} \cong \bar{W}$  — все гиперболические плоскости изометричны, понятно, что можно достроить так, чтобы  $\bar{\psi}(U_0) = W_0$ . Согласно предыдущей теореме (теорема 5.9.4) эту изометрию можно продолжить на всё  $V$ .  $\square$

**Теорема 5.9.7** (Витт о разложении).  $(V, B)$  — пространство над  $K$ ,  $(B)$  симметрическое,  $\text{char}(K) \neq 2$ . Тогда  $V$  представимо в виде

$$V_0 \boxplus \underbrace{H \boxplus \cdots \boxplus H}_s \boxplus \text{Rad}(V)$$

$s$  — индекс Витта

где  $V_0$  анизотропно, причём класс изометрий  $V_0$  и  $s$  определены однозначно.

*Доказательство.* Индукция по  $\dim V$ . Для начала избавимся от радикала, включив его прямым слагаемым.

Пока существуют ненулевые изотропные векторы, будем включать их в гиперболические гиперплоскости. В результате останутся только анизотропные векторы, образующие  $V_0$ .

Единственность разложения следует из теоремы Витта о сокращении: все гиперболические плоскости изометричны, на них можно сокращать.  $\square$

Такое разложение пространства на анизотропную, гиперболическую, и вырожденную части называется *разложением Витта*. Естественно выбирать ортогональный базис в анизотропной части, гиперплоскостной базис в гиперболической части (и любой — в радикале, всё равно там  $B \equiv 0$ ) — это *базис Витта*.

Пусть  $V = H_1 \boxplus \cdots \boxplus H_s$ . Выберем полученный гиперплоскостной базис  $H_i = \langle e_i, e_{-i} \rangle$ .

Определим  $U = \langle e_1, \dots, e_s \rangle, U' = \langle e_{-1}, \dots, e_{-s} \rangle$ . Получим разложение  $V = U \oplus U'$ , причём  $B_U \equiv 0$  и  $B_{U'} \equiv 0$ .

**Определение 5.9.2** (Вполне изотропное пространство  $U$ ). Все векторы  $U$  изотропны.

Если характеристика не 2, то во вполне изотропных пространствах  $B_U \equiv 0$  (иначе (лемма 5.5.4)).

**Следствие 5.9.1.** Если  $V$  невырождено, то  $V \cong V_0 \boxplus (U \oplus U')$ , где  $V_0$  анизотропно,  $U, U'$  — вполне изотропны.

**Факт 5.9.1.**  $U, U'$  — максимальные (и по размерности, и по включению) вполне изотропные подпространства в  $V$ .

*Доказательство.* Максимальность по включению очевидна — никакой вектор не добавить.

Согласно теореме Витта о сокращении, в невырожденном  $V$  все максимальные по включению вполне изотропные подпространства изометричны.

А именно, пусть  $U, \tilde{U} \leq V$  — вполне изотропные подпространства, причём  $\dim(U) < \dim(\tilde{U})$ . Тогда  $U$  изометрично некому подпространству в  $\tilde{U}$ . Изометрию можно продолжить на всё  $V$ , получается,  $U$  содержится в большем вполне изотропном подпространстве. Противоречие.  $\square$

## Лекция XX

3 мая 2023 г.

### 5.10 Полуторалинейные скалярные произведения

Иноязычно полуторалинейные называют sesquilinear, полулинейные — semilinear.

#### 5.10.1 Полулинейные отображения, инволюции

Раньше было так:  $R$  — кольцо,  $U, V$  — два модуля над ним,  $\phi: U \rightarrow V$  — линейное отображение:

$$\begin{aligned}\phi(u + v) &= \phi(u) + \phi(v) \\ \phi(v\lambda) &= \phi(v)\lambda\end{aligned}$$

Пусть теперь  $U$  —  $R$ -модуль,  $V$  —  $S$ -модуль. Что естественно понимать под морфизмом  $U \rightarrow V$ ? Первое свойство удобно сохранить:  $\phi(u + v) = \phi(u) + \phi(v)$ . Так как  $V$  — не  $R$ -модуль, то при вынесении скаляра из  $R$  надо его преобразовать в скаляр из  $S$ .

Зададим **унитальный** гомоморфизм колец  $\psi : R \rightarrow S$ .

**Определение 5.10.1** ( $\psi$ -полулинейное отображение). Такое аддитивное  $\phi : U \rightarrow V$ , что

$$\forall u \in U, \lambda \in R : \phi(u\lambda) = \phi(u)\psi(\lambda)$$

Линейное отображение можно понимать, как полулинейное, где  $R = S$ . До сих пор  $\psi$  было тождественным.

**Определение 5.10.2** (Инволюция). Антиавтоморфизм порядка 2. Часто обозначается чертой:

$$\bar{\cdot} : R \rightarrow R, \lambda \mapsto \bar{\lambda}$$

*Свойства.*

- $\overline{\lambda + \mu} = \bar{\lambda} + \bar{\mu}$  — определение антиавтоморфизма.
- $\overline{\lambda \cdot \mu} = \bar{\mu} \cdot \bar{\lambda}$  — определение антиавтоморфизма.
- $\bar{\bar{1}} = 1$ .
- $\bar{\bar{\lambda}} = \lambda$  — порядок 2.

*Примеры.*

- Комплексное сопряжение — ещё и автоморфизм, так как кольцо коммутативно.
- Кватернионное сопряжение:  $a + bi + cj + dk \mapsto a - bi - cj - dk$ .

$$\begin{aligned} w + \bar{w} &= 2a \in \mathbb{R} \\ w\bar{w} &= a^2 + b^2 + c^2 + d^2 \in \mathbb{R} \end{aligned}$$

- Инволюция на  $\mathbb{Q}(\sqrt{2}) : a + b\sqrt{2} \mapsto a - b\sqrt{2}$ .
- Инволюция на  $\mathbb{F}_{q^2}$ :

$$\text{Frob} : \mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}; \quad x \mapsto x^q$$

- Пусть  $R$  — коммутативное кольцо. Тогда  $R = R^o$  и транспонирование — инволюция:  $M(n, R) \rightarrow M(n, R^o); \quad x \mapsto x^t$ .
- Главная инволюция группового кольца  $K[G] \rightarrow K[G]; \quad g \mapsto g^{-1}$ .

Пусть  $U, V$  — модули над **коммутативным** кольцом  $R$  с инволюцией.

**Определение 5.10.3** (Полулинейное отображение  $\phi : U \rightarrow V$  по отношению к инволюции). Аддитивное  $\phi$ , такое, что  $\phi(u\lambda) = \phi(u)\bar{\lambda}$ .

В 1840-е годы Эрмит ввёл это для комплексных чисел, Гамильтон — для кватернионов.

## 5.10.2 Полуторалинейные скалярные произведения

Никаких билинейных анизотропных скалярных произведений (кроме одномерных) над  $\mathbb{C}$  нет: всегда уравнение  $z^2 + w^2 = 0$  имеет решение.

А анизотропность иногда бывает удобна. Поэтому над  $\mathbb{C}$  билинейные скалярные произведения не позволяют построить такую же геометрию, как над  $\mathbb{R}$ . Эрмит предложил заменить сумму квадратов на сумму  $z\bar{z} + w\bar{w}$ , которая никогда не 0 (разве что  $z = w = 0$ ). Для этого пришлось отказаться от линейности по одному из аргументов.

---

Пусть  $K$  — поле с инволюцией,  $V$  — векторное пространство над  $K$ .



**Определение 5.10.4** (Полуторалинейная форма  $B : V \times V \rightarrow K$ ).  $B$ , линейное по одному аргументу, и полуглинейное — по второму:

$$\begin{aligned} B(u+v, w) &= B(u, w) + B(v, w) \\ B(u, v+w) &= B(u, v) + B(u, w) \\ B(u\lambda, v\mu) &= \bar{\lambda} \cdot B(u, v) \cdot \mu \text{ — для правых модулей} \\ B(\lambda u, \mu v) &= \lambda \cdot B(u, v) \cdot \bar{\mu} \text{ — для левых модулей} \end{aligned}$$

**Определение 5.10.5** (Полуторалинейное скалярное произведение). Полуторалинейная форма, в которой ортогональность симметрична:  $B(u, v) = 0 \iff B(v, u) = 0$ .

**Определение 5.10.6** (Эрмитова полуторалинейная форма). Такая форма  $B$ , что  $B(u, v) = \overline{B(v, u)}$ . Также называется *эрмитовски симметричной формой*.

*Замечание.* Казалось бы, можно ввести эрмитовски антисимметричную форму:  $B(u, v) = -\overline{B(v, u)}$ . Но смысла в этом нет: если  $B$  эрмитовски симметрична, то  $i \cdot B$  — эрмитовски антисимметрична.

*Интересный факт.* Все полуторалинейные скалярные произведения с точностью до нормировки — эрмитовски симметричны.

