

Конспект лекций по алгебре  
Факультет математики и компьютерных наук  
СПбГУ  
поток “Математика”-2019

А.В.Степанов



## Оглавление

Глава 1. Введение	6
1. Определение основных алгебраических структур	6
Глава 2. Векторные пространства	8
1. Основные определения	8
2. Матрицы	9
3. Другие определения базиса и его существование	12
4. Размерность пространства	13
5. Изоморфизм и классификация векторных пространств	14
6. Прямая сумма и прямое произведение	14
7. Замена базиса	15
8. Матрица линейного отображения	16
9. Размерность ядра и образа, прямая сумма, формула Грассмана	17
10. Факторпространство	18
11. Ранг, RQ-разложение	19
12. Разложения Бруа и Гаусса	20
Глава 3. Начала теории групп	23
1. Простейшие конструкции	23
2. Гомоморфизмы, ядро и образ	23
3. Порождение, циклические группы, порядок элемента	24
4. Смежные классы и теорема Лагранжа	24
5. Факторгруппа и теорема о гомоморфизме	25
6. Сопряженные элементы, коммутаторы и коммутант	26
7. Группа унитарных матриц и второе доказательство разложения Гаусса	27
8. Симметрическая группа	29
9. Экспонента группы	30
Глава 4. Коммутативные кольца	31
1. Гомоморфизмы колец, ядро и образ	31
2. Порождение	31
3. Факторкольцо и теорема о гомоморфизме	32
4. Комплексные числа	32
5. Евклидовы кольца	35
6. Китайская теорема об остатках	35
7. Простые и максимальные идеалы	36
8. Простые и неприводимые элементы	36
9. Нетеровы кольца и разложение на неприводимые	37
10. Факториальность колец главных идеалов	38
11. Наибольший общий делитель	39
12. Локализация	40
13. Поле частных и разложение на простейшие дроби	41
14. Многочлены	42
15. Формальная производная и кратность корня	44

16. Основная теорема алгебры	46
17. Экспонента мультипликативной группы кольца вычетов	47
18. О простых числах	48
Глава 5. Определители	51
1. Полилинейные и антисимметричные формы.	51
2. Определение определителя	52
3. Свойства определителя	54
4. Формула для элементов обратной матрицы, формулы Крамера и минорный ранг	56
Глава 6. Собственные числа и жорданова форма	58
1. Собственные числа и вектора	58
2. Жорданова форма и теорема Гамильтона–Кэли	61
3. Разложение Жордана	63
4. Функции от матриц	66
5. Другое доказательство жордановой формы	67
6. Дифференциальные и рекуррентные уравнения	68
7. Модули над кольцами	69
8. Подмодули свободного модуля над ОГИ	70
9. Конечнопорожденные модули над кольцами главных идеалов	72
10. Единственность разложения на примарные	74
Глава 7. Билинейные и квадратичные формы	76
1. Формы и их матрицы	76
2. Диагонализация эрмитовой формы	77
3. Вещественные квадратичные формы	79
4. Пространства со скалярным произведением	81
5. Нормальные операторы	84
6. Матричные разложения	88
7. Гильбертово пространство	90
8. Кватернионы и движения трехмерного пространства	92
9. Теоремы Витта	95
10. Симплектические формы	97
Глава 8. Теория групп	99
1. Свободные группы, задание группы образующими и соотношениями	99
2. Подгруппы свободной группы	101
3. Действие группы на множестве и лемма Бернсайда	105
4. Классификация $G$ -множеств	107
5. Несколько приложений действия группы на множестве	108
6. Теоремы о гомоморфизме и лемма о бабочке	109
7. Теоремы Силова	110
8. Полупрямое произведение	112
9. Субнормальные ряды	114
10. Примеры простых групп	116
11. Разрешимые и нильпотентные группы	117
Глава 9. Начала теории категорий	122
1. Категория, универсальные объекты, типы морфизмов	122
2. Функторы	125
3. Естественные преобразования	127
4. Эквалайзеры, произведения и универсальные квадраты	129
5. Универсальные алгебраические конструкции	132

6. Сопряженные функторы	137
7. Пределы	141
8. Обзор других тем теории категорий	144
Глава 10. Полилинейная алгебра	147
1. Простейшие свойства тензорного произведения	147
2. Тензоры	149
3. Тензорная алгебра и алгебра Грассмана	151
4. Вычисления в алгебре Грассмана	154
Глава 11. Теория представлений	158
1. Основные определения	158
2. Строение артиновых колец	160
3. Лемма Шура	163
4. Полная приводимость	164
5. Характеры представления	165
6. Соотношения ортогональности	166
7. Разложение регулярного представления	168
8. Количество неприводимых представлений	169
9. Таблицы характеров	170
10. Представления прямого произведения	172
11. Целые алгебраические числа	173
12. Степени неприводимых представлений	174
13. Индуцированные представления	175
Глава 12. Многочлены	178
1. Определения кольца многочленов	178
2. Нетеровость кольца многочленов	179
3. Факториальность кольца многочленов	180
4. Теорема Гильберта о нулях и основы алгебраической геометрии	181
5. Симметрические многочлены	184
6. Результант	186
7. Доказательство слабой теоремы о нулях с помощью результанта	189
8. Дискриминант	190
9. Базисы Гребнера	191
Глава 13. Теория Галуа	196

## Введение

## 1. Определение основных алгебраических структур

**ОПРЕДЕЛЕНИЕ 1.1.** Операцией называется функция  $X_1 \times \cdots \times X_n \rightarrow X$ . Чаще всего рассматривается ситуация, когда  $X_1 = \cdots = X_n = X$ . В этом случае операция называется  $n$ -арной операцией на множестве  $X$ . Декартово произведение пустого набора множеств по определению равно одноточечному множеству. Поэтому 0-арная операция на  $X$  – это выбор фиксированной точки множества  $X$ . 1-арная операция называется унарной, а 2-арная – бинарной. Бинарные операции обычно обозначаются не буквами, а значками, например  $\star$ , и вместо  $\star(x, y)$  пишут  $x \star y$ .

Пусть  $X$  – множество, а  $\star$  – бинарная операция на  $X$ . Рассмотрим следующие свойства.

- (1)  $\forall x, y, z \in X : (x \star y) \star z = x \star (y \star z)$  (ассоциативность).
- (2)  $\exists e \in X \forall x \in X : e \star x = x \star e = x$  ( $e$  называется нейтральным элементом).
- (3)  $\forall x \in X \exists x' \in X : xx' = x'x = e$  ( $x'$  называется элементом обратным к  $x$ ).
- (4)  $\forall x, y \in X : x \star y = y \star x$  (коммутативность).

**ОПРЕДЕЛЕНИЕ 1.2.** Множество  $X$  с операцией  $\star$  называется

- полугруппой, если операция ассоциативна;
- моноидом, если операция ассоциативна и существует нейтральный элемент;
- группой, если выполнены свойства (1)–(3).

Полугруппа, моноид или группа называется коммутативной, если выполнено свойство (4). Коммутативную группу называют абелевой группой.

Элемент моноида называется обратимым, если для него существует обратный.

Нейтральный элемент относительно операции умножения обычно обозначается символом 1, а относительно сложения – 0. Если из контекста неясно, нейтральным элементом какого множества является данный элемент, то пишут  $e_X$ ,  $1_X$  и  $0_X$  для нейтрального элемента множества  $X$  относительно различных операций.

Обратный к  $x$  элемент относительно сложения обозначается через  $-x$ , относительно других операций – через  $x^{-1}$ .

**ЛЕММА 1.3.** Нейтральный элемент единственен (это утверждение не зависит даже от ассоциативности).

Если операция ассоциативна и обладает нейтральным элементом, то элемент, обратный к данному, единственный.

**ЛЕММА 1.4.** Если в моноиде элементы  $x$  и  $y$  обратимы, то  $x \star y$  обратим, причем  $(x \star y)^{-1} = y^{-1} \star x^{-1}$ .

Множество обратимых элементов моноида является группой.

**ОПРЕДЕЛЕНИЕ 1.5.** Пусть теперь на множестве  $R$  заданы операции сложения и умножения, причем  $R$  является абелевой группой по сложению и полугруппой по умножению. Предположим, что выполнено следующее свойство:

5.  $\forall x, y, z \in R : (x + y)z = xz + yz$  и  $z(x + y) = zx + zy$  (дистрибутивность).

Тогда  $R$  называется (ассоциативным) кольцом.

Если существует нейтральный элемент по умножению, то кольцо называется кольцом с единицей, если умножение коммутативно, то коммутативным кольцом.

Поле – это коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

**ЛЕММА 1.6.** *Для любого элемента  $r$  произвольного кольца  $R$ :  $0 \cdot r = r \cdot 0 = 0$ .  
Если  $R$  – кольцо с единицей, то  $(-1) \cdot r = -r$ .*

Как следует из леммы 1.4, множество обратимых (по умножению) элементов кольца  $R$  является группой. Эта группа называется мультипликативной подгруппой кольца и обозначается через  $R^*$ .

**ОПРЕДЕЛЕНИЕ 1.7.** Пусть  $V$  – абелева группа в аддитивной записи,  $F$  – поле, и задана операция (умножение)  $V \times F \rightarrow V$ . Предположим, что для любых  $u, v \in V$  и  $\alpha, \beta \in F$  выполнены следующие свойства:

- (1)  $v(\alpha\beta) = (v\alpha)\beta$ ;
- (2)  $v(\alpha + \beta) = v\alpha + v\beta$ ;
- (3)  $(u + v)\alpha = u\alpha + v\alpha$ ;
- (4)  $v \cdot 1 = v$ .

Тогда  $V$  называется векторным пространством над полем  $F$ .

**ОПРЕДЕЛЕНИЕ 1.8.** Пусть  $A$  – векторное пространство над полем  $F$  и, одновременно, кольцо с той же операцией сложения. Если выполнено свойство  $(ab)\alpha = a(b\alpha)$  для любых  $a, b \in A$  и  $\alpha \in F$ , то  $A$  называется (ассоциативной) алгеброй над полем  $F$ .

Если отказаться от аксиомы ассоциативности кольцевого умножения, то получится неассоциативная алгебра. Изучение таких объектов в общем виде бесперспективно, даже если требовать конечномерность над полем. Однако если заменить ассоциативность какой-нибудь другой аксиомой, то получаются очень содержательные объекты. В частности, одной из важнейших алгебраической структур являются алгебры Ли, в которых ассоциативность заменена тождеством Якоби.

Если в  $A$  есть нейтральный элемент относительно умножения (обозначим его символом  $e$ ), то элементы  $\alpha \in F$  отождествляются с элементами  $e \cdot \alpha \in A$ . Таким образом, если  $A$  – алгебра с единицей, то можно считать, что она содержит поле  $F$ . Обратно, если есть кольцо, содержащее поле  $F$ , то оно естественным образом является алгеброй над  $F$  (внешняя операция умножения в векторном пространстве  $A \times F \rightarrow A$  является сужением операции умножения в кольце  $A \times A \rightarrow A$ ).

## Векторные пространства

### 1. Основные определения

Далее в настоящей главе используются следующие обозначения и соглашения.

- $F$  – поле.
- $V$  – векторное пространство над  $F$ .
- $F^n$  – множество столбцов высоты  $n$  над  $F$ .
- ${}^nF$  – множество строк длины  $n$  над  $F$ .
- Допуская вольность речи, элементы линейного пространства обычно называют векторами, а элементы поля  $F$  – числами;
- По умолчанию, греческие буквы обозначают числа, строчные латинские – элементы линейного пространства и столбцы, а прописные латинские – множества, линейные операторы и матрицы;
- словосочетание “почти все” означает “все, кроме конечного числа”.

Подмножество  $U \subseteq V$  называется подпространством, если оно само является векторным пространством относительно тех же операций, которые заданы в  $V$ .

**ПРЕДЛОЖЕНИЕ 1.1** (критерий подпространства). *Подмножество  $U \subseteq V$  является подпространством в том и только том случае, если  $u + v$ ,  $u\alpha \in U$  для любых  $u, v \in U$  и  $\alpha \in F$ .*

Пусть  $u_1, \dots, u_n \in V$ , а  $\alpha_1, \dots, \alpha_n \in F$ . Сумма

$$\sum_{k=1}^n u_k \alpha_k$$

называется линейной комбинацией векторов  $u_1, \dots, u_n \in V$  с коэффициентами  $\alpha_1, \dots, \alpha_n \in F$ . Линейная комбинация называется тривиальной, если все ее коэффициенты равны нулю. Пусть  $S \subseteq V$ , и задан набор чисел  $\alpha_s \in F$ ,  $s \in S$ . Если множество  $S$  бесконечно, то операция взятия бесконечной суммы  $\sum_{s \in S} s \alpha_s$  не определена. Однако, если почти все  $\alpha_s$  равны 0, то в сумме остается только конечное число слагаемых. Таким образом, символ  $\sum_{s \in S} s \alpha_s$  будет употребляться в дальнейшем и для бесконечных множеств  $S$  при условии, что почти все  $\alpha_s$  равны 0.

Линейной оболочкой набора  $S$  называется подпространство, порожденное  $S$ , т.е. наименьшее подпространство, содержащее  $S$ . Она обозначается через  $\langle S \rangle$ .

**ПРЕДЛОЖЕНИЕ 1.2.**  $\langle S \rangle = \left\{ \sum_{k=1}^n u_k \alpha_k \mid u_1, \dots, u_n \in S, \alpha_1, \dots, \alpha_n \in F \right\}$ .

Если  $\langle S \rangle = V$ , то  $S$  называется системой образующих пространства  $V$ . Другими словами,  $S$  является системой образующих, если любой вектор выражается в виде линейной комбинации векторов из  $S$ .

Кортеж векторов  $(u_1, \dots, u_n)$  называется линейно независимым, если нетривиальная линейная комбинация этих векторов не равна нулю. Множество  $S \subseteq V$  называется линейно независимым, если любой кортеж, составленный из конечного числа различных векторов из  $S$ , является линейно независимым. Другими словами,  $S$  линейно независимо, если для любого набора чисел  $\alpha_s \in F$ , почти все из которых равны нулю, из равенства  $\sum_{s \in S} s \alpha_s = 0$  следует, что все  $\alpha_s$  равны нулю.

**ОПРЕДЕЛЕНИЕ 1.3.** Базисом называется линейно независимая система образующих.



## 2. Матрицы

В дальнейшем мы будем широко использовать матричные обозначения, в частности для линейных комбинаций. Каждому элементу векторного пространства будет сопоставлен (возможно бесконечный) столбец (одномерный массив). Аналогично, линейному отображению будет сопоставлена матрица (двумерный массив). Сейчас мы введем операции на множестве матриц и укажем их простейшие свойства.

Обычно рассматриваются матрицы, строки и столбцы которых занумерованы натуральными числами и являются элементами некоторого поля или кольца. Приведем сначала определение таких матриц и изучим их свойства, а потом рассмотрим более общий случай.

**ОПРЕДЕЛЕНИЕ 2.1.** Двумерный массив  $m \times n$  элементов поля  $F$  называется матрицей размера  $m \times n$  над  $F$ . Множество всех таких матриц обозначается  $M_{m \times n}(F)$ . Если  $m = n$ , то вместо  $M_{n \times n}(F)$  пишут  $M_n(F)$ . Элемент матрицы  $A$  в позиции  $(i, j)$  (т.е. в  $i$ -й строке и  $j$ -м столбце) обычно обозначается через  $a_{ij}$ .

Для двух матриц одинакового размера их сумма определена поэлементно, т.е.  $(A + B)_{ij} = a_{ij} + b_{ij}$ . Также поэлементно определяется произведение матрицы на число:  $(A\alpha)_{ij} = a_{ij}\alpha$ .

Произведением матрицы  $A \in M_{m \times n}(F)$  на матрицу  $B \in M_{n \times k}(F)$  называется матрица  $C = AB \in M_{m \times k}(F)$  элементы которой вычисляются по формуле

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}.$$

В случае, когда количество столбцов левой матрицы не равно количеству строк правой, произведение матриц не определено.

Строка отождествляется с матрицей  $1 \times n$ , а столбец – с матрицей  $n \times 1$ . Таким образом, произведение строки длины  $n$  на столбец высоты  $n$  – это матрица  $1 \times 1$ , которая отождествляется с числом. Произведение же столбца на строку определено всегда, но является не числом, а матрицей соответствующего размера. Заметим, что произведение матриц некоммутативно, даже если размеры получившихся матриц равны.

**ТЕОРЕМА 2.2.** Множество  $M_{m \times n}(F)$  с операциями сложения и умножения на число является векторным пространством над полем  $F$ .

Произведение матриц ассоциативно, дистрибутивно и перестановочно с умножением на число, т.е. для любых матриц  $A, B, C$  и числа  $\alpha \in F$ , как только определены соответствующие произведения, так

$$(1) \quad (AB)C = A(BC); \quad A(B+C) = AB+AC; \quad (B+C)A = BA+CA; \quad (AB)\alpha = A(B\alpha) = (A\alpha)B.$$

Множество  $M_n(F)$  с операциями сложения и умножения является алгеброй с единицей над полем  $F$ .

**ДОКАЗАТЕЛЬСТВО.** Элемент произведения  $(AB)C$  в позиции  $(i, j)$  равен

$$\sum_k \left( \sum_l a_{il}b_{lk} \right) c_{kj} = \sum_k \sum_l (a_{il}b_{lk})c_{kj}.$$

Элемент матрицы  $A(BC)$  на соответствующем месте равен

$$\sum_l a_{il} \left( \sum_k b_{lk} \right) c_{kj} = \sum_l \sum_k a_{il}(b_{lk}c_{kj}).$$

Так как умножение в  $F$  ассоциативно, а сложение – ассоциативно и коммутативно, то эти элементы равны.

Обозначим через  $E$  квадратную матрицу с 1 на главной диагонали (с левого верхнего в правый нижний угол) и остальными нулями. Другими словами  $e_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ . Такая матрица называется единичной, ее размер обычно определяется из контекста, но при необходимости пишут  $E_n$  для обозначения единичной матрицы размера  $n \times n$ . Нетрудно вычислить, что при умножении данной (не обязательно квадратной) матрицы на единичную слева или справа она не меняется. В частности,  $E_n$  является мультипликативным нейтральным элементом в  $M_n(F)$ . Остальные утверждения теоремы проверяются непосредственным вычислением.  $\square$

Заметим, что в алгебре матриц элементы поля  $F$  не принято отождествлять со скалярными матрицами  $E\alpha$ .

Следом матрицы  $A \in M_n(F)$  называется сумма ее диагональных элементов:

$$\text{Tr } A := \sum_{i=1}^n a_{ii}.$$

**УПРАЖНЕНИЕ 2.3.** Докажите, что для любых матриц  $A \in M_{n,k}(F)$  и  $B \in M_{k,n}(F)$  верно равенство .

На самом деле мы хотим умножать двумерные массивы более общего вида. Предположим, что даны множества  $X_{ij}$ ,  $Y_{jh}$ , коммутативные моноиды  $Z_{ih}$  в аддитивной записи, где  $i = 1, \dots, m$ ,  $j = 1, \dots, n$ ,  $h = 1, \dots, k$ , и функции “умножения”  $X_{ij} \times Y_{jh} \rightarrow Z_{ih}$ ,  $(x, y) \mapsto xy$ . Обозначим через  $X$ ,  $Y$  и  $Z$  наборы множеств  $X_{ij}$ ,  $Y_{jh}$  и  $Z_{ih}$ , соответственно, через  $M(X)$  – множество матриц  $A$  с элементами  $a_{ij} \in X_{ij}$ , и аналогично введем обозначения  $M(Y)$  и  $M(Z)$ . Тогда можно определить произведение матриц  $A \in M(X)$  и  $B \in M(Y)$  как матрицу  $C = AB \in M(Z)$  с элементами  $c_{ih} = \sum_{j=1}^n a_{ij}b_{jh}$ .

Если все  $X_{ij}$  и  $Y_{jh}$  будут коммутативными моноидами, а функции “умножения” дистрибутивными, то умножение матриц также будет дистрибутивным и, также как произведение обычных матриц, ассоциативным. Точную формулировку этих свойств приведем после того, как определим матрицы, строки и столбцы которых индексированы элементами произвольных множеств.

Одно из приложений описанной выше конструкции – произведение строки векторов на столбец чисел, что является просто другой записью линейной комбинации. В этих терминах линейная независимость кортежа векторов равносильна возможности сокращать на него. Действительно, если кортеж  $v = (v_1, \dots, v_n)$  линейно независим, то для  $a, b \in F^n$  имеет место:  $va = vb \iff v(a - b) = 0 \iff a - b = 0 \iff a = b$ . Очевидно, верно и обратное, т.е. из возможности сокращать следует линейная независимость. Другое приложение – блочное произведение матриц (это очень легко показать на доске, и очень долго писать, поэтому пока не пишу).

Пусть теперь  $I$  и  $J$  – произвольные множества (возможно бесконечные), элементами которых мы будем индексировать строки и столбцы матриц. Предположим, что для каждого  $i \in I$  и  $j \in J$  задано множество  $X_{ij}$ , и обозначим этот набор множеств через  $X$ .<sup>1</sup> Тогда матрицей размера  $I \times J$  над  $X$  называется функция  $A : I \times J \rightarrow \cup X_{ij}$ ,  $(i, j) \mapsto a_{ij}$ , такая что  $a_{ij} \in X_{ij}$ . Множество всех матриц размера  $I \times J$  над  $X$  обозначается через  $M_{I \times J}(X)$ . Если  $I = \{1\}$ , то матрицы размера  $I \times J$  будут называться строками длины  $J$ , а если  $J = \{1\}$ , то столбцами высоты  $I$ . Множества всех строк (столбцов) данной длины (соотв. высоты) будет обозначаться через  ${}^JX$  (соотв.  $X^J$ ).

<sup>1</sup>Формально надо говорить, что есть некоторый набор множеств, а  $X$  – это отображение из  $I \times J$  в этот набор. Но нельзя говорить, что  $X$  – отображение из  $I \times J$  в множество всех множеств, так как последнего не существует из за парадокса Рассела.

В дальнейшем мы будем рассматривать только ситуацию, когда все  $X_{ij}$  являются абелевыми группами в аддитивной записи. Тогда для двух матриц из одинакового размера их сумма определена поэлементно, т. е.  $(A+B)_{ij} = a_{ij} + b_{ij}$ . Если же все  $X_{ij}$  являются векторными пространствами над полем  $F$ , то также поэлементно определяется произведение матрицы на число:  $(A\alpha)_{ij} = a_{ij}\alpha$ .

Теперь, если мы хотим определить умножение матрицы из  $M_{I \times J}(X)$  на матрицу из  $M_{J \times H}(Y)$  нам недостаточно иметь операции умножения  $X_{ij} \times Y_{jh} \rightarrow Z_{ih}$  как в первой части параграфа, потому что мы можем получить бесконечные суммы, которые не определены. Однако мы можем определить такую сумму, если почти все слагаемые будут равны нулю. Для того чтобы гарантировать последнее условие, мы постулируем, что все операции умножения  $X_{ij} \times Y_{jh} \rightarrow Z_{ih}$  дистрибутивны, и в каждом столбце матрицы  $Y$  почти все элементы равны 0. Аналогично, мы могли бы потребовать, чтобы в каждой строке матрицы  $X$  почти все элементы были бы нулевыми, но в нашей системе обозначений именно условие на столбцы будет выполнено. Дистрибутивность умножения нужна для того, чтобы выполнялось равенство  $a \cdot 0 = 0$ .

Итак, обозначим через  $M_{J \times H}^{c.f.}(Y)$  подмножество в  $M_{J \times H}(Y)$ , состоящее из всех матриц  $B$ , у которых для любого фиксированного  $h \in H$  почти все элементы  $b_{jh}$  равны 0.<sup>2</sup>

**ОПРЕДЕЛЕНИЕ 2.4.** Предположим, что для любых  $i \in I$ ,  $j \in J$ ,  $h \in H$  заданы операции умножения  $X_{ij} \times Y_{jh} \rightarrow Z_{ih}$ , причем для любых  $x, x' \in X_{ij}$  и любых  $y, y' \in Y_{jh}$  имеют место равенства  $(x + x')y = xy + x'y$  и  $x(y + y') = xy + xy'$ . Из этих равенств легко вывести, что  $x \cdot 0 = 0 \cdot y = 0$ . Тогда определим произведение матриц  $A \in M_{I \times J}(X)$  и  $B \in M_{J \times H}^{c.f.}(Y)$  как матрицу  $AB \in M_{I \times H}(Z)$  с элементами

$$(AB)_{ih} = \sum_{j \in J} a_{ij} b_{jh}.$$

При этом суммы определены, так как почти все слагаемые равны нулю.

Аналогично определяется умножение матриц  $A \in M_{I \times J}^{r.f.}(X)$  и  $B \in M_{J \times H}(Y)$

**ЛЕММА 2.5.** Обычные свойства умножения матриц (1) выполнены, как только определены все входящие в формулы операции.

Если для всех  $i, j, h \in I$  заданы дистрибутивные операции умножения  $X_{ij} \times X_{jh} \rightarrow X_{ih}$ , то множество  $M_{I \times I}^{c.f.}(X)$  является кольцом с единицей.

В случае, когда все  $X_{ij}$  – это одно и то же поле  $F$  будем писать  $M_{I \times J}(F)$  вместо  $M_{I \times J}(X)$ . Если  $I = J$ , то пишем  $M_I(F)$  вместо  $M_{I \times I}(F)$ . В стандартной ситуации, когда  $I = \{1, \dots, n\}$  в обозначениях множеств матриц заменяем  $I$  на  $n$ . Например,  $M_{n \times m}(F)$  обозначает множество прямоугольных матриц с  $n$  строками и  $m$  столбцами, элементы которых берутся из поля  $F$ .

**ОПРЕДЕЛЕНИЕ 2.6.** Множество обратимых элементов кольца  $M_n(F)$  называется полной линейной группой степени  $n$  над  $F$  и обозначается через  $GL_n(F)$ .

Для множества  $M_{I \times \{1\}}^{c.f.}(F)$  введем специальное обозначение  $F_{fin}^I$  и будем называть его множеством финитных столбцов высоты  $F$  над  $R$ . Другими словами,  $F_{fin}^I$  – это множество финитных функций из  $I$  в  $F$ , т. е. тех функций, у которых почти все значения равны 0. Аналогично, положим  ${}^J F_{fin} = M_{\{1\} \times J}^{r.f.}(F)$ .

Есть еще одна полезная унарная операция с матрицами – транспонирование.

**ОПРЕДЕЛЕНИЕ 2.7.** Пусть  $A \in M_{I \times J}(F)$ . Матрица  $A^T \in M_{J \times I}(F)$  с элементами  $(A^T)_{ij} = a_{ji}$  называется транспонированной к  $A$ .

На начальном этапе освоения материала польза транспонирования состоит в том, что оно меняет порядок сомножителей.

**ПРЕДЛОЖЕНИЕ 2.8.**  $(AB)^T = B^T A^T$ .

<sup>2</sup>c.f. – сокращение от “column finite”, аналогично r.f. будет использоваться, как сокращение для “row finite”.

Смысл же этой операции будет ясен при изучении сопряженного пространства.

Из чисто полиграфических соображений (для экономии места) для обозначения столбца часто пишется строка со знаком транспонирования, например,  $(a_1, \dots, a_n)^\top$ .

### 3. Другие определения базиса и его существование

**ТЕОРЕМА 3.1** (эквивалентные определения базиса). *Следующие условия на подмножество  $v$  векторного пространства  $V$  эквивалентны.*

- (1)  $v$  – линейно независимая система образующих.
- (2)  $v$  – максимальная линейно независимая система.
- (3)  $v$  – минимальная система образующих.
- (4) Любой элемент  $x \in V$  представляется в виде линейной комбинации набора  $v$ , причем единственным образом.

**ДОКАЗАТЕЛЬСТВО.** В обозначениях предыдущего параграфа линейная комбинация набора векторов  $v \subseteq V$  может быть записана в виде  $va \sum_{y \in v} ya_y$  для некоторого столбца  $a \in F_{fin}^v$  (так как столбец  $a$  финитный, в сумме только конечное число ненулевых слагаемых). Пусть  $v$  – базис пространства  $V$ , в частности набор  $v$  является системой образующих. По определению это означает, что для любого  $x \in V$  существует  $a \in F_{fin}^v$ , такое что  $x = va$ . Условие же линейной независимости набора  $v$  равносильно единственности такого представления. Действительно, мы уже видели, что линейная независимость равносильна возможности сокращать равенство  $va = vb$  на  $v$ . Это доказывает эквивалентность пунктов 1 и 4. Доказательство того, что остальные пункты эквивалентны первому, оставляется читателю в качестве упражнения.  $\square$

**ОПРЕДЕЛЕНИЕ 3.2.** Пусть  $v$  – базис пространства  $V$ ,  $a \in F_{fin}^v$ , а  $x \in V$ . Если  $x = va$ , то  $a$  называется столбцом координат вектора  $x$  в базисе  $v$  и обозначается через  $x_v$ .

Если  $V = F^n$ , а  $e$  – стандартный базис, т. е. базис, состоящий из столбцов единичной матрицы, то получаем  $x = ex_e$ . Легко видеть, что можно отождествить строку из столбцов с матрицей. Следовательно,  $x = Ex_e = x_e$  (столбец координат столбца в стандартном базисе совпадает с ним самим). Если это формалистика пока непонятна, то просто разложите столбец в линейную комбинацию столбцов единичной матрицы и запишите коэффициенты этой линейной комбинации в столбец.

**ТЕОРЕМА 3.3** (о существовании базиса). *Пусть  $X, Y \subseteq V$ , причем набор  $X$  линейно независим, а  $Y$  – система образующих. Тогда существует базис  $Z$ , содержащий  $X$  и содержащийся в  $Y$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\mathcal{A}$  – набор всех линейно независимых подмножеств  $Y$ , содержащих  $X$ . Этот набор не пуст, так как он содержит  $X$ . Пусть  $\mathcal{L}$  – линейно упорядоченный поднабор в  $\mathcal{A}$ . Обозначим через  $S$  объединение всех множеств из  $\mathcal{L}$ . Так как любое подмножество  $C \in \mathcal{L}$  лежит между  $X$  и  $Y$ , то этим свойством обладает и  $S$ . Возьмем произвольное конечное подмножество  $\{v_1, \dots, v_n\} \subseteq S$ . По определению объединения множеств для каждого  $i = 1, \dots, n$  существует  $B_i \in \mathcal{L}$ , содержащее вектор  $v_i$ . Так как набор  $\mathcal{L}$  линейно упорядочен, среди множеств  $B_1, \dots, B_n$  найдется наибольшее, скажем,  $B_k$ . Тогда  $v_1, \dots, v_n \in B_k$ , а так как  $B_k$  линейно независимо, то и множество  $\{v_1, \dots, v_n\}$  линейно независимо. Следовательно,  $S$  линейно независимо, откуда  $S \in \mathcal{A}$ . По лемме Цорна заключаем, что  $\mathcal{A}$  содержит максимальный элемент. Обозначим его через  $Z$ . Таким образом,  $Z$  – максимальное из линейно независимых подмножеств  $Y$ , содержащих  $X$ .

Пусть  $y \in Y \setminus Z$ . По максимальной  $Z$  множество  $Z \cup \{y\}$  линейно зависимо, т. е. существуют  $a \in F_{fin}^Z$  и  $a_y \in F$  такие, что  $ya_y + Za = 0$ . Коэффициент  $a_y$  не может быть равен нулю, это противоречило бы линейной независимости множества  $Z$ . Следовательно,  $y$  принадлежит линейной оболочке множества  $Z$ . Поэтому все множество  $Y$  содержится в  $\langle Z \rangle$ . С другой стороны,  $V = \langle Y \rangle$  – наименьшее подпространство, содержащее  $Y$ . Следовательно,  $\langle Z \rangle \supseteq V$ , т. е.  $Z$  – система образующих, а значит и базис.  $\square$

#### 4. Размерность пространства

**ЛЕММА 4.1** (о замене). Пусть  $u = \{u_1, \dots, u_n\}$  – линейно независимый набор из  $n$  векторов, а  $v$  – система образующих пространства  $V$ . Тогда существуют элементы  $v_1, \dots, v_n \in v$  такие, что множество  $w = v \setminus \{v_1, \dots, v_n\} \cup u$  также является системой образующих.

При этом, если набор  $v$  линейно независим, то  $w$  обладает тем же свойством.

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство индукцией по  $n$ . В качестве базы индукции можно взять случай  $n = 0$ , который тривиален. Пусть теперь  $n > 0$ . По индукционному предположению найдутся вектора  $v_1, \dots, v_{n-1} \in v$  такие, что  $w' = v \setminus \{v_1, \dots, v_{n-1}\} \cup \{u_1, \dots, u_{n-1}\}$  является системой образующих. Причем, если  $v$  был линейно независимым, то  $w'$  – базис. Вектор  $u_n$  выражается через линейную комбинацию набора  $w'$ , скажем  $u_n = \sum_{i=1}^{n-1} u_i \alpha_i + \sum_{j=1}^m w_j \beta_j$  для некоторых  $\alpha_i, \beta_j \in F$  и  $w_j \in v \setminus \{v_1, \dots, v_{n-1}\}$ . Заметим, что хотя бы один из коэффициентов  $\beta_j$  не равен нулю, иначе это противоречило бы линейной независимости набора  $u$ . Без ограничения общности можно считать, что  $\beta_m \neq 0$ . Положим  $v_n = w_m$ . Тогда  $v_n$  выражается через линейную комбинацию набора  $w = w' \setminus \{v_n\} \cup \{u_n\}$ . Таким образом,  $w' \subseteq \langle w \rangle$  и, следовательно,  $w$  является системой образующих.

Предположим, что набор  $v$ , а, следовательно, и  $w'$ , линейно независим. Положим  $w'' = w' \setminus \{v_n\}$  и рассмотрим линейную комбинацию  $w''a + u_n\alpha$  набора  $w$ , где  $a \in F_{fin}^{w''}$ . Подставляя выражение для  $u_n$  и приравнявая эту комбинацию к нулю получим

$$0 = w''a + u_n\alpha = w'' + \sum_{i=1}^{n-1} u_i \alpha_i \alpha + \sum_{j=1}^m w_j \beta_j \alpha = w''b + v_n \beta_m \alpha,$$

где  $b \in F_{fin}^{w''}$  (нетрудно понять, как он выражается через  $a, \alpha_i, \beta_j$  и  $\alpha$ ). Если  $\alpha \neq 0$ , то  $w''b + v_n \beta_m \alpha$  является нетривиальной линейной комбинацией набора  $w'' \cup \{v_n\} = w'$ . Равенство такой комбинации нулю противоречит линейной независимости  $w'$ . Поэтому  $\alpha = 0$ , откуда  $w''a = 0$  и из линейной независимости  $w'' \subseteq w'$  следует, что  $a = 0$ . Таким образом, все коэффициенты исходной линейной комбинации равны 0, что и означает линейную независимость набора  $w$ .  $\square$

**ТЕОРЕМА 4.2** (количество элементов в базисе). Любые два базиса пространства  $V$  равно-мощны.

**ДОКАЗАТЕЛЬСТВО.** Приведем доказательство для случая, когда один из базисов конечен. Доказательство для бесконечномерного случая в каком-то смысле проще (если предполагать случай конечного базиса известным). Его можно найти в курсе лекций Николая Верещагина и Александра Шеня “Введение в теорию множеств”, лекция 11, теорема 36 (в настоящий момент она доступна по ссылке <http://www.intuit.ru/studies/courses/1034/144/lecture/3994?page=4>).

Пусть  $v$  и  $u = \{u_1, \dots, u_n\}$  – базисы пространства  $V$ . Не умоляя общности можно считать, что мощность множества  $v$  больше  $n$ . Перенумеровав при необходимости элементы базиса  $u$  можно считать, что  $u_1, \dots, u_k \notin v$ , а  $u_{k+1}, \dots, u_n \in v$ . Тогда по лемме о замене существует подмножество  $\{v_1, \dots, v_k\} \subseteq v$  такое, что  $w = v \setminus \{v_1, \dots, v_k\} \cup \{u_1, \dots, u_k\}$  – базис. Легко видеть, что  $u \subseteq w$ , а  $|v| = |w|$  (сколько элементов выкинули, столько не лежащих в  $v$  и добавили). Однако, так как базис – это максимальная линейно независимая система, то один базис не может строго содержаться в другом. Поэтому  $w = u$ , откуда  $|v| = n$ .  $\square$

**ОПРЕДЕЛЕНИЕ 4.3.** Размерностью пространства называется мощность (любого) базиса этого пространства.

Пространство называется конечномерным, если в нем существует конечный базис. В этом случае удобнее индексировать базисные вектора и координаты векторов в этом базисе натуральными числами. Поэтому для конечномерных пространств мы будем считать по умолчанию, что базис – это строка из  ${}^n V$ , а координаты вектора – столбец из  $F^n$ . Тогда равенство  $x = vx_v$ , где  $v$  – базис, а  $x_v$  – столбец координат, которое является фактически определением координат, по-прежнему

будет выполнено. Другими словами, будем считать, что базис конечномерного пространства – это не множество, а кортеж векторов. При необходимости уточнить, какое из определений базиса имеется в виду, мы будем говорить что кортеж векторов – это упорядоченный базис.

Обратите внимание, что линейная независимость кортежа  $(v_1, \dots, v_n)$  равносильна тому, что  $v_i \neq v_j$  при всех  $i \neq j$  и множество  $\{v_1, \dots, v_n\}$  линейно независимо.

## 5. Изоморфизм и классификация векторных пространств

**ОПРЕДЕЛЕНИЕ 5.1.** Пусть  $V$  и  $U$  – векторные пространства, а  $L$  – функция  $V \rightarrow U$ . Она называется линейным отображением, если для любых  $x, y \in V$  и любого  $\alpha \in F$

$$L(x + y) = L(x) + L(y) \text{ и } L(x\alpha) = L(x)\alpha.$$

Другими словами, линейное отображение – это гомоморфизм векторных пространств.

Как обычно, изоморфизмом называется биективный гомоморфизм.

Линейное отображение из пространства в самого себя обычно называют линейным оператором, хотя некоторые авторы используют термин “оператор”, как полный синоним термина “отображение”. Отображение из пространства в основное поле часто (особенно в функциональном анализе) называют функционалом. В алгебре принято еще слово “форма” для отображений в основное поле, хотя словосочетание “линейная форма” не так распространено, как “квадратичная” или “билинейная форма”, которые мы будем изучать в следующем семестре.

Ясно, что линейные отображения характеризуются тем, что сохраняют линейные комбинации векторов. Для строки векторов  $v = (v_1, \dots, v_n)$  и отображения  $L : V \rightarrow U$  положим  $L(v) = (L(v_1), \dots, L(v_n)) \in {}^nU$ . Если набор  $v$  бесконечный, то аналогичное обозначение формально выглядит следующим образом: строка  $L(v) \in {}^vU$  задана равенством  $L(v)_x = L(x)$  для каждого  $x \in v$ .

В этих обозначениях свойство линейности можно выразить следующей формулой:

$$L(va) = L(v)a, \text{ где } a \in F^n \text{ или, в случае бесконечного набора, } a \in F^v.$$

**ЛЕММА 5.2.** Пусть  $V$  – векторное пространство над полем  $F$ , а  $v$  – базис  $V$ . Отображение  $\varphi_v : V \rightarrow F^v$ , заданное равенством  $\varphi_v(x) = x_f$ , является изоморфизмом векторных пространств.

**СЛЕДСТВИЕ 5.3** (классификация векторных пространств). Любое векторное пространство изоморфно пространству  $F^I$  для некоторого множества  $I$  (мощность которого равна размерности пространства).

Два пространства изоморфны между собой тогда и только тогда, когда их размерности равны.

**СЛЕДСТВИЕ 5.4.** Количество элементов конечного поля равно степени простого числа.

## 6. Прямая сумма и прямое произведение

Пусть  $U$  и  $V$  – подпространства векторного пространства  $W$  над полем  $F$ . Суммой  $U + W$  называется совокупность всевозможных векторов вида  $x + y$ , где  $x \in U$ ,  $y \in V$ . Сумма подпространств есть подпространство. Пересечение подпространств является подпространством.

**ОПРЕДЕЛЕНИЕ 6.1.** Пространство  $W$  называется (внутренней) прямой суммой подпространств  $U$  и  $V$ , если каждый элемент  $z \in W$  может быть единственным способом представлен в виде суммы  $z = x + y$ , где  $x \in U$ , а  $y \in V$ . Эквивалентная формулировка:  $W = U + V$  и  $U \cap V = \{0\}$ .

Пусть теперь  $U$  и  $V$  – произвольные векторные пространства. Их (внешней) прямой суммой называется их декартово произведение с покомпонентными операциями.

Обозначение и внешней и внутренней прямой суммы  $W = U \oplus V$ .

Пространства  $U$  и  $V$  естественно вкладываются в их внешнюю прямую сумму:  $U \ni x \mapsto (x, 0)$ , а  $V \ni y \mapsto (0, y)$ . Если отождествить  $U$  и  $V$  с их образами, то внешняя прямая сумма превращается в прямую сумму подпространств.

**ПРЕДЛОЖЕНИЕ 6.2.** Пусть  $U, V \leq W$ , а  $U \oplus V$  обозначает их внешнюю прямую сумму. Зададим отображение  $\varphi : U \oplus V \rightarrow W$  формулой  $\varphi(x, y) = x + y$ . Тогда отображение  $\varphi$  – изоморфизм тогда и только тогда, когда  $W$  является внутренней прямой суммой подпространств  $U$  и  $V$ .

Если  $W = U \oplus V$ , то объединение базисов подпространств  $U$  и  $V$  есть базис пространства  $W$ . Поэтому  $\dim(U \oplus V) = \dim(U) + \dim(V)$ .

**ПРЕДЛОЖЕНИЕ 6.3.** Для любого подпространства  $U \leq W$  существует подпространство  $V \leq W$  такое, что  $W = U \oplus V$ .

**ДОКАЗАТЕЛЬСТВО.** Выберем базис  $u$  подпространства  $U$  и дополним его до базиса  $u \cup v$  всего пространства. Если  $V = \langle v \rangle$ , то легко проверить, что  $W = U \oplus V$ .  $\square$

Прямая сумма конечного количества подпространств определяется по индукции. Так как  $(U \oplus V) \oplus W$  естественно изоморфно  $U \oplus (V \oplus W)$  (элемент  $((x, y), z)$  отождествляется с  $(x, (y, z))$ ) то в расстановке скобок не играет роли (говорят, что прямая сумма ассоциативна, но надо понимать, что речь не идет об операции на множестве элементов векторного пространства, а об операции на классе векторных пространств).

**ПРЕДЛОЖЕНИЕ 6.4.** Для подпространств  $U_1, \dots, U_n \leq V$  следующие условия эквивалентны.

- (1) Отображение  $U_1 \oplus \dots \oplus U_n \rightarrow V$ ,  $(x_1, \dots, x_n) \mapsto x_1 + \dots + x_n$  является изоморфизмом.
- (2) Любой элемент  $x \in V$  единственным образом раскладывается в сумму элементов  $x_1 \in U_1, \dots, x_n \in U_n$ .
- (3)  $V = U_1 + \dots + U_n$  и  $U_i \cap (\sum_{j \neq i} U_j) = \{0\}$  для любого  $i = 1, \dots, n$ .
- (4) Объединение базисов подпространств  $U_1, \dots, U_n$  является базисом пространства  $V$ .

Если выполнены условия последнего предложения, то говорят, что  $V$  является прямой суммой подпространств  $U_1, \dots, U_n$ .

**ОПРЕДЕЛЕНИЕ 6.5.** Пусть  $I$  некоторое (возможно бесконечное) множество, и для каждого  $i \in I$  задано подпространство  $U_i \leq V$ . Прямой суммой  $\bigoplus_{i \in I} U_i$  называется множество финитных функций  $f : I \rightarrow \bigcup_{i \in I} U_i$  таких, что  $f(i) \in U_i$ . Неформально это называется множество потенциально бесконечных последовательностей элементов из  $U_i$ .

В отличие от прямой суммы, прямым произведением  $\prod_{i \in I} U_i$  называется множество всех функций  $f : I \rightarrow \bigcup_{i \in I} U_i$  таких, что  $f(i) \in U_i$  (множество реально бесконечных последовательностей).

Названия “прямая сумма” и “прямое произведение” мотивированы универсальными свойствами, которыми обладают эти объекты. Мы изучим их позже в более общем виде в главе о теории категорий.

## 7. Замена базиса

В дальнейшем мы формулируем все утверждения для конечномерных пространств и для базисов, индексированных натуральными числами. Формулировка и доказательство бесконечномерных версий оставляется читателю в качестве упражнения.

**ЛЕММА 7.1.** Пусть  $v \in {}^nV$ , а  $A \in \text{GL}_n(F)$ . Если  $v$  линейно независим, то и  $vA$  линейно независим. Линейные оболочки  $v$  и  $vA$  равны.

**ПРЕДЛОЖЕНИЕ 7.2.** Пусть  $v$  – базис  $n$ -мерного пространства  $V$  над полем  $F$ . Набор  $u = (u_1, \dots, u_n)$  является базисом тогда и только тогда, когда существует  $A \in \text{GL}_n(F)$  такая, что  $u = vA$  (в бесконечномерной версии матрица  $A$  должна быть конечностолбцовой, т. е. почти все элементы каждого столбца должны быть равны 0).

Если  $u$  и  $v$  – базисы, то  $A$  называется матрицей перехода от  $v$  к  $u$  и обозначается через  $C_{v \rightarrow u}$ . При этом:

- (1) Столбец матрицы  $C_{v \rightarrow u}$  с номером  $k$  равен столбцу координат вектора  $u_k$  в базисе  $v$ .  
Одной формулой:  $(C_{v \rightarrow u})_k = (u_k)_v$ .
- (2)  $C_{v \rightarrow u}^{-1} = C_{u \rightarrow v}$ .
- (3) Если матрица двусторонне обратима, то она квадратная.

Если  $V = F^n$ , а  $e$  – стандартный базис, то  $C_{e \rightarrow u}$  матрица, составленная из столбцов базиса  $u$ . Проще всего это запомнить, написав определение матрицы перехода в виде  $eC_{e \rightarrow u} = u$  и отождествив строчки из столбцов с матрицами.

**ПРЕДЛОЖЕНИЕ 7.3** (Преобразование координат при замене базиса). Пусть  $v$  и  $u$  – базисы пространства  $V$ . Для  $x \in V$  имеет место равенство  $x_v = C_{v \rightarrow u}x_u$ .

**ДОКАЗАТЕЛЬСТВО.** По определению столбца координат  $x = vx_v = ux_u$ . Заменяя  $u$  на  $vC_{v \rightarrow u}$  получим  $vx_v = vC_{v \rightarrow u}x_u$ . Пользуясь ассоциативностью произведения матриц и сокращая на  $v$  (это можно сделать, так как  $v$  линейно независим), получаем требуемое равенство.  $\square$

## 8. Матрица линейного отображения

**ПРЕДЛОЖЕНИЕ 8.1.** Пусть  $L : U \rightarrow V$  – линейное отображение,  $u = (u_1, \dots, u_n)$  – базис  $U$ , а  $v = (v_1, \dots, v_m)$  – базис  $V$ . Существует единственная матрица  $A \in M_{m \times n}(F)$  такая, что для любого  $x \in U$  имеет место равенство  $L(x)_v = Ax_u$ . Столбцы матрицы  $A$  вычисляются по формуле  $a_{*k} = L(u_k)_v$ .

**ДОКАЗАТЕЛЬСТВО.** По определению столбца координат  $x = ux_u$ . Применяя к этому равенству отображения  $L$  и  $\varphi_v$  из леммы 5.2 и пользуясь их линейностью, получаем  $\varphi_v \circ L(x) = \varphi_v \circ L(ux_u)$ . Применяя обозначение из параграфа 5 имеем

$$L(x)_v = \varphi_v(L(x)) = \varphi_v(L(u))x_u$$

Таким образом, положив  $A = \varphi_v(L(u)) = (L(u_1)_v, \dots, L(u_n)_v)$  получаем существование матрицы  $A$  и формулу для ее столбцов. Единственность следует из несложного утверждения про матрицы: если  $Ax = Bx$  для любого столбца  $x$  соответствующей высоты, то матрицы  $A$  и  $B$  равны.  $\square$

Матрица  $A$  из последнего предложения называется матрицей отображения  $L$  в базисах  $u$  и  $v$  и обозначается через  $L_{uv}$ . В случае, когда  $U = V$ , а  $u = v$ , говорят о матрице оператора  $L$  в базисе  $u$  и обозначают ее через  $L_u$ . Таким образом, для любого  $x \in U$  имеют место равенства

$$L(x)_v = L_u^v x_v \text{ или } L(x)_u = L_u x_u \text{ в случае } U = V, u = v.$$

Пусть  $A$  – матрица размера  $n \times n$ , а  $L : F^n \rightarrow F^n$  – оператор умножения на матрицу  $A$ , т. е.  $L(x) = Ax$  для всех  $x \in F^n$ . Если  $e$  обозначает стандартный базис (как в  $F^m$ , так и в  $F^n$ ), то легко видеть, что  $L_e^e = A$ . В связи с этим естественным отождествлением матрицы и оператора умножения на нее, последний будет часто обозначаться той же буквой, что и сама матрица.

Следующее утверждение является причиной именно такого определения произведения матриц. С другой стороны, его доказательство непосредственно вытекает из ассоциативности произведения матриц.

**ПРЕДЛОЖЕНИЕ 8.2.** Матрица композиции линейных операторов является произведением матриц этих операторов. Точнее, если  $U, V$  и  $W$  – конечномерные линейные пространства с базисами  $u, v$  и  $w$ , соответственно, а  $L : U \rightarrow V$  и  $M : V \rightarrow W$  – линейные отображения, то  $(M \circ L)_u^w = M_v^w L_u^v$ . В частности, при  $U = V = W$  и  $u = v = w$  получаем  $(M \circ L)_u = M_u L_u$ .



Нетрудно проверить, что множество линейных отображений  $V \rightarrow V$  с операциями поточечного сложения, композиции и умножения на число является алгеброй с единицей. Эта алгебра обычно обозначается  $\text{End}(V)$  и называется кольцом эндоморфизмов пространства  $V$ .

**СЛЕДСТВИЕ 8.3.** Пусть  $f$  – базис  $n$ -мерного пространства  $V$ . Определим отображение  $\theta_f : \text{End}(V) \rightarrow M_n(F)$  формулой  $\theta_f(L) = L_f$ . Тогда  $\theta_f$  является изоморфизмом алгебр.

Выясним связи между матрицей оператора и матрицей перехода.

**ЗАМЕЧАНИЕ 8.4.** Нетрудно видеть, что матрица перехода  $C_{u \rightarrow v}$  между двумя различными базисами  $u$  и  $v$  пространства  $V$  совпадает с матрицей тождественного отображения  $\mathbb{1}_V$  в базисах  $u$  и  $v$ .

**ЛЕММА 8.5.** Пусть  $u = (u_1, \dots, u_n)$  – базис пространства  $U$ , а  $v = (v_1, \dots, v_n) \in {}^nV$  – произвольный набор векторов пространства  $V$ . Тогда существует единственное линейное отображение  $L : U \rightarrow V$  такое, что  $L(u) = v$ . При этом  $L$  инъективно тогда и только тогда, когда  $u$  линейно независим;  $L$  сюръективно тогда и только тогда, когда  $u$  – система образующих;  $L$  – изоморфизм тогда и только тогда, когда  $u$  – базис.

**ДОКАЗАТЕЛЬСТВО.** Для любого  $x \in U$  имеем  $x = ux_u$ . Тогда  $L(x) = L(u)x_u$  для любого линейного отображения  $L$ . Таким образом, линейное отображение  $L$  удовлетворяющее равенству  $L(u) = v$ , должно быть задано формулой  $L(x) = vx_u$ . С другой стороны, несложно проверить, что отображение, заданное такой формулой, линейно.

Остальные утверждения леммы вытекают непосредственно из определений.  $\square$

**ЗАМЕЧАНИЕ 8.6.** Пусть  $u$  и  $v$  – базисы пространства  $V$ . Тогда матрица отображения  $L$  из предыдущего предложения в базисе  $u$  совпадает с матрицей перехода  $C_{u \rightarrow v}$ .

**ПРЕДЛОЖЕНИЕ 8.7.** Пусть  $u$  и  $u'$  – базисы пространства  $U$ ,  $v$  и  $v'$  – базисы пространства  $V$ , а  $L : V \rightarrow U$  – линейное отображение. Тогда

$$L_{u'}^{v'} = C_{v' \rightarrow v} L_u^v C_{u \rightarrow u'}.$$

В частности, при  $U = V$ ,  $u = v$  и  $u' = v'$  получим

$$Lu' = C_{u' \rightarrow u} L_u C_{u \rightarrow u'}.$$

## 9. Размерность ядра и образа, прямая сумма, формула Грассмана

Образом функции  $f : X \rightarrow Y$  называется множество  $\text{Im } f = \{f(x) \mid x \in X\}$ . По-другому образ обозначается через  $f(X)$ , что совпадает с общим правилом действия функции на множестве: для  $A \subseteq X$  положим  $f(A) = \{f(x) \mid x \in A\}$ .

Полным прообразом подмножества  $B \subseteq Y$  называется множество всех  $x \in X$ , которые отображаются в  $B$  под действием  $f$ , т.е.  $f(x) \in B$ . Полный прообраз  $B$  обозначается через  $f^{-1}(B)$ . Если  $B = \{y\}$  – одноточечное множество, то говорят о о полном прообразе точки  $y$ , который еще называется слоем отображения над этой точкой. В случае биективной функции  $f$  обозначение  $f^{-1}(y)$  двузначно: оно может обозначать значение обратной функции  $f^{-1} : Y \rightarrow X$  в точке  $y$ , а может обозначать полный прообраз точки  $y$ , т.е. одноэлементное множество. Несмотря на то, что одноэлементное множество формально нельзя отождествлять с его единственным элементом, это довольно часто делается. При этом отождествлении двузначность обозначения  $f^{-1}(y)$  пропадает.

**ОПРЕДЕЛЕНИЕ 9.1.** Пусть  $L : U \rightarrow V$  – линейное отображение. Тогда

$$\text{Ker } L = L^{-1}(0) := \{x \in U \mid L(x) = 0\} \text{ – ядро отображения } L;$$

$$\text{Im } L = \{L(x) \mid x \in U\} \text{ – образ отображения } L.$$

**ПРЕДЛОЖЕНИЕ 9.2.** Ядро и образ линейного отображения  $L : U \rightarrow V$  являются подпространствами.

Все слои отображения  $L$  являются сдвигами ядра. Точнее, пусть  $L(x) = y$ , где  $x \in U$ . Тогда

$$L^{-1}(y) = x + \text{Ker } L.$$

В частности,  $L$  инъективно тогда и только тогда, когда  $\text{Ker } L = \{0\}$ .

**ТЕОРЕМА 9.3** (о размерности ядра и образа). Пусть  $L : U \rightarrow V$  – линейное отображение. Тогда  $\dim \text{Im } L + \dim \text{Ker } L = \dim U$ .

**ДОКАЗАТЕЛЬСТВО.** Выберем базис  $(u_1, \dots, u_k)$  подпространства  $\text{Ker } L$  и дополним его до базиса  $(u_1, \dots, u_n)$  всего пространства  $U$  (здесь  $n \geq k$ ). Рутинная проверка показывает, что набор  $(L(u_{k+1}), \dots, L(u_n))$  является базисом в  $\text{Im } L$ .  $\square$

**СЛЕДСТВИЕ 9.4.** Если  $\dim U = \dim V$ , то инъективность  $L$  равносильна сюръективности.

**ТЕОРЕМА 9.5** (Размерность суммы и пересечения подпространств или формула Грассмана). Если  $U$  и  $V$  – подпространства линейного пространства  $W$ , то

$$\dim U + \dim V = \dim(U + V) + \dim(U \cap V).$$

**ДОКАЗАТЕЛЬСТВО.** Зададим линейное отображение  $L$  из внешней прямой суммы  $U \oplus V$  в  $W$  формулой  $L(u, v) = u + v$ . Легко проверить, что  $\text{Im } L = U + V$ , а  $\text{Ker } L = \{(u, -u) \mid u \in U \cap V\} \cong U \cap V$ . Теперь теорема следует из теоремы о размерности ядра и образа.  $\square$

## 10. Факторпространство

Задача этого параграфа – построить линейное отображение из данного пространства  $V$  с данным ядром  $U$ . Из предложения 9.2 мы знаем, что все слои линейного отображения – сдвиги ядра, т. е. точки образа находятся во взаимно однозначном соответствии с аффинными подпространствами  $x + U$ , где  $x$  пробегает  $V$ . Это наталкивает на мысль, определить область значений нашего отображения, как множество этих аффинных подпространств. Аффинное подпространство  $x + U$  называют еще смежным классом  $V$  по  $U$ . Заметим, что  $y \in x + U \iff y - x \in U$ . Можно определить отношение эквивалентности  $y \sim_U x \iff y - x \in U$  (проверьте, что это эквивалентность). Тогда смежный класс, это в точности класс эквивалентности.

**ОПРЕДЕЛЕНИЕ 10.1.** Множество смежных классов  $V$  по  $U$  с операциями:

$$\begin{aligned} (x + U) + (y + U) &= (x + y) + U, \\ (x + U)\alpha &= x\alpha + U \end{aligned}$$

называется факторпространством  $V$  по  $U$  и обозначается  $V/U$ .

Определения операций в  $V/U$  зависят от выбора представителя смежного класса, однако легко показать, что результат не зависит от этого выбора (это тот случай, когда необходимо доказывать корректность определения; как и все непосредственные проверки, это доказательство оставлено читателю в качестве упражнения).

Обозначим через  $\pi_U : V \rightarrow V/U$  естественную проекцию:  $\pi_U(x) = x + U$ . Нетрудно проверить, что это отображение линейно, сюръективно, а его ядро равно  $U$ . По теореме о размерности ядра и образа получим

$$\dim V/U = \dim V - \dim U.$$

Факторпространство обладает следующим универсальным свойством.

**ПРЕДЛОЖЕНИЕ 10.2.** Для любого линейного отображения  $L : V \rightarrow W$ , ядро которого содержит  $U$  существует единственное отображение  $\tilde{L} : V/U \rightarrow W$  такое, что  $L = \tilde{L} \circ \pi_U$ . При этом, сюръективность  $\tilde{L}$  равносильна сюръективности  $L$ , а инъективность  $\tilde{L}$  – тому, что  $\text{Ker } L = U$ .

**ДОКАЗАТЕЛЬСТВО.** Положим  $\tilde{L}(x+U) = L(x)$ . Легко проверить, что эта формула не зависит от выбора представителя смежного класса и задает линейное отображение. С другой стороны, эта формула равносильна равенству  $L = \tilde{L} \circ \pi_U$ . Следовательно,  $\tilde{L}$  существует и единственно.

Утверждение о сюръективности сразу следует из сюръективности  $\pi_U$  и равенства  $L = \tilde{L} \circ \pi_U$ . Отображение  $\tilde{L}$  инъективно  $\iff \text{Ker } \tilde{L} = \{0 + U\}$  (здесь  $0 + U$  – нулевой элемент пространства  $V/U$ ).

$$x + U \in \text{Ker } \tilde{L} \iff \tilde{L}(x + U) = 0 \iff L(x) = 0 \iff x \in \text{Ker } L.$$

Таким образом, если  $\text{Ker } L = U$ , то  $\text{Ker } \tilde{L} = \{0 + U\}$ , и наоборот.  $\square$

**СЛЕДСТВИЕ 10.3** (теорема о гомоморфизме). *Для любого линейного отображения  $L : V \rightarrow W$  имеем*

$$V / \text{Ker } L \cong \text{Im } L.$$

Пусть теперь  $L : V \rightarrow V$  линейный оператор, а  $U \leq V$ . Подпространство  $U$  называется инвариантным относительно  $L$  (короче,  $L$ -инвариантным), если  $L(x) \in U$  для любого  $x \in U$ . Пусть,  $u$  – базис  $U$ , а  $v = u \cup w$  – базис  $V$ . Если  $U$  является  $L$ -инвариантным, то матрица оператора  $L$  в базисе  $v$  имеет вид  $\begin{pmatrix} A & * \\ 0 & B \end{pmatrix}$ , где  $A$  имеет размер  $\dim U \times \dim U$ , а размер  $B$  равен  $(\dim V - \dim U) \times (\dim V - \dim U)$ . Из формулы для столбцов матрицы оператора видно, что  $A$  является матрицей сужения оператора  $L$  на подпространство  $U$  в базе  $u$ .

Так как  $U$  является  $L$ -инвариантным, можно определить отображение  $\bar{L} : V/U \rightarrow V/U$  формулой  $\bar{L}(x + U) = L(x) + U$  (проверьте, что определение корректно). Обозначим через  $\bar{w} = (w_1 + U, \dots, w_k + U)$  базис факторпространства  $V/U$  (проверьте, что это базис). Тогда матрица  $B$  – это матрица оператора  $\bar{L}$  в базисе  $\bar{w}$ . Действительно,  $L(w_i) = \sum u_i \alpha_i + \sum w_j b_{ji}$ , откуда  $\bar{L}(\bar{w}_i) = \sum \bar{w}_j b_{ji}$ .

## 11. Ранг, PDQ-разложение

**ОПРЕДЕЛЕНИЕ 11.1.** Рангом набора векторов называется размерность линейной оболочки этого набора. Рангом линейного оператора называется размерность образа этого оператора. Столбцовым (строчным) рангом матрицы называется ранг набора ее столбцов (строк).