**Определение 5.10.7** (Унитарное пространство).  $(V, B)$ , где  $B$  — полуторалинейное эрмитово скалярное произведение.

**Определение 5.10.8** (Унитарная группа). Группа изометрий унитарного пространства:  $\{\phi | B(\phi u, \phi v) = B(u, v)\}$ .

*Пример* (Классический пример).  $V = \mathbb{C}^n$ ,  $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto \bar{z}$   $B(u, v) = \bar{u}_1 v_1 + \dots + \bar{u}_n v_n$ .

$B$  здесь положительно определено:

- $B(u, u) \geq 0$  — положительная полуопределённость.
- Равенство наступает при  $u = 0$ .

Пространство называют *конечномерным гильбертовым* или *классическим унитарным пространством*.

Для таких пространств можно заново переизложить теорию, описанную в данной главе.

Так, матрица Грама  $G(B)$  — такая матрица, что  $B(u, v) = \bar{u}^t G(B) v$ .

**Теорема 5.10.1.** Любое эрмитово скалярное произведение над  $\mathbb{C}$  имеет вид

$$B(u, v) = \bar{u}_1 v_1 + \dots + \bar{u}_p v_p - \bar{u}_{p+1} v_{p+1} - \dots - \bar{u}_{p+q} v_{p+q}$$

Это аналог теоремы Сильвестра: всякое скалярное произведение определяется тремя числами,  $n, p, q$ .

*Набросок доказательства.*  $B(u, u) = \overline{B(u, u)} \Rightarrow B(u, u) \in \mathbb{R}$ . Домножая вектор  $u$  на  $\lambda$  получаем  $B(u\lambda, u\lambda) = \lambda \bar{\lambda} B(u, u)$ , то есть можно заменить число на любое того же знака — привести в  $\{-1, 0, +1\}$ .  $\square$

*Предостережение* (Гильбертово пространство намного сложнее евклидова). Гильбертово пространство включает в себя и симметрическое, и симплектическое произведения, причём они связаны. Об этом ниже.

### 5.10.3 Вещественная и мнимая часть эрмитова скалярного произведения

Пусть  $K = \mathbb{C}$ , рассмотрим единственную непрерывную нетривиальную инволюцию  $z \mapsto \bar{z}$ .

Пусть  $V = \mathbb{C}^n$ ,  $B : V \times V \rightarrow \mathbb{C}$  — скоро будет полуторалинейным скалярным произведением

Можно «забыть про комплексную структуру»:  $V_{\mathbb{R}} \cong \mathbb{R}^{2n}$ .

Введём два новых отображения:  $A(u, v) = \Re(B(u, v)); C(u, v) = \Im(B(u, v))$ . Они скоро будут билинейными вещественными скалярными произведениями:  $A, C : V_{\mathbb{R}} \times V_{\mathbb{R}} \rightarrow \mathbb{R}$ .

**Теорема 5.10.2.** Следующие условия эквивалентны:

1.  $B$  — эрмитово скалярное произведение (полулинейное по первому аргументу, линейное — по второму).
2. (a)  $A$  симметрическое,  $C$  симплектическое.  
 (b)  $A(ui, vi) = A(u, v); \quad C(ui, vi) = C(u, v).$   
 (c)  $A(ui, v) = C(u, v); \quad C(ui, v) = -A(u, v).$

*Доказательство.*

$$\Rightarrow. \quad (a) \quad B(u, v) = \overline{B(v, u)}.$$

$$(b) \quad B(ui, vi) = \bar{i}iB(u, v) = B(u, v).$$

$$(c) \quad A(ui, v) + iC(ui, v) = B(ui, v) = \bar{i}B(u, v) = \bar{i}(A(u, v) + iC(u, v)) = C(u, v) - iA(u, v).$$

$\Leftarrow$ . Из определения  $B(u, v) = A(u, v) + iC(u, v)$  видно, что форма линейна по отношению к вещественным числам. Запишем

$$\begin{cases} A(u, vi) = A(vi, u) = C(v, u) = -C(u, v) \\ C(u, vi) = -C(vi, u) = A(v, u) = A(u, v) \end{cases}$$

Теперь проверим линейность по второму аргументу, полулинейность по первому, эрмитовость:

$$B(u, vi) = A(u, vi) + iC(u, vi) = -C(u, v) + iA(u, v) = i(A(u, v) + iC(u, v)) = iB(u, v)$$

$$B(ui, v) = A(ui, v) + iC(ui, v) = C(u, v) - iA(u, v) = \bar{i}(A(u, v) + iC(u, v))$$

$$B(u, v) = \overline{B(v, u)}$$

□

# Глава 6

## Теория групп

### Лекция XXI

10 мая 2023 г.

#### 6.1 Действия групп

##### 6.1.1 Действия групп на множествах

Пусть  $G$  — группа,  $X$  — множество.

**Определение 6.1.1** ( $G$  действует на  $X$  слева). Задано отображение (*левое действие*)

$$\text{act} : G \times X \rightarrow X \quad g, x \mapsto gx \text{ или } {}^g x \text{ (или ещё как-то обозначается)}$$

При действии группы должны быть выполнены аксиомы:

- Внешней ассоциативности:  $h(gx) = (hg)x$ .
- Унитальности:  $1_G \cdot x = x$ .

Также говорят « $X$  —  $G$ -множество».

При правом действии  $x(hg) = (xh)g$ .

*Замечание.* Для групп любое левое  $G$ -множество можно превратить в правое и наоборот:

$$xg \rightsquigarrow g \cdot x = xg^{-1}$$

Чаше будем рассматривать левые действия — действия группы аналогичны применениям функций, а функции мы применять привыкли слева. Например, левым действиям будут соответствовать гомоморфизмы, а не антигомоморфизмы.

*Замечание.* Возникавшие у нас группы на самом деле возникали уже вместе с действиями.

*Примеры.*

- Естественное действие  $S_n \stackrel{\text{def}}{=} \text{Bij}(\underline{n})$ , где  $\underline{n} \stackrel{\text{def}}{=} \{1, \dots, n\}$ . Значит,  $S_n$  естественно действует на  $\underline{n}$ :

$$S_n \times \underline{n} \rightarrow \underline{n} \quad \pi, i \mapsto \pi(i)$$

Вообще, для любого множества  $X$  (необязательно конечного):  $S_X$  действует на  $X$ .

**Лемма 6.1.1.** *Других действий нет. При фиксированных  $G, X$  действиям  $G \curvearrowright X$  биективно сопоставляются гомоморфизмы  $\phi : G \rightarrow S_X \quad g \mapsto (x \mapsto gx)$ . Отображения  $L_g : X \rightarrow X, x \mapsto gx$  называются левыми трансляциями на  $g$ .*

*Доказательство.* Определение очевидно корректно, проверим, что  $\phi$  — гомоморфизм. Аксиомами действия являются  $L_{gh} = L_g L_h$  и  $L_1 = \text{id}_X$ , откуда следует, что  $(L_g)^{-1} = L_{g^{-1}}$ .

Обратно: гомоморфизму  $\phi : G \rightarrow S_X$  сопоставим ему левое действие  $G$  на  $X$ :  $gx = \phi(g)(x)$ .  $\square$

Как раз-таки правые действия соответствовали бы не гомоморфизмам, а антигомоморфизмам.

**Определение 6.1.2** (Перестановочное представление). Выше рассмотренный гомоморфизм  $\phi : G \rightarrow S_X$ .

- Естественное действие  $GL(n, R) \curvearrowright R^n$ :

$$GL(n, R) \times R^n \rightarrow R^n \quad g, u \mapsto gu$$

Левое действие — векторное представление  $GL(n, R)$  на  $R^n$ .

Также есть правое действие  ${}^n R \curvearrowright GL(n, R)$ , которому можно сопоставить  $GL(n, R) \times R^n \rightarrow R^n, g, u \mapsto g^{-t}u$  — *ковекторное представление*.

**Определение 6.1.3** (Линейные действия). Действия  $G \times V \rightarrow V$ , удовлетворяющие аксиомам  $g(u + v) = gu + gv$  и  $g(u\lambda) = (gu)\lambda$ .

**Лемма 6.1.2.** При фиксированных  $G, R^n$  линейным действиям  $G \curvearrowright R^n$  биективно соответствует гомоморфизмы  $\phi : G \rightarrow GL(n, R)$ .

**Определение 6.1.4** (Линейное представление). Вышеописанный гомоморфизм  $G \rightarrow GL(n, R)$ .

- Действие группы  $SL(2, \mathbb{C}) \times \overline{\mathbb{C}} \rightarrow \overline{\mathbb{C}}$ , где  $\overline{\mathbb{C}}$  — одноточечная компактификация  $\mathbb{C}$ , сфера Римана,  $\mathbb{C} \cup \{\infty\}$ .

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \mapsto \frac{az+b}{cz+d}$ . Если знаменатель обнуляется, то (так как  $ad - bc = 1$ ) числитель не обнуляется, по определению  $z \mapsto \infty$ . Если  $z = \infty$ , то  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \begin{cases} \frac{a}{c}, & c \neq 0 \\ \infty, & c = 0 \end{cases}$ . Проверка того, что это действие, оставляется читателю в качестве упражнения.

## 6.1.2 Действие группы на себе. Теорема Кэли

Давайте для группы  $G$  считать, что множество  $X = G$ , посмотрим, что получится.

**Определение 6.1.5** (Левое регулярное представление). Действие  $G$  на себе левыми сдвигами:  $G \times G \rightarrow G \quad g, x \mapsto gx$ .

$L_g : G \rightarrow G, x \mapsto gx$  — левая трансляция. Так как в группе есть сокращение, то  $L_g \in S_G$

**Теорема 6.1.1** (Кэли). Отображение  $G \rightarrow S_G, g \mapsto L_g$  задаёт вложение  $G$  в  $S_G$ .

*Доказательство.*

- $L_g \in S_G$ .
- Это гомоморфизм.
- $L_h = L_g \Rightarrow h = g$  — проверим в любой точке, например, в 1:  $h = L_h(1) = L_g(1) = g$ .  $\square$

**Следствие 6.1.1.**  $|G| = n \Rightarrow G \leq S_n$ .

Это ни в коем случае не биекция, например, так как порядок  $S_{|G|} = |G|!$ , что бы это не значило для бесконечных групп.

**Определение 6.1.6** (Правое регулярное представление). Действие  $G$  на себе правыми сдвигами:  $G \times G \rightarrow G, g, x \mapsto xg^{-1}$ .

$R_g : G \rightarrow G, x \mapsto xg^{-1}$  — правая трансляция. Так как в группе есть сокращение, то  $R_g \in S_G$

*Замечание.* И правое представление, и левое представление — левые действия. Мы рассматриваем левые действия, потому что они соответствуют гомоморфизмам, а не антигомоморфизмам.

**Теорема 6.1.2** (Кэли). Отображение  $G \rightarrow S_G, g \mapsto R_g$  задаёт вложение  $G$  в  $S_G$ .

*Замечание.* Любая левая трансляция коммутирует с любой правой трансляцией:  $L_h R_g(x) = h(xg^{-1}) = (hx)g^{-1} = R_g L_h(x)$ . Таким образом, на  $G$  действует даже не сама группа  $G$ , а

$$G \times G \curvearrowright G \quad (G \times G) \times G \rightarrow G \quad (h, g), x \mapsto hxg^{-1}$$

Это, правда, уже необязательно вложение, например, в абелевой группе вообще  $L_g = R_{g^{-1}}$ .

В частности, совместив с диагонализацией  $\text{diag} : G \rightarrow G \times G, g \mapsto (g, g)$  получим *действие сопряжения*:  $G \times G \rightarrow G, g, x \mapsto {}^g x = gxg^{-1}$ .

Это отображение называется  $I_g : G \rightarrow G, x \mapsto gxg^{-1} = {}^g x$  — внутренний автоморфизм  $G$ . Отображение  $G \rightarrow S_G, g \mapsto I_g$  уже не является вложением, его ядро — центр группы,  $\text{Cent}(G)$ .

### 6.1.3 Действие группы на однородных пространствах. Обобщённая теорема Кэли

Зафиксируем подгруппу  $H \leq G$  — в предыдущем разделе  $H = \{1\}$ . Ей соответствует  $G/H = \{xH \mid x \in G\}$ .

**Определение 6.1.7** (Стандартное действие  $G$  на  $G/H$ ).  $L_g : G \times G/H \rightarrow G/H, g, xH \mapsto gxH$ .

Аналогично  $H \backslash G \times G \rightarrow H \backslash G, Hx, g \mapsto Hxg^{-1}$ .

Получили гомоморфизм  $G \rightarrow S_{G/H}, g \mapsto L_g$ , не обязательно являющийся вложением. Найдём ядро этого гомоморфизма.

Ядро любого гомоморфизма, вообще-то — нормальная подгруппа, а ещё ядро должно быть как-то связано с  $H$ . С  $H$  связаны две нормальные подгруппы  $G$ :  $H_G \leq H \leq H^G$  — *сердцевина*  $H$  (наибольшая нормальная подгруппа  $G$ , содержащаяся в  $H$ ) и нормальная подгруппа  $G$ , порождённая  $H$  (наименьшая нормальная подгруппа  $G$ , содержащая  $H$ ) соответственно. А именно,

$$H_G = \bigcap_{g \in G} H^g \quad H^G = \langle h^g \mid h \in H, g \in G \rangle$$

**Теорема 6.1.3** (Обобщённая теорема Кэли). Ядро гомоморфизма  $L : G \rightarrow S_{G/H}, g \mapsto L_g$  равно сердцевине —  $H_G$ .

*Доказательство.* Мы знаем, что  $L$  — гомоморфизм, вычислим его ядро.

$$\begin{aligned} g \in \text{Ker}(L) &\iff L_g = \text{id}_{G/H} \iff \forall x \in G : L_g(xH) = xH \iff \forall x \in G : gxH = xH \iff \\ &\iff \forall x \in G : x^{-1}gx \in H \iff \forall x \in G : g^x \in H \iff \forall x \in G : g \in H^{x^{-1}} \end{aligned}$$

Отсюда действительно получается, что  $g \in \text{Ker}(L) \iff \forall x \in G : g \in H^x \iff g \in H_G$ . □

Это очень сильная теорема.

**Следствие 6.1.2.**  $|G : H| = n \Rightarrow |G : H_G| \mid n!$ .

*Доказательство.*  $G/H_G \hookrightarrow S_{G/H}$ . Так как  $|G/H| = n$ , то  $|S_{G/H}| = n!$ . □

**Следствие 6.1.3** (Теорема Пуанкаре). *Подгруппа конечного индекса содержит нормальную подгруппу конечного индекса, то есть  $|G : H| < \infty \Rightarrow |G : H_G| < \infty$ .*

**Следствие 6.1.4.** *Если  $p$  — наименьшее простое, делящее порядок  $G$  и  $|G : H| = p$ , то  $H \trianglelefteq G$ .*

*Доказательство.* Согласно (следствие 6.1.2):  $|G : H_G| \mid p!$ ; помимо этого,  $|G : H_G| \mid |G|$ , откуда

$$|G : H_G| \mid \gcd(p!, |G|) = p \Rightarrow H_G = H \quad \square$$

Пусть  $X, Y$  — два  $G$ -множества. Гомоморфизмом  $G$ -множеств  $\phi : X \rightarrow Y$  называют отображение  $\phi(gx) = g\phi(x)$ . Должна быть коммутативна диаграмма

$$\begin{array}{ccc} G \times X & \xrightarrow{\text{act}_X} & X \\ \downarrow \text{id}_G \times \phi & & \downarrow \phi \\ G \times Y & \xrightarrow{\text{act}_Y} & Y \end{array}$$

Если же на множествах действуют разные группы,  $G \curvearrowright X, H \curvearrowright Y$ , то надо ввести ещё *эквивариантное отображение*  $\psi : G \rightarrow H$ , тогда коммутативной должна быть диаграмма

$$\begin{array}{ccc} G \times X & \xrightarrow{\text{act}_X} & X \\ \downarrow \psi \times \phi & & \downarrow \phi \\ H \times Y & \xrightarrow{\text{act}_Y} & Y \end{array} \quad \phi(gx) = \psi(g)\phi(x)$$

## Лекция XXII

13 мая 2023 г.

Пусть  $G \curvearrowright X$ . Рассмотрим  $x \in X$ , с ним можно связать две вещи.

**Определение 6.1.8** (Орбита  $x$ ).  $Gx \stackrel{\text{def}}{=} \{gx | g \in G\} \subset X$ .

**Определение 6.1.9** (Стабилизатор  $x$ ).  $G_x \stackrel{\text{def}}{=} \{g \in G | gx = x\} \leq G$ . В зависимости от конкретной природы действия его также называют *централизатор, нормализатор, подгруппа изотропии*.

**Определение 6.1.10** ( $G$  действует на  $X$  транзитивно).  $X$  состоит из одной орбиты:

$$\exists x \in X : Gx = X \stackrel{\text{здесь эквивалентно}}{\iff} \forall x \in X : Gx = X \stackrel{\text{здесь эквивалентно}}{\iff} \forall x, y \in X : \exists g \in G : gx = y$$

Ещё говорят  $X$  является *однородным  $G$ -множеством*.

**Теорема 6.1.4.**  $Gx \cong G/G_x$  — изоморфизм  $G$ -множеств.

*Доказательство.* Рассмотрим  $y \in Gx \iff \exists g \in G : y = gx$ . Так как  $\forall h \in G_x : x = hx$ , то  $\forall h \in G_x : y = (gh)x$ .