Так как из любой системы образующих можно выбрать базис, то ранг набора векторов – это наибольшее количество линейно независимых векторов из данного набора. Так как образы базисных векторов порождают образ оператора, то ранг оператора равен рангу набора, состоящего из образов базисных векторов. Легко понять, что он равен также столбцовому рангу матрицы этого оператора (независимо от выбора базисов). Далее в этом параграфе мы докажем, что строчный и столбцовый ранги матрицы равны.

**ЛЕММА 11.2.** Пусть  $A \in M_{m \times n}(F)$ .

- (1) Набор столбцов матрицы  $A$  линейно независим тогда и только тогда, когда ее столбцовый ранг равен  $n$ .
- (2) Набор столбцов матрицы  $A$  порождает  $F^m$  тогда и только тогда, когда ее столбцовый ранг равен  $m$ .
- (3) Набор столбцов матрицы  $A$  является базисом в  $F^m$  тогда и только тогда, когда ее столбцовый ранг равен  $t = n$ . В этом случае матрица  $A$  обратима.
- (4) Если все строки  $A$  линейно независимы, и все ее столбцы обладают тем же свойством, то  $t = n$ , а матрица  $A$  обратима.

**ДОКАЗАТЕЛЬСТВО.** Утверждения (1) и (2) очевидны. Из них следует, что столбцовый ранг равен  $t = n$  тогда и только тогда, когда набор столбцов является базисом. В этом случае  $A$  является матрицей перехода от стандартного базиса пространства  $F^m$  к базису из столбцов матрицы  $A$  и, следовательно, является обратимой.

Количество линейно независимых столбцов не может быть больше размерности пространства, откуда  $n \leq m$ . Аналогичное рассуждение для строк доказывает обратное неравенство, т. е.  $m = n$ .  $\square$

**ЛЕММА 11.3.** *Умножение матрицы на обратимую (слева или справа) не меняет ее столбцовый и строчный ранг.*

**ДОКАЗАТЕЛЬСТВО.** Умножение матрицы оператора слева на обратимую матрицу соответствует замене базиса в его области значений, а справа – в области определения. Так как столбцовый ранг матрицы оператора не зависит от выбора базиса, то столбцовый ранг не меняется при умножении на обратимую.

Второе утверждение следует из того, что строчный ранг матрицы равен столбцовому рангу транспонированной к ней, а транспонированная к обратимой – обратима.  $\square$

**ТЕОРЕМА 11.4** (PDQ-разложение). *Для любого линейного отображения  $L : U \rightarrow V$ , где  $U$  и  $V$  – конечномерные пространства, существуют базисы пространств  $U$  и  $V$ , в которых матрица отображения  $L$  имеет вид  $\begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$ .*

Любая матрица  $A \in M_{m,n}(F)$  представляется в виде  $A = PDQ$ , где  $P \in GL_m(F)$ ,  $Q \in GL_n(F)$ , а  $D$  записывается в блочном виде  $D = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix}$ . При этом размер единичной матрицы в формуле для  $D$  равен строчному и столбцовому рангу  $A$ .

**ДОКАЗАТЕЛЬСТВО.** Доказательство первого утверждения следует из доказательства теоремы о размерности ядра и образа. Выберем базис  $(f_1, \dots, f_k)$  ядра оператора  $L$  и дополним его до базиса  $u = (g_1, \dots, g_l, f_1, \dots, f_k)$  пространства  $U$ . Тогда вектора  $L(g_1), \dots, L(g_l)$  линейно независимы, и их можно дополнить до базиса  $v$  пространства  $V$ . Теперь легко видеть, что матрица отображения  $L$  в базисах  $u$  и  $v$  имеет требуемый вид.

Пусть  $L : F^n \rightarrow F^m$  – оператор умножения на матрицу  $A$ . Выберем базис  $u$  пространства  $F^n$  и  $v$  – пространства  $F^m$  так, чтобы  $L_v^u = D$ . Тогда

$$A = A_e^e = C_{e \rightarrow u} L_v^u C_{v \rightarrow e} = PDQ,$$

где  $e$  обозначает стандартный базис пространства столбцов.

Последнее утверждение сразу следует из предыдущей леммы.  $\square$

Аналогичная теорема верна с заменой поля на хорошее кольцо (область главных идеалов), а единичной матрицы на диагональную, впрочем, доказательство уже менее банально. Если в качестве кольца взять  $\mathbb{Z}$ , то это утверждение является ключевым шагом классификации конечнопорожденных абелевых групп.

**ЛЕММА 11.5.** *Квадратная матрица обратима тогда только тогда, когда ее ранг равен ее размеру.*

Следующее тривиальное утверждение во многих книгах преподносится, как верх математической мысли (справедливости ради, надо сказать, что ранг матрицы в этих книгах определяется, как минорный ранг, см. § 4 главы 5). При нашем определении ранга оно сразу следует из того, что система линейных уравнений  $Ax = b$  имеет решение тогда и только тогда, когда  $b$  содержится в линейной оболочке столбцов матрицы  $A$ .

**ТЕОРЕМА 11.6** (Кронекера–Капелли). *Система  $Ax = b$  совместна тогда и только тогда, когда ранг матрицы  $A$  равен рангу расширенной матрицы  $(Ab)$ .*

## 12. Разложения Брюа и Гаусса

Матрица  $a$  называется верхней (нижней) треугольной, если  $a_{ij} = 0$  при всех  $i > j$  (соотв.  $i < j$ ). Треугольная матрица с 1 на главной диагонали называется унитреугольной. Обозначим

множество верхних (нижних) обратимых треугольных матриц через  $B = B_n(F)$  (соотв.  $B^- = B_n^-(F)$ ). Аналогично, множества унитарных матриц обозначаются через  $U = U_n(F)$  и  $U^- = U_n^-(F)$ . В теории алгебраических групп  $B$  и  $B^-$  называются противоположными борелевскими подгруппами, а  $U$  и  $U^-$  – их унитарными радикалами. Через  $W = W_n$  обозначим множество матриц перестановок, т.е. матриц, отличающихся от единичной перестановкой столбцов (группа Вейля).

**ЛЕММА 12.1.** *Множества  $W$ ,  $B$ ,  $B^-$ ,  $U$  и  $U^-$  являются подгруппами в  $\mathrm{GL}_n(F)$ .*

**ТЕОРЕМА 12.2** (Разложение Брюа).  $\mathrm{GL}_n(F) = BWB$ .

**ДОКАЗАТЕЛЬСТВО.** Требуется доказать, что любая матрица  $a \in \mathrm{GL}_n(F)$  представляется в виде  $a = bwc$ , для некоторых  $b, c \in B$  и  $w \in W$ . Индукцией по  $n$  докажем, что домножая  $a$  слева и справа на верхнетреугольные матрицы можно получить матрицу перестановки. Так как обратная к верхнетреугольной является верхнетреугольной, из этого следует результат.

Пусть  $i$  – наибольший индекс, для которого  $a_{i1} \neq 0$ . Запишем  $a$  в виде

$$a = \begin{pmatrix} x & * \\ a_{i1} & z \\ 0 & * \end{pmatrix} \text{ где } x = \begin{pmatrix} a_{11} \\ \vdots \\ a_{i-1,1} \end{pmatrix}, \text{ а } z = (a_{i2}, \dots, a_{in}).$$

Домножая  $a$  слева на верхнетреугольную матрицу получим матрицу, у которой первый столбец совпадает с  $i$ -м столбцом единичной матрицы. После этого, домножая справа на подходящую верхнетреугольную матрицу можем сделать  $i$ -ю строку равной первой строке единичной матрицы. Точнее

$$\begin{pmatrix} E & -\frac{x}{a_{i1}} & 0 \\ 0 & \frac{1}{a_{i1}} & 0 \\ 0 & 0 & E \end{pmatrix} \begin{pmatrix} x & * \\ a_{i1} & z \\ 0 & * \end{pmatrix} \begin{pmatrix} 1 & -z/a_{i1} \\ 0 & E \end{pmatrix} = \begin{pmatrix} 0 & f \\ 1 & 0 \\ 0 & g \end{pmatrix}$$

для некоторых матриц  $f, g$ . Заметим, что, так как строки полученной матрицы линейно независимы, то и строки матрицы  $\begin{pmatrix} f \\ g \end{pmatrix}$  также являются линейно независимыми. Поэтому последняя матрица обратима, и к ней можно применить индукционное предположение. Следовательно, существуют матрицы  $u, v \in B_{n-1}(F)$  такие, что  $u \begin{pmatrix} f \\ g \end{pmatrix} v \in W_{n-1}$ . Пусть  $u = \begin{pmatrix} u^{(1)} & u^{(2)} \\ 0 & u^{(3)} \end{pmatrix}$ , где  $u^{(1)} \in B_{i-1}(F)$ , а  $u^{(3)} \in B_{n-i}(F)$ . Тогда

$$\begin{pmatrix} u^{(1)} & u^{(2)} \\ 0 & u^{(3)} \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} \cdot v$$

является матрицей-перестановкой, а, следовательно, и

$$\begin{pmatrix} u^{(1)} & 0 & u^{(3)} \\ 0 & 1 & 0 \\ 0 & 0 & u^{(2)} \end{pmatrix} \begin{pmatrix} 0 & f \\ 1 & 0 \\ 0 & g \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix}$$

– также матрица-перестановка. □

Множество  $BwB$  при фиксированном  $w \in W$  называется клеткой Брюа.

**ПРЕДЛОЖЕНИЕ 12.3.** *Две различные клетки Брюа не пересекаются.*

**ТЕОРЕМА 12.4** (Разложение Гаусса).  $\mathrm{GL}_n(F) = WB^-B$ .

В параграфе 7 мы докажем, что клетка Брюа  $BwB$  содержится в клетке Гаусса  $wB^-B$ . В частности, разложение Гаусса является следствием разложения Брюа. Здесь же мы дадим непосредственное доказательство разложения Гаусса. Оно сразу вытекает из следующих трех лемм. Сформулируем в двух словах основную идею. Сначала надо выбрать перестановку строк так, чтобы все квадратные подматрицы (любого размера), стоящие в левом верхнем углу, были бы обратимы. При доказательстве возможности этого ключевым замечанием является то, что ранг

подматрицы, составленной из первых  $k$  столбцов матрицы  $a$ , равен  $k$  (все столбцы обратимой матрицы линейно независимы), поэтому существует  $k$  линейно независимых строк этой подматрицы. Затем матрица приводится к верхнетреугольному виду элементарными преобразованиями с ведущими элементами на главной диагонали.

Главной подматрицей матрицы  $a$  порядка  $k$  называется подматрица, стоящая на пересечении первых  $k$  строк и первых  $k$  столбцов матрицы  $a$ .

**ЛЕММА 12.5.** *Умножение матрицы на нижнюю унитреугольную слева и на верхнюю унитреугольную справа не меняет обратимости главных подматриц.*

**ДОКАЗАТЕЛЬСТВО.** С помощью блочного умножения матриц нетрудно убедиться, что при указанных в формулировке леммы действиях  $k \times k$ -подматрица, стоящая в левом верхнем углу, умножается на унитреугольные матрицы. Теперь утверждение следует из того, что унитреугольные матрицы обратимы.  $\square$

**ЛЕММА 12.6.** *Все главные подматрицы обратимы тогда и только тогда, когда матрица раскладывается в произведение обратимых нижнетреугольной и верхнетреугольной.*

**ДОКАЗАТЕЛЬСТВО.** Если матрица является произведением обратимых нижнетреугольной и верхнетреугольной, то из леммы 12.1 следует, что все главные подматрицы обратимы.

Доказательство обратной импликации проведем индукцией по размеру  $n$  матрицы  $a$ . Для  $n = 1$  доказывать нечего. Пусть  $a = \begin{pmatrix} \tilde{a} & x \\ y & \alpha \end{pmatrix}$ , где  $\alpha \in F$ ,  $x \in F^{n-1}$ ,  $y \in {}^{n-1}F$ , а  $\tilde{a} \in M_{n-1}(F)$ . Заметим, что по условию все главные подматрицы в  $\tilde{a}$  обратимы. Поэтому к  $\tilde{a}$  применимо индукционное предположение. С другой стороны,

$$a = \begin{pmatrix} E & 0 \\ y\tilde{a}^{-1} & 1 \end{pmatrix} \begin{pmatrix} \tilde{a} & x \\ 0 & \alpha - y\tilde{a}^{-1}x \end{pmatrix}.$$

Раскладывая  $\tilde{a}$  по индукционному предположению, получаем результат.  $\square$

**ЛЕММА 12.7.** *Для любой матрицы  $a \in GL_n(F)$  существует матрица-перестановка  $w$  такая, что все главные подматрицы в матрице  $wa$  обратимы.*

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство индукцией по  $n$ . При  $n = 1$  доказывать нечего. Пусть  $n > 1$ . Ранг подматрицы, составленной из первых  $n - 1$  столбцов матрицы  $a$ , равен  $n - 1$ , так как все столбцы обратимой матрицы линейно независимы. Поэтому существует  $n - 1$  линейно независимых строк этой матрицы. Переставим эти строки на первые  $n - 1$  мест. Тогда главная подматрица порядка  $n - 1$  станет обратимой. Далее используем индукционное предположение для главной подматрицы порядка  $n - 1$ .  $\square$

## Начала теории групп

### 1. Простейшие конструкции

Подструктурой алгебраической структуры называется подмножество структуры, замкнутое относительно всех операций, включая взятие нейтрального и обратного элемента, если аксиомы структуры гарантируют их наличие. Из этого вытекает, что подструктура является структурой того же типа, потому что выполнение свойств (кроме существования) в подмножестве следует из выполнения этих свойств во всем множестве (в этом смысле считать, что группа – это множество с одной 0-арной, одной унарной и одной бинарной операциями; тогда свойства формулируются без квантора существования).

**ОПРЕДЕЛЕНИЕ 1.1.** Непустое подмножество  $H$  группы  $G$  называется подгруппой, если элементы  $ab$  и  $a^{-1}$  принадлежат  $H$  для любых  $a, b \in H$ .

Если  $a \in H$ , то  $a^{-1} \in H$ , а, следовательно, и их произведение равно нейтральному элементу лежит в подгруппе  $H$ . Ясно, что подгруппа сама является группой относительно тех же операций, которые заданы в объемлющей группе. Если  $H$  – подгруппа в  $G$ , то пишут  $H \leq G$ . В любой группе есть две тривиальные подгруппы: сама группа и множество состоящее из одного нейтрального элемента.

Прямое произведение алгебраических структур одного типа называется декартовым произведением множеств с покомпонентными операциями. В случае, если одна из операций называется сложением, обычно говорят о прямой сумме, а не о прямом произведении. Надо отметить, что эта терминология не совпадает с терминологией теории категорий, которая приобретает все большую популярность.

**ОПРЕДЕЛЕНИЕ 1.2.** Пусть  $G_1$  и  $G_2$  – группы с операциями  $\star_1$  и  $\star_2$  соответственно. Прямое произведение  $G = G_1 \times G_2$  – это декартово произведение  $G_1$  и  $G_2$  с операцией  $\star$ , заданной следующим образом:  $(g_1, g_2) \star (h_1, h_2) = (g_1 \star_1 h_1, g_2 \star_2 h_2)$ , где  $g_1, h_1 \in G_1$ , а  $g_2, h_2 \in G_2$ .

Аналогично определяется прямое произведение любого (даже не обязательно конечного) семейства групп. Если группы коммутативны, операция обозначена знаком  $+$ , а их количество конечно, то вместо термина “прямое произведение” обычно употребляют термин “прямая сумма” и обозначают ее знаком  $\bigoplus$ , например,  $G = \bigoplus_{k=1}^n G_n$ .

### 2. Гомоморфизмы, ядро и образ

Гомоморфизмом алгебраических структур данного типа называется функция из одной такой структуры в другую, сохраняющая все операции. Для того, чтобы придать этому определению точный смысл, необходимо сначала строго определить, что такое алгебраическая структура, что увело бы нас в дебри науки, называемой универсальной алгеброй. Так что разберемся отдельно с группами, а в соответствующем месте с кольцами.

**ОПРЕДЕЛЕНИЕ 2.1.** Пусть  $G$  с операцией  $\star$  и  $H$  с операцией  $\#$  – группы. Функция  $f : G \rightarrow H$  называется гомоморфизмом, если  $f(a \star b) = f(a) \# f(b)$  для любых  $a, b \in G$ .

Образ гомоморфизма  $f : X \rightarrow Y$  – это его образ как функции, т.е.  $\text{Im } f = \{f(x) \mid x \in X\}$ .

Ядро гомоморфизма  $\text{Ker } f = f^{-1}(e)$ .

Инъективный гомоморфизм называется мономорфизмом, сюръективный – эпиморфизмом, а биективный – изоморфизмом. Если между двумя группами существует изоморфизм, то они называются изоморфными.

**ЛЕММА 2.2.** Если  $f : G \rightarrow H$  – гомоморфизм групп, то  $f(e_G) = e_H$ , а  $f(x^{-1}) = f(x)^{-1}$  для любого  $x \in G$ .

**ЛЕММА 2.3.** Пусть  $f : G \rightarrow H$  – гомоморфизм групп,  $g \in G$ , а  $h = f(g)$ . Тогда  $f^{-1}(h) = g \operatorname{Ker} f$ .

Гомоморфизм инъективен тогда и только тогда, когда его ядро состоит из одного элемента.

**ОПРЕДЕЛЕНИЕ 2.4.** Подгруппа  $H$  группы  $G$  называется нормальной, если для любых  $g \in G$  и  $h \in H$  имеет место включение  $g^{-1}hg \in H$ . В других обозначениях:  $\forall g \in G : g^{-1}Hg \subseteq H$ .

Заметим, что любая подгруппа абелевой группы является нормальной.

**ЛЕММА 2.5.** Подгруппа  $H$  нормальна в группе  $G$  тогда и только тогда, когда  $\forall g \in G : gH = Hg$ .

**ЛЕММА 2.6.** Образ гомоморфизма групп является подгруппой, а ядро – нормальной подгруппой.

### 3. Порождение, циклические группы, порядок элемента

**ОПРЕДЕЛЕНИЕ 3.1.** Пусть  $X$  – подмножество группы  $G$ . Подгруппой, порожденной множеством  $X$ , называется наименьшая подгруппа в  $G$ , содержащая  $X$ . Подгруппа, порожденная  $X$ , обозначается  $\langle X \rangle$ . Подгруппа, порожденная одним элементом (точнее, одноэлементным множеством) называется циклической.

Так как пересечение подгрупп снова является подгруппой, то подгруппа, порожденная  $X$ , всегда существует. Действительно, это пересечение всех подгрупп, содержащих  $X$ .

**ЛЕММА 3.2.**  $\langle X \rangle$  состоит из всех элементов вида  $x_1 \cdots x_k$ , где  $k$  – некоторое натуральное число, а  $x_i \in X \cup X^{-1}$  (здесь, как обычно,  $X^{-1} = \{x^{-1} \mid x \in X\}$ ). Обратите внимание, что здесь элементы  $x_1, \dots, x_k$  не обязательно различны. Если групп абелева, то произведение этих элементов приводится к виду  $x_1^{i_1} \cdots x_m^{i_m}$ , где  $x_1, \dots, x_m$  различны, а  $i_j \in \mathbb{Z}$ . В аддитивной записи это превращается в линейную комбинацию элементов из  $X$  с целыми коэффициентами.

**ПРЕДЛОЖЕНИЕ 3.3.** Любая циклическая подгруппа изоморфна аддитивной группе  $\mathbb{Z}$  или  $\mathbb{Z}_n$  (остатки от деления на  $n$  с операцией сложения по модулю  $n$ ).

**ДОКАЗАТЕЛЬСТВО.** По определению циклическая группа  $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ . Если  $g^k \neq g^m$  при  $k \neq m$ , то отображение  $\mathbb{Z} \rightarrow \langle g \rangle$ ,  $k \mapsto g^k$ , является изоморфизмом.

Если  $g^k = g^m$  при некоторых  $k > m$ , то  $g^{k-m} = 1$ . Пусть  $n$  – наименьшее натуральное число (не 0) такое, что  $g^n = 1$ . Любое целое  $l$  можно разделить на  $n$  с остатком:  $l = ns + r$ ,  $0 \leq r < n$ . Тогда  $g^l = g^{ns}g^r = g^r$ . Таким образом,  $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$ . Нетрудно видеть, что отображение  $\mathbb{Z}_n \rightarrow \langle g \rangle$ ,  $k \mapsto g^k$ , является изоморфизмом.  $\square$

**ОПРЕДЕЛЕНИЕ 3.4.** Пусть  $g$  – элемент группы  $G$ . Порядок циклической подгруппы, порожденной  $g$ , называется порядком элемента  $g$ , т.е.  $\operatorname{ord} g = |\langle g \rangle|$ . Как видно из доказательства предыдущего утверждения, порядок элемента  $g$  – это наименьшее натуральное число  $n$  такое, что  $g^n = 1$ .

### 4. Смежные классы и теорема Лагранжа

**ОПРЕДЕЛЕНИЕ 4.1.** Пусть  $H \leq G$ . Множества  $gH$  и  $Hg$  называются левым (соотв. правым) смежными классами по подгруппе  $H$ . Множество левых смежных классов обозначается через  $G/H$ , а правых –  $H \backslash G$  (не путать с  $H \setminus G = H \setminus G$ ; я специально немного опустил  $H$  и приподнял  $G$ , но не во всех книгах это делается). Элемент смежного класса часто называют его представителем.



Как мы заметили в параграфе 2, левые смежные классы по ядру гомоморфизма совпадают с правыми. Кроме того, из леммы 2.3 следует, что группа разбивается в дизъюнктное объединение смежных классов по ядру. Сейчас мы выясним, какие свойства выживают для смежных классов по произвольным подгруппам.

Определим отношение “сравнимости по модулю  $H$ ” на множестве  $G$  по формуле:  
 $a \equiv b \pmod{H} \iff a \in bH$ . На самом деле мы определили “сравнимость по модулю  $H$  слева”. Сравнимость по модулю  $H$  справа определяется включением  $a \in Hb$ . Везде, кроме следующей леммы мы будем использовать понятие сравнимости по модулю  $H$ , только когда  $H$  – нормальная подгруппа в  $G$ . В этом случае по лемме 2.5  $gH = Hg$ , и сравнимость слева и справа совпадают.

**ЛЕММА 4.2.** *Сравнимость по модулю  $H$  является отношением эквивалентности. Два смежных класса либо не пересекаются, либо совпадают.*

**ДОКАЗАТЕЛЬСТВО.** Рефлексивность:  $a = ae \in aH$ . Симметричность:  $a \in bH \implies \exists h \in H : a = bh \implies b = ah^{-1} \in aH$ . Транзитивность: если  $a \in bH$  и  $b \in cH$ , т.е.  $a = bh$  и  $b = ch'$  для некоторых  $h, h' \in H$ , то  $a = ch'h \in cH$ .

Ясно, что классы сравнимости по модулю  $H$  – это левые смежные классы по подгруппе  $H$ , откуда вытекает второе утверждение леммы.  $\square$

**ЛЕММА 4.3.** *Любые два смежных класса равномощны, т.е. между ними существует биекция. В частности, если они конечны, то они содержат одинаковое количество элементов.*

**ТЕОРЕМА 4.4** (теорема Лагранжа). *Если  $H$  – подгруппа конечной группы  $G$ , то  $|G| = |H| \cdot |G/H|$ .*

**ЛЕММА 4.5.** *Множества  $G/H$  и  $H \backslash G$  равномощны, т.е. между ними существует биекция.*

**ДОКАЗАТЕЛЬСТВО.** Биекция  $G/H \rightarrow H \backslash G$  задается по правилу  $aH \mapsto (aH)^{-1} = Ha^{-1}$  (здесь  $(aH)^{-1} = \{(ah)^{-1} \mid h \in H\}$ ).  $\square$

В частности, если количество левых или правых смежных классов конечно, то  $|G/H| = |H \backslash G|$ . Это число называют индексом подгруппы  $H$  в  $G$  и обозначают через  $|G : H|$  (если количество смежных классов бесконечно, пишут  $|G : H| = \infty$ ). Индекс подгруппы может быть конечен, даже если сама группа бесконечна, например  $H = 2\mathbb{Z}$  в  $G = \mathbb{Z}$ .

## 5. Факторгруппа и теорема о гомоморфизме

**ПРЕДЛОЖЕНИЕ 5.1.** *Для любой нормальной подгруппы  $H$  группы  $G$  существует группа  $F$  и эпиморфизм  $\pi : G \rightarrow F$ , ядро которого равно  $H$ .*

**ДОКАЗАТЕЛЬСТВО.** Положим  $F = G/H$  и зададим отображение  $\pi : G \rightarrow F$  по формуле  $\pi(x) = xH$ . Зададим операцию в  $F$  по формуле  $(xH) \cdot (yH) = xyH$ . Так как  $H$  – нормальная подгруппа, то эта операция не зависит от выбора представителей  $x$  и  $y$  смежных классов  $xH$  и  $yH$ . Действительно,  $xhyh' = xy(y^{-1}hy)h' \in xyH$ . Ассоциативность операции следует из ассоциативности операции в группе  $G$ , нейтральным элементом является смежный класс  $eH = H$ , а обратным для  $xH$  – смежный класс  $x^{-1}H$ . Таким образом,  $F$  является группой. Тот факт, что  $\pi$  – гомоморфизм, сразу следует из формулы умножения смежных классов. Очевидно, что  $\pi$  сюръективен. Уравнение  $\pi(x) = e_{G/H} = H$  равносильно тому, что  $x \in H$  (иначе смежные классы  $\pi(x) = xH$  и  $H$  не совпадают). Следовательно,  $\text{Ker } \pi = H$ .  $\square$

**ОПРЕДЕЛЕНИЕ 5.2.** Группа  $G/H$ , построенная в доказательстве, называется факторгруппой  $G$  по  $H$ , а отображение  $\pi$  – канонической проекцией или гомоморфизмом редукции по модулю  $H$ .

**ТЕОРЕМА 5.3.** *Пусть  $f : G \rightarrow H$  гомоморфизм групп, а  $N \trianglelefteq G$ . Если  $\text{Ker } f \geq N$ , то существует единственный гомоморфизм  $g : G/N \rightarrow H$  такой, что  $f = g \circ \pi$ . Если  $f$  – эпиморфизм, то и  $g$  – эпиморфизм. Если  $\text{Ker } f = N$ , то  $g$  – мономорфизм.*

ДОКАЗАТЕЛЬСТВО. Пусть  $x \in G$ . Из равенства  $f = g \circ \pi$  следует, что

$$g(xN) = f(x).$$

Если  $y$  – другой представитель смежного класса  $xN$ , то  $y = xn$  для некоторого  $n \in N$ , и  $g(yN) = f(y) = f(x)f(n) = f(x)$ , так как  $n \in N \leq \text{Ker } f$ . Таким образом, вынесенная формула корректно определяет отображение. Из определения умножения смежных классов следует, что это отображение является гомоморфизмом. Очевидно, что отображение, удовлетворяющее равенству  $f = g \circ \pi$ , единственно.

Если композиция сюръективна, то левый гомоморфизм (тот, который применяется последним) обязан быть сюръективным. Пусть теперь  $\text{Ker } f = N$ . Тогда

$$xN \in \text{Ker } g \iff x \in \text{Ker } f = N \iff xN = 1_{G/N}.$$

□

**СЛЕДСТВИЕ 5.4** (Теорема о гомоморфизме групп). Пусть  $f : G \rightarrow H$  – гомоморфизм групп. Тогда  $\text{Im } f \cong G/\text{Ker } f$ .

ДОКАЗАТЕЛЬСТВО. Отображение  $\bar{f} : G \rightarrow \text{Im } f$  заданное формулой  $\bar{f}(x) = f(x)$  является эпиморфизмом, причем его ядро равно  $\text{Ker } f$ . По предыдущей теореме существует изоморфизм  $\text{Im } f \rightarrow G/\text{Ker } f$ . □

## 6. Сопряженные элементы, коммутаторы и коммутант

Пусть  $x, y, z$  – элементы группы  $G$ . Элемент  $x^y := y^{-1}xy$  называется (правым) сопряженным к  $x$  при помощи  $y$ , а  ${}^yx = x^{y^{-1}} = yxy^{-1}$  – левым сопряженным к  $x$  при помощи  $y$ .

**ЛЕММА 6.1.**  $(xy)^z = x^zy^z$  и  ${}^zxy = {}^zx \cdot {}^zy$ , т. е. сопряжение при помощи  $z$  является гомоморфизмом;

${}^y{}^zx = {}^z({}^yx)$ , т. е. отображение из группы  $G$  в группу автоморфизмов группы  $G$ , переводящее элемент в левое сопряжение при помощи этого элемента, является гомоморфизмом (проверьте, что множество автоморфизмов группы  $G$  является группой относительно композиции).

Отношение “ $x$  сопряжено с  $y$ ” очевидно является отношением эквивалентности. Классы этой эквивалентности называются классами сопряженных элементов.

Заметим, что для доказательства нормальности подгруппы  $H$  в группе  $G$ , достаточно проверить условие нормальности только на образующих.

**ЛЕММА 6.2.** Пусть  $H = \langle X \rangle$  – подгруппа в группе  $G$ , а  $Y$  – симметричное множество образующих группы  $G$ . Тогда  $H$  нормальна в  $G$  тогда и только тогда, когда  $x^y \in H$  для любых  $x \in X$  и  $y \in Y$ .

ДОКАЗАТЕЛЬСТВО. Если  $H \trianglelefteq G$ , то включения очевидны. Обратно, пусть  $h \in H$ , а  $g = y_1 \cdots y_m \in G$ , где  $y_1, \dots, y_m \in Y$ . Индукцией по  $m$  докажем, что  $h^g \in H$ , откуда будет следовать нормальность. При  $m = 0$  это очевидно, так как  $g = 1$ . Пусть  $m \geq 1$ . По индукционному предположению  $h^{y_1 \cdots y_{m-1}} \in H$ , следовательно,  $h^{y_1 \cdots y_{m-1}} = x_1 \cdots x_n$  для некоторого  $n \in \mathbb{N}$  и  $x_1, \dots, x_n \in X \cup X^{-1}$ . Тогда  $h^g = (x_1 \cdots x_n)^{y_m} = x_1^{y_m} \cdots x_n^{y_m}$ , а каждый сомножитель лежит в  $H$  по условию. □

Наименьшая нормальная подгруппа группы  $G$ , содержащая подгруппу  $H$  называется нормальным замыканием  $H$  в  $G$  и обозначается  $H^G$ . Нетрудно видеть, что она порождена всеми элементами вида  $h^g$ ,  $h \in H$ ,  $g \in G$ .

Коммутатором называется элемент  $[x, y] = xyx^{-1}y^{-1}$ .

**ЛЕММА 6.3.** Выполнены следующие коммутаторные формулы.

- (1)  $[x, y]^{-1} = [y, x]$ .
- (2)  $[x, yz] = [x, y] \cdot {}^y[x, z]$ .