Обратно:  $y = g_1x = g_2x \Rightarrow g_2^{-1}g_1x = x \Rightarrow g_2^{-1}g_1 \in G_x$ , то есть  $g_1G_x = g_2G_x$ .

Таким образом,  $g_1x = g_2x \iff g_1G_x = g_2G_x$ . Значит, можно сопоставить

$$Gx \longleftrightarrow G/G_x \quad gx \longleftrightarrow gG_x$$

Теперь проверим, что это не просто изоморфизм множеств, а изоморфизм  $G$ -множеств:

$$\forall f \in G : fy = f(gx) = (fg)x \quad \square$$

Другими словами, теорема утверждает, что никаких других однородных  $G$ -множеств, кроме факторов по стабилизаторам, нет.

**Следствие 6.1.5.**  $|Gx| = |G : G_x|$ .

**Лемма 6.1.3.** Две орбиты либо не пересекаются, либо совпадают.

*Доказательство.*  $\exists h, g \in G : hx = gy \Rightarrow y = g^{-1}hx \Rightarrow y \in Gx \Rightarrow Gy \subset Gx$ . Аналогично  $Gx \subset Gy$ .  $\square$

*Предостережение.* Пусть  $S$  — моноид, действующий на  $X$ . Тогда нужно различать орбиты и траектории.  $Sx = \{sx | s \in S\}$  — траектория.

Из того, что нашлись  $h, g \in G : hx = gy$  совсем не следует, что траектории  $x$  и  $y$  совпадают — преобразование необратимо. Чтобы получить орбиты, надо взять транзитивное замыкание траекторий:



Согласно аксиоме выбора существует система представителей — *трансверсаль* к действию  $G$  на  $X$ .

**Теорема 6.1.5.**  $X = \bigsqcup_{x \in Y} Gx$ , где  $Y$  — трансверсаль.

Для конечного трансверсали  $X = X_1 \sqcup \dots \sqcup X_m$ , где  $X_i$  — однородные  $G$ -множества.

*Примеры.*

- Подгруппа  $H \leq G$  может действовать на группе трансляциями:  $H \curvearrowright G; h, g \mapsto hg$ . В этом случае орбиты — смежные классы  $H \backslash G$ , стабилизатор любого элемента —  $\{1\}$ . Можно выбрать трансверсаль  $T, G = \bigsqcup_{x \in T} xH$ .

Каждая орбита изоморфна  $H \curvearrowright H$ .

**Определение 6.1.11** ( $X$  — главное однородное пространство для  $G$ ).  $X \cong G$  как  $G$ -множество, то есть

$$\forall x, y \in X : \exists! g : gx = y$$

Как только изоморфизм фиксируется:  $1 \mapsto x$  для конкретного  $x$ ,  $X$  перестанет отличаться от  $G$ .

Прослеживается аналогия с евклидовым пространством, в котором не выбрали начало координат.

- $G \curvearrowright G, g, x \mapsto {}^g x = gxg^{-1}$ . В данном частном случае орбиты — *классы сопряжённых*, стабилизатор — *центральный*:  $C_G(x) = \{g \in G | {}^g x = x\}$ .

Согласно предыдущей теореме  $x^G \cong G/C_G(x)$ .

- Группа  $G$  может действовать на  $2^G$ . В данном частном случае стабилизаторы — *нормализаторы*: для  $Y \subset X: N_G(Y) \stackrel{\text{def}}{=} \{g \in G | {}^g Y = Y\}$ .

*Замечание.* Вычисление жордановой формы — задача вычисления трансверсали орбит группы  $GL(n, R)$ , на которой она сама  $(GL(n, R))$  действует сопряжением.

## 6.2 Классификация $G$ -множеств

Как мы уже знаем,  $\forall G$ -множества  $X: X = \bigsqcup_i X_i$ , где  $X_i$  — однородное  $G$ -множество.

Всякое же однородное  $G$ -множество изоморфно  $G/H$  для  $H \leq G$ .

Когда для двух подгрупп  $F, H \leq G: G/F \cong G/H$  — изоморфизм  $G$ -множеств?

Выберем произвольный  $x \in G$ . Пусть  $X = Gx, y \in X$ . Значит  $X \cong G/G_x$ , но так как  $X = Gy$ , то ещё и  $X \cong G/G_y$ . Рассмотрев  $h \in G_y$  (используя, что  $y = gx$  для некоего  $g \in G$ ) получаем, что  $g^{-1}hg \in G_x$ .

**Лемма 6.2.1.**  $\forall g \in G : (y = gx \Rightarrow g^{-1}G_y g = G_x)$ , то есть стабилизаторы точек в одной орбите сопряжены.

**Следствие 6.2.1.**  $F$  сопряжено с  $H \Rightarrow G/F \cong G/H$  — изоморфизм  $G$ -множеств.

**Теорема 6.2.1** (Классификация однородных пространств). Пусть  $F, H \leq G$ . Тогда  $G/F \cong G/H \iff F \sim H$  ( $F$  и  $H$  сопряжены).

*Доказательство.*

$\Leftarrow$ . Доказано выше.

$\Rightarrow$ . Пусть  $G/F \cong G/H$ . Выберем  $g \in G : F \mapsto gH$ . Стабилизатор точки  $F$  (при действии  $G \curvearrowright G/F$ ) — это  $F$ , стабилизатор точки  $gH$  (при действии  $G \curvearrowright G/H$ ) —  $gHg^{-1}$ . Значит,  $F \sim H$ .  $\square$

Таким образом, чтобы описать все  $G$ -множества, надо описать все подгруппы с точностью до сопряжения. Это, правда, дикая задача.

## 6.3 Конечные группы

Будем рассматривать конечные группы, действующие на конечных множествах.

### 6.3.1 Центр $p$ -группы, теоремы Коши

Обозначим  $\text{Fix}_G(X) = X^G \stackrel{\text{def}}{=} \{x \in X | \forall g \in G : gx = x\}$ . К сожалению,  $X^G$  уже ранее было задействовано в другом смысле. Очень жаль. . .

Пусть  $p \in \mathbb{P}$  — простое.

**Лемма 6.3.1.** Пусть  $\forall H \leq G : H \neq G \Rightarrow |G : H| \vdots p$ . При действии  $G \curvearrowright X : |X^G| \equiv |X| \pmod{p}$ .

*Доказательство.* Посмотрим на орбиты.  $X^G = \bigsqcup \tilde{X}_i$ , где  $\tilde{X}_i$  — одноэлементные орбиты. Значит,  $X = X^G \sqcup X_1 \cdots \sqcup X_m$ , где  $X_i$  — различные орбиты, такие, что  $|X_i| > 1$ . Так как  $|Gx_i| = |G : G_{x_i}|$ , то  $|Gx_i| \vdots p$ .  $\square$

**Определение 6.3.1** ( $G$  —  $p$ -группа).  $|G| = p^m$  для некоего  $m \in \mathbb{N}_0$ .

**Теорема 6.3.1** (Доказал Силлов, но пока ещё не теорема Силова). Если  $G$  —  $p$ -группа, то её центр нетривиален.

*Доказательство.* Рассмотрим  $G \curvearrowright G$  — действие сопряжением. Центр — множество инвариантов (неподвижных точек) этого действия. Значит,  $|\text{Cent}(G)| \equiv |G| \pmod{p}$ .  $\square$

**Следствие 6.3.1** (Нетте). Группы порядка  $p$  и  $p^2$  абелевы.

*Доказательство.* Для  $|G| = p$  её центр — она сама. Предположим, что  $|G| = p^2$ ,  $|\text{Cent}(G)| = p$ . Тогда  $|G/\text{Cent}(G)| = p$ , то есть  $G/\text{Cent}(G) \cong C_p$ , откуда  $G$  — абелева (всякий элемент  $G$  представим в виде  $g^i h$ , где  $0 \leq i < p, h \in \text{Cent}(G)$ ). Легко видеть, что они коммутируют)  $\square$

**Теорема 6.3.2** (Коши). Пусть  $|G| \vdots p$ . Тогда количество решений уравнения  $x^p = 1$  делится на  $p$ .



*Доказательство Маккея.* Положим  $X = \{(x_1, \dots, x_p) | x_i \in G; x_1 \cdot \dots \cdot x_p = 1\}$   $\cong$   $G^{p-1}$ .  
 $|X| : p$ .

Рассмотрим действие  $C_p \curvearrowright X$  оператором  $\text{RotateRight} : X \rightarrow X$ ;  $\text{RotateRight}(x_1, \dots, x_{p-1}, x_p) = (x_p, x_1, \dots, x_{p-1})$  — это действие произвольной образующей  $C_p$ , остальные определяются однозначно.