Пусть  $X, Y$  – подгруппы в  $G$ . Взаимным коммутантом этих подгрупп называется подгруппа, порожденная всеми коммутаторами  $[x, y]$ ,  $x \in X$ ,  $y \in Y$ . Так как сопряженный с коммутатором является коммутатором, то взаимный коммутант двух нормальных подгрупп является нормальной подгруппой. Однако и для подгрупп, не являющихся нормальными, их взаимный коммутант нормален, хотя и не во всей группе.

**ЛЕММА 6.4.** Пусть  $X$  и  $Y$  – подгруппы в  $G$ . Тогда  $[X, Y] \trianglelefteq \langle X \cup Y \rangle$ .

**ДОКАЗАТЕЛЬСТВО.** Докажем, что  $[x, y]^z \in [X, Y]$  при всех  $x \in X$  и  $y, z \in Y$ . Действительно, по формуле 6.3(2)

$$[x, y]^z = z^{-1}[x, y] = [x, z^{-1}]^{-1} \cdot [x, z^{-1}y] \in [X, Y].$$

Аналогично, при  $x, z \in X$  и  $y \in Y$  имеем

$$[x, y]^z = ([y, x]^{-1})^z = (z^{-1}[y, x])^{-1} = ([y, z^{-1}]^{-1} \cdot [y, z^{-1}x])^{-1} = [z^{-1}x, y] \cdot [z^{-1}, y]^{-1} \in [X, Y].$$

Теперь результат следует из леммы 6. □

Почти то же самое рассуждение показывает, что взаимный коммутант является наименьшей подгруппой в  $\langle X \cup Y \rangle$ , содержащей все коммутаторы образующих групп  $X$  и  $Y$ .

**ЛЕММА 6.5.** Пусть  $S_X$  и  $S_Y$  – множества образующих подгрупп  $X$  и  $Y$  соответственно. Тогда  $[X, Y] = \langle [s, t] \mid s \in S_X, t \in S_Y \rangle^{\langle X \cup Y \rangle}$ .

**ДОКАЗАТЕЛЬСТВО.** Обозначим правую часть последнего равенства через  $Z$ . По предыдущей лемме она содержится в левой. Поэтому достаточно показать, что любой образующий элемент левой группы содержится в  $Z$ . Пусть, сначала,  $s \in S_X$ , а  $y = t_1 \dots t_n$ , где  $t_1, \dots, t_n \in S_Y$ . Индукцией по  $n$  докажем, что  $[s, y] \in Z$ . База индукции ( $n = 1$ ) выполнена по определению  $Z$ . При  $n > 1$  по формуле (2) леммы 6.3 имеем  $[s, y] = [s, t_1] \cdot {}^{t_1}[s, t_2 \dots t_n]$ . По индукционному предположению  $[s, t_2 \dots t_n] \in Z$ , следовательно,  $[s, y] \in Z$  для любого  $s \in S_X$  и  $y \in Y$ . Замена образующей группы  $X$  на любой образующий элемент этой группы происходит аналогично (то, что мы уже доказали, является базой индукции). □

## 7. Группа унитарных матриц и второе доказательство разложения Гаусса

Пусть  $F$  – поле или, в большей общности, коммутативное кольцо с 1. Положим

$$U_n^{(k)} = U_n^{(k)}(F) = \{a \in M_n(F) \mid a_{ii} = 1, a_{ij} = 0 \text{ при всех } i \neq j, j - i < k\},$$

$$U_n = U_n(F) := U_n^{(1)}(F) \text{ и } U_n^{(k)} = \{1\} \text{ при } k \geq n.$$

**ЛЕММА 7.1.** Группа  $U_n^{(k)}$  порождена трансвекциями  $t_{ij}(\alpha)$  по всем  $\alpha \in F$  и  $j - i \geq k$ .

Для доказательства следующих утверждений нам потребуются следующие формулы, которые легко проверить непосредственным вычислением. Пусть  $i, j, k, h$  – попарно различные индексы. Тогда

$$\begin{aligned} t_{ij}(\alpha)t_{ij}(\beta) &= t_{ij}(\alpha + \beta) \\ [t_{ij}(\alpha), t_{jk}(\beta)] &= t_{ik}(\alpha\beta) \\ [t_{ij}(\alpha), t_{ki}(\beta)] &= t_{kj}(-\alpha\beta) \\ [t_{ij}(\alpha), t_{hk}(\beta)] &= e. \end{aligned} \tag{2}$$

**ЛЕММА 7.2.** Группа  $U_n^{(k)}$  нормальна в  $U_n$ . Более того,  $[U_n^{(k)}, U_n^{(m)}] = U_n^{(k+m)}$ .

**ДОКАЗАТЕЛЬСТВО.** Заметим, что плохой случай  $[t_{ij}(\alpha), t_{ji}(\beta)]$  не может встретиться в верхнетреугольной группе. Поэтому с помощью формул (2) легко проверить условия леммы 6.2, откуда вытекает нормальность.

Из тех же формул легко видеть, что коммутатор образующих групп  $U_n^{(k)}$  и  $U_n^{(m)}$  лежит в  $U_n^{(k+m)}$ . Так как последняя подгруппа нормальна, то по лемме 6.5 и весь взаимный коммутант  $[U_n^{(k)}, U_n^{(m)}]$  содержится в этой подгруппе. С другой стороны, каждая образующая группы  $U_n^{(k+m)}$  является коммутатором образующих групп  $U_n^{(k)}$  и  $U_n^{(m)}$ , откуда вытекает требуемое равенство.  $\square$

**ЛЕММА 7.3.** *Любой элемент группы  $U_n$  единственным образом выражается в виде произведения  $\prod_{j>i} t_{ij}(\alpha_{ij})$  в любом наперед заданном порядке на множестве пар  $(i, j)$ ,  $j > i$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $u \in U_n$ . Индукцией по  $k$  докажем, что

$$u \in \prod_{1 \leq j-i < k} t_{ij}(\alpha_{ij}) \cdot U_n^{(k)},$$

где произведение берется в заданном порядке. При  $k = 1$  доказывать нечего. Пусть  $k > 1$ , а  $u \in \prod_{1 \leq j-i < k-1} t_{ij}(\alpha_{ij}) \cdot U_n^{(k-1)}$  – представление  $u$ , существующее по индукционному предположению. Легко видеть, что любой элемент  $a$  из  $U_n^{(k-1)}$  лежит в смежном классе  $\prod_{t_{ii+k-1}}(\alpha_{ii+k-1})U_n^{(k)}$ , где  $\alpha_{ii+k-1}$  – элемент матрицы  $a$  на позиции  $(i, i+k-1)$ . По лемме 7.2 трансвекции  $t_{ii+k-1}(\alpha_{ii+k-1})$  коммутируют с элементами  $U_n$  по модулю  $U_n^{(k)}$ . Поэтому эти трансвекции можно поставить в нужное место произведения  $\prod_{1 \leq j-i < k-1} t_{ij}(\alpha_{ij})$  чтобы получить требуемое включение.  $\square$

Напомним, что через  $W = W_n$  мы обозначаем множество матриц перестановок. Для  $w \in W$  положим

$$U_w = \langle t_{ij}(\alpha) \mid 1 \leq i < j \leq n, \alpha \in F, t_{ij}(\alpha)^w \in U_n^- \rangle.$$

Напомним, что  $B_n = B_n(F)$  обозначает множество обратимых верхнетреугольных,  $B_n^- = B_n^-(F)$  – обратимых нижнетреугольных, а  $U_n^- = U_n^-(F)$  – нижних унитарных матриц размера  $n \times n$ .

**ТЕОРЕМА 7.4** (приведенное разложение Брюа). *Пусть  $w \in W$ . Тогда  $B_n w B_n = U_w w B_n$ , следовательно,  $\text{GL}_n(F) = U_w w B_n$ . При этом разложение данного элемента единственно, т. е. для любого  $g \in \text{GL}_n(F)$  существуют единственные  $w \in W$ ,  $u \in U_w$  и  $b \in B_n$  такие, что  $g = uw b$ .*

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $T_n = T_n(F)$  множество обратимых диагональных матриц. Любая обратимая треугольная матрица однозначно представляется в виде произведения унитарной на диагональную, т. е.  $B_n = U_n T_n$ . Ясно также, что  $T_n^w = T_n$ . Поэтому  $B_n w B_n = U_n w B_n$ .

Обозначим  $\bar{U}_w = \langle t_{ij}(\alpha) \mid t_{ij}(\alpha)^w \in U_n^- \rangle$ . Тогда по лемме 7.3  $U_n = U_w \bar{U}_w$ . Следовательно,

$$B_n w B_n = U_n w B_n = U_w \bar{U}_w w B_n = U_w w \bar{U}_w^w B_n \subseteq U_w w U_n B_n = U_w w B_n.$$

Обратное включение очевидно.

Докажем теперь единственность. Пусть  $uwb = u'w'b'$ , где  $w, w' \in W$ ,  $u \in U_w$ ,  $u' \in U_{w'}$ , и  $b, b' \in B_n$ . Тогда  $(w')^{-1}(u')^{-1}uw = b'b^{-1} \in B_n$ . Обозначим последнюю матрицу через  $c$ . Пусть  $w$  соответствует перестановке  $\sigma$ , т. е.  $w_{i, \sigma(i)} = 1$  для некоторой перестановки  $\sigma \in S_n$ , и  $w_{ij} = 0$  при  $j \neq \sigma(i)$ . Пусть, далее,  $w'$  соответствует  $\sigma' \in S_n$ . Тогда у матрицы  $(w')^{-1}$  единицы стоят в позициях  $(\sigma'(i), i)$ . Следовательно,  $c_{\sigma'(i) \sigma(i)} = ((u')^{-1}u)_{ii} = 1$ . Если  $\sigma' \neq \sigma$ , то найдется такой индекс  $i$ , что  $\sigma'(i) > \sigma(i)$ . Но тогда предыдущее равенство противоречит тому факту, что  $c$  – верхнетреугольная матрица. Таким образом,  $\sigma' = \sigma$  и  $w' = w$ .

По определению  $U_w$  имеем  $(u')^{-1}u \in U_w$  и  $c = w^{-1}(u')^{-1}uw \in U_n^-$ . Так как  $U_n^- \cap B_n = \{e\}$ , то  $u' = u$  и  $b' = b$ .  $\square$

Заметим, что из последнего рассуждения следует единственность матрицы перестановки в обычном разложении Брюа, т. е. тот факт, что клетки Брюа не пересекаются.

**СЛЕДСТВИЕ 7.5.** Любая клетка Брюа содержится в соответствующей клетке Гаусса.

ДОКАЗАТЕЛЬСТВО.  $B_n w B_n = U_w w B_n = w U_w^w B_n \subseteq w U_n^- B_n = w B_n^- B_n$ .  $\square$

## 8. Симметрическая группа

Одним из важных примеров групп является симметрическая группа. Она будет полезна нам как для иллюстрации понятий теории групп, так и в линейной алгебре при изучении антисимметричных форм и определителя матрицы.

**ОПРЕДЕЛЕНИЕ 8.1.** Пусть  $X$  – множество. Множество биекций  $X \rightarrow X$  с операцией композиции называется симметрической группой множества  $X$  и обозначается через  $S_X$ . Если  $X = \{1, \dots, n\}$ , то  $S_X$  обозначается через  $S_n$  и называется симметрической группой порядка  $n$ .

Ясно, что множество всех функций  $X \rightarrow X$  является моноидом (нейтральный элемент – тождественное отображение  $id(x) = x \forall x \in X$ ), а  $S_X$  является его группой обратимых элементов. Далее будем изучать группу  $S_n$ . Тождественная перестановка обычно обозначается буквой  $e$ .

Пусть  $\sigma \in S_n$ . Определим отношение эквивалентности на множестве  $\{1, \dots, n\}$  по правилу  $i \sim j \iff i = \sigma^k(j)$  для некоторого  $k \in \mathbb{Z}$ . В каждом классе эквивалентности выберем представителя и запишем все элементы класса в виде цикла:  $(i \sigma(i) \dots \sigma^{m-1}(i))$ , где  $\sigma^m(i) = i$ . Записав все классы эквивалентности в виде циклов получим циклическую запись перестановки  $\sigma$ . Эта запись единственна с точностью до перестановки циклов и выбора первого элемента каждого цикла. Циклы длины 1 обычно не пишут. Набор из длин независимых циклов называется циклическим (или цикленным) типом перестановки. Например, перестановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 3 & 6 & 7 & 5 \end{pmatrix} = (12)(34)(567)$$

Имеет циклический тип  $2 + 2 + 3$ . Транспозицией называется цикл длины 2.

**ЛЕММА 8.2.**  $\sigma \circ (i_1 \dots i_k) \circ \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$ .

Следовательно, сопряжение не меняет циклического типа перестановки.

**СЛЕДСТВИЕ 8.3.** Класс сопряженных элементов в  $S_n$  состоит из всех перестановок данного циклического типа. Количество классов сопряженных элементов равно количеству разбиений числа  $n$  в сумму натуральных чисел (порядок слагаемых не важен).

**ОПРЕДЕЛЕНИЕ 8.4.** Пусть  $\sigma \in S_n$ . Инверсией называется пара  $(i, j)$ ,  $1 \leq i < j \leq n$ , такая, что  $\sigma(i) > \sigma(j)$ . Четность количества инверсий называется четностью перестановки  $\sigma$ .

**ЛЕММА 8.5.** Любая перестановка записывается в виде произведения транспозиций соседних индексов.

ДОКАЗАТЕЛЬСТВО. Если  $\sigma \neq e$ , то существует индекс  $i$  такой, что  $\sigma(i) > \sigma(i+1)$ . Тогда в перестановке  $\sigma \circ (ii+1)$  инверсий на 1 меньше, чем в  $\sigma$ . Далее индукция по числу инверсий.  $\square$

**ЛЕММА 8.6.** Если перестановка представлена в виде произведения  $m$  транспозиций соседних индексов, то ее четность равна четности  $m$ .

ДОКАЗАТЕЛЬСТВО. Если  $\sigma(i) > \sigma(i+1)$ , то в перестановке  $\sigma \circ (ii+1)$  инверсий на 1 меньше, чем в  $\sigma$ , в противном случае – на 1 больше.  $\square$

**ТЕОРЕМА 8.7.** Отображение  $\varepsilon : S_n \rightarrow \mathbb{Z}_2$ , сопоставляющее перестановке ее четность, удовлетворяет соотношению  $\varepsilon(\sigma\tau) = \varepsilon(\sigma) + \varepsilon(\tau) \pmod{2}$ , т. е. является гомоморфизмом групп.

**СЛЕДСТВИЕ 8.8.** Четность перестановки циклического типа  $k_1 + \dots + k_m$  равна  $k_1 + \dots + k_m - m \pmod{2}$ .

**ДОКАЗАТЕЛЬСТВО.** Так как  $\varepsilon$  является гомоморфизмом, достаточно доказать, что четность цикла длины  $k$  равна  $k - 1 \pmod 2$ . Гомоморфизм в абелеву группу переводит сопряженные элементы в одно и то же. По следствию 8.3 любой цикл длины  $m$  сопряжен с циклом  $(1\ 2\ \dots\ m)$ . В этой перестановке легко посчитать количество транспозиций.

Альтернативно, можно представить цикл длины  $m$  в виде произведения цикла длины  $m - 1$  и транспозиции, посчитать количество инверсий в транспозиции (оно будет нечетным) и применить индукцию по  $m$ .  $\square$

## 9. Экспонента группы

**ОПРЕДЕЛЕНИЕ 9.1.** Экспонентой (или показателем) группы  $G$  называется наименьшее натуральное число  $d$  такое, что  $g^d = e$  для любого  $g \in G$ . Если такого  $d$  не существует, то говорят, что экспонента группы равна бесконечности.

**ЛЕММА 9.2** (свойства экспоненты группы).

- (1) Экспонента группы равна наименьшему общему кратному порядков ее элементов.
- (2) Если группа конечна, то ее экспонента делит ее порядок.
- (3) Экспонента прямого произведения групп  $G_1 \times \dots \times G_l$  равна наименьшему общему кратному экспонент групп  $G_1, \dots, G_l$ .
- (4) Если  $G$  – абелева группа конечной экспоненты, то существует элемент, порядок которого равен ее экспоненте.
- (5) Конечная абелева группа является циклической тогда и только тогда, когда ее экспонента равна ее порядку.

**ДОКАЗАТЕЛЬСТВО.** Все пункты кроме пункта (4) доказываются легко. Пусть  $d = p_1^{k_1} \dots p_l^{k_l}$  – экспонента группы  $G$ , где  $p_1, \dots, p_l$  – различные простые числа. Тогда существуют элементы  $g_1, \dots, g_l \in G$ , порядки которых делятся на  $p_1^{k_1}, \dots, p_l^{k_l}$  соответственно. Ясно, что если  $\text{ord } g = mn$ , то  $\text{ord } g^m = n$ . Возводя элементы  $g_1, \dots, g_l$  в подходящие степени, можно считать, что  $\text{ord } g_i = p_i^{k_i}$  при всех  $i = 1, \dots, l$ .

Пусть теперь  $G$  – абелева группа. Покажем, что для элементов  $a, b \in G$  взаимно простых порядков имеет место равенство  $\text{ord}(ab) = \text{ord } a \text{ ord } b$ . Пересечение  $\langle a \rangle \cap \langle b \rangle$  является подгруппой и в  $\langle a \rangle$  и в  $\langle b \rangle$ . По теореме Лагранжа его порядок делит  $\text{ord } a$  и  $\text{ord } b$ , а так как они взаимно просты, то  $\langle a \rangle \cap \langle b \rangle = \{e\}$ . Другими словами,  $a^s = b^t \iff a^s = b^t = e$ , что эквивалентно тому, что  $s$  делится на  $\text{ord } a$ , а  $t$  – на  $\text{ord } b$ . Если  $(ab)^n = e$ , то  $a^n = b^{-n}$ , откуда  $n$  делится на  $\text{ord } a$  и  $\text{ord } b$ . Так как эти порядки взаимно просты, то  $n$  делится на их произведение, а так как при  $n = \text{ord } a \text{ ord } b$  верно, то  $\text{ord}(ab) = \text{ord } a \text{ ord } b$ .

Теперь индукцией по  $l$  легко доказать, что  $\text{ord}(g_1 \dots g_l) = \text{ord } g_1 \dots \text{ord } g_l = d$ .  $\square$

## Коммутативные кольца

Как следует из названия, все кольца в этой главе являются коммутативными. Мы также будем предполагать, что они содержат единицу. Однако в параграфах 1–3 ни коммутативность, ни наличие единицы практически не дает никакого упрощения. Поэтому в этих параграфах можно рассматривать произвольные ассоциативные кольца.

### 1. Гомоморфизмы колец, ядро и образ

**ОПРЕДЕЛЕНИЕ 1.1.** Пусть  $R$  и  $A$  – кольца. Функция  $f : R \rightarrow A$  называется гомоморфизмом колец, если  $f(a + b) = f(a) + f(b)$  и  $f(a \cdot b) = f(a) \cdot f(b)$  для любых  $a, b \in R$ . Для гомоморфизма колец с единицей будем требовать также, чтобы  $f(1_R) = 1_A$ .<sup>1</sup>

Образ гомоморфизма  $f : R \rightarrow A$  – это его образ как функции, т. е.  $\text{Im } f = \{f(x) \mid x \in R\}$ .

Ядро гомоморфизма  $\text{Ker } f = f^{-1}(0)$ .

Инъективный гомоморфизм называется мономорфизмом, сюръективный – эпиморфизмом, а биективный – изоморфизмом. Если между двумя кольцами существует изоморфизм, то они называются изоморфными.

**ЛЕММА 1.2.** Пусть  $f : R \rightarrow A$  – гомоморфизм колец. Тогда  $f(0) = 0$ , а  $f(-x) = -f(x)$  для любого  $x \in R$ .

Если  $f$  – гомоморфизм колец с 1, а  $x \in R^*$ , то  $f(x) \in A^*$  и  $f(x^{-1}) = f(x)^{-1}$ .

**ЛЕММА 1.3.** Пусть  $f : R \rightarrow A$  – гомоморфизм колец,  $x \in R$ , а  $y = f(x)$ . Тогда  $f^{-1}(y) = x + \text{Ker } f$ .

Гомоморфизм инъективен тогда и только тогда, когда его ядро равно  $\{0\}$ .

**ОПРЕДЕЛЕНИЕ 1.4.** Аддитивная подгруппа  $I$  кольца  $R$  называется левым (правым) идеалом, если для любых  $r \in R$  и  $x \in I$  имеет место включение  $rx \in I$  (соотв.,  $xr \in I$ ). Другими словами, для левого идеала  $RI = I$ , а для правого –  $IR = I$ . Двусторонний идеал – это идеал, являющийся и левым, и правым.

**ЛЕММА 1.5.** Образ гомоморфизма колец является подкольцом, а ядро – двусторонним идеалом.

### 2. Порождение

**ОПРЕДЕЛЕНИЕ 2.1.** Пусть  $X$  – подмножество кольца  $R$ . Подкольцом, порожденным множеством  $X$ , называется наименьшее подкольцо в  $R$ , содержащее  $X$ .

Аналогично, (левым, правым или двусторонним) идеалом, порожденным подмножеством  $X$  кольца  $R$ , называется наименьший (левый, правый или двусторонний) идеал, содержащий  $X$ .

Стандартного обозначения для подкольца, порожденного  $X$ , нет. Левый (правый) идеал, порожденный подмножеством  $X$ , обозначается  $\sum_{x \in X} xR$  (соотв.,  $\sum_{x \in X} Rx$ ). Если  $R$  – коммутативное кольцо, то идеал, порожденный подмножеством  $X \subseteq R$ , иногда обозначается  $(X)$ .

Идеал коммутативного кольца, порожденный одним элементом, называется главным идеалом.

<sup>1</sup>В отличие от гомоморфизма групп сохранение единицы не вытекает из сохранения умножения. Например, отображение  $f : \mathbb{Z} \rightarrow \mathbb{Z}_6$ , заданное равенством  $f(x) = 4x \pmod 6$  является гомоморфизмом колец, но не является гомоморфизмом колец с 1, несмотря на то, что оба кольца содержат 1.

Так как пересечение подколец (идеалов) снова является подкольцом (соотв., идеалом), то подкольцо (соотв., идеал), порожденное  $X$ , всегда существует. Действительно, это пересечение всех подколец (соотв., идеалов), содержащих  $X$ .

**ЛЕММА 2.2.** *Подкольцо, порожденное  $X$ , состоит из всевозможных сумм элементов вида  $x_1 \cdots x_k$ , где  $k$  – некоторое натуральное число, а  $x_i \in X \cup \{1\}$  (если имеется в виду подкольцо без 1, то  $x_i \in X$ ).*

*Левый (правый, двусторонний) идеал кольца  $R$ , порожденный  $X$ , состоит из всевозможных сумм элементов вида  $rx$  (соотв.,  $xr$ ,  $rxs$ ), где  $r, s \in R$ , а  $x \in X$ .*

### 3. Факторкольцо и теорема о гомоморфизме

**ТЕОРЕМА 3.1.** *Для любого двустороннего идеала  $I$  кольца  $R$  существует кольцо  $A$  и эпиморфизм  $\pi : R \rightarrow A$ , ядро которого равно  $I$ .*

**ДОКАЗАТЕЛЬСТВО.** Так как  $I$  – подгруппа аддитивной группы кольца, то можно рассмотреть факторгруппу  $R/I$ . Зададим на ней умножение по формуле  $(r + I) \cdot (s + I) = rs + I$ , где  $r, s \in R$  (это не является равенством множеств, для множеств выполнено только включение  $(r + I) \cdot (s + I) \subseteq rs + I$ ). Если  $r + x \in r + I$  и  $s + y \in s + I$  – другие представители тех же смежных классов (т.е.  $x, y \in I$ ), то  $(r + x)(s + y) = rs + (ry + xs + xy) \in rs + I$ . Поэтому определение корректно, т.е. не зависит от выбора представителей смежных классов. Тот факт, что операции в  $R/I$  удовлетворяют свойствам кольца, сразу следует из соответствующих свойств кольца  $R$ . Наконец, отображение  $\pi$  задается так же, как и для групп, где уже проверено, что оно сохраняет сложение, найдено ядро  $\pi$  и отмечено, что это отображение сюръективно. Осталось проверить, что  $\pi$  сохраняет умножение, но это сразу следует из определения произведения смежных классов.  $\square$

**ОПРЕДЕЛЕНИЕ 3.2.** Кольцо  $R/I$ , построенное в доказательстве, называется факторкольцом  $R$  по  $I$ , а отображение  $\pi = \pi_I$  – канонической проекцией или гомоморфизмом редукции по модулю  $I$ .

Для двустороннего идеала  $I$  кольца  $R$  определено отношение “сравнение по модулю  $I$ ”, которое в соответствии с обсуждением в параграфе 4 является отношением эквивалентности. Доказательства утверждений настоящего параграфа показывают, что сравнения можно складывать и умножать, например, если  $a \equiv b \pmod{I}$ , а  $c \equiv d \pmod{I}$ , то  $ac \equiv bd \pmod{I}$ . Таким образом, сравнения – это просто другая запись вычислений в факторгруппе или факторкольце.

Доказательства следующих утверждений про кольца очень похожи на доказательства для групп (на самом деле единственное, что надо проверить по сравнению с предыдущими доказательствами, это то, что отображение  $g$  сохраняет умножение, т.е. не просто является гомоморфизмом аддитивных групп, а и гомоморфизмом колец).

**ТЕОРЕМА 3.3.** *Пусть  $R$  и  $R'$  – кольца,  $I$  – двусторонний идеал в  $R$ , а  $f : R \rightarrow R'$  – гомоморфизм. Если  $I \subseteq \text{Ker } f$ , то существует единственный гомоморфизм  $g : R/I \rightarrow R'$  такой, что  $f = g \circ \pi$ . Если  $\text{Ker } f = I$ , то  $g$  инъективен. Если  $f$  сюръективен, то и  $g$  сюръективен.*

**СЛЕДСТВИЕ 3.4** (Теорема о гомоморфизме колец). *Пусть  $f : R \rightarrow R'$  – гомоморфизм колец. Тогда  $\text{Im } f \cong R/\text{Ker } f$ .*

## 4. Комплексные числа

**ОПРЕДЕЛЕНИЕ 4.1.** Факторкольцо  $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$  называется полем комплексных чисел (то факт, что это поле, мы скоро проверим).

Композиция отображений  $\mathbb{R} \hookrightarrow \mathbb{R}[t] \rightarrow \mathbb{C}$  является гомоморфизмом колец с 1, а так как  $\mathbb{R}$  – поле, то она инъективна (ее ядро – идеал в  $\mathbb{R}$ , поэтому оно тривиально). Будем отождествлять элементы поля  $\mathbb{R}$  с их образами под действием этого мономорфизма и считать, что  $\mathbb{R}$  – подполе в  $\mathbb{C}$ .



Обозначим через  $i$  смежный класс  $t + (t^2 + 1)\mathbb{R}[t]$ . Заметим, что  $i^2 + 1 = t^2 + 1 + (t^2 + 1)\mathbb{R}[t] = 0$  (имеется в виду ноль поля  $\mathbb{C}$ ), откуда  $i^2 = -1$ . Так как в любом смежном классе  $p(t) + (t^2 + 1)\mathbb{R}[t]$  есть единственный многочлен степени  $\leq 1$  (остаток от деления на  $t^2 + 1$ ), то любой элемент поля  $\mathbb{C}$  может быть однозначно записан в виде  $a + bi$  для некоторых  $a, b \in \mathbb{R}$ . Ясно, что сложение определено по правилу

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Учитывая равенство  $i^2 = -1$  получаем формулу умножения в  $\mathbb{C}$ :

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Таким образом, наше определение совпадает с классическим. Пусть  $x, y \in \mathbb{R}$ , а  $z = x + iy$ . Тогда  $x = \operatorname{Re} z$  называется вещественной частью, а  $y = \operatorname{Im} z$  — мнимой частью числа  $z$ . Число  $\bar{z} = x - iy$  называется комплексно сопряженным к  $z$ . Из определения сразу следует, что  $z \in \mathbb{R} \iff z = \bar{z}$ ,  $z + \bar{z}, z\bar{z} \in \mathbb{R}$ . Как мы узнаем позже, из неприводимости многочлена  $t^2 + 1$  в  $\mathbb{R}[t]$  следует, что  $\mathbb{C}$  является полем. Однако нетрудно явно найти мультипликативный обратный к любому ненулевому элементу. Для этого достаточно просто домножить числитель и знаменатель на сопряженное к знаменателю:

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i.$$

Следующее утверждение проверяется непосредственно.

**ЛЕММА 4.2.** *Отображение  $\mathbb{C} \rightarrow \mathbb{C}$ , отображающее  $z$  в  $\bar{z}$  является автоморфизмом поля  $\mathbb{C}$ .*

Так как комплексное число  $a + bi$  однозначно определяется парой вещественных чисел  $(a, b)$ , то его удобно изображать точкой на плоскости с координатами  $(a, b)$  или ее радиус-вектором. Ясно, что сумма комплексных чисел изображается суммой векторов, соответствующих слагаемым. Произведение также имеет некоторый геометрический смысл, который следует из тригонометрической формы комплексного числа. Назовем модулем комплексного числа длину вектора, который его изображает, а его аргументом — тригонометрический угол между положительным направлением вещественной оси и этим вектором. Другими словами,

$$|a + bi| = \sqrt{a^2 + b^2}, \quad \operatorname{Arg}(a + bi) = \arg(a + bi) + 2\pi\mathbb{Z}, \quad \text{где } \arg(a + bi) = \begin{cases} \arctg(b/a), & a > 0 \\ \arctg(b/a) + \pi, & a < 0 \\ \pi/2, & a = 0, b > 0 \\ -\pi/2, & a = 0, b < 0 \end{cases}.$$

Обратите внимание, что тригонометрический угол определен с точностью до целого кратного  $2\pi$ , т. е. принимает значения в аддитивной группе  $\mathbb{R}/2\pi\mathbb{Z}$ . Пусть  $r = |a + bi|$ , а  $\varphi = \operatorname{Arg}(a + bi)$ . Из определения синуса и косинуса следует, что  $a = r \cos \varphi$ ,  $b = r \sin \varphi$  и, следовательно,

$$a + bi = r(\cos \varphi + i \sin \varphi).$$

Правая часть последнего равенства называется тригонометрической формой комплексного числа.

Перемножая комплексные числа в тригонометрической форме, и используя формулы для синуса и косинуса суммы, получим:

$$zw = |z| \cdot |w| (\cos(\operatorname{Arg} z + \operatorname{Arg} w) + i \sin(\operatorname{Arg} z + \operatorname{Arg} w)).$$

Другими словами, при перемножении комплексных чисел их модули перемножаются, а аргументы складываются. Геометрически это означает, что при умножении на  $w$  вектор, изображающий  $z$ , растягивается в  $|w|$  раз и поворачивается на угол  $\operatorname{Arg} w$ . Из последней формулы для целого  $n$  получаем:

$$z^n = |z|^n (\cos(n \operatorname{Arg} z) + i \sin(n \operatorname{Arg} z)).$$

Последняя формула называется формулой Муавра.