Неподвижные точки  $X^{C_p}$  — это в точности  $\{(x, \dots, x) | x^p = 1\}$ . Поэтому количество решений уравнения сравнимо с  $|X|$  по модулю  $p$ .  $\square$

*Интересный факт* (Теорема Фробениуса). Если  $|G| : n$ , то количество решений уравнения  $x^n = 1$  в  $G$  делится на  $n$ .

**Следствие 6.3.2.** В частности, в группе порядка, делящегося на  $p$ , существует  $x \neq 1 : x^p = 1$  *здесь эквивалентно*  $o(x) = p$ .

**Следствие 6.3.3.** В  $p$ -группе нормализатор любой собственной подгруппы строго больше чем она.

### 6.3.2 Теоремы Силова

Если  $G$  — абелева, то  $G = \bigoplus_{p \in \mathbb{P}, p \mid |G|} G_p$ , где  $G_p$  — примарные компоненты. В неабелевых группах будет что-то отдалённо похожее.

**Определение 6.3.2** ( $G_p \leq G$  — силовская  $p$ -подгруппа).

1.  $G_p$  —  $p$ -группа.
2.  $|G : G_p| \perp p$ .

**Теорема 6.3.3** (Силов,  $E_p$  (existence)). Пусть  $G$  — конечная группа. Для любого  $p \in \mathbb{P} : \exists H \leq G$  — силовская  $p$ -подгруппа.

**Теорема 6.3.4** (Силов,  $C_p$  (conjugacy)). Для данного  $p$  любые две силовские  $p$ -подгруппы сопряжены в  $G$ .

**Теорема 6.3.5** (Силов,  $D_p$ ). Если  $H \leq G$ ,  $H = p^l$ , то найдётся силовская  $p$ -подгруппа, содержащая  $H$ .

**Теорема 6.3.6** (Силов — Фробениус,  $F_p$  (Anzahlssatz)). Для любого  $l \in \mathbb{N}_0 : p^l \mid |G| \Rightarrow |\{H \leq G | |H| = p^l\}| \equiv 1 \pmod{p}$ .

В частности, количество силовских  $p$ -подгрупп делится на  $p$  с остатком 1.

*Пример.* Рассмотрим  $GL(n, q) \stackrel{\text{def}}{=} GL(n, \mathbb{F}_q)$ , где  $q = p^m$ .

$$|GL(n, q)| = (q^n - 1)(q^n - q) \cdot \dots \cdot (q^n - q^{n-1}) = q^{n(n-1)/2} (q^n - 1) \cdot \dots \cdot (q - 1)$$

так как каждый столбец необходимо выбирать так, что он не лежит в линейной оболочке предыдущих.

Рассмотрим подгруппу  $U(n, q)$ , состоящую из верхних унитреугольных матриц  $\begin{pmatrix} 1 & * & * \\ & 1 & * \\ 0 & & 1 \end{pmatrix}$ .  $|U(n, q)| = q^{n(n-1)/2}$ . Значит,  $U(n, q)$  — силовская  $p$ -подгруппа в  $GL(n, q)$ .

#### Первое доказательство Фробениуса теоремы Силова

*Доказательство  $E_p$ .*  $G \xrightarrow{\text{теорема Кэли}} S_{|G|} \xrightarrow{\text{матрицы перестановки}} GL(|G|, p)$ . Пусть  $H = U(|G|, p)$  — силовская  $p$ -подгруппа в  $GL(|G|, p)$ .

Рассмотрим двойные смежные классы  $G \backslash GL(|G|, p) / H$ . Пусть  $\{x_1, \dots, x_m\}$  — трансверсаль. Согласно формуле индекса Фробениуса

$$|GL(|G|, p) : H| = |G : (G \cap x_1 H x_1^{-1})| + \dots + |G : (G \cap x_m H x_m^{-1})|$$

Так как левая часть взаимно проста с  $p$ , то  $\exists x_i : |G : (G \cap x_i H x_i^{-1})| \perp p$ . Таким образом,  $G \cap x_i H x_i^{-1}$  — силовская  $p$ -подгруппа в  $G$ .  $\square$

*Замечание.* У Фробениуса вместо  $GL(|G|, p)$  была симметрическая группа, в которой  $p$ -подгруппу построить весьма нетривиально.

*Доказательство  $C_p$  и  $D_p$ .* Пусть  $H, P \leq G$  причём  $|P| = |G|_p$ , где  $|G|_p$  —  $p$ -часть числа, наибольшая степень  $p$ , делящая  $|G|$ .

Докажем, что если  $|H| = p^m$ , то  $\exists g \in G : H^g \leq P$ .

$$H \backslash G/P = Hx_1P \sqcup \dots \sqcup Hx_sP.$$

$$p \perp |G : P| = |H : (H \cap x_1 P x_1^{-1})| + \dots + |H : (H \cap x_s P x_s^{-1})|$$

Так как  $H$  —  $p$ -группа, то в правой части — степени  $p$ . Значит,  $\exists x_i : H = H \cap x_i P x_i^{-1} \Rightarrow H^{x_i} \leq P$ .  $\square$

*Доказательство частного случая  $F_p$  — для  $p^l = |G|_p$ .* Рассмотрим множество силовских  $p$ -подгрупп  $\text{Syl}_p(G)$ . Пусть  $P \in \text{Syl}_p(G)$ , рассмотрим действие сопряжениями  $P \curvearrowright \text{Syl}_p(G)$ . Если  $Q$  — неподвижная точка действия, то  $P$  нормализует  $Q$ , то есть  $PQ = QP$ , откуда  $PQ \leq G$ .

Согласно формуле произведения  $|PQ| \mid |P| \cdot |Q|$ . Значит,  $PQ$  —  $p$ -группа. Если  $P \neq Q$ , то  $P \leq PQ$ , силовская  $p$ -подгруппа не максимальна, противоречие.

Значит, у действия ровно одна неподвижная точка, откуда  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$ .  $\square$

### Формула классов, второе доказательство Фробениуса

*Доказательство  $E_p$ .* Пусть  $|G| < \infty, p \mid |G|$ . Значит,  $\exists x \in G : o(x) = p$ .

Рассмотрим действие сопряжением  $G \curvearrowright G$ , выберем трансверсаль  $X$  к орбитам.

$$X = \text{Cent}(G) \cup \underbrace{\{x_1, \dots, x_m\}}_{\text{представители нецентральных классов}}$$

Формула классов:

$$|G| = |\text{Cent}(G)| + |G : C_G(x_1)| + \dots + |G : C_G(x_m)|$$

Индукция по  $|G|$ .

- Либо  $|\text{Cent}(G)| \geq p$ , тогда  $\exists x \in \text{Cent}(G) : x^p = 1$ , тогда  $|G/\langle x \rangle| \leq |G|$ . В факторгруппе силовская  $p$ -подгруппа уже есть,  $|Q| = p^{h-1}$ , где  $p^h = |G|_p$ . Прообраз  $Q$  в  $G$  — группа  $\pi^{-1}(Q)\langle x \rangle$ , её порядок — как нужно.
- Либо  $|\text{Cent}(G)| \not\geq p$ . Значит, из формулы классов выше  $\exists x_i : C_G(x_i) \leq G$ , но  $|G : C_G(x_i)| \perp p$ . Тогда получается, что  $|C_G(x_i)|_p = |G|_p$ , найдём силовскую  $p$ -подгруппу по индукции.  $\square$

*Пример* (Силовские  $p$ -подгруппы в  $S_n$ ). Силовская подгруппа в  $S_p$  — это  $C_p$ . Силовская подгруппа в  $S_{p^2}$  порядка  $|p^{p+1}|$  — это сплетение  $C_p \wr C_p$  — можно переставлять элементы в каждом столбце таблицы  $p \times p$ , а ещё — переставлять сами столбцы.

---

**Определение 6.3.3** ( $H \leq G$  — холловская подгруппа).  $|H| \perp |G : H|$ .

Пусть  $\pi \subset \mathbb{P}$ .

**Определение 6.3.4** ( $G$  —  $\pi$ -группа).  $p \mid |G| \Rightarrow p \in \pi$ .

**Определение 6.3.5** ( $H$  — холловская  $\pi$ -подгруппа в  $G$ ).  $H$  —  $\pi$ -группа и  $|G : H|$  взаимно прост со всеми  $p \in \pi$ .

Оказывается,  $E_\pi, C_\pi, D_\pi, F_\pi$  — ничего из этого неверно.

Но можно добавить условие разрешимости  $G$  (определение было в I семестре, есть цепочка подгрупп, фактор следующей по предыдущей абелев, последняя подгруппа тривиальна). В разрешимых группах  $E_\pi, C_\pi, D_\pi, F_\pi$  выполнены.

Более того, если для каждого  $p \in \pi$  существует холловская  $p$ -подгруппа, то сама группа разрешима??

## 6.4 Тожества с коммутаторами

Пусть  $G$  — произвольная группа.

**Определение 6.4.1** (Левонормированный коммутатор).  $[x, y] = xyx^{-1}y^{-1}$

**Определение 6.4.2** (Коммутант).  $[G, G] = \langle [x, y] \mid x, y \in G \rangle$ .

Из I семестра мы помним, что  $[G, G] \trianglelefteq G$ ,  $G/[G, G] = G^{\text{ab}}$  — абелева группа (абелианизация  $G$ ), причём если  $H \trianglelefteq G$ ,  $G/H$  — абелева, то  $H \geq [G, G]$ .

**Определение 6.4.3** (Взаимный коммутант).  $[F, H] = \langle [f, h] \mid f \in F, h \in H \rangle$ .

**Предложение 6.4.1.**  $H \trianglelefteq G \iff [H, G] \leq H$ .

1.  $[x, y]^{-1} = xyx^{-1}y^{-1} = yxy^{-1}x^{-1} = [y, x]$
2.  $[xy, z] = xyzy^{-1} \underbrace{x^{-1}z^{-1}}_{z^{-1}x^{-1}xz} = {}^x[y, z] \cdot [x, z]$

соответствует дистрибутивности аддитивного коммутатора  $[x, y] \stackrel{\text{def}}{=} xy - yx$  по первому аргументу.

3.  $[x, yz] = xy \underbrace{zx^{-1}z^{-1}y^{-1}}_{x^{-1}y^{-1}yx} = [x, y] \cdot {}^y[x, z]$

соответствует дистрибутивности аддитивного коммутатора по второму аргументу.

4.

**Определение 6.4.4** (Тройной коммутатор).  $[x, y, z] = [[x, y], z] = xyx^{-1}y^{-1}zyxy^{-1}x^{-1}z^{-1}$ .

**Определение 6.4.5** (Кратный коммутатор).  $[x_1, \dots, x_n] = [[x_1, \dots, x_{n-1}], x_n]$ .

**Лемма 6.4.1** (Холл — Витт).

$$[x, y^{-1}, z^{-1}]^x \cdot [z, x^{-1}, y^{-1}]^z \cdot [y, z^{-1}, x^{-1}]^y = 1$$

*Доказательство.* «Мы оставляем читателю в качестве упражнения расписать тройные коммутаторы»  $\square$

**Определение 6.4.6.**  $[A, B, C] = [[A, B], C]$ .

**Лемма 6.4.2** (О трёх подгруппах). Пусть  $A, B, C \leq G$ ;  $H \trianglelefteq G$ . Если две из трёх

$$[A, B, C] \quad [B, C, A] \quad [C, A, B]$$

содержатся в  $H$ , то и третья — тоже.

*Доказательство.* Тожество Холла — Витта.  $\square$

# Лекция XXIII

16 мая 2023 г.

## 6.5 Прямое произведение двух подгрупп

Если  $F, H$  — произвольные группы, то определено внешнее прямое произведение — группа, в которую они обе вкладываются.

**Определение 6.5.1** (Внешнее прямое произведение).  $F, H \rightsquigarrow F \times H \stackrel{\text{def}}{=} \{(f, h) | f \in F, h \in H\}$ , где операции покомпонентны.

$$F \hookrightarrow F \times H \hookleftarrow H; \quad f \mapsto (f, 1) \quad (1, h) \mapsto h$$

Пусть теперь  $F, H \leq G$ . Когда  $G \cong F \times H$ ? Нас даже интересует естественный изоморфизм, когда вложения  $F, H \hookrightarrow F \times H$  тождественные.

**Теорема 6.5.1.**  $G$  является прямым произведением  $F$  и  $H$ , если выполнены условия

1.  $\langle F, H \rangle = G$ .
2.  $F \cap H = \{1\}$ .
3.  $F, H \trianglelefteq G$ .

*Доказательство.* Если  $G$  — прямое произведение  $F, H$ , то условия выполнены. Докажем в другую сторону.

Из 1+3 вытекает  $G = FH = HF$ , то есть  $\forall g \in G : \exists f, h, f', h' : g = fh = h'f'$ .

Из 2+3 вытекает  $[F, H] = \{1\}$ . В самом деле,

$$[f, h] = \underbrace{(fhf^{-1})}_{\in H} h^{-1} = f \underbrace{(hf^{-1}h)}_{\in F}$$

Далее получаем, что все элементы  $F, H$  коммутируют, поэтому  $\forall g \in G : \exists! f \in F, h \in H : g = fh = hf$ . Единственность легко показать от противного.

Сопоставим всякому  $g \in G : (f, h) \in F, H : fh = g$  (такая пара единственна).

$$g_1 = f_1 h_1, g_2 = f_2 h_2 \Rightarrow g_1 g_2 = (f_1 h_1)(f_2 h_2) = (f_1 f_2)(h_1 h_2) \quad \square$$

Теперь займёмся ослаблением условий теоремы.

**Определение 6.5.2** ( $G$  — центральное произведение  $F, H \leq G$ ).

1.  $\langle F, H \rangle = G$ .
2.  $[F, H] = \{1\}$ .
3.  $F, H \trianglelefteq G$ .

Доказательство остаётся прежним, по-прежнему каждому элементу  $g \in G$  можно (но уже необязательно единственным образом) сопоставить  $(f, h) \in F \times H : fh = g$ . Центральные элементы  $z \in F \cap H$  можно перебрасывать:  $g = (fz)(z^{-1}h)$  (они центральные, так как они коммутируют и с  $F$ , и с  $H$ ).

**Определение 6.5.3** ( $G$  — почти прямое произведение  $F, H \leq G$ ).

1.  $\langle F, H \rangle = G$ .
2.  $|F \cap H| < \infty$ .
3.  $F, H \trianglelefteq G$ .

**Определение 6.5.4** ( $G$  — подпрямое произведение  $F, H \leq G$ ).

1.  $G \leq F \times H$ .
2. Проекция  $G$  на  $F$  и  $H$  сюръективны.

### 6.5.1 Прямое произведение нескольких подгрупп

Пусть  $H_1, \dots, H_m \leq G$ . Когда  $G \cong H_1 \times \dots \times H_m$  естественным образом, то есть естественные включения — вложения?

**Теорема 6.5.2.**  $G$  является прямым произведением  $H_1, \dots, H_m$ , если выполнены условия

1.  $\langle H_1, \dots, H_m \rangle = G$ .
2.  $H_i \cap \langle H_1, \dots, \widehat{H_i}, \dots, H_m \rangle = \{1\} \iff H_i \cap (H_1 \cdot \dots \cdot \widehat{H_i} \cdot \dots \cdot H_m) = \{1\}$ .
3.  $H_1, \dots, H_m \trianglelefteq G$ .

*Доказательство.* Оставлено читателю в качестве упражнения. Легче всего по индукции. □

### 6.5.2 Прямое произведение многих подгрупп

Что такое  $\prod_{i \in I} G_i$ , где  $G_i \leq G, I$  — произвольное множество индексов?

Элементы произведения —  $\{(g_i)_{i \in I} | g_i \in G_i\}$ , либо  $\{(g_i)_{i \in I} | g_i \in G_i, \text{ почти все } g_i = 1\}$ . В алгебре «почти все» — все кроме конечного числа.

Обе конструкции — частный случай *ограниченного прямого произведения*:

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I} | g_i \in G_i, \text{ почти все } g_i \in H_i\}$$

## 6.6 Полупрямое произведение

Пусть  $F, H \leq G$ .

**Определение 6.6.1** ( $G$  — полупрямое произведение нормальной подгруппы  $H$  и дополнительной подгруппы  $F$ ).

1.  $\langle F, H \rangle = G$ .
2.  $|F \cap H| = \{1\}$ .
3.  $H \trianglelefteq G$ .

Обозначают  $G = F \ltimes H = H \rtimes F$ .

По-прежнему  $G = FH = HF$ , но они уже необязательно коммутируют: известно лишь, что  $[F, H] \leq H$ .

$$\forall g \in G : \exists! f, f' \in F, h, h' \in H : g = fh = h'f'$$

Так как коммутант лежит в  $H$ , то на самом деле  $f = f' : h'f' = (fhf^{-1})f$ .

Как эти элементы перемножать?

$$g_1 = h_1 f_1, g_2 = h_2 f_2 \Rightarrow g_1 g_2 = (h_1 f_1)(h_2 \underbrace{f_2}_{f_1^{-1} f_1}) = (h_1 f_1 h_2 f_1^{-1})(f_1 f_2) = (h_1 \cdot {}^{f_1} h_2)(f_1 f_2)$$

*Замечание.* При перемножении  $f_1 h_1 \cdot f_2 h_2$  появляется сопряжение не элементом  $f_1$ , а элементом  $f_1^{-1}$ , что потом породит не гомоморфизмы, а антигомоморфизмы.

Пусть нам даны

1. Группы  $F$  и  $H$ .
2. Гомоморфизм  $\theta : F \rightarrow \text{Aut}(H)$ .