Единственность представления комплексного числа в тригонометрической форме и формулу для произведения в тригонометрической форме можно выразить следующим образом:

$$(3) \quad \mathbb{C}^* \cong \mathbb{R}_{>0}^* \times \mathbb{R}/2\pi\mathbb{Z}.$$

Учитывая, что  $\ln : \mathbb{R}_{>0}^* \rightarrow \mathbb{R}$  является изоморфизмом, получим следующий результат.

**ПРЕДЛОЖЕНИЕ 4.3.**  $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z}$ .

**ДОКАЗАТЕЛЬСТВО.** Отображения  $z \mapsto (\ln |z|, \operatorname{Arg} z)$  и  $(r, x) \mapsto e^r(\cos x + i \sin x)$  являются взаимно обратными гомоморфизмами.  $\square$

Так как  $\mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{R}/\mathbb{Z}$ , можно получить более короткую запись:  $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/\mathbb{Z}$ , но она менее интуитивна (соответствует замене единицы измерения углов).

В курсе математического анализа вы узнаете, что тригонометрические функции и экспонента раскладываются в степенные ряды (ряды Тэйлора) следующим образом:

$$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}, \quad \sin t = \sum_{k=0}^{\infty} (-1)^k \frac{t^{2k+1}}{(2k+1)!}, \quad \cos t = \sum_{k=0}^{\infty} (-1)^k \frac{t^{2k}}{(2k)!}.$$

При этом из теории функций комплексной переменной известно, что если две функции  $\mathbb{C} \rightarrow \mathbb{C}$  раскладываются в ряды, которые сходятся во всей комплексной плоскости, и совпадают на вещественной оси, то они равны. Поэтому указанные ряды разумно принять за определения комплексной экспоненты, синуса и косинуса. Подставляя  $z = it$  в формулу для экспоненты, получим  $e^{it} = \cos t + i \sin t$ . Так как свойства экспоненты следуют из правила умножения рядов, для  $t, u \in \mathbb{R}$  имеем

$$e^{u+it} = e^u(\cos t + i \sin t),$$

причем  $e^u = |e^{u+it}|$ , а  $t \in \operatorname{Arg}(e^{u+it})$ . В этих терминах предложение 4.3 можно переписать в виде:

$$\mathbb{C}^* \cong \mathbb{C}/(2\pi i\mathbb{Z}),$$

где изоморфизм справа налево задается экспонентой. Естественно, что обратную функцию называют логарифмом. Обратите внимание, что комплексный логарифм принимает значения не в  $\mathbb{C}$ , а в аддитивной группе  $\mathbb{C}/(2\pi i\mathbb{Z})$ .

Уравнение

$$z^n = w, \text{ где } w \in \mathbb{C}$$

называется уравнением деления круга. Пусть  $z = re^{i\varphi}$ ,  $w = se^{i\psi}$ , где  $r, s \in \mathbb{R}_{>0}$ , а  $\varphi, \psi \in \mathbb{R}/2\pi\mathbb{Z}$ . Используя изоморфизм (3) получаем

$$z^n = w \iff r^n = s \& n\varphi = \psi \iff r = \sqrt[n]{s} \& \varphi = \frac{\psi}{n} + \frac{2\pi k}{n},$$

где  $k \in \mathbb{Z}/n\mathbb{Z}$ . Таким образом,

$$z = \sqrt[n]{|w|} e^{i \frac{\psi + 2\pi k}{n}}, \text{ где } k \in \mathbb{Z}/n\mathbb{Z}.$$

Решения уравнения деления круга называются корнями из  $w$ . Обратите внимание, что символ  $\sqrt[n]{w}$  обозначает множество всех корней из  $w$ . В частности, если  $w = 1$ , то  $\sqrt[n]{1}$  является множеством всех корней из 1. Так как возведение в  $n$ -ую степень является гомоморфизмом  $\mathbb{C} \rightarrow \mathbb{C}$ , то  $\sqrt[n]{1} = \{e^{\frac{2\pi k}{n}} \mid k \in \mathbb{Z}/n\mathbb{Z}\}$  является его ядром и, следовательно, подгруппой. Ясно, что эта подгруппа циклическая порядка  $n$ . Образующие этой подгруппы называются первообразными корнями из 1. Другими словами, первообразный корень из 1 – это элемент группы  $\mathbb{C}^*$  порядка  $n$ , в отличие от корней из 1 не являющихся первообразными, порядок которых делит  $n$ , но не равен ему. Число  $e^{\frac{2\pi k}{n}}$  является первообразным корнем из 1 тогда и только тогда, когда  $k \in (\mathbb{Z}/n\mathbb{Z})^*$ .

### 5. Евклидовы кольца

В этом параграфе и далее все кольца коммутативны и имеют 1, если не оговорено противное.

**ОПРЕДЕЛЕНИЕ 5.1.** Элемент  $a$  кольца  $R$  называется делителем нуля, если существует  $b \in R \setminus \{0\}$  такой, что  $ab = 0$ . Кольцо называется областью целостности, если там нет нетривиальных делителей нуля (тривиальный делитель нуля – это ноль).

**ОПРЕДЕЛЕНИЕ 5.2.** Пусть  $R$  – область целостности. Предположим, что задана функция  $f : R \rightarrow \mathbb{N} \cup \{-\infty\}$  обладающая следующими свойствами:

- (1)  $f(0) < f(r)$  для любого  $r \in R \setminus \{0\}$ .
- (2) Для любых элементов  $a$  и  $b \neq 0$  кольца  $R$  существуют  $q, r \in R$  такие, что  $a = bq + r$  и  $f(r) < f(b)$ .

Тогда  $R$  называется евклидовым кольцом с евклидовой нормой  $f$ .

Кольцо целых чисел является евклидовым кольцом с евклидовой нормой “модуль числа”, а кольцо многочленов  $F[t]$  над полем  $F$  – с нормой “степень многочлена” (степень 0 по определению считается равной  $-\infty$ ).

**ОПРЕДЕЛЕНИЕ 5.3.** Кольцо  $R$  называется кольцом главных идеалов, если любой идеал в  $R$  является главным (напомним, что это означает, что он имеет вид  $aR$  для некоторого  $a \in R$ ). Область главных идеалов (ОГИ) – это область целостности, в которой любой идеал главный.

**ТЕОРЕМА 5.4.** *Евклидово кольцо является ОГИ.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $I$  – нетривиальный идеал в  $R$ . Возьмем ненулевой элемент  $b \in I$  с наименьшей возможной евклидовой нормой. Пусть  $a \in I$ . Тогда существуют  $q, r \in R$  такие, что  $a = bq + r$  и  $f(r) < f(b)$ . Элемент  $r = a - bq$  принадлежит  $I$  и его норма меньше, чем норма  $b$ . Следовательно, он должен быть равен нулю. Мы доказали, что произвольный элемент из  $I$  делится на  $b$ , поэтому  $I \subseteq aR$ . Обратное включение следует из того, что  $a \in I$ .  $\square$

Примеры евклидовых колец:  $\mathbb{Z}$ ,  $F[x]$ ,  $\mathbb{Z}[i]$ ,  $\mathbb{Z}[\sqrt{-2}]$ . Кольцо  $\mathbb{Z}[\sqrt{-19}]$  является кольцом главных идеалов, но не является евклидовым. Доказательство обоих фактов нетривиально.

### 6. Китайская теорема об остатках

Пусть  $R$  – кольцо, а  $I$  и  $J$  – идеалы в  $R$ . Легко проверить, что сумма  $I + J = \{a + b \mid a \in I, b \in J\}$  является идеалом, причем это наименьший идеал, содержащий  $I \cup J$ . В отличие от этого обычное произведение множеств  $I$  и  $J$ , т. е.  $\{ab \mid a \in I, b \in J\}$  в общем случае не является идеалом, потому что не замкнуто относительно сложения. Поэтому произведением идеалов будем называть идеал  $IJ$ , порожденный элементами  $ab$  по всем  $a \in I$  и  $b \in J$ . Другими словами,

$$IJ = \left\{ \sum_{i=1}^k a_i b_i \mid k \in \mathbb{N}, a_i \in I, b_i \in J \right\}.$$

**ОПРЕДЕЛЕНИЕ 6.1.** Идеалы  $I$  и  $J$  кольца  $R$  называются взаимно простыми, если  $I + J = R$ .

**ЛЕММА 6.2.** *Если  $I$  и  $J$  взаимно простые идеалы, то  $I \cap J = IJ$ .*

**ДОКАЗАТЕЛЬСТВО.** По определению идеала  $IJ \subseteq I \cap J$ . Обратно, пусть  $x \in I \cap J$ . Так как  $I$  и  $J$  взаимно просты, то существуют  $a \in I$  и  $b \in J$  такие, что  $a + b = 1$ . Тогда  $x = xa + xb \in (I \cap J)I + (I \cap J)J \subseteq IJ$ .  $\square$

**ТЕОРЕМА 6.3.**  $R/IJ \cong R/I \oplus R/J$ .

**ДОКАЗАТЕЛЬСТВО.** Естественный гомоморфизм  $R \rightarrow R/I \oplus R/J$  имеет ядро  $I \cap J = IJ$ . Осталось доказать, что он сюръективен. Пусть  $a + b = 1$  для некоторых  $a \in I$  и  $b \in J$ . Тогда очевидно, что  $xb + ya$  является прообразом элемента  $(x + I, y + J)$ .  $\square$

**ЛЕММА 6.4.** Если идеал  $J$  взаимно прост с каждым из идеалов  $I_1, \dots, I_n$ , то он взаимно прост с их произведением.

**ДОКАЗАТЕЛЬСТВО.**  $R = J + I_1 = J + I_1R = J + I_1(J + I_2) = (J + I_1J) + I_1I_2 \subseteq J + I_1I_2$ . Далее по индукции.  $\square$

**СЛЕДСТВИЕ 6.5** (китайская теорема об остатках).  $R/(I_1 \cdots I_n) \cong R/I_1 \oplus \cdots \oplus R/I_n$ .

На самом деле, это качественная формулировка К.Т.О. Количественная формулировка включает в себя формулу для вычисления элемента из  $R/(I_1 \cdots I_n)$  по набору сравнений  $x \equiv y_k \pmod{I_k}$ ,  $k = 1, \dots, n$ .

**СЛЕДСТВИЕ 6.6.** Если  $x \equiv y_k \pmod{I_k}$ ,  $k = 1, \dots, n$ , то

$$x \equiv \sum_{k=1}^n y_k c_k \pmod{I_1 \cdots I_n}, \text{ где } c_k \in \left( \prod_{j \neq k} I_j \right) \cap (1 + I_k)$$

(такие элементы  $c_k$  существуют, так как  $I_k$  взаимно прост с произведением остальных идеалов по лемме 6.4).

**ЗАМЕЧАНИЕ 6.7.** Если  $R$  некоммутативно, то  $IJ$  надо заменить на  $IJ + JI$ .

## 7. Простые и максимальные идеалы

**ОПРЕДЕЛЕНИЕ 7.1.** Собственный идеал  $I$  называется простым, если  $ab \in I$  влечет  $a \in I$  или  $b \in I$ .

Собственный идеал  $I$  называется максимальным, если он не содержится ни в каком другом собственном идеале.

**ЛЕММА 7.2.** Для любого собственного идеала существует максимальный идеал, содержащий его.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $I \triangleleft R$ . Объединение линейно упорядоченного (по включению) набора собственных идеалов в  $R$ , содержащих  $I$ , является идеалом, содержащим  $I$ . Так как собственный идеал не содержит 1, то это объединение – собственный идеал. По лемме Цорна в множестве собственных идеалов, содержащих  $I$ , существует максимальный. Ясно, что он является максимальным и среди всех собственных идеалов.  $\square$

**ОПРЕДЕЛЕНИЕ 7.3.** Кольцо называется областью целостности (или просто областью), если  $\{0\}$  является простым идеалом. Другими словами,  $R$  – область целостности, если  $R \neq \{0\}$  и  $ab \neq 0$  для любых  $a, b \in R \setminus \{0\}$ .

**ЛЕММА 7.4.** Прообраз простого идеала – простой. Прообраз максимального идеала при эпиморфизме – максимальный.

**СЛЕДСТВИЕ 7.5.** Идеал  $I$  простой тогда и только тогда, когда  $R/I$  – область целостности. Идеал  $I$  максимальный тогда и только тогда, когда  $R/I$  – поле. Любой максимальный идеал является простым.

## 8. Простые и неприводимые элементы

**ОПРЕДЕЛЕНИЕ 8.1.** Элементы  $a, b \in R$  называются ассоциированными, если  $aR = bR$ .

Необратимый элемент  $a \in R$  называется неприводимым, если из равенство  $a = bc$  следует, что  $b$  или  $c$  ассоциирован с  $a$ .

Заметим, что если  $aR$  – максимальный из собственных главных идеалов, то  $a$  неприводим. Обратное неверно, что показывает пример  $p = 0$  в области целостности. В области целостности это – единственный пример, как показывает следующее утверждение.

**ЛЕММА 8.2.** Пусть  $R$  область целостности. Элементы  $a, b \in R$  ассоциированы тогда и только тогда, когда  $a = b\varepsilon$  для некоторого  $\varepsilon \in R^*$ .

Необратимый элемент  $a \in R$  неприводим, если он не раскладывается в произведение необратимых элементов.

Ненулевой необратимый элемент  $a$  неприводим тогда и только тогда, когда  $aR$  максимальный в множестве главных идеалов.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $aR = bR$ . Если  $a = 0$ , то и  $b = 0$  и утверждение очевидно. Иначе  $a = b\varepsilon$  и  $b = a\delta$  для некоторых  $\varepsilon, \delta \in R$ , откуда  $a = a\delta\varepsilon$ . Так как  $R$  область целостности, то можно сокращать на ненулевой элемент, следовательно,  $1 = \delta\varepsilon$ , т.е.  $\varepsilon \in R^*$ . Обратное утверждение очевидно.

Пусть  $a = bc$ . Если  $b$  или  $c$  обратим, то другой ассоциирован с  $a$ . Обратно, если, скажем,  $b$  ассоциирован с  $a$ , то из первого абзаца доказательства следует, что  $c$  обратим.

$$aR \subseteq bR \iff a = bc \iff b \in R^* \vee c \in R^* \iff bR = R \vee bR = aR. \quad \square$$

**ОПРЕДЕЛЕНИЕ 8.3.** Необратимый элемент  $p$  кольца  $R$  называется простым, если  $pR$  – простой идеал.

**ЛЕММА 8.4.** Любой простой элемент неприводим. Обратное, вообще говоря, неверно.

**ДОКАЗАТЕЛЬСТВО.** Если  $p$  – простой, то

$$ab = p \implies ab \in pR \implies a \in pR \text{ или } b \in pR \implies aR = pR \text{ или } bR = pR,$$

т.е.  $p$  ассоциирован с  $a$  или с  $b$ .

Контрпример к обратному утверждению дает, например, кольцо  $\mathbb{Z}[\sqrt{-3}]$ , в котором  $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ . Действительно, элемент этого кольца обратим тогда и только тогда, когда квадрат модуля равен 1. Так как квадрат модуля каждого сомножителя равен 4, то он может раскладываться в произведение необратимых элементов только с квадратами модулей равными 2, а таких элементов в нашем кольце нет. Поэтому все сомножители являются неприводимыми, но ни один не является простым.  $\square$

**ЛЕММА 8.5.** Пусть  $R$  – область главных идеалов, а  $p \in R \setminus \{0\}$ . Тогда следующие условия эквивалентны.

- (1)  $pR$  – максимальный идеал.
- (2)  $pR$  – простой идеал (т.е.  $p$  – простой элемент).
- (3)  $p$  неприводим.

**ДОКАЗАТЕЛЬСТВО.** Импликации (1)  $\implies$  (2)  $\implies$  (3) доказаны в следствии 7.5 и лемме 8.4. Если  $p$  неприводим, то по лемме 8.2  $pR$  максимальный в множестве собственных главных идеалов, а так как любой идеал в  $R$  является главным, то и в множестве всех собственных идеалов.  $\square$

## 9. Нетеровы кольца и разложение на неприводимые

**ОПРЕДЕЛЕНИЕ 9.1.** Кольцо называется нетеровым, если любое линейно упорядоченное (по включению) множество идеалов содержит наибольший элемент.

**ПРЕДЛОЖЕНИЕ 9.2.** Кольцо является нетеровым, если любой его идеал порожден конечным числом элементов.

**ТЕОРЕМА 9.3.** Любой необратимый элемент нетерова кольца раскладывается в произведение неприводимых.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $r = r_1 \in R$  – необратимый элемент. Если  $r$  приводим, то существуют  $r_2, r_3 \in R$  такие, что  $r_1 = r_2r_3$ ,  $r_1R \subsetneq r_2R$  и  $r_1R \subsetneq r_3R$ . По индукции для каждого приводимого  $r_i$  найдем  $r_{2i}$  и  $r_{2i+1}$  такие, что  $r_i = r_{2i}r_{2i+1}$ ,  $r_iR \subsetneq r_{2i}R$  и  $r_iR \subsetneq r_{2i+1}R$ . Получим бинарное дерево. Каждая ветка этого дерева конечна за счет нетеровости кольца  $R$ . Следовательно, все дерево

конечно (иначе строим бесконечную ветку, выбирая ребро, на котором висит бесконечное поддерево). Очевидно, что листья дерева неприводимы. По индукции нетрудно доказать, что  $r$  равно произведению всех листьев.  $\square$

Другое доказательство, немного длиннее, чуть проще, но годится только для областей целостности.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $r \in R$  – необратимый элемент. Построим возрастающую цепочку главных идеалов, содержащих  $rR$ , следующим образом. Если  $r$  приводим, то существует  $r_1 \in R$  такой, что  $rR \subsetneq r_1R$ . Далее по индукции: если  $r_n$  приводим, то существует  $r_{n+1} \in R$  такой, что  $r_nR \subsetneq r_{n+1}R$ . По определению нетерова кольца эта цепочка обрывается, следовательно, идеал  $r_mR$  максимален среди главных идеалов, т. е.  $r_m$  неприводим.<sup>2</sup> Таким образом, любой необратимый элемент делится на неприводимый.

Получаем:  $r = p_1s_1 = p_1p_2s_2 = \dots$ , где  $p_i$  – неприводимы. Тогда

$$rR \subseteq s_1R \subseteq \dots \subseteq s_nR \subseteq \dots$$

Эта цепочка идеалов обрывается за счет нетеровости кольца  $R$ , скажем на  $n$ -м шаге. Это значит, что  $s_n$  неприводим, а  $r$  раскладывается в произведение неприводимых  $r = p_1 \dots p_ns_n$ .  $\square$

## 10. Факториальность колец главных идеалов

**ОПРЕДЕЛЕНИЕ 10.1.** Область целостности  $R$  называется факториальным кольцом, если любой ненулевой необратимый элемент раскладывается в произведение неприводимых единственным образом. Единственность понимается в следующем смысле: если  $\prod_{i=1}^m p_i$  ассоциировано с  $\prod_{j=1}^n q_j$  для некоторых неприводимых элементов  $p_i, q_j \in R$ , то  $m = n$  и существует перестановка  $\sigma \in S_n$  такая, что  $p_i$  ассоциирован с  $q_{\sigma(i)}$  для всех  $i = 1, \dots, n$ .

Задача настоящего параграфа – доказать, что область главных идеалов является факториальным кольцом.

**ЛЕММА 10.2.** Пусть  $R$  – область целостности, в которой каждый неприводимый элемент порождает простой идеал. Если каждый необратимый элемент раскладывается в произведение неприводимых, то кольцо  $R$  факториально.

**ДОКАЗАТЕЛЬСТВО.** Пусть

$$\varepsilon p_1 \dots p_n = \theta q_1 \dots q_m,$$

где все элементы  $p_k$  и  $q_k$  неприводимы, а  $\varepsilon, \theta$  – обратимы. Индукцией по  $\min(m, n)$  докажем, что  $m = n$  и существует перестановка  $\sigma \in S_n$  такая, что  $p_k$  ассоциирован с  $q_{\sigma(k)}$  для всех  $k$  от 1 до  $n$ .

База индукции: если  $m = 0$ , то правая часть обратима, поэтому  $n = 0$ .

Индукционный переход. По условию идеал  $p_nR$  простой. Поэтому найдется  $l$  такое, что  $q_l \in p_nR$ . Так как  $q_l$  неприводим, то  $q_l = \delta p_n$ , где  $\delta$  обратимо. Подставляя это в исходное равенство и сокращая на  $p_n$  получим  $\varepsilon p_1 \dots p_{n-1} = \theta \delta q_1 \dots q_m / q_l$ . По индукционному предположению  $n - 1 = m - 1$  и существует биекция  $\tau : \{1, \dots, n - 1\} \rightarrow \{1, \dots, m\} \setminus \{l\}$  такая, что  $p_k$  ассоциирован с  $q_{\tau(k)}$  для всех  $k$  от 1 до  $n - 1$ . Положив  $\sigma(k) = \tau(k)$  при всех  $k$  от 1 до  $n - 1$ , а  $\sigma(n) = l$ , получаем результат.  $\square$

В качестве упражнения: сформулируйте и докажите обратное утверждение.

Из предыдущей леммы и леммы 8.5 непосредственно вытекает следующий факт.

**ТЕОРЕМА 10.3.** Область главных идеалов является факториальным кольцом.

<sup>2</sup>Доказательство этого факта с использованием леммы Цорна было бы чуть короче, но считается, что использование аксиомы выбора без необходимости – дурной тон.

На самом деле кольцо многочленов над факториальным кольцом также является факториальным, так что области главных идеалов – это далеко не все факториальные кольца. Однако в настоящий момент мы не будем это доказывать.

Кольцо  $\mathbb{Z}[\sqrt{-3}]$  не является областью главных идеалов. Действительно,  $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2$  является примером неоднозначного разложения на неприводимые множители.

## 11. Наибольший общий делитель

**ОПРЕДЕЛЕНИЕ 11.1.** Пусть  $a, b \in R$ . Элемент  $d$  кольца  $R$  называется наибольшим общим делителем элементов  $a$  и  $b$ , если он делит и  $a$ , и  $b$ , и делится на любой другой общий делитель  $a$  и  $b$ .

Другими словами,  $d$  – наибольший общий делитель, если  $dR$  – наименьший главный идеал, содержащий  $a$  и  $b$ . В этом нет ничего удивительного, потому что отношение делимости на множестве элементов кольца и отношение “ $\subseteq$ ” на множестве главных идеалов совпадают, т. е.  $x$  делится на  $y$  тогда и только тогда, когда  $xR \subseteq yR$ .

Наибольший общий делитель  $a$  и  $b$  обозначается через  $\gcd(a, b)$ . Как следует из последней формулировки,  $\gcd(a, b)$  определен с точностью до ассоциированности.

Заметим, что идеал содержит  $a$  и  $b$  тогда и только тогда, когда он содержит идеал  $aR + bR$ .

**ТЕОРЕМА 11.2** (о линейном представлении НОД.). Пусть  $R$  – кольцо главных идеалов. Для любых  $a, b \in R$  существуют  $x, y \in R$  такие, что  $ax + by = \gcd(a, b)$ .

**ДОКАЗАТЕЛЬСТВО.** Идеал  $aR + bR$  является минимальным идеалом, содержащим  $a$  и  $b$ , а по условию он является главным. Таким образом,  $aR + bR = dR$ , и по определению НОД  $d = \gcd(a, b)$ .  $\square$

**СЛЕДСТВИЕ 11.3.** Пусть  $R$  – кольцо главных идеалов. Идеалы  $aR$  и  $bR$  являются взаимно простыми, если у элементов  $a$  и  $b$  нет необратимых общих делителей (такие элементы называются взаимно простыми).

Для нахождения НОД в евклидовом кольце используется алгоритм Евклида. Он использует следующую лемму.

**ЛЕММА 11.4.** Для любых  $a, b, c \in R$  имеет место равенство  $\gcd(a, b) = \gcd(a - bc, b)$ .

**ДОКАЗАТЕЛЬСТВО.** Ясно, что  $a - bc$  и  $b$  содержатся в идеале  $aR + bR$ , поэтому  $(a - bc)R + bR \subseteq aR + bR$ . С другой стороны,  $a = (a - bc) + bc \in (a - bc)R + bR$ , откуда следует обратное включение. Так как  $(a - bc)R + bR = aR + bR$ , то и наименьший главный идеал, содержащий эти идеалы, одинаковый.  $\square$

Обозначим  $r_0 = a$  и  $r_1 = b$  и положим  $i = 1$ . Алгоритм Евклида состоит из следующих шагов.

- (1) Разделить  $r_{i-1}$  на  $r_i$  с остатком:  $r_{i-1} = r_i q_i + r_{i+1}$ .
- (2) Если  $r_{i+1} \neq 0$ , то увеличить  $i$  и вернуться к первому шагу.
- (3) Если на  $k$ -ом круге  $r_{k+1} = 0$ , то  $\gcd(a, b) = r_k$ .

Действительно, так как  $r_{i+1} = r_{i-1} - r_i q_i$ , то по предыдущей лемме  $\gcd(r_{i-1}, r_i) = \gcd(r_{i+1}, r_i)$ , а  $\gcd(r_k, 0) = r_k$ .

Для нахождения линейного представления НОД используется обратный ход алгоритма Евклида. А именно,  $\gcd(a, b) = r_k = r_{k-2}x_{k-2} + r_{k-1}y_{k-2}$ , где  $x_{k-2} = 1$ , а  $y_{k-2} = -q_{k-1}$ . Подставляя в это равенство  $r_{k-1} = r_{k-3} - r_{k-2}q_{k-2}$  получаем выражение  $\gcd(a, b) = r_{k-3}x_{k-3} + r_{k-2}y_{k-3}$ . Продолжая процесс, в итоге получим  $\gcd(a, b) = r_0x_0 + r_1y_0 = ax_0 + by_0$ , что и требовалось.

Аналогичное НОД понятие с обращением включений – это наименьшее общее кратное (НОК).

**ОПРЕДЕЛЕНИЕ 11.5.** Пусть  $a, b \in R$ . Элемент  $c$  кольца  $R$  называется наименьшим общим кратным элементов  $a$  и  $b$ , если он делится на  $a$  и на  $b$ , и делит любое другое общее кратное  $a$  и  $b$ .

Другими словами,  $c$  – наименьшее общее кратное, если  $cR$  – наибольший главный идеал, содержащийся в  $aR \cap bR$ .

Наименьшее общее кратное элементов  $a$  и  $b$  обозначается через  $\text{lcm}(a, b)$ .

**ЛЕММА 11.6.** Если  $R$  – область главных идеалов,  $a, b \in R \setminus \{0\}$ , то  $\text{lcm}(a, b) = \frac{ab}{\text{gcd}(a, b)}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $d = \text{gcd}(a, b)$ ,  $a = a'd$ , а  $b = b'd$ . По теореме о линейном представлении НОД существуют  $x, y \in R$  такие, что  $ax + by = d$ . Так как  $R$  – область целостности, а  $d \neq 0$ , можно сократить на  $d$  и получить равенство  $a'x + b'y = 1$ . Если  $c \in aR \cap bR$ , то  $c = ca'x + cb'y \in ba'R + ab'R = a'b'dR$ . Таким образом,  $aR \cap bR \subseteq a'b'dR$ , а обратное включение очевидно. Осталось заметить, что  $a'b'd = \frac{ab}{\text{gcd}(a, b)}$ .  $\square$

## 12. Локализация

Идея состоит в том, чтобы обратить некоторый набор элементов универсальным образом. Заметим, что обратимый элемент не может быть делителем нуля. Поэтому, если мы хотим обратить хоть один делитель нуля, то все элементы, которые в произведении с ним дают 0, должны обратиться в 0. Заметим также, что если два элемента стали обратимыми, то обратимым стало и их произведение. Так как 1 уже обратима, то включение 1 в наше множество ничего не изменит. Поэтому мы будем говорить только об обращении элементов из некоторого мультипликативно замкнутого подмножества с 1. Другими словами, наше множество всегда будет мультипликативным моноидом, содержащим 1 кольца. Коротко такое множество называется мультипликативным.

**ОПРЕДЕЛЕНИЕ 12.1.** Пусть  $S$  – мультипликативное подмножество кольца  $R$ . Локализацией кольца  $R$  в  $S$  называется кольцо  $S^{-1}R$  вместе с локализационным гомоморфизмом  $\lambda_S : R \rightarrow S^{-1}R$  удовлетворяющее следующим свойствам.

- (1) Для любого  $s \in S$  элемент  $\lambda_S(s)$  обратим в  $S^{-1}R$ .
- (2) Для любого гомоморфизма  $\varphi : R \rightarrow A$ , при котором  $\varphi(s) \in A^*$  для всех  $s \in S$ , существует единственный гомоморфизм  $\psi : S^{-1}R \rightarrow A$  такой, что  $\psi \circ \lambda_S = \varphi$ .

Это определение ничего не говорит о существовании локализации. На самом деле она всегда существует и, как и все универсальные конструкции, единственна с точностью до единственного изоморфизма. Определим отношение “ $\sim$ ” на множестве  $R \times S$  по следующему правилу:

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S : ss_2r_1 = ss_1r_2.$$

Проверим, что “ $\sim$ ” является отношением эквивалентности. Рефлексивность и симметричность очевидны. Пусть  $(r_1, s_1) \sim (r_2, s_2) \sim (r_3, s_3)$ , т.е.  $sr_1s_2 = sr_2s_1$  и  $s'r_2s_3 = s'r_3s_2$  для некоторых  $s, s' \in S$ . Домножая первое равенство на  $s's_3$ , а второе – на  $ss_1$ , получим  $s'ss_2r_1s_3 = s'sr_2s_1s_3 = ss's_2r_3s_1$ . Так как  $ss's_2 \in S$ , то  $(r_1, s_1) \sim (r_3, s_3)$ , что доказывает транзитивность.

Положим  $S^{-1}R = R \times S / \sim$ . Класс эквивалентности, содержащий  $(r, s)$  обозначается  $\frac{r}{s}$ .

Определим отображение  $\lambda_S : R \rightarrow S^{-1}R$  формулой  $\lambda_S(r) = \frac{r}{1}$ .

**ТЕОРЕМА 12.2.** Пусть  $S$  – мультипликативное подмножество кольца  $R$ . Определим операции на  $S^{-1}R$  следующими формулами:

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2} \quad \text{и} \quad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_1r_2 + s_2r_1}{s_1s_2}.$$

Тогда  $S^{-1}R$  является локализацией кольца  $R$  в мультипликативном подмножестве  $S$  с локализационным гомоморфизмом  $\lambda_S$ .

**ДОКАЗАТЕЛЬСТВО.** Докажем, что наше определение сложения и умножения не зависит от выбора представителей классов эквивалентности. Пусть  $\frac{r'_1}{s'_1} = \frac{r_1}{s_1}$  и  $\frac{r'_2}{s'_2} = \frac{r_2}{s_2}$ , т.е.  $sr_1s'_1 = sr'_1s_1$  и



$s'r_2s'_2 = s'r'_2s_2$  для некоторых  $s, s' \in S$ . Перемножая последние равенства получаем  $ss'r_1s'_1r_2s'_2 = ss'r'_1s_1r'_2s_2$ , откуда  $\frac{r_1r_2}{s_1s_2} = \frac{r'_1r'_2}{s'_1s'_2}$ . Далее,

$$ss'(r_1s_2 + r_2s_1)s'_1s'_2 = ss'(r_1s_2s'_1s'_2 + r_2s_1s'_1s'_2) = ss'(r'_1s_2s_1s'_2 + r'_2s_1s'_1s_2) = ss'(r'_1s'_2 + r'_2s'_1)s_1s_2,$$

что доказывает равенство  $\frac{r_1s_2+r_2s_1}{s_1s_2} = \frac{r'_1s'_2+r'_2s'_1}{s'_1s'_2}$ .

Непосредственно проверяется, что заданные операции коммутативны, ассоциативны, и выполнена дистрибутивность. Проверим для примера ассоциативность сложения (самое длинное вычисление).

$$\begin{aligned} \left( \frac{r_1}{s_1} + \frac{r_2}{s_2} \right) + \frac{r_3}{s_3} &= \frac{r_1s_2 + r_2s_1}{s_1s_2} + \frac{r_3}{s_3} = \frac{r_1s_2s_3 + r_2s_1s_3 + r_3s_1s_2}{s_1s_2s_3} \\ \frac{r_1}{s_1} + \left( \frac{r_2}{s_2} + \frac{r_3}{s_3} \right) &= \frac{r_1}{s_1} + \frac{r_2s_3 + r_3s_2}{s_2s_3} = \frac{r_1s_2s_3 + r_2s_3s_1 + r_3s_2s_1}{s_1s_2s_3}. \end{aligned}$$

Нейтральным элементом по сложению является  $\frac{0}{1} = \frac{0}{s}$ , обратным к  $\frac{r}{s} - \frac{-r}{s}$ . Мультипликативно нейтральным является  $\frac{1}{1} = \frac{s}{s}$ . Сразу видно, что  $\lambda$  – гомоморфизм. Для  $s \in S$  имеем  $\lambda(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = 1$ , так что первое свойство локализации выполнено.

Пусть теперь  $\varphi : R \rightarrow A$  – гомоморфизм из второго свойства определения 12.1. Определим отображение  $\psi : S^{-1}R \rightarrow A$  равенством  $\psi(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$ . Если  $\frac{r'}{s'} = \frac{r}{s}$ , то  $s''r's = s''rs'$  для некоторого  $s'' \in S$ , и  $\varphi(s'')\varphi(r')\varphi(s) = \varphi(s'')\varphi(r)\varphi(s')$ . Домножая на  $\varphi(s'')^{-1}\varphi(s)^{-1}\varphi(s')^{-1}$  получаем  $\varphi(r')\varphi(s')^{-1} = \varphi(r)\varphi(s)^{-1}$ , что доказывает корректность определения  $\psi$ . Учитывая, что  $\varphi(1) = 1$ , из определения сразу следует, что  $\varphi = \psi \circ \lambda_S$ . Легко проверить, что  $\psi$  является гомоморфизмом.

Равенство  $\varphi = \psi \circ \lambda_S$  однозначно задает,  $\psi(\frac{r}{1}) = \varphi(r)$ . Так как  $\psi$  должен быть гомоморфизмом, то

$$\varphi(r) = \psi(\frac{r}{1}) = \psi(\frac{r}{s} \cdot \frac{s}{1}) = \psi(\frac{r}{s}) \cdot \varphi(s).$$

Учитывая, то  $\varphi(s)$  по условию обратимо, получаем  $\psi(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$ . Таким образом,  $\psi$  однозначно определяется своими свойствами.  $\square$

Приведем несколько часто используемых примеров мультипликативных подмножеств и локализаций в них.

- (1) Для  $s \in R$  положим  $\langle s \rangle = \{s^n \mid n \in \mathbb{N}_0\}$ . Локализация  $\langle s \rangle^{-1}R$  обозначается через  $R_s$  и называется главной локализацией в элементе  $s$  (по аналогии с главным идеалом).
- (2) Если  $P$  – простой идеал кольца  $R$ , то  $R \setminus P$  является мультипликативным подмножеством. В этом случае локализация  $R_P := (R \setminus P)^{-1}$  называется локализацией кольца  $R$  в простом идеале  $P$ .

$R_P$  является локальным кольцом, т.е. кольцом с единственным максимальным идеалом (равносильно: множество необратимых элементов является аддитивной подгруппой).

- (3)  $S$  – множество всех элементов в  $R$ , не являющихся делителями 0 (сам 0 является делителем 0). Тогда  $S^{-1}R$  называется полным кольцом частных кольца  $R$ . Это максимальная локализация, для которой гомоморфизм локализации инъективен.
- (4)  $R = K[x]$ , где  $K$  – кольцо,  $S$  – множество унитарных многочленов.

### 13. Поле частных и разложение на простейшие дроби

Если  $R$  – область целостности, то  $\{0\}$  является простым идеалом. Локализация в этом идеале, очевидно, будет полем, которое называется полем частных кольца  $R$ . Другими словами, поле частных – это полное кольцо частных области целостности. Локализационный гомоморфизм в этом случае – универсальное вложение  $R$  в поле в следующем смысле.

**ЛЕММА 13.1.** Пусть  $R$  – область целостности, а  $S = R \setminus \{0\}$ . Тогда  $F = S^{-1}R$  является полем, а гомоморфизм локализации  $\lambda_S : R \rightarrow F$  инъективен. При этом  $\lambda_S$  удовлетворяет следующему универсальному свойству: для любого поля  $K$  и мономорфизма  $\varphi : R \rightarrow K$  существует единственный мономорфизм  $\psi : F \rightarrow K$  такой, что  $\varphi = \psi \circ \lambda_S$ .

Обычно мы отождествляем элементы  $R$  с их образами в поле частных  $F$  под действием гомоморфизма локализации и считаем, что  $R \subseteq F$ .

Пусть теперь  $R$  – область главных идеалов. В этом случае поле частных кольца  $R$  аддитивно порождено дробями, знаменатели которых являются степенями неприводимых элементов. Это сразу следует из линейного представления НОД. Для евклидовых колец можно еще ограничить евклидову норму числителя.

**ОПРЕДЕЛЕНИЕ 13.2.** Пусть  $R$  – евклидово кольцо с евклидовой нормой  $f$ , а  $F$  – его поле частных. Простейшей дробью называется элемент  $\frac{r}{s^n} \in F$ , где  $r, s \in R$ ,  $s$  – неприводим, и  $f(r) < f(s)$ .

**ТЕОРЕМА 13.3.** Пусть  $R$  – евклидово кольцо, а  $F$  – его поле частных. Любой элемент из  $F$  представляется в виде суммы элемента из  $R$  и простейших дробей.

**ДОКАЗАТЕЛЬСТВО.** Разложим сначала  $\frac{a}{bc}$ ,  $a, b, c \in R$ ,  $\gcd(b, c) = 1$  в сумму дробей со знаменателями  $b$  и  $c$ . По теореме о линейном представлении НОД существуют такие  $x, y \in R$ , что  $1 = bx + cy$ . Тогда  $\frac{a}{bc} = \frac{abx + acy}{bc} = \frac{ax}{c} + \frac{ay}{b}$ . По индукции легко доказать, что любая дробь со знаменателем  $p_1^{k_1} \cdots p_m^{k_m}$ , где  $p_1, \dots, p_m \in R$  – неприводимые элементы, раскладывается в сумму дробей  $\sum \frac{r_i}{p_i^{k_i}}$  (заметим, что до сих пор мы пользовались только тем, что  $R$  – кольцо главных идеалов).

Для завершения доказательства осталось показать, что любая дробь  $\frac{r}{p^k}$ ,  $r, p \in R$ ,  $p$  неприводим, раскладывается в сумму простейших и элемента из  $R$ . Докажем это индукцией по  $k$ . При  $k = 0$  наша дробь лежит в  $R$  и доказывать нечего. Пусть  $k > 0$ . Обозначим через  $f$  евклидову норму в  $R$  и разделим с остатком  $r$  на  $p$ :  $r = sp + q$ , где  $f(q) < f(p)$ . Тогда  $\frac{r}{p^k} = \frac{s}{p^{k-1}} + \frac{q}{p^k}$ . Вторая дробь является простейшей, а первая раскладывается в сумму простейших и элемента из  $R$  по индукционному предположению.  $\square$

## 14. Многочлены

Пусть  $F$  – коммутативное кольцо с 1 (которое в дальнейшем будет полем). Кольцо  $A$  с 1 (не обязательно коммутативное) вместе с гомоморфизмом  $\varphi : F \rightarrow A$  называется  $F$ -алгеброй. При этом для  $\alpha \in F$  и  $x \in A$  мы определяем произведение  $\alpha x = \varphi(\alpha)x$ . Нетрудно видеть, что в случае, когда  $F$  – поле, это определение совпадает с определением 1.8. Гомоморфизм  $\theta$  алгебры  $(A, \varphi)$  на алгебру  $(B, \psi)$  – это гомоморфизм колец  $\theta : A \rightarrow B$  такой, что  $\psi = \theta \circ \varphi$ .

**ОПРЕДЕЛЕНИЕ 14.1.** Многочленом  $p$  от одной переменной  $t$  над  $F$  называется конечный набор элементов поля  $(\alpha_0, \dots, \alpha_n)$ , записанный в виде  $p(t) = \alpha_0 + \alpha_1 t + \dots + \alpha_n t^n$ . При этом  $n = \deg p$  называется степенью многочлена  $p$ .

Многочлены складываются покомпонентно (при этом отсутствующие компоненты считаются равными 0), а перемножаются по правилу: коэффициент произведения  $pq$ , где  $q(t) = \beta_0 + \beta_1 t + \dots + \beta_m t^m$ , при  $t^k$  равен

$$\sum_{0 \leq i \leq n, 0 \leq j \leq m, i+j=k} \alpha_i \beta_j.$$

Множество всех многочленов с операциями сложения и умножения является алгеброй над  $F$  и обозначается  $F[t]$ . Пусть  $A$  – алгебра над  $F$ . Определим полиномиальную функцию  $\tilde{p} : A \rightarrow A$  формулой  $\tilde{p}(a) = \alpha_0 + \alpha_1 a + \dots + \alpha_n a^n$ . Допуская вольность речи, будем обозначать полиномиальную функцию тем же символом, что и многочлен, т. е. писать  $p$  вместо  $\tilde{p}$ .

Последнее соглашение общепринято, но не так безобидно, как кажется на первый взгляд. Например, если  $A = F = \mathbb{F}_2$ , то  $p(t) = t$  и  $q(t) = t^2$  являются разными многочленами, но задают одну и ту же полиномиальную функцию. Как мы увидим, это невозможно для бесконечного поля  $F$ .

Пусть  $A$  – алгебра над  $F$ , а  $a \in A$ . Операции над многочленами специально определены так, чтобы отображение

$$\varepsilon_a : F[t] \rightarrow A, \quad \varepsilon_a(p) = p(a)$$

являлось гомоморфизмом  $F$ -алгебр. Он называется гомоморфизмом подстановки или вычисления значения в точке  $a$ .

**ПРЕДЛОЖЕНИЕ 14.2** (универсальное свойство кольца многочленов). *Для любого  $a \in A$  существует единственный гомоморфизм  $F$ -алгебр  $\varepsilon : F[t] \rightarrow A$ , отображающий  $t$  в  $a$ .*

**ДОКАЗАТЕЛЬСТВО.** Существование:  $\varepsilon = \varepsilon_a$ .

Из того, что  $\varepsilon$  гомоморфизм  $F$ -алгебр мы знаем образы всех элементов из  $F$  под действием  $\varepsilon$ , а  $\varepsilon(t)$  задано. Так как  $\varepsilon$  сохраняет сумму и произведение, а любой многочлен получается из  $t$  и элементов кольца  $F$  при помощи этих операций, образ любого многочлена под действием  $\varepsilon$  определен однозначно.  $\square$

Далее  $F$  является полем.

**ТЕОРЕМА 14.3.** *Кольцо многочленов  $F[t]$  над полем  $F$  является евклидовым кольцом с евклидовой нормой  $\deg$ .*

Заметим, что в отличие от целых чисел с евклидовой нормой “модуль”, деление с остатком в кольце многочленов с евклидовой нормой  $\deg$  единственно.

**ТЕОРЕМА 14.4** (теорема Безу). *Пусть  $\alpha \in F$ , а  $p \in F[t]$ , где  $F$  – поле. Остаток от деления многочлена  $p$  на  $t - \alpha$  равен  $p(\alpha)$ .*

*Элемент  $\alpha$  является корнем многочлена  $p$  тогда и только тогда, когда  $p$  делится на  $t - \alpha$ . Многочлен степени  $n$  не может иметь больше, чем  $n$  корней.*

Следующее утверждение вытекает из последней фразы предыдущего и критерия цикличности абелевой группы. Оно играет важную роль в классификации конечных полей.

**ТЕОРЕМА 14.5.** *Любая конечная подгруппа мультипликативной группы поля циклическая.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $F$  – поле,  $G \leq F^*$ , а  $|G| = n$ . Пусть  $k = \exp G$ . Это означает, что многочлен  $t^k - 1$  имеет  $n$  корней (все элементы группы  $G$  – его корни). По теореме 14.4  $n \leq k$ . С другой стороны, по лемме 9.2  $n$  делится на  $k$ , откуда  $n = k$ . По той же самой лемме группа  $G$  циклическая.  $\square$

В случае, когда мы рассматриваем сравнения в кольце  $F[t]$  по модулю многочленов первой степени, китайская теорема об остатках превращается в интерполяционную формулу Лагранжа. Конечно, эту формулу легко проверить и непосредственно, связь ее с китайской теоремой об остатках скорее позволяет лучше понять доказательство самой китайской теоремы.

**ТЕОРЕМА 14.6.** *Пусть  $t_0, y_0, \dots, t_n, y_n \in F$ , причем  $t_i \neq t_j$  при  $i \neq j$ . Существует единственный многочлен  $p$  степени не выше  $n$ , удовлетворяющий условиям  $p(t_i) = y_i$  для любого  $i = 0, \dots, n$ . Этот многочлен можно найти по формуле*

$$p(t) = \sum_{i=0}^n y_i \frac{\prod_{j \neq i} (t - t_j)}{\prod_{j \neq i} (t_i - t_j)}.$$

**ДОКАЗАТЕЛЬСТВО.** По теореме Безу условия  $p(t_i) = y_i$  равносильны условиям  $p \equiv y_i \pmod{(t - t_i)}$ . По китайской теореме об остатках существует единственный по модулю  $w(t) = \prod_{i=0}^n (t - t_i)$  многочлен, удовлетворяющий этим сравнениям. Единственный многочлен степени, не превосходящей  $n$ , — это остаток от деления любого такого многочлена на  $w$ . Формулу легко проверить непосредственно, или получить, применив доказательство китайской теоремы об остатках.  $\square$

Другой, итерационный, способ решить задачу интерполяции называется интерполяцией по Ньютону. На  $k$ -ом шаге строится многочлен степени  $\leq k - 1$ , удовлетворяющий первым  $k$  условиям. На первом шаге положим  $p_0(t) = y_0$ . Предположим, что построен многочлен  $p_k$ , удовлетворяющий условиям  $\deg p_k \leq k - 1$  и  $p_k(t_i) = y_i$  для любого  $i = 0, \dots, k - 1$ . Будем искать  $p_{k+1}$  в виде  $p_{k+1}(t) = p_k(t) + \lambda(t - t_0) \cdots (t - t_{k-1})$ . Первые  $k$  условий выполнены независимо от значения  $\lambda$ . Поэтому  $\lambda$  можно найти из условия  $p_{k+1}(t_k) = y_k$ . Очевидно, что тогда все требования к  $p_{k+1}$  будут выполнены.

## 15. Формальная производная и кратность корня

Так как поле  $F$  произвольно, то невозможно определить производную многочлена средствами дифференциального исчисления. Однако понятие формальной производной оказывается почти ничем не хуже. По некоторым соображениям нам будет удобно определить формальную производную для многочленов с коэффициентами в произвольном коммутативном кольце с единицей.

**ОПРЕДЕЛЕНИЕ 15.1.** Пусть  $R$  — коммутативное кольцо с единицей. Формальной производной многочлена  $p(t) = a_n t^n + \cdots + a_1 t + a_0 \in R[t]$  называется многочлен  $p'(t) = a_n n t^{n-1} + \cdots + a_1$  (здесь натуральное число  $n$  понимается, как сумма  $n$  единиц кольца  $R$ , в частности, оно может оказаться равным нулю).

**ЛЕММА 15.2.** Формальная производная удовлетворяет всем обычным свойствам производной. Для любых  $p, q \in R[t]$  и  $\alpha \in R$  имеют место равенства:

- (1)  $(p + q)' = p' + q'$ ,  $(\alpha p)' = \alpha p'$ ;
- (2)  $(pq)' = p'q + pq'$ ;
- (3)  $(p \circ q)' = (p' \circ q) \cdot q'$ .

Приведем 2 доказательства этой леммы: непосредственное и “методом общего элемента”. Непосредственное доказательство в данном случае может быть даже проще, но “метод общего элемента” при небольшой привычке к нему позволяет вообще не думать о доказательстве подобного рода утверждений.

**НЕПОСРЕДСТВЕННОЕ ДОКАЗАТЕЛЬСТВО.** Линейность формальной производной очевидна. Учитывая это, второе свойство достаточно проверить для одночленов:

$$(t^n \cdot t^m)' = (m + n)t^{m+n-1} = nt^{n-1}t^m + mt^n t^{m-1} = (t^n)' \cdot t^m + t^n \cdot (t^m)'.$$

Аналогично, последнее свойство достаточно проверить для случая, когда  $p = t^n$ . В этом случае доказательство можно провести индукцией по  $n$ , используя свойство 2. База индукции,  $n = 1$ , очевидна. При  $n > 1$ , используя индукционное предположение, имеем

$$(q^n)' = (q \cdot q^{n-1})' = q' \cdot q^{n-1} + q \cdot (n-1)q^{n-2}q' = nq^{n-1}q'.$$

$\square$

Для доказательства свойств производной методом общего элемента нам потребуются 2 леммы. Первую из них мы примем пока без доказательства (доказательство использует сведения про расширения полей, которые мы изучим позже).

**ЛЕММА 15.3.** Для любого натурального  $n$  кольцо многочленов от  $n$  переменных над  $\mathbb{Z}$  вкладывается (т. е. изоморфно подкольцу) в  $\mathbb{R}$ .

Следующее утверждение – это обобщение универсального свойства кольца многочленов на многочлены нескольких переменных.

**ЛЕММА 15.4.** Пусть  $R$  коммутативное кольцо с 1,  $n \in \mathbb{N}$ , а  $c_1, \dots, c_n \in R$ . Существует единственный гомоморфизм  $\varphi : \mathbb{Z}[z_1, \dots, z_n] \rightarrow R$  такой, что  $\varphi(z_k) = c_k$  при всех  $k = 1, \dots, n$ .

**ДОКАЗАТЕЛЬСТВО.** Для того чтобы выполнялись требуемые равенства мы должны положить  $\varphi(z) = z(c_0, \dots, c_n)$  для любого многочлена  $z \in \mathbb{Z}[z_1, \dots, z_n]$ . С другой стороны, ясно, что значение в данной точке суммы (произведения) многочленов равно сумме (соотв. произведению) его значений. Поэтому приведенная формула для  $\varphi$  задает требуемый гомоморфизм  $\varphi : \mathbb{Z}[z_1, \dots, z_n] \rightarrow R$  и он единственный.  $\square$

Еще нам понадобится определение гомоморфизма колец многочленов, индуцированного гомоморфизмом колец коэффициентов. Пусть  $\varphi : A \rightarrow B$  – гомоморфизм колец. Обозначим через  $\hat{\varphi} : A[t] \rightarrow B[t]$  гомоморфизм, заданный формулой  $\hat{\varphi}(\sum_{k=0}^l c_k t^k) = \sum_{k=0}^l \varphi(c_k) t^k$  и назовем его гомоморфизмом, индуцированным  $\varphi$ .

**ДОКАЗАТЕЛЬСТВО ЛЕММЫ 15.2 МЕТОДОМ ОБЩЕГО ЭЛЕМЕНТА.** Я не смогу сейчас объяснить, что такое “общий элемент для некоторой задачи”, придется ограничиться определением общего элемента для нашей конкретной задачи – доказательства свойств формальной производной.

Зафиксируем степени  $m$  и  $n$  многочленов  $p$  и  $q$ . Тогда свойства производной включают в себя элементы  $a_0, \dots, a_n, b_0, \dots, b_m$  (коэффициенты многочленов  $p$  и  $q$ ) и  $\alpha$  кольца  $R$ . При этом между этими элементами нет никаких соотношений, кроме тех, которые следуют из свойств коммутативного кольца с единицей. Наиболее общая ситуация, когда такие элементы существуют – кольцо многочленов  $P = \mathbb{Z}[x_0, \dots, x_n, y_0, \dots, y_m, \beta]$  от  $n + m + 3$  переменных. Обозначим  $f(t) = \sum_{k=0}^n x_k t^k \in P[t]$  и  $g(t) = \sum_{k=0}^m y_k t^k \in P[t]$ . Набор  $(f, g, \beta)$  и будет общим элементом для нашей задачи.

По лемме 15.4 для любого кольца  $R$ , элемента  $\alpha \in R$  и многочленов  $p, q \in R[t]$  степеней не превосходящих  $n$  и  $m$ , соответственно, существует единственный гомоморфизм  $\varphi : P \rightarrow R$  такой, что  $\varphi(x_k) = a_k$ ,  $\varphi(y_k) = b_k$  и  $\varphi(\beta) = \alpha$ . Ясно, что эти равенства равносильны равенствам  $\hat{\varphi}(f) = p$ ,  $\hat{\varphi}(g) = q$  и  $\varphi(\beta) = \alpha$ . Эти свойства и означают, что  $P$  – универсальное кольцо, а  $(f, g, \beta)$  общий элемент для нашей задачи.

Легко видеть, что дифференцирование коммутирует с гомоморфизмами, т.е. гомоморфизма колец  $\psi : A \rightarrow B$  и многочлена  $h \in A[t]$  имеет место равенство  $\psi(h)' = \psi(h')$ . Поэтому выполнение свойств формальной производной для  $\beta \in P$  и многочленов  $f, g \in P[t]$  влечет выполнение этих свойств для их образов при любом гомоморфизме. Учитывая сказанное в предыдущем абзаце, выполнение свойств формальной производной для конкретного  $\beta \in P$  и конкретных многочленов  $f, g \in P[t]$  влечет выполнение этих свойств для любых многочленов степеней не выше, чем  $n$  и  $m$ , а так как  $n$  и  $m$  произвольные, то и вообще для любых многочленов над любым коммутативным кольцом.

По лемме 15.3 кольцо  $P$  вкладывается в поле вещественных чисел, а над полем вещественных чисел свойства производной известны из математического анализа. Так как свойства сохраняются при изоморфизме, то можно считать, что  $P \subseteq \mathbb{R}$ , поэтому свойства производной выполнены для общего элемента, а, значит, и в общем случае.  $\square$

Единственная неприятность, с которой можно столкнуться, используя формальную производную над полем ненулевой характеристики, – это то, что она может оказаться равной нулю для многочлена ненулевой степени. Например, при  $F = \mathbb{F}_p$  производная многочлена  $t^p - 1$  тождественно равна нулю.

**ОПРЕДЕЛЕНИЕ 15.5.** Число  $\alpha \in F$  имеет кратность  $k$  в многочлене  $p \in F[t]$ , если  $k$  наибольшее натуральное число, для которого  $p$  делится на  $(t - \alpha)^k$ . Используя теорему Безу можно переформулировать это определение следующим образом:  $\alpha$  имеет кратность  $k$  в  $p$ , если  $p(t) = (t - \alpha)^k g(t)$ , причем  $g(\alpha) \neq 0$ .

Ясно, что  $\alpha$  имеет кратность больше 0 в  $p$  тогда и тогда, когда  $\alpha$  – корень  $p$ . Корни первой кратности называются простыми корнями, а корни кратности не меньше 2 – кратными. С помощью формальной производной легко искать кратные корни многочлена, это опирается на следующее утверждение.

**ЛЕММА 15.6.** Пусть  $\alpha$  – корень многочлена  $p$  кратности  $k$ . Кратность  $\alpha$  в  $p'$  не меньше  $k - 1$ . Если  $k \neq 0$  в поле  $F$ , то  $\alpha$  имеет кратность ровно  $k - 1$  в  $p'$ , в частности,  $k = 1 \iff p'(\alpha) \neq 0$ .

**ДОКАЗАТЕЛЬСТВО.** По условию  $p(t) = (t - \alpha)^k g(t)$ , причем  $g(\alpha) \neq 0$ . По свойствам дифференцирования

$$p'(t) = k(t - \alpha)^{k-1}g(t) + (t - \alpha)^k g'(t) = (t - \alpha)^{k-1}(kg(t) + (t - \alpha)g'(t)).$$

Сразу видно, что  $p'$  делится на  $(t - \alpha)^{k-1}$ . Если  $k \neq 0$  в поле  $F$ , то  $kg(\alpha) + (\alpha - \alpha)g'(\alpha) = kg(\alpha) \neq 0$ .  $\square$

Доказательство следующего утверждения мы отложим на потом, когда мы будем заниматься многочленами над кольцами. Сейчас же только приведем его формулировку, потому что оно очень полезно при решении учебных задач.

**ТЕОРЕМА 15.7.** (о рациональных корнях многочлена) Пусть  $p(t) = a_n t^n + \dots + a_0$  – многочлен с целыми коэффициентами. Тогда рациональными корнями  $p$  могут быть только числа вида  $\frac{c}{d}$ , где  $c$  – делитель свободного члена  $a_0$ , а  $d$  – делитель старшего коэффициента  $a_n$ .

## 16. Основная теорема алгебры

**СЛЕДСТВИЕ 16.1.** Пусть  $g \in \mathbb{C}[t]$ , а  $w \in \mathbb{C}$ . Обозначим через  $\bar{g}$  многочлен, коэффициенты которого сопряжены с коэффициентами многочлена  $g$ .

- (1)  $\overline{g(w)} = \bar{g}(\bar{w})$ .
- (2) Если  $g \in \mathbb{R}[t]$ , то  $\overline{g(w)} = g(\bar{w})$ .
- (3) Пусть  $g \in \mathbb{R}[t]$ , а  $w \in \mathbb{C}$ . Кратность  $w$  в  $g$  равна кратности  $\bar{w}$  в  $g$ . В частности, если  $g(w) = 0$ , то  $g(\bar{w}) = 0$ .

**ДОКАЗАТЕЛЬСТВО.** Первые 2 утверждения очевидно следуют из леммы.

Обозначим через  $k$  кратность  $w$  в  $g$ . Тогда  $g(t) = (t - w)^k f(t)$ , где  $f \in \mathbb{C}[t]$ . Взяв комплексно сопряженные к обеим частям равенства получим  $g(t) = \bar{g}(t) = (t - \bar{w})^k \bar{f}(t)$ , причем  $\bar{f}(\bar{w}) = \overline{f(w)} \neq 0$ , что и означает, что кратность  $\bar{w}$  в  $g$  равна  $k$ .  $\square$

При построении поля комплексных чисел мы присоединили корень многочлена  $t^2 + 1$ , но оказывается, что присоединились корни всех многочленов!

**ОПРЕДЕЛЕНИЕ 16.2.** Поле  $F$  называется алгебраически замкнутым, если любой многочлен из  $F[t]$  степени  $\geq 1$  имеет хотя бы один корень в  $F$ .

**ТЕОРЕМА 16.3** (Основная теорема алгебры). Поле комплексных чисел алгебраически замкнуто.

**ЛЕММА 16.4.** Если поле  $F$  алгебраически замкнуто, то любой многочлен из  $F[t]$  раскладывается на множители степени 1.

**СЛЕДСТВИЕ 16.5.** Любой многочлен степени  $\geq 3$  из кольца  $\mathbb{R}[x]$  приводим. Следовательно, любой многочлен над  $\mathbb{R}$  раскладывается на множители степени  $\leq 2$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $p \in \mathbb{R}[t] \subseteq \mathbb{C}[t]$ ,  $\deg p \geq 3$ . По основной теореме алгебры он имеет комплексный корень  $w$ . Если  $w \in \mathbb{R}$ , то по теореме Безу  $p$  делится на  $t - w$ . В противном случае по лемме 4.2  $p(\bar{w}) = 0$ . Так как в этом случае  $t - w$  и  $t - \bar{w}$  взаимно просты, а по теореме Безу  $p$  делится на каждый из этих многочленов, то он делится и на их произведение  $(t - w)(t - \bar{w}) = t^2 - (w + \bar{w})t + w\bar{w}$ , которое имеет вещественные коэффициенты. В обоих случаях  $p$  делится на многочлен степени 1 или 2, и степень частного не меньше 1.

Второе утверждение следует из факториальности кольца многочленов.  $\square$

## 17. Экспонента мультипликативной группы кольца вычетов

Разберем подробнее кольцо целых чисел. Так как  $\mathbb{Z}$  является евклидовым кольцом, то оно является областью главных идеалов. По лемме 8.5 любой ненулевой простой идеал является максимальным, откуда  $\mathbb{Z}/p\mathbb{Z}$  является полем тогда и только тогда, когда  $p$  – простое число.

Если числа  $n_1, \dots, n_l$  – попарно взаимно простые, то имеет место китайская теорема об остатках:

$$\mathbb{Z}/(n_1 \cdots n_l \mathbb{Z}) \cong \mathbb{Z}/n_1 \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_l \mathbb{Z}.$$

**ОПРЕДЕЛЕНИЕ 17.1.** Порядок мультипликативной группы  $(\mathbb{Z}/n\mathbb{Z})^*$  обозначается  $\varphi(n)$ . Функция  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  называется функцией Эйлера.

**ЛЕММА 17.2.** Образ числа  $m \in \mathbb{Z}$  обратим в кольце  $\mathbb{Z}/n\mathbb{Z}$ , если и только если  $\gcd(m, n) = 1$ . Таким образом,  $\varphi(n)$  равна количеству чисел от 0 до  $n - 1$ , взаимно простых с  $n$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\bar{m}$  – образ  $m$  в  $\mathbb{Z}/n\mathbb{Z}$ . Элемент  $\bar{m}$  обратим тогда и только тогда, когда существует  $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$  такой, что  $\bar{m}\bar{x} = 1$ . Если  $x \in \mathbb{Z}$  прообраз  $\bar{x}$ , то последнее условие можно переписать в виде  $mx \in 1 + n\mathbb{Z}$ , другими словами, идеалы  $m\mathbb{Z}$  и  $n\mathbb{Z}$  взаимно просты. А это по следствию 11.3 означает, что  $m$  взаимно просто с  $n$ .