**Определение 6.6.2** (Полупрямое произведение, отвечающее «действию автоморфизмами»  $\theta$ ).  $H \rtimes_{\theta} F \stackrel{\text{def}}{=} \{(h, f) | h \in H, f \in F\}$  с действием, определённым так:

$$(h_1, f_1) \cdot (h_2, f_2) = (h_1 \theta(f_1)(h_2), f_1 f_2)$$

**Теорема 6.6.1.**  $H \rtimes_{\theta} F$  — группа, изоморфная полупрямому произведению своих подгрупп  $H^1 = \{(h, 1) | h \in H\}$  и  $F^1 = \{(1, f) | f \in F\}$ .

Группа является полупрямым произведением подгрупп, если факторгруппа вкладывается.

Более общим примером, примером *расширения* является конструкция  $\mathbb{Z}/100\mathbb{Z}$  из групп единиц и десятков:

$$1 \rightarrow \mathbb{Z}/10\mathbb{Z} \rightarrow \mathbb{Z}/100\mathbb{Z} \rightarrow \mathbb{Z}/10\mathbb{Z} \rightarrow 1$$

*Замечание.* Для нетривиального действия полупрямое произведение двух абелевых групп вполне может стать неабелевым.

*Примеры* (Полупрямое произведение).

- Рассмотрим следующие подгруппы в  $GL(n, K)$ :

$$B(n, K) = \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix} \quad D(n, K) = \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \quad U(n, K) = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Борелевские — (верхне) треугольные матрицы      диагональные матрицы      (верхние) унитреугольные матрицы

$$\boxed{B = D \ltimes U}$$

- $N(n, K)$  — группа мономиальных матриц, то есть  $N = \left\{ x \in GL(n, K) \mid \begin{cases} \forall i : \exists ! j : x_{i,j} \neq 0 \\ \forall j : \exists ! i : x_{i,j} \neq 0 \end{cases} \right\}$ .
- $W_n$  — матрицы перестановки, то есть  $W_n = \{x \in N(n, K) | \forall i, j : x_{i,j} = 0 \vee x_{i,j} = 1\}$ .  $W_n \cong S_n$ .

$$\boxed{N = W_n \ltimes D}$$

- Группа аффинных матриц  $Aff(n, K) = \left\{ \begin{pmatrix} g & u \\ 0 & 1 \end{pmatrix} \mid g \in GL(n, K), u \in K^n \right\}$ . Группа отвечает аффинным движениям, то есть композиции вращения относительно начала координат (за это отвечает  $GL(n, K)$ ) и параллельного переноса (за это отвечает  $K^n$ ).

$$\begin{pmatrix} g_1 & u_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} g_2 & u_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} g_1 g_2 & g_1 u_2 + u_1 \\ 0 & 1 \end{pmatrix}$$

$$\boxed{GL(n, K) \ltimes K^n = Aff(n, K)}$$

## 6.7 Группы порядка $pq$

Пусть  $p < q$  — различные простые числа,  $G$  — группа ( $|G| = pq$ ). Как она выглядит?

В ней совершенно точно есть силовские подгруппы  $P, Q \leq G, |P| = p, |Q| = q$ . Число силовских  $q$ -подгрупп сравнимо с 1 (mod  $q$ ), но так как это число — делитель  $pq$  (число классов сопряжённости

к  $Q$ ), то оно равно 1. Значит, в  $G$  ровно одна силовская  $q$ -подгруппа, она инвариантна относительно сопряжения, то есть  $Q \triangleleft G \Rightarrow G = P \ltimes Q$ .

Как известно, группа простого порядка  $p$  единственна с точностью до изоморфизма — все порядки элементов делят размер группы, таким образом, есть элемент порядка  $p$ , то есть группа циклическая.

$G$  определяется действием  $P \curvearrowright Q$  автоморфизмами  $\theta : P \rightarrow \text{Aut}(Q)$ . Автоморфизмы  $C_q$  отправляют произвольную образующую в произвольную, они изоморфны  $C_{q-1}$ .

Очевидно, есть тривиальный  $\theta : P \rightarrow \text{id}$ . Он соответствует абелевой группе  $C_p \times C_q$ .

Заметим, что нетривиальный гомоморфизм  $\theta$  существует, если  $p \mid q-1$ .

Зафиксируем результат:

**Теорема 6.7.1.** Неабелевы группы порядка  $pq$ , где  $p < q, p, q \in \mathbb{P}$  существуют только если  $p \mid q-1$ .

*Примеры.*

- Все группы порядка 15 абелевы.
- Есть неабелева группа (группа Фробениуса) порядка 21.

Вообще, верен более общий факт:

*Интересный факт* (Теорема Диксона).  $\gcd(n, \phi(n)) = 1 \iff \exists! |G| = n$  (и эта группа абелева).

## Лекция XXIV

17 мая 2023 г.

### 6.8 Крохотный кусок комбинаторной теории групп

#### 6.8.1 Свободные группы

Пусть  $X$  — множество.

**Определение 6.8.1** (Свободная группа  $F_X$  со свободным множеством образующих  $X$ ). Группа вместе с вложением  $X \hookrightarrow F_X$ , такая, что  $\forall$  группы  $G, \forall \phi : X \rightarrow G: \exists! \psi : F_X \rightarrow G$  — гомоморфизм групп, делающий следующую диаграмму коммутативной.

$$\begin{array}{ccc} X & \xrightarrow{\eta} & F_X \\ & \searrow \phi & \swarrow \psi \\ & & G \end{array}$$

Обычно  $X$  конечно, мы будем рассматривать конечнопорождённые свободные группы. В таком случае если  $|X| = n$ , то пишут  $F_n$  вместо  $F_X$ .

*Замечание.* Если бы в определении были абелевы группы, то это были бы в точности свободные модули над  $\mathbb{Z}$ .

*Замечание.* Если свободная группа существует, то она единственна, причём с точностью до единственного изоморфизма.

В самом деле, если есть две свободные группы  $F_X$  и  $\widetilde{F}_X$  со вложениями  $\eta : X \hookrightarrow F_X, \tilde{\eta} : X \hookrightarrow \widetilde{F}_X$ , то существуют и единственны гомоморфизмы групп  $\psi : F_X \rightarrow \widetilde{F}_X, \tilde{\psi} : \widetilde{F}_X \rightarrow F_X$ , такие, что

$$\forall x \in X : \psi(\eta(x)) = \tilde{\eta}(x) \quad \tilde{\psi}(\tilde{\eta}(x)) = \eta(x)$$

Таким образом, видно (например, из конструкции свободной группы, которая приведена ниже), что  $\psi$  и  $\tilde{\psi}$  взаимно обратные отображения, то есть  $\psi : F_X \rightarrow \widetilde{F}_X$  — изоморфизм. Он единственный, так как единственный гомоморфизм групп  $\psi : F_X \rightarrow \widetilde{F}_X$ .

**Определение 6.8.2** (Свободный моноид  $W_X$  со свободным множеством образующих  $X$ ). Моноид вместе с вложением  $X \hookrightarrow W_X$ , такой, что  $\forall$  моноида  $S, \forall \phi : X \rightarrow S: \exists! \psi : W_X \rightarrow S$  — гомоморфизм моноидов, делающий следующую диаграмму коммутативной.

$$\begin{array}{ccc} X & \xrightarrow{\eta} & W_X \\ & \searrow \phi & \swarrow \psi \\ & S & \end{array}$$

**Лемма 6.8.1.** Свободный моноид уж точно существует.

*Доказательство.* Моноид с множеством образующих  $X$  — это просто набор слов. Так, для  $X = \{a, b\}$ :  $W_X \stackrel{\text{def}}{=} \{\wedge, a, b, aa, ab, ba, bb, aba, \dots\}$ .

Операцией в моноиде является конкатенация:  $(x_1 \dots x_n) * (y_1 \dots y_m) = x_1 \dots x_n y_1 \dots y_m$ . Эта операция ассоциативна, но некоммутативна.

Таким образом,  $(W_X, *, \wedge)$  — свободный моноид (слова равны, если они физически равны; для отображения  $\phi : X \rightarrow S$  гомоморфизмом  $\psi : W_X \rightarrow S$  является тот, который отправляет слово  $x_1 \dots x_n \in W_X$  в  $\phi(x_1) \cdot \dots \cdot \phi(x_n) \in S$ ).  $\square$

**Теорема 6.8.1.** Для любого множества образующих  $X$  существует свободная группа.

*Доказательство.* Удвоим алфавит: выберем множество  $X' : |X'| = |X|$  вместе с биекцией  $X \leftrightarrow X'; x \leftrightarrow x'$  и построим свободный моноид  $W_{X \sqcup X'}$ . Введём на  $W_{X \sqcup X'}$  отношение эквивалентности  $\sim$ , являющееся транзитивным замыканием отношения предэквивалентности

$$\forall u, v \in W_{X \sqcup X'}, x \in X : uxx'v \sim uv \sim ux'xv$$

Определим  $F_X \stackrel{\text{def}}{=} (W_{X \sqcup X'}) / \sim$  с наследованной от моноида операцией. Очевидно, она определена корректно:  $w_1 \sim w'_1; w_2 \sim w'_2 \Rightarrow w_1 w_2 \sim w'_1 w'_2$ . Более того, она осталась ассоциативной, а класс эквивалентности пустого слова  $[\wedge]$  — нейтральный элемент. Операция взятия обратного в группе работает так:  $(x_1 \dots x_n)^{-1} = x'_n \dots x'_1$ .