Второе утверждение очевидно.  $\square$

**ЛЕММА 17.3.** Если кольцо  $R$  с единицей (не обязательно коммутативное) является прямой суммой колец  $R_1 \oplus \cdots \oplus R_k$ , то  $R^* \cong R_1^* \times \cdots \times R_k^*$ . Если  $R^*$  конечна, то  $|R^*| = |R_1^*| \cdots |R_k^*|$ .

**ТЕОРЕМА 17.4.** Если  $\gcd(a, b) = 1$ , то  $\varphi(ab) = \varphi(a)\varphi(b)$ .

Если  $p$  – простое число, а  $k \in \mathbb{N}$ , то  $\varphi(p^k) = p^k - p^{k-1}$ .

Пусть  $p_1, \dots, p_l$  – различные простые числа,  $k_1, \dots, k_l \in \mathbb{N}$ , а  $n = \prod_{i=1}^l p_i^{k_i}$ . Тогда

$$\varphi(n) = \prod_{i=1}^l (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^l \frac{p_i - 1}{p_i}.$$

**ТЕОРЕМА 17.5** (теорема Эйлера). Если  $a$  взаимно просто с  $n$ , то  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

Частный случай этой теоремы для простого  $n$  называется малой теоремой Ферма. На самом деле несложно получить более точный результат, а именно заменить произведение чисел  $\varphi(p_i^{k_i})$  на их наименьшее общее кратное с помощью понятия экспоненты группы.

Определим функцию  $\varphi' : \mathbb{N} \rightarrow \mathbb{N}$  равенством

$$\varphi'\left(\prod_{i=1}^l p_i^{k_i}\right) = \text{lcm}_{1 \leq i \leq l}(p_i^{k_i} - p_i^{k_i-1}).$$

**ТЕОРЕМА 17.6.** Если  $a$  взаимно просто с  $n$ , то  $a^{\varphi'(n)} \equiv 1 \pmod{n}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $n = \prod_{i=1}^l p_i^{k_i}$ . По теореме Эйлера экспонента группы  $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$  делит  $p_i^{k_i} - p_i^{k_i-1}$ . По пункту 3 леммы 9.2 экспонента группы  $(\mathbb{Z}/n\mathbb{Z})^*$  равна наименьшему общему кратному экспонент групп  $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$ , а, значит, делит  $\varphi'(n)$ . Последнее означает, что  $x^{\varphi'(n)} = 1$  для любого  $x \in (\mathbb{Z}/n\mathbb{Z})^*$ , что и требуется.  $\square$

Оценка экспоненты группы  $(\mathbb{Z}/n\mathbb{Z})^*$  из последней теоремы почти точна, ее можно уточнить только в случае, когда  $n$  делится на 8.

**ЛЕММА 17.7.** *Группа  $(\mathbb{Z}/p^k\mathbb{Z})^*$  циклическая для любого простого  $p \neq 2$  и при  $p = 2$ ,  $k \leq 2$ . При  $k \geq 3$  экспонента группы  $(\mathbb{Z}/2^k\mathbb{Z})^*$  равна  $2^{k-2}$  (т. е. в 2 раза меньше ее порядка).*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $p$  – нечетное простое число. Поле  $\mathbb{Z}/p\mathbb{Z}$  является факторкольцом кольца  $\mathbb{Z}/p^k\mathbb{Z}$  по идеалу, порожденному  $p$ . Каноническая проекция  $\mathbb{Z}/p^k\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$  индуцирует гомоморфизм мультипликативных групп  $(\mathbb{Z}/p^k\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ , который сюръективен, так как все числа от 1 до  $p-1$  взаимно просты с  $p^k$  и, следовательно, из класса вычетов обратимы. По теореме 14.5 существует элемент  $a \in \mathbb{Z}/p\mathbb{Z}$  порядка  $p-1$ . Порядок любого его прообраза в  $(\mathbb{Z}/p^k\mathbb{Z})^*$  делится на  $p-1$ . Таким образом, экспонента группы  $(\mathbb{Z}/p^k\mathbb{Z})^*$  делится на  $p-1$ .

Докажем теперь, что при  $k \geq 2$  она делится также и на  $p^{k-1}$ . Для этого докажем, что элемент  $1+p$  имеет порядок  $p^{k-1}$  в этой группе. Точнее, индукцией по  $k$  докажем, что  $(1+p)^{p^{k-1}} = 1+p^k y$ , где  $y$  не делится на  $p$ . При  $k=1$  это очевидно. Пусть  $k \geq 2$ . По индукционному предположению  $(1+p)^{p^{k-2}} = 1+p^{k-1}x$ , где  $x$  не делится на  $p$ .

$$(1+p)^{p^{k-1}} = (1+p^{k-1}x)^p = 1 + p \cdot p^{k-1}x + \sum_{i=2}^p \binom{p}{i} p^{i(k-1)} x^i.$$

Так как  $\binom{p}{i}$  делится на  $p$ , то каждое слагаемое суммы делится на  $p^{1+2(k-1)} = p^{k+1}p^{k-2}$ . Так как  $k \geq 2$ , то сумма равна  $p^{k+1}z$ , а  $(1+p)^{p^{k-1}} = 1+p^k y$ , где  $y = x + pz$  не делится на  $p$ .

Таким образом, порядок элемента  $1+p$  в группе  $(\mathbb{Z}/p^k\mathbb{Z})^*$  делит  $p^{k-1}$ . Заменяя  $k$  на  $k-1$  и учитывая, что  $y$  не делит  $p$ , видим, что этот порядок не делит  $p^{k-2}$  и, следовательно, равен  $p^{k-1}$ .

При  $p=2$  и  $k \geq 2$  аналогичным образом докажем, что  $(1+4z)2^{k-2} = 1+2^k y$ , где  $y$  имеет ту же четность, что и  $z$  (нам нужно только  $k \geq 3$ , но это верно и при  $k=2$ , которое удобно сделать базой индукции). Итак, при  $k \geq 3$  по индукционному предположению  $(1+4z)2^{k-3} = 1+2^{k-1}x$ , где  $x \equiv z \pmod{2}$ .

$$(1+4z)2^{k-2} = (1+2^{k-1}x)^2 = 1 + 2 \cdot 2^{k-1}x + 2^{2k-2}x^2 = 1 + 2^k(x + 2^{k-2}x^2).$$

Так как  $k \geq 3$ , то  $y = x + 2^{k-2}x^2 \equiv x \equiv z \pmod{2}$ . Так же, как и в первой части доказательства заключаем, что при нечетном  $z$  порядок  $1+4z$  в группе  $\mathbb{Z}/2^k\mathbb{Z})^*$  равен  $k-2$ .

С другой стороны, при любом  $t$  имеем  $(1+2t)^2 = 1+4z$ , где  $z = t + t^2$  четно. Поэтому

$$(1+2t)^{2^{k-2}} = (1+4z)^{2^{k-3}} = 1 + 2^{k-1}y \equiv 1 \pmod{2^k},$$

так как  $y$  четно. Следовательно, порядок любого элемента группы  $(\mathbb{Z}/2^k\mathbb{Z})^*$  делит  $2^{k-2}$ .  $\square$

Определим функцию Кармайкла  $\lambda : \mathbb{N} \rightarrow \mathbb{N}$  как точное значение экспоненты группы  $(\mathbb{Z}/n\mathbb{Z})^*$ . Тогда утверждения, приведенные в этом абзаце можно сформулировать следующим образом.

**ТЕОРЕМА 17.8.** *Если  $n$  не делится на 8, то  $\lambda(n) = \varphi'(n)$ . Если  $n = 2^k m$ , где  $m$  нечетно, а  $k \geq 3$ , то  $\lambda(n) = \text{lcm}(\varphi'(m), 2^{k-2})$ .*

## 18. О простых числах

В этом параграфе приводятся несколько утверждений, полезных, в частности, для приложений в RSA-шифровании. Читателю рекомендуется прочитать идею RSA хотя бы в Википедии <https://ru.wikipedia.org/wiki/RSA>.

**ТЕОРЕМА 18.1.** *Пусть  $R$  – нетерова область целостности с конечной мультипликативной группой или кольцо многочленов над нетеровой областью целостности. Тогда в нем существует бесконечно много неприводимых элементов.*



**ДОКАЗАТЕЛЬСТВО.** Пусть  $p_1, \dots, p_m$  – все неприводимые элементы кольца  $R$ . Тогда произведение  $p_1^k \cdots p_m^k + 1$  не делится ни на один простой для любого  $k \in \mathbb{N}$ . Все такие элементы различны, так как  $R$  – область целостности. Если мультипликативная группа кольца  $R$  конечна, то все такие элементы не могут быть обратимы, однако по теореме 9.3 необратимый элемент обязан делиться на неприводимый, противоречие.

Если  $R$  – кольцо многочленов над конечной областью целостности, то можно применить соображения выше (кольцо многочленов над нетеровым кольцом нетерово – это теорема Гильберта о базисе, которая еще появится в курсе). Если же базовое кольцо бесконечно, то многочлены  $t - a$  неприводимы для всех  $a$  из базового кольца, а таких уже бесконечно много.  $\square$

Вероятно, для кольца многочленов над произвольным кольцом это утверждение тоже верно.

**ТЕОРЕМА 18.2** (Теорема Дирихле о простых в арифметической прогрессии). Пусть  $R = \mathbb{Z}$  или  $R = \mathbb{F}_q[t]$ . Если  $a$  и  $b$  взаимно простые элементы кольца  $R$ , то множество  $a + bR$  содержит бесконечно много простых элементов (заметим, что в таком кольце  $R$  неприводимость элемента совпадает с его простотой).

**ТЕОРЕМА 18.3** (распределение простых чисел). Обозначим через  $\pi(n)$  количество простых чисел от 2 до  $n$ . Тогда  $\frac{\pi(n)}{n/\ln n} \rightarrow 1$  при  $n \rightarrow \infty$ .

Практически важной задачей является нахождение больших простых чисел. В соответствии с предыдущей теоремой простых чисел достаточно много. Поэтому, если алгоритм тестирования числа  $n$  на простоту требует  $g(n)$  операций, то нахождение ближайшего к  $n$  простого числа статистически требует  $g(n) \ln n$  операций. Таким образом, важно иметь тесты числа на простоту порядка  $\ln^k n$  для небольших  $k$ . Все (известные мне) такие тесты являются вероятностными и строятся следующим образом. Для нечетного  $n > 1$  определяется некоторое подмножество  $T \subseteq \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ , которое совпадает со всем множеством в случае простого  $n$ . Обычно числа, не взаимно простые с  $n$ , не принадлежат  $T$ , но статистически их мало, поэтому ими пренебрегают. Отношение  $\frac{|T|}{n}$  для данного непростого  $n$  показывает, насколько хорош наш тест для данного  $n$ . На самом деле, можно оценить  $\sup \frac{|T|}{\varphi(n)}$  по всем непростым  $n$ . Если этот супремум не меньше 1, то тест плохой и применять его в коммерческих целях нецелесообразно. Те числа  $n$ , для которых  $\frac{|T|}{\varphi(n)} \geq 1$  (т.е. любое число, взаимно простое с  $n$ , принадлежит  $T$ ), называются псевдопростыми для данного теста.

В следующей таблице собраны простейшие тесты. Ясно, что если для теста существуют псевдопростые числа, то  $\sup \frac{|T|}{\varphi(n)}$  по всем непростым  $n$  равен 1. В последнем столбике таблицы приведена оценка для этого супремума по всем  $n$ , кроме псевдопростых.

Название	Множество $T$	Псевдопростые числа	$\sup \frac{ T }{\varphi(n)}$
Ферма	$\{a \mid a^{n-1} = 1\}$	561, 1105, 1729, ...	$\leq 1/2$
Эйлера	$\{a \mid a^{\frac{n-1}{2}} = \pm 1\}$	1729, 2465, ...	$\leq 1/2$
Миллера–Рабина	$\{a \mid a^k = 1 \text{ или } \exists j < m : a^{2^j k} = -1\}$ где $n - 1 = 2^m k$ , а $k$ нечетно	$\emptyset$	$\leq 1/4$

**ЛЕММА 18.4.** Нечетное псевдопростое число Ферма свободно от квадратов и не равно произведению двух простых.

**ДОКАЗАТЕЛЬСТВО.** Докажем сначала, что если  $n$  делится на квадрат или равно произведению двух простых, то  $n - 1$  не делится на экспоненту группы  $G = (\mathbb{Z}/n\mathbb{Z})^*$ .

Если  $n$  делится на квадрат, то  $n = p^k m$  для некоторого простого  $p \neq 2$ , натурального  $k > 1$  и натурального  $m$ , не делящегося на  $p$ . Тогда экспонента группы  $G = (\mathbb{Z}/n\mathbb{Z})^*$  равна  $\text{lcm}(p^k - p^{k-1}, \lambda(m))$  и, следовательно, делится на  $p$ , в то время как  $n - 1$  не делится на  $p$ .

Если  $n = pq$ , где  $p$  и  $q$  – различные простые числа, то экспонента группы  $G$  равна  $\text{lcm}(p-1, q-1)$ . Если  $pq-1$  делится на эту экспоненту, то оно делится на  $p-1$  и на  $q-1$ . Тогда  $q-1 = (pq-1) - q(p-1)$  делится на  $p-1$  и, аналогично,  $p-1$  делится на  $q-1$ , что невозможно.

Так как  $n-1$  не делится на экспоненту группы  $G$ , которая равна НОК порядков элементов  $G$ , то существует элемент  $g \in G$ , порядок которого не делит  $n-1$ . Тогда  $g^{n-1} \neq 1$  в  $G$ . Множество решений уравнения  $t^{n-1} = 1$  является ядром гомоморфизма “возведение в степень  $n-1$ ”, то есть подгруппой, не содержащей  $g$ . Индекс собственной подгруппы не меньше 2, таким образом,  $\frac{|T|}{\varphi(n)} \leq \frac{1}{2}$ .  $\square$

**ЛЕММА 18.5.** *Если  $p$  – простое число, то тест Миллера–Рабина выполнен для любого  $a$ , взаимно простого с  $p$ .*

**ДОКАЗАТЕЛЬСТВО.** Все вычисления приведены в поле  $\mathbb{Z}/p\mathbb{Z}$ . Заметим, что в любом поле уравнение  $x^2 = 1$  имеет ровно два решения:  $x = \pm 1$ . Так как  $a^{p-1} = 1$ , то  $a^{\frac{p-1}{2}} = \pm 1$ . Если  $\frac{p-1}{2} = m$  нечетно или  $a^{\frac{p-1}{2}} = -1$ , то тест выполнен. Иначе  $a^{\frac{p-1}{4}} = \pm 1$ , и т. д.  $\square$

Доказательства того, что псевдопростых чисел Миллера–Рабина не существует, оставляется читателю в качестве упражнения.

## Определители

### 1. Полилинейные и антисимметричные формы.

Пусть  $V$  – векторное пространство над полем  $F$ .

**ОПРЕДЕЛЕНИЕ 1.1.** Отображение  $f : \underbrace{V \times \cdots \times V}_{m \text{ раз}} \rightarrow F$  называется *полилинейной* (точнее,  *$m$ -линейной*) *формой*, если оно линейно по каждому аргументу, т.е. для любых  $a, b \in V$  и  $\lambda \in F$  выполнены следующие равенства

$$\begin{aligned} f(\dots, a + b, \dots) &= f(\dots, a, \dots) + f(\dots, b, \dots), \\ f(\dots, \lambda a, \dots) &= \lambda f(\dots, a, \dots) \end{aligned}$$

Заметим, что если среди аргументов полилинейного отображения  $f$  есть 0, то  $f$  принимает значение 0. Это сразу следует из линейности по каждому аргументу. Пусть  $v = (v_1, \dots, v_n)$  – базис пространства  $V$ . Тогда полилинейная форма полностью определяется  $m$ -мерным массивом своих значений на базисных векторах. Точнее, выполнено следующее утверждение.

**ЛЕММА 1.2.** Если  $f$  –  $m$ -линейная форма на  $V$ , а  $x_1, \dots, x_m \in V$ , то

$$f(x_1, \dots, x_m) = \sum_{i_1, \dots, i_m=1}^n f(v_{i_1}, \dots, v_{i_m}) a_{i_1 1} \dots a_{i_m m},$$

где  $A = ((x_1)_v, \dots, (x_m)_v)$ .

**ДОКАЗАТЕЛЬСТВО.** Для доказательства достаточно разложить каждый  $x_k$  в линейную комбинацию базисных векторов:  $x_k = \sum_{i_k=1}^n v_{i_k} a_{i_k k}$  после чего вынести знаки суммирования и константы за знак отображения  $f$ , что можно сделать по определению полилинейности.  $\square$

Прежде, чем формулировать следствие последней леммы для антисимметричных форм, изучим два различных определения антисимметричности.

**ОПРЕДЕЛЕНИЕ 1.3.** Пусть  $X$  – множество. Функция  $f : X \times X \rightarrow F$  называется *антисимметричной*, если для любых  $x, y \in X$  выполнены следующие условия:

- (1)  $f(x, y) = -f(y, x)$ ;
- (2)  $f(x, x) = 0$ .

Условия (1) и (2) редко бывают независимыми. Что из чего следует и при каких условиях, изложено в следующей лемме.

**ЛЕММА 1.4.** Если  $\text{char } F \neq 2$ , то (1)  $\implies$  (2). Если же  $X$  – векторное пространство, а форма  $f$  билинейна, то (2)  $\implies$  (1).

**ДОКАЗАТЕЛЬСТВО.** Первое утверждение очевидно. Второе вытекает из следующего вычисления:

$$0 = f(x + y, x + y) = f(x, x) + f(x, y) + f(y, x) + f(y, y) = f(x, y) + f(y, x) \implies f(x, y) = -f(y, x).$$

$\square$

Полилинейная форма называется антисимметричной, если она обращается в ноль, как только два ее аргумента равны. Пусть теперь в лемме 1.2  $m = n = \dim V$ , а форма  $f$  антисимметрична. Напомним, что  $\varepsilon(\sigma)$  обозначает четность перестановки  $\sigma \in S_n$ , см. определение 8.4.

**ЛЕММА 1.5.** Пусть  $f : \underbrace{V \times \cdots \times V}_{n \text{ раз}} \rightarrow F$  – полилинейная антисимметричная форма,  $v = (v_1, \dots, v_n)$  – базис пространства  $V$ ,  $x_1, \dots, x_n \in V$ , а  $A = ((x_1)_v, \dots, (x_n)_v)$ . Тогда

$$f(x_1, \dots, x_n) = f(v_1, \dots, v_n) \sum_{\sigma \in S_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^n a_{\sigma(i)i}.$$

**ДОКАЗАТЕЛЬСТВО.** Так как  $f$  антисимметрична, то  $f(v_{i_1}, \dots, v_{i_m}) = 0$  как только  $i_k = i_l$  при  $k \neq l$ . Таким образом, суммирование в формуле из леммы 1.2 достаточно вести по всем наборам различных индексов  $(i_1, \dots, i_n)$ . Пусть  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  – функция, заданная равенством  $\sigma(k) = i_k$ . Так как  $i_k \neq i_l$  при  $k \neq l$ , а область определения  $\sigma$  совпадает с ее множеством значений, то  $\sigma$  – биекция, т.е.  $\sigma \in S_n$ . Заметим, что за счет антисимметричности  $f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = (-1)^{\varepsilon(\sigma)} f(v_1, \dots, v_n)$ . С учетом этого формула из леммы 1.2 превращается в доказываемое равенство.  $\square$

**ОПРЕДЕЛЕНИЕ 1.6.** Ненулевая антисимметричная  $n$ -линейная форма на  $n$ -мерном векторном пространстве называется формой объема.

В заключении параграфа сформулируем еще одно полезное свойство полилинейных антисимметричных отображений.

**ЛЕММА 1.7.** Пусть  $f$  – полилинейное антисимметричное отображение. Тогда его значение не меняется при первом элементарном преобразовании с аргументами, т.е. при любом  $\alpha \in F$

$$f(\dots, v_i, \dots, v_j, \dots) = f(\dots, v_i + v_j \alpha, \dots, v_j, \dots).$$

## 2. Определение определителя

**ОПРЕДЕЛЕНИЕ 2.1.** Определителем матрицы  $A \in M_n(F)$  называется число

$$\det A = \sum_{\sigma \in S_n} (-1)^{\varepsilon(\sigma)} a_{\sigma(1)1} \cdots a_{\sigma(n)n}.$$

Мы уже доказали в предыдущем параграфе, что любая форма объема пропорциональна определителю. Как ни странно, из этого не следует, что сам определитель является полилинейной и антисимметричной формой. К счастью, это так, иначе на свете не существовало бы ни одной формы объема!

**ЛЕММА 2.2.** Определитель является полилинейной антисимметричной формой столбцов матрицы, а  $\det E = 1$ .

**ДОКАЗАТЕЛЬСТВО.** Если в формуле из определения 2.1 зафиксировать все элементы матрицы  $A$  кроме элементов  $k$ -ого столбца, то получится линейная комбинация элементов  $k$ -ого столбца, т.е.  $\det A = b a_{*k}$  для некоторой строки  $b \in {}^n F$ . Ясно, что это выражение линейно по  $a_{*k}$ , что и доказывает полилинейность. Утверждение  $\det E = 1$  очевидно.

Для доказательства антисимметричности предположим, что  $a_{*i} = a_{*j}$ . Разложим симметрическую группу в объединение смежных классов по знакопеременной:  $S_n = A_n \sqcup A_n \tau$ , где в качестве  $\tau$  можно взять любую нечетную перестановку. Для наших целей удобно взять транспозицию  $\tau = (ij)$ . Тогда

$$(4) \quad \det A = \sum_{\sigma \in A_n} \prod_{k=1}^n a_{\sigma(k)k} - \sum_{\rho \in A_n \tau} \prod_{k=1}^n a_{\rho(k)k}.$$

Заменяя  $\rho = \sigma\tau$  получим

$$\sum_{\rho \in A_n} \prod_{k=1}^n a_{\rho(k)k} = \sum_{\sigma \in A_n} \prod_{k=1}^n a_{\sigma\tau(k)k} = \sum_{\sigma \in A_n} a_{\sigma(j)i} a_{\sigma(i)j} \prod_{k \neq i,j} a_{\sigma(k)k}$$

Учитывая, что  $a_{\sigma(j)i} = a_{\sigma(j)j}$  и  $a_{\sigma(i)j} = a_{\sigma(i)i}$ , эта сумма совпадает с первой суммой в формуле (4), получаем  $\det A = 0$ .  $\square$

**СЛЕДСТВИЕ 2.3.** Пусть  $f$  форма объема на  $V$ ,  $v$  – базис  $V$ , а  $x_1, \dots, x_n \in V$ . Тогда

$$f(x_1, \dots, x_n) = f(v_1, \dots, v_n) \det A, \text{ где } A = ((x_1)_v, \dots, (x_n)_v).$$

Множество форм объема на данном векторном пространстве является одномерным векторным пространством.

Если  $f$  – форма объема на  $F^n$ , то  $f(A) = f(E) \cdot \det A$  для любой матрицы  $A$  размера  $n \times n$  (здесь матрица отождествляется с набором своих столбцов).

**ЛЕММА 2.4.** Пусть  $f$  – форма объема на  $V$ .

- (1) Набор векторов  $v = (v_1, \dots, v_n)$  является базисом, если и только если  $f(v_1, \dots, v_n) \neq 0$ .
- (2) Если  $u$  и  $v$  два базиса пространства  $V$ , то  $f(u) = f(v) \det C_{v \rightarrow u}$ .
- (3) Определитель квадратной матрицы не равен нулю тогда и только тогда, когда ее строки (столбцы) линейно независимы.

**ДОКАЗАТЕЛЬСТВО.** Так как  $f \neq 0$ , то найдется набор векторов  $x_1, \dots, x_n \in V$ , для которых  $f(x_1, \dots, x_n) \neq 0$ . Если  $v$  – базис, то по следствию 2.3  $f(x_1, \dots, x_n) = f(v_1, \dots, v_n) \det A$ , следовательно,  $f(v_1, \dots, v_n) \neq 0$ .

Обратно, если  $v$  не базис, то один из элементов выражается в виде линейной комбинации остальных, скажем,  $v_i = \sum_{j \neq i} v_j \alpha_j$ . По лемме 1.7 в выражении  $f(v_1, \dots, v_n)$  можно заменить  $v_i$  на  $v_i - \sum_{j \neq i} v_j \alpha_j$ , то есть на 0. Следовательно,  $f(v_1, \dots, v_n) = f(\dots, 0, \dots) = 0$ .

Второе утверждение непосредственно следует из следствия 2.3.

Третье утверждение следует из первого, так как определитель является формой объема на  $F^n$ , а  $n$  элементов  $n$ -мерного пространства являются базисом тогда и только тогда, когда они линейно независимы.  $\square$

**ЛЕММА 2.5.** Пусть  $L : V \rightarrow V$  – линейный оператор,  $f$  форма объема на  $V$ , а  $v$  – базис  $V$ .

- Функция  $f_L : V \times \dots \times V \rightarrow F$ , заданная формулой  $f_L(x_1, \dots, x_n) = f(L(x_1), \dots, L(x_n))$ , является формой объема или тождественно равна нулю.
- Отношение  $f_L(v_1, \dots, v_n) / f(v_1, \dots, v_n)$  не зависит от выбора формы объема и базиса и равно определителю матрицы  $L_v$ .

**ДОКАЗАТЕЛЬСТВО.** Для доказательства пункта (1) достаточно проверить, что форма  $f_L$  полилинейна и антисимметрична, что не составляет труда. Заметим, что по лемме 2.4  $f(v_1, \dots, v_n) \neq 0$ , так что частное из пункта (2) всегда имеет смысл. Если  $(u_1, \dots, u_n)$  – другой базис пространства  $V$ , то по той же лемме

$$\frac{f_L(u_1, \dots, u_n)}{f(u_1, \dots, u_n)} = \frac{f_L(v_1, \dots, v_n) \det C_{v \rightarrow u}}{f(v_1, \dots, v_n) \det C_{v \rightarrow u}} = \frac{f_L(v_1, \dots, v_n)}{f(v_1, \dots, v_n)}.$$

Если  $g$  – другая форма объема, то

$$g_L(v_1, \dots, v_n) = g(L(v_1), \dots, L(v_n)) = g(v_1, \dots, v_n) \det L_v$$

в соответствии со следствием 2.3.  $\square$

Определителем линейного оператора  $L : V \rightarrow V$  называется коэффициент изменения формы объема, т. е. отношение  $f_L(v_1, \dots, v_n) / f(v_1, \dots, v_n)$  из леммы 2.5.

### 3. Свойства определителя

Следующее свойство сразу следует из определения определителя линейного оператора и леммы 2.5.

**ПРЕДЛОЖЕНИЕ 3.1.** *Определитель композиции операторов равен произведению их определителей.*

*Определитель произведения квадратных матриц равен произведению их определителей.*

**ПРЕДЛОЖЕНИЕ 3.2.**  $\det A = \det A^T$ . Поэтому все свойства, сформулированные для столбцов матрицы  $A$  верны и для ее строк.

ДОКАЗАТЕЛЬСТВО. По определению 2.1,

$$\det A^T = \sum_{\sigma \in S_n} (-1)^{\varepsilon(\sigma)} a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Переставив множители  $a_{1\sigma(1)}, \dots, a_{n\sigma(n)}$  в соответствии с перестановкой  $\sigma^{-1}$  получим:

$$\begin{aligned} \det A^T &= \sum_{\sigma \in S_n} (-1)^{\varepsilon(\sigma)} a_{\sigma(\sigma^{-1}(1)), \sigma^{-1}(1)} \cdots a_{\sigma(\sigma^{-1}(n)), \sigma^{-1}(n)} = \\ &= \sum_{\sigma \in S_n} (-1)^{\varepsilon(\sigma)} a_{1, \sigma^{-1}(1)} \cdots a_{n, \sigma^{-1}(n)}. \end{aligned}$$

Так как  $\varepsilon$  является гомоморфизмом  $S_n \rightarrow \mathbb{Z}_2$ , то  $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$ . С другой стороны, отображение  $S_n \rightarrow S_n$ , заданное правилом  $\sigma \mapsto \sigma^{-1}$ , биективно (оно обратное самому себе). Поэтому в последней сумме  $\sigma^{-1}$  пробегает все множество  $S_n$ . Таким образом,

$$\det A^T = \sum_{\sigma^{-1} \in S_n} (-1)^{\varepsilon(\sigma^{-1})} a_{1, \sigma^{-1}(1)} \cdots a_{n, \sigma^{-1}(n)} = \det A.$$

□

В следующем утверждении мы для удобства использования повторим свойства полилинейных антисимметричных отображений в терминах определителя.

**ПРЕДЛОЖЕНИЕ 3.3.**

- (1) *Определитель матрицы с нулевым столбцом (строкой) равен нулю.*
- (2) *Определитель матрицы, в которой есть два пропорциональных столбца (строки), равен нулю.*
- (3) *Определитель не изменяется при первом преобразовании Гаусса.*
- (4) *Общий множитель столбца (строки) выносится за знак определителя.*
- (5) *При транспозиции столбцов (строк) матрицы ее определитель меняет знак.*

**ПРЕДЛОЖЕНИЕ 3.4** (определитель клеточно треугольной матрицы). *Определитель клеточно треугольной матрицы равен произведению определителей диагональных блоков. В частности, определитель треугольной матрицы равен произведению диагональных элементов.*

ДОКАЗАТЕЛЬСТВО. Пусть сначала  $A = \begin{pmatrix} E & * \\ 0 & E \end{pmatrix}$ . Так как эта матрица легко получается из

единичной с помощью серии первых преобразований Гаусса, то ее определитель равен 1.

Рассмотрим теперь  $n$ -форму  $f$  на  $F^n$ , сопоставляющую квадратной матрице  $B$  число  $f(B) = \det \begin{pmatrix} B & * \\ 0 & E \end{pmatrix}$ . Легко проверить, что  $f$  – полилинейная антисимметричная форма. По следствию 2.3

$f(B) = \det B \cdot f(E)$ , что равно  $\det B$  в соответствие с первым абзацем доказательства. Из свойства 3.2 легко вывести теперь, что  $\det \begin{pmatrix} B & 0 \\ * & E \end{pmatrix}$  также равен  $\det B$ .

В качестве следующего шага доказательства зафиксируем квадратную матрицу  $B$  и рассмотрим  $m$ -форму  $G$  на  $F^m$ , заданную формулой  $G(C) = \det \begin{pmatrix} B & 0 \\ * & C \end{pmatrix}$ , где  $C$  – квадратная матрица  $m \times m$ . Снова очевидно, что  $f$  – полилинейная антисимметричная форма, и по следствию 2.3  $G(C) = \det C \cdot G(E)$ , а  $G(E) = \det B$  по предыдущему абзацу доказательства.