Определим  $\psi : W_{X \sqcup X'} \rightarrow G$  аналогично:  $\psi(x_1 \dots x_n) = \phi(x_1) \cdot \dots \cdot \phi(x_n)$  (правда для этого придётся доопределить  $\phi$  на  $X'$ :  $\phi(x'_i) := \phi(x_i)^{-1}$ ).

Так как отношение эквивалентности лежит в ядре (множество элементов, эквивалентных тривиальному слову лежит в  $\text{Ker}(\psi)$ ), то  $\psi$  пропускается через фактор:

$$\begin{array}{ccc} X & \xrightarrow{\eta} & W_{X \sqcup X'} \\ & \searrow \phi & \swarrow \psi \\ & F_X & \\ & \searrow & \swarrow \\ & G & \end{array}$$

Пропущенный через фактор  $\psi$  и есть искомый гомоморфизм групп — он сохраняет произведение, единицу и обратные. Более того, из построения видно, что это — единственный способ его построить, поэтому гомоморфизм групп действительно единственный.  $\square$

**Определение 6.8.3** (Редуцированное (приведённое) слово  $w \in W_{X \sqcup X'}$ ). Слово, в котором нет фрагментов вида  $xx'$  или  $x'x$ .

**Теорема 6.8.2.** В каждом классе эквивалентности слов есть единственное редуцированное.



*Доказательство.* Пусть есть два редуцированных слова  $w_1 \sim w_2$ . Они эквивалентны, так как есть цепочка отношений предэквивалентностей  $w_1 = u_1 \sim \dots \sim u_n = w_2$ .



Выберем среди всех таких цепочек цепочку с минимальной длиной максимального слова, а среди этих — с минимальным количеством слов максимальной длины.

Так как слова редуцированные, то в цепочке отношений предэквивалентности первый шаг был вверх — в удлинение слова, а последний — вниз. Значит, где-то был пик. Надо рассмотреть три варианта:

1. Врисовали и вычеркнули одну и ту же пару — эти два шага можно взаимоуничтожить.
2. Врисовали и вычеркнули соседнюю пару букв — лишь один символ задействован в обеих операциях. Эти два шага тоже можно взаимоуничтожить.
3. Врисовали и вычеркнули различную пару букв. Эти два шага можно поменять местами.

Во всех случаях получили новую цепочку, у которой либо длина максимального слова меньше, либо та же, но слов такой длины меньше. Противоречие — мы выбрали уже минимальную. Значит, пика нет, слова просто равны:  $w_1 = w_2$ .

Существование редуцированного слова очевидно, так как можно взять самое короткое в классе — его не укоротить.  $\square$

Обозначим  $\bar{w}$  — приведённое слово в классе  $[w]$ .

**Следствие 6.8.1.** В качестве  $F_X$  можно выбрать не фактормоноид, а множество редуцированных слов. Тогда вместо конкатенации  $*$  надо ввести операцию на группе  $w_1, w_2 \mapsto [w_1 * w_2]$ .

Из единственности редуцированного слова можно проверить, что новая операция тоже ассоциативна:  $\overline{u * v} = \overline{u} * \overline{v}$

Основная свободная группа, которая нам встретится в топологии — фундаментальная группа букета окружностей (или плоскости с выколотыми точками), котёнок с катушкой.

Ещё свободную группу можно мыслить так:



Эту картинку надо рисовать не на евклидовой плоскости, а на гиперболической, тогда все стрелки будут одинакового размера и всё поместится.

Если же отождествить  $xu$  и  $yx$ , так как на ровной картинке они попадают в одну точку, то это будет уже абелева группа.

## 6.8.2 Задание группы образующими соотношениями

Пусть  $G = \langle g_1, \dots, g_n \rangle$ ,  $X = \{x_1, \dots, x_m\}$ .

По определению свободной группы существует и единственный гомоморфизм  $\psi : F_X \rightarrow G, x_i \mapsto g_i$ . Значит,  $G$  является факторгруппой свободной группы.

$$1 \rightarrow R \rightarrow F_X \rightarrow G \rightarrow 1$$

$R$  — первая буква слова relations, соотношения,  $g_i$  — generators, образующие.

Значит,  $G \cong F_X/R$ , как же описать  $R$ ? Проблема в том, что кроме тривиальных случаев  $R$  бесконечно велико.

Хочется взять образующие для  $R$ , но оказывается, что в общем случае даже их бесконечно много. Однако  $R$  — ядро гомоморфизма, то есть нормальная подгруппа в  $F_X$ . Значит, можно взять её образующие, как образующие нормальной подгруппы.

Если  $\psi(w) = 1_G$ , то  $\psi(uwu^{-1}) = \psi(u)\psi(w)\psi(u)^{-1} = 1_G$ , то есть соотношения выписываются с точностью до сопряжения. Любая такая система образующих — система определяющих соотношений (defining relations).

**Определение 6.8.4** (Группа с образующими  $g_1, \dots, g_n$  и определяющими соотношениями  $w_1, \dots, w_m$ ).  $G \cong \langle g_1, \dots, g_n | w_1, \dots, w_m \rangle$

Сама такая запись группы — presentation, копредставление или задание образующими соотношениями.

*Примеры.*

- Свободная абелева группа  $\mathbb{Z}^n \cong \langle x_1, \dots, x_n | x_i x_j = x_j x_i \rangle \cong \langle x_1, \dots, x_n | [x_i, x_j] \rangle$ . Часто удобно писать соотношения в виде  $w_1 = w_2$ , это по определению то же самое, что и соотношение  $w_1 w_2^{-1}$ .
- $C_n = \langle g | g^n \rangle = \langle g | g^n = 1 \rangle$  — возможно, вторая запись нагляднее.
- $D_n = \langle x, y | x^2 = y^2 = (xy)^n = 1 \rangle$ .
- $Q_8 = \langle x, y | x^4 = y^4 = 1, x^2 = y^2, xy = yx^3 \rangle$ . Здесь есть ровно восемь слов:  $1, x, y, x^2 = y^2, xy = yx^3, \dots$
- $S_n = \langle s_1, \dots, s_{n-1} | (s_i^2 = 1) \wedge (\forall i, j : |i - j| > 2 \Rightarrow [s_i, s_j] = 1) \wedge \underbrace{s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}}_{(s_i s_{i+1})^3 = 1} \rangle$ ,

где  $s_i = ([i][i+1])$  — фундаментальная транспозиция, они же кокстеровские образующие. Соотношение  $xyx = yxy$  носит название braid relation, отношение в группе кос (косы имеются в виду те, которые девушки заплетают).



Эти косы гомотопически изоморфны.

Если в копредставлении  $S_n$  забыть про отношение  $s_i^2 = 1$ , то получим группу кос

$$B_n = \langle s_1, \dots, s_{n-1} | (\forall i, j : |i - j| > 2 \Rightarrow [s_i, s_j] = 1) \wedge s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \rangle$$

**Факт 6.8.1.** *Группа с большим множеством соотношений — факторгруппа группы с меньшим числом соотношений:*

$$\langle X | R \rangle \rightarrow \langle X | R \cup S \rangle \rightarrow 1$$

*Доказательство.* Теорема фон Дика. □

**Следствие 6.8.2.**  $B_n \rightarrow S_n \rightarrow 1$ : симметрическая группа — факторгруппа группы кос.

*Примеры.*

- $PSL(2, \mathbb{Z}) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  — фактор  $SL(2, \mathbb{Z})$  по центру.  $x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ ,  $y = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ .  $PSL(2, \mathbb{Z}) = \langle x, y | x^2 = y^3 = 1 \rangle$ . Что здесь произошло? Определяющие соотношения бьются на соотношения по разным образующим, это называют свободным произведением:

$$\langle X \sqcup Y | R \sqcup S \rangle = \langle X | R \rangle \star \langle Y | S \rangle$$

где  $R$  — соотношения только на  $X$ ,  $S$  — соотношения только на  $Y$ .

Получается,  $PSL(2, \mathbb{Z}) \cong C_2 \star C_3$  — свободное произведение двух очень маленьких групп — бесконечно.

- Для  $SL(2, \mathbb{Z})$  фактора по центру нет.  $SL(2, \mathbb{Z}) = C_4 \star_{C_2} C_6$  — уже не свободное произведение, а какое-то хитрое.