Наконец, пусть

$$A = \begin{pmatrix} A^{(1)} & 0 & 0 \\ * & \ddots & 0 \\ * & * & A^{(k)} \end{pmatrix}.$$

Докажем индукцией по  $k$ , что  $\det A = \det A^{(1)} \dots \det A^{(k)}$ . При  $k = 1$  доказывать нечего. При  $k > 1$  обозначим  $C = A^{(k)}$  и

$$B = \begin{pmatrix} A^{(1)} & 0 & 0 \\ * & \ddots & 0 \\ * & * & A^{(k-1)} \end{pmatrix}.$$

По индукционному предположению  $\det B = \det A^{(1)} \dots \det A^{(k-1)}$ , а по предыдущему абзацу доказательства  $\det A = \det B \cdot \det C = \det A^{(1)} \dots \det A^{(k)}$ .

Таким образом, свойство доказано для нижних клеточно треугольных матриц. Доказательство для верхних клеточно треугольных матриц легко следует теперь из свойства 3.2.  $\square$

**ОПРЕДЕЛЕНИЕ 3.5.** Пусть  $B$  – матрица размера  $n \times n$ , а  $i$  и  $j$  – индексы от 1 до  $n$ . Обозначим через  $M^{(ij)}$  или  $M^{(ij)}(B)$  матрицу, полученную из  $B$  вычеркиванием  $i$ -ой строки и  $j$ -ого столбца. *Минором* в позиции  $(i, j)$  матрицы  $B$  называется число  $M_{ij} = \det M^{(ij)}$ . *Алгебраическим дополнением* позиции  $(i, j)$  матрицы  $B$ , называется число  $A_{ij} = (-1)^{i+j} M_{ij}$ . В том случае, когда хочется явно указать, для какой матрицы вычисляется алгебраическое дополнение (минор), его обозначают через  $A_{ij}(B)$  (соотв.  $M_{ij}(B)$ ).

**ПРЕДЛОЖЕНИЕ 3.6** (разложение по столбцу (строке)). Пусть  $A$  – матрица размера  $n \times n$ , а  $j$  – индекс от 1 до  $n$ . Тогда

$$\det B = \sum_{i=1}^n b_{ji} A_{ji} = \sum_{i=1}^n b_{ij} A_{ij}.$$

**ДОКАЗАТЕЛЬСТВО.** Пусть сначала  $j = 1$ . Первый столбец матрицы  $B$  раскладывается в сумму  $\sum_{i=1}^n b_{i1} e^{(i)}$ . По линейности определителя

$$\det B = \begin{vmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ 0 & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{vmatrix} + \cdots + \begin{vmatrix} 0 & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & b_{n-1,2} & \cdots & b_{n-1,n} \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{vmatrix}$$

По свойству 3.4 первый определитель из суммы равен  $b_{11}A_{11}(B)$ . Для вычисления  $i$ -го слагаемого последней суммы переставим  $i$ -ую строку на первое место так, чтобы порядок следования остальных строк не изменился. Очевидно, это можно сделать с помощью  $i - 1$  транспозиций строк. По свойству антисимметричности получим

$$\begin{vmatrix} 0 & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & b_{i-1,2} & \cdots & b_{i-1,n} \\ b_{i1} & b_{i2} & \cdots & b_{in} \\ 0 & b_{i+1,2} & \cdots & b_{i+1,n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{vmatrix} = (-1)^{i-1} \begin{vmatrix} b_{i1} & b_{i2} & \cdots & b_{in} \\ 0 & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & b_{i-1,2} & \cdots & b_{i-1,n} \\ 0 & b_{i+1,2} & \cdots & b_{i+1,n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & b_{n2} & \cdots & b_{nn} \end{vmatrix},$$

что по свойству 3.4 равно  $b_{i1}A_{i1}(B)$ . Таким образом, мы доказали разложение определителя по первому столбцу.

Для доказательства разложения по  $j$ -ому столбцу переставим его на первое место так, чтобы порядок следования остальных столбцов не изменился. Воспользуемся антисимметричностью определителя и уже доказанным разложением по первому столбцу. Разложение по строке легко вывести из разложения по столбцу при помощи свойства 3.2.  $\square$

#### 4. Формула для элементов обратной матрицы, формулы Крамера и минорный ранг

В этом параграфе мы выведем формулы для элементов обратной матрицы через алгебраические дополнения и определитель исходной. Первым шагом является следующее предложение.

**ПРЕДЛОЖЕНИЕ 4.1.** *Сумма произведений элементов столбца (строки) матрицы на алгебраические дополнения другого столбца (строки) равна нулю. Точнее, если  $j \neq k$ , то*

$$\sum_{i=1}^n b_{ij}A_{ik} = \sum_{i=1}^n b_{ji}A_{ki} = 0$$

**ДОКАЗАТЕЛЬСТВО.** Заменим  $k$ -й столбец матрицы  $B$  на  $j$ -й, оставив все остальное без изменений, т.е. рассмотрим матрицу  $\tilde{B}$  с элементами  $\tilde{b}_{im} = b_{im}$  при  $m \neq k$  и  $\tilde{b}_{ik} = b_{ij}$ . В полученной матрице будет два одинаковых столбца, следовательно, ее определитель будет равен нулю. С другой стороны, заметим, что алгебраические дополнения элементов  $k$ -го столбца не зависят от элементов этого столбца, поэтому  $A_{ik}(\tilde{B}) = A_{ik}(B)$ . Раскладывая, по свойству 3.6, определитель матрицы  $\tilde{B}$  по  $k$ -ому столбцу, получим  $0 = \det \tilde{B} = \sum_{i=1}^n \tilde{b}_{ik}A_{ik} = \sum_{i=1}^n b_{ij}A_{ik}$ .

Доказательство второго равенства (для строк) совершенно аналогично.  $\square$

**ОПРЕДЕЛЕНИЕ 4.2.** Матрица называется *невыврожденной*, если она квадратная, а ее определитель не равен нулю. Квадратная матрица с нулевым определителем называется *выврожденной*.

**ЛЕММА 4.3.** *Если матрица  $A$  обратима, то она невырождена.*

**ДОКАЗАТЕЛЬСТВО.** Мы уже доказывали, что обратимые матрицы обязательно квадратные. Если  $A^{-1}$  и  $A$  – квадратные, то по свойству 3.1 имеем  $1 = \det E = \det(A^{-1}A) = \det(A^{-1}) \cdot \det A$ , откуда  $\det A \neq 0$ .  $\square$

**ОПРЕДЕЛЕНИЕ 4.4.** Пусть  $B$  – матрица размера  $n \times n$ . Присоединенной к  $B$  называется матрица  $B^{\text{ad}}$ , транспонированная к матрице из алгебраических дополнений матрицы  $B$ , т.е. элемент матрицы  $B^{\text{ad}}$  в позиции  $(i, j)$  равен  $A_{ji}(B)$ .



**ТЕОРЕМА 4.5.** Если  $A \in M_n(F)$ , то

$$AA^{\text{ad}} = A^{\text{ad}}A = E \det A.$$

В частности, если матрица  $A$  невырождена, то она обратима, и

$$A^{-1} = \frac{1}{\det A} A^{\text{ad}}.$$

**ДОКАЗАТЕЛЬСТВО.** Положим  $B = A \cdot A^{\text{ad}}$ . Элемент матрицы  $A^{\text{ad}}$  в позиции  $(k, j)$  равен  $A_{jk}$ . Получаем:  $b_{ij} = \sum_{k=1}^n a_{ik} A_{jk}$ . При  $i = j$ , по свойству 3.6,  $b_{ij} = \det A$ , а при  $i \neq j$ , по свойству 4.1,  $b_{ij} = 0$ . Таким образом,  $B = E \det A$ . Аналогично,  $A^{\text{ad}}A = E \det A$ . Второе утверждение сразу вытекает из первого.  $\square$

**ТЕОРЕМА 4.6** (Формулы Крамера). Пусть  $A$  – матрица размера  $n \times n$ , а  $b$  столбец высоты  $n$ . Обозначим через  $\Delta$  определитель матрицы  $A$ , а через  $\Delta_i$  – определитель матрицы, полученной из  $A$  заменой  $i$ -ого столбца столбцом  $b$ . Система линейных уравнений  $Ax = b$  имеет единственное решение тогда и только тогда, когда  $\Delta \neq 0$ , причем  $x_i = \frac{\Delta_i}{\Delta}$ .

**ДОКАЗАТЕЛЬСТВО.** Если  $\Delta = 0$ , то оператор  $F^n \rightarrow F^n$  умножения на матрицу  $A$  необратим. Следовательно, он не инъективен и не сюръективен, т.е. система имеет либо ни одного, либо бесконечно много решений.

Если  $\Delta \neq 0$ , то, умножая равенство  $Ax = b$  слева на  $A^{-1}$  получим  $x = A^{-1}b$ . Подставляя формулу для обратной матрицы из теоремы 4.5, получим  $x = \frac{1}{\Delta} A^{\text{ad}}b$  или  $x_i = \frac{1}{\Delta} \sum_{k=1}^n A_{ki} b_k$ . Осталось заметить, что по теореме 3.6  $\sum_{k=1}^n A_{ki} b_k = \Delta_i$ .  $\square$

Следующее определение ранга матрицы более общепринято, чем строчный или столбцовый ранг.

**ОПРЕДЕЛЕНИЕ 4.7.** Минорным рангом матрицы  $A \in M_{m,n}(F)$  называется наибольший размер квадратной подматрицы, определитель которой не равен нулю.

**ТЕОРЕМА 4.8.** Минорный ранг матрицы равен ее строчному (столбцовому) рангу.

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $k$  минорный ранг  $A$ , а через  $r$  – ее строчный ранг. По определению минорного ранга существует квадратная подматрица размера  $k \times k$ , определитель которой не равен нулю. По лемме 2.4 строки этой подматрицы линейно независимы, а значит, линейно независимы и  $k$  строк матрицы  $A$ , в которых стоит выбранная подматрица. Следовательно,  $k \leq r$ .

Обратно, возьмем подматрицу  $r \times n$ , состоящую из линейно независимых строк матрицы  $A$ . По теореме 11.4 столбцовый ранг этой подматрицы также равен  $r$ , следовательно, в ней найдется  $r$  линейно независимых столбцов. Наконец, по лемме 2.4 квадратная матрица с линейно независимыми столбцами имеет ненулевой определитель, откуда  $k \geq r$ .  $\square$

## Собственные числа и жорданова форма

### 1. Собственные числа и вектора

В этой главе мы будем искать базис, в котором матрица оператора  $L : V \rightarrow V$  выглядит наиболее просто. В частности, этот параграф посвящен ситуации, когда эта матрица диагональна.

**ОПРЕДЕЛЕНИЕ 1.1.** Оператор называется диагонализуемым, если существует базис, в котором его матрица диагональна. Матрица называется диагонализуемой, если диагонализуем оператор умножения на эту матрицу.

Основной целью настоящего параграфа является выяснение того, когда оператор диагонализуем. Из определения матрицы оператора следует, что если

$$L_u = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

то базисные вектора базиса  $u = (u_1, \dots, u_n)$  удовлетворяют условию  $L(u_k) = \lambda_k u_k$ . Это наблюдение является мотивировкой для следующего определения.

**ОПРЕДЕЛЕНИЕ 1.2.** Ненулевой вектор  $v \in V$  называется собственным вектором оператора  $L : V \rightarrow V$ , соответствующим числу  $\lambda \in F$ , если

$$L(x) = v\lambda.$$

При этом  $\lambda$  называется собственным числом.

Столбец  $x \in F^n$  называется собственным вектором матрицы  $A \in M_n(F)$ , соответствующим числу  $\lambda \in F$ , если он является собственным вектором оператора умножения на эту матрицу, т. е.  $Ax = x\lambda$ .

Ясно, что вектор  $v \in V$  является собственным вектором оператора  $L$  тогда и только тогда, когда столбец  $v_f$  является собственным вектором матрицы  $L_f$  (где  $f$  – произвольный базис пространства  $V$ ). Из этого следует также, что собственные числа оператора  $L$  и его матрицы в любом базисе совпадают. Поэтому мы сосредоточим внимание на поиске собственных векторов и собственных чисел матриц.

**ПРЕДЛОЖЕНИЕ 1.3.** Число  $\lambda \in F$  является собственным числом матрицы  $A \in M_n(F)$  тогда и только тогда, когда  $\det(A - \lambda E) = 0$ .

**ДОКАЗАТЕЛЬСТВО.** Уравнение  $Ax = x\lambda$  равносильно уравнению  $(A - \lambda E)x = 0$ , которое имеет ненулевое решение тогда и только тогда, когда  $\det(A - \lambda E) = 0$ . Действительно, определитель равен нулю тогда и только тогда, когда столбцы матрицы линейно зависимы, а линейная зависимость – это и есть ненулевое решение уравнения.  $\square$

Матрица  $A - tE$ , принадлежит матричному кольцу  $M_n(F[t])$  над кольцом многочленов  $F[t]$ <sup>1</sup>. Поэтому ее определитель является многочленом. Из формулы для определителя следует, что степень этого многочлена равна  $n$  (моном старшей степени возникает из произведения диагональных элементов и равен  $(-1)^n t^n$ ).

**ОПРЕДЕЛЕНИЕ 1.4.** Многочлен  $\det(A - tE)$  называется характеристическим многочленом матрицы  $A$  и обозначается через  $\chi_A$ .

Как следует из предложения 1.3, собственные числа матрицы  $A$  и только они являются корнями характеристического многочлена. Так собственные числа матрицы оператора не зависят от выбора базиса, то неудивительно, что и характеристический многочлен обладает тем же свойством.

**ПРЕДЛОЖЕНИЕ 1.5.** Для любых базисов  $u$  и  $v$  пространства  $V$  характеристические многочлены матриц  $L_u$  и  $L_v$  равны.

ДОКАЗАТЕЛЬСТВО. Пусть  $C = C_{u \rightarrow v}$ . Тогда  $L_v = C^{-1}L_u C$  и

$$\chi_{L_v}(t) = \det(L_v - tE) = \det(C^{-1}L_u C - tE) = \det(C^{-1}(L_u - tE)C) = \det(L_u - tE) = \chi_{L_u}(t).$$

□

**ОПРЕДЕЛЕНИЕ 1.6.** Характеристический многочлен оператора – это характеристический многочлен его матрицы в некотором (любом) базисе.

Так как у многочлена  $n$ -ой степени не может быть больше, чем  $n$  корней, то у оператора в  $n$ -мерном пространстве может быть максимум  $n$  собственных чисел. Оказывается, что если их ровно  $n$ , то оператор диагонализуем. Это вытекает из следующего утверждения.

**ТЕОРЕМА 1.7.** Собственные вектора, соответствующие различным собственным числам, линейно независимы.

ДОКАЗАТЕЛЬСТВО. Пусть  $x_1, \dots, x_m$  – собственные вектора оператора  $L$ , соответствующие различным собственным числам  $\lambda_1, \dots, \lambda_m$ , т.е. выполнены равенства  $L(x_k) = \lambda_k x_k$ . Проведем доказательство индукцией по  $m$ . При  $m = 1$  утверждение следует из того, что собственный вектор по определению не равен 0. Пусть  $m > 1$ , и

$$\sum_{k=1}^m x_k \alpha_k = 0.$$

Применяя к этому равенству оператор  $L$ , получим

$$\sum_{k=1}^m L(x_k) \alpha_k = \sum_{k=1}^m x_k \lambda_k \alpha_k = 0,$$

а умножая его на  $\lambda_m$ :

$$\sum_{k=1}^m x_k \lambda_m \alpha_k = 0.$$

Вычитая последнее равенство из предпоследнего, имеем:

$$\sum_{k=1}^m x_k (\lambda_k - \lambda_m) \alpha_k = \sum_{k=1}^{m-1} x_k (\lambda_k - \lambda_m) \alpha_k = 0.$$

По индукционному предположению набор из  $m - 1$  собственного вектора линейно независим, поэтому  $(\lambda_k - \lambda_m) \alpha_k = 0$  при всех  $k = 1, \dots, m - 1$ . Так как  $\lambda_k \neq \lambda_m$  при  $k \neq m$ , то  $\alpha_k = 0$  при всех  $k = 1, \dots, m - 1$ . Подставляя эти значения в исходную формулу, получаем  $x_m \alpha_m = 0$ , откуда  $\alpha_m = 0$ . □

<sup>1</sup>Если быть абсолютно строгим, то она принадлежит кольцу  $M_n(F)[t]$  многочленов с матричными коэффициентами, но эти кольца очевидным образом изоморфны и мы отождествляем их.

Если у многочлена  $n$ -й степени нет  $n$  корней даже с учетом кратности, то это можно исправить, расширяя базовое поле. Следующее определение посвящено ситуации, когда характеристический многочлен имеет кратные корни.

**ОПРЕДЕЛЕНИЕ 1.8.** Алгебраической кратностью собственного числа называется его кратность в характеристическом многочлене.

Собственным подпространством, соответствующим собственному числу  $\lambda$ , называется ядро оператора  $L - \lambda I$ . Другими словами, собственное подпространство – это множество собственных векторов, соответствующих данному собственному числу, дополненное нулем.

Геометрической кратностью собственного числа называется размерность собственного подпространства.

**ЛЕММА 1.9.** Геометрическая кратность собственного числа не превосходит его алгебраической кратности.

**ДОКАЗАТЕЛЬСТВО.** Обозначим через  $k = \dim \text{Ker}(L - \lambda I)$  геометрическую кратность собственного числа  $\lambda$ . Выберем базис  $(u_1, \dots, u_k)$  пространства  $\text{Ker}(L - \lambda I)$  и дополним его до базиса  $u = (u_1, \dots, u_n)$  всего пространства  $V$ . Так как  $L(u_i) = u_i \lambda$  при всех  $i = 1, \dots, k$ , первые  $k$  столбцов матрицы  $L_u$  совпадают с соответствующими столбцами матрицы  $\lambda E$ . Поэтому  $\chi_L = \det(L_u - tE)$  делится на  $(\lambda - t)^k$ , следовательно, алгебраическая кратность  $\lambda$  не меньше  $k$ .  $\square$

В следующей теореме собраны различные условия диагонализуемости оператора.

**ТЕОРЕМА 1.10.** Пусть  $L : V \rightarrow V$  – оператор на  $n$ -мерном пространстве  $V$ .

- (1)  $L$  диагонализуем тогда и только тогда, когда существует базис из его собственных векторов (такой базис называется собственным базисом оператора).
- (2)  $L$  диагонализуем тогда и только тогда, когда  $V$  равно прямой сумме собственных подпространств.
- (3) Если существует  $n$  различных собственных чисел оператора  $L$ , то он диагонализуем (это условие не является необходимым).
- (4) Предположим, что поле  $F$  алгебраически замкнуто. Оператор  $L$  диагонализуем тогда и только тогда, когда геометрическая кратность каждого собственного числа равна его алгебраической кратности.
- (5) Если характеристический многочлен не имеет кратных корней, а поле  $F$  алгебраически замкнуто, то оператор диагонализуем.

**ДОКАЗАТЕЛЬСТВО. 1.** Это утверждение обсуждалось в самом начале параграфа.

**2.** Если  $V$  равно прямой сумме собственных подпространств, то объединение базисов этих подпространств является базисом пространства  $V$ , состоящим из собственных векторов. Обратно, каждый собственный вектор лежит в каком-то собственном подпространстве. Поэтому если существует базис из собственных векторов, то  $V$  является суммой собственных подпространств. Тот факт, что сумма прямая, следует из теоремы о линейной независимости собственных векторов.

**3.** Пусть оператор  $L$  имеет  $n$  различных собственных чисел. Выберем по одному собственному вектору для каждого собственного числа. По теореме о линейной независимости собственных векторов они линейно независимы, а так как их число равно размерности пространства, то они образуют базис.

**4.** Так как поле алгебраически замкнуто, то сумма алгебраических кратностей собственных чисел равна степени характеристического многочлена, которая равна размерности пространства. Если геометрические кратности равны алгебраическим, то сумма размерностей собственных подпространств равна размерности пространства. Из теоремы о линейной независимости собственных векторов следует, что сумма собственных подпространств является прямой (сумма всех, кроме одного, имеет с этим одним тривиальное пересечение). По следствию о размерности прямой суммы,

размерность суммы собственных подпространств равна сумме их размерностей, т. е. размерности пространства. Теперь диагонализуемость оператора следует из пункта 2.

Обратно, если  $L$  диагонализуем, то  $n$  равно сумме геометрических кратностей и сумме алгебраических кратностей. Так как геометрические кратности не превосходят алгебраических, то они должны быть равны.

5. Если характеристический многочлен не имеет кратных корней, то над замкнутым полем он имеет  $n$  различных корней, и утверждение следует из пункта 3.  $\square$

## 2. Жорданова форма и теорема Гамильтона–Кэли

Из предыдущей теоремы видно, что даже над алгебраически замкнутым полем существуют недиагонализуемые операторы. В этом параграфе мы докажем, что можно и их привести к довольно простому виду, называемому жордановой формой оператора.

**ОПРЕДЕЛЕНИЕ 2.1.** Обозначим через  $J = J_n$  матрицу размера  $n \times n$  с единицами во всех позициях  $(k, k + 1)$ ,  $k = 1, \dots, n - 1$ , и остальными нулями. Жордановым блоком называется матрица  $\lambda E + J$ . Жордановой матрицей называется блочно диагональная матрица с жордановыми блоками по диагонали.

**ТЕОРЕМА 2.2.** Пусть  $V$  – конечномерное векторное пространство над алгебраически замкнутым полем  $F$ , а  $L : V \rightarrow V$  – линейный оператор. Тогда существует базис  $\mathcal{B}$  пространства  $V$  такой, что матрица  $L_{\mathcal{B}}$  является жордановой. Она называется жордановой формой оператора  $L$  и определена единственным образом с точностью до перестановки блоков.

Доказательство этой теоремы будет дано после изучения модулей над областями главных идеалов, а сейчас мы выведем некоторые следствия этой теоремы. Для этого нам понадобится несколько простых утверждений.

**ЛЕММА 2.3.** Матрица  $J_n^m$  имеет 1 во всех позициях  $(k, k + m)$ ,  $1 \leq k \leq n - m$ . Если  $N \in M_m(F)$  – верхнетреугольная матрица с нулями по главной диагонали, то  $N^m = 0$ .

Следующая лемма позволяет во многих случаях заменять матрицу на ее жорданову форму.

**ЛЕММА 2.4.** Отображение  $A \mapsto C^{-1}AC$  является автоморфизмом матричного кольца, следовательно, для любого многочлена  $p$ :  $p(C^{-1}AC) = C^{-1}p(A)C$ .

Следующее утверждение показывает, как работать с блочно-диагональными матрицами. Обозначим через  $\text{diag}(A^{(1)}, \dots, A^{(m)})$  диагональную матрицу с квадратными диагональными блоками  $A^{(1)}, \dots, A^{(m)}$ .

**ЛЕММА 2.5.** Множество блочно диагональных матриц с квадратными диагональными блоками фиксированного размера является подкольцом матричного кольца, изоморфным прямой сумме матричных колец соответствующих размеров. В частности, для любого многочлена  $p$

$$p(\text{diag}(A^{(1)}, \dots, A^{(m)})) = \text{diag}(p(A^{(1)}), \dots, p(A^{(m)})).$$

Первое применение жордановой формы – доказательство следующего утверждения.

**ТЕОРЕМА 2.6** (теорема Гамильтона–Кэли). Пусть  $A$  – квадратная матрица или линейный оператор на конечномерном пространстве. Тогда  $\chi_A(A) = 0$ .

**ДОКАЗАТЕЛЬСТВО.** Ясно, что доказывать можно только для случая матриц. Пусть  $A \in M_n(F)$ . Как мы узнаем позже, любое поле  $F$  вкладывается в алгебраически замкнутое поле  $\bar{F}$ . Поэтому  $A \in M_n(\bar{F})$ , и по теореме 2.2 существует  $C \in M_n(\bar{F})$  такая, что  $A = C^{-1}A'C$ , где  $A'$  – жорданова форма матрицы  $A$  (матрица оператора умножения на  $A$  в жордановом базисе). По лемме 2.4 равенство  $\chi_A(A) = 0$  равносильно равенству  $\chi_A(A') = 0$ , а так как  $A$  и  $A'$  – матрицы одного и того же оператора в разных базисах, то  $\chi_A = \chi_{A'}$ . По определению  $A' = \text{diag}(\lambda_1 E_{k_1} + J_{k_1}, \dots, \lambda_m E_{k_m} + J_{k_m})$  для некоторых  $m, k_1, \dots, k_m \in \mathbb{N}$  и  $\lambda_1, \dots, \lambda_m \in \bar{F}$ . Тогда

$\chi_{A'}(t) = \prod_{i=1}^m (\lambda_i - t)^{k_i}$ . Если подставить  $i$ -й диагональный блок матрицы  $A'$  в  $i$ -й сомножитель многочлена  $\chi_{A'}$ , то в соответствие с леммой 2.3 получится 0 (напомним, что при подстановке матрицы в многочлен свободный член многочлена умножается на единичную матрицу). Следовательно, значение  $\chi_{A'}$  на любом диагональном блоке матрицы  $A'$  равно 0. Теперь требуемое равенство следует из леммы 2.5  $\square$

Полезно знать и непосредственное доказательство теоремы Гамильтона–Кэли, без использования жордановой формы.

**ВТОРОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ГАМИЛЬТОНА–КЭЛИ.** Заметим, что матричное кольцо  $M_n(F[t])$  над кольцом многочленов изоморфно кольцу  $M_n(F)[t]$  многочленов с матричными коэффициентами.<sup>2</sup> Рассмотрим матрицу  $A - tE \in M_n(F[t])$ . По теореме 4.5 главы 5

$$(5) \quad (A - tE)(A - tE)^{\text{ad}} = (A - tE)^{\text{ad}}(A - tE) = \det(A - tE)E = \chi_A(t)E.$$

Переписывая это равенство в кольце  $M_n(F)[t]$  получаем

$$(A - tE)(B_0 + B_1t + \dots + B_{n-1}t^{n-1}) = \chi_A(t)E,$$

где  $B_i \in M_n(F)$  – коэффициенты в разложении матрицы  $(A - tE)^{\text{ad}}$  по степеням  $t$ .

Как видно, для доказательства теоремы достаточно подставить в это равенство  $A$  вместо  $t$ . Однако, такая подстановка законна только если  $A$  лежит в центре кольца коэффициентов. Действительно, формально, подстановка элемента  $a$  алгебры  $R$  в многочлен – это вычисление значения гомоморфизма  $\varphi_a : R[t] \rightarrow R$ , посылающего  $t$  в  $a$  и оставляющего на месте все элементы  $R$ . Но  $t$  коммутирует со всеми элементами кольца  $R$ , а гомоморфизм сохраняет это свойство. Обратно, если  $a$  коммутирует со всеми элементами из  $R$ , то простая проверка показывает, что формула  $\varphi_a(r_0 + \dots + r_mt^m) = r_0 + \dots + r_ma^m$  задает требуемый гомоморфизм (это небольшое обобщение универсального свойства кольца многочленов 14.2 главы 4).

Определим  $R$ , как минимальную  $F$ -подалгебра в  $M_n(F)$ , содержащую матрицы  $A$  и  $B_1, \dots, B_{n-1}$ . Так как  $A - tE$  коммутирует с  $(A - tE)^{\text{ad}}$ , то и  $A$  коммутирует с этой матрицей. Следовательно,  $A(B_0 + \dots + B_{n-1}t^{n-1}) = (B_0 + \dots + B_{n-1}t^{n-1})A$ , откуда сразу следует, что  $AB_i = B_iA$  при всех  $i$ . Таким образом,  $A$  лежит в центре алгебры  $R$  и, значит, ее можно подставить вместо  $t$  в равенство (5). В левой части этого равенства, очевидно, получается 0, следовательно, и правая часть  $\chi_A(A)E = 0$ .  $\square$

Пусть  $R$  – ассоциативная (возможно некоммутативная) алгебра с 1 над полем  $F$ . Напомним, что для любого  $r \in R$  существует единственный гомоморфизм  $F$ -алгебр

$$\varepsilon_r : F[t] \rightarrow R, \quad p \mapsto p(r),$$

отображающий независимую переменную  $t$  в  $r$ . Ядро этого гомоморфизма – идеал кольца  $F[t]$ . Так как  $F[t]$  – область главных идеалов, то  $\text{Ker } \varepsilon_r$  – главный идеал. Образующая этого идеала называется минимальным многочленом элемента  $r$  и обозначается  $\varphi_r$ . Этот многочлен определен однозначно с точностью до умножения на обратимый элемент кольца  $F[t]$ , т.е. ненулевую константу.

По теореме о гомоморфизме наименьшая подалгебра с 1 в  $R$ , содержащая  $r$ , изоморфна  $F[t]/(\varphi_r)$ . Она обозначается через  $F[r]$ . Таким образом, каждому многочлену от  $r$  (элементу  $F[r]$ ) однозначно сопоставляется смежный класс этого многочлена в  $F[t]/(\varphi_r)$ . Как мы знаем, этот смежный класс имеет единственного представителя наименьшей степени, а именно, остаток от деления на  $\varphi_r$ .

Пусть теперь  $R = M_n(F)$ , а  $A \in R$ .

**ЛЕММА 2.7.** *Характеристический многочлен матрицы  $A$  делится на минимальный. Любое собственное число является корнем минимального многочлена.*

<sup>2</sup>Мы определяли только кольцо многочленов над коммутативным кольцом, но определение над некоммутативным кольцом ничем не отличается. Важно только понимать, что независимая переменная  $t$  коммутирует со всеми элементами кольца.

**ДОКАЗАТЕЛЬСТВО.** Первое утверждение сразу следует из теоремы Гамильтона–Кэли. Второе также несложно вывести из теоремы о жордановой форме, но мы дадим непосредственное доказательство. Действительно, если  $Ax = \lambda x$ , то  $A^n x = \lambda^n x$  и, следовательно,  $p(A)x = p(\lambda)x$  для любого многочлена  $p \in F[t]$ . Следовательно,  $0 = \varphi_A(A)x = \varphi_A(\lambda)x$ , откуда (т.к.  $x \neq 0$ ) следует, что  $\varphi_A(\lambda) = 0$ .  $\square$

**ЗАМЕЧАНИЕ 2.8.** С использованием жордановой формы нетрудно доказать, что кратность собственного числа в минимальном многочлене матрицы равна размеру наибольшей жордановой клетки с этим собственным числом.

### 3. Разложение Жордана

Элемент  $r$  кольца  $R$  называется нильпотентным, если  $r^m = 0$  для некоторого натурального  $m$ . Наименьшее такое  $m$  называется степенью нильпотентности элемента  $r$ . Из того, что матрица  $J_n$  нильпотентна, а сопряжение при помощи обратимой матрицы является автоморфизмом матричного кольца, следует существование аддитивного и мультипликативного разложения Жордана над замкнутым полем.

Для формулировки и доказательства аддитивного разложения Жордана над незамкнутым полем нам понадобится небольшой экскурс в теорию Галуа, т.е. некоторые сведения о расширениях полей. Доказательства приведенных утверждений появятся позже, в главе 13. Если даны два поля  $F \subseteq K$ , то обычно пишут “дано расширение полей  $K/F$ ” (читается “ $K$  над  $F$ ”; обозначение не имеет никакого отношения к факторгруппе) или “пусть  $K$  – расширение поля  $F$ ”. Элемент  $a \in K$  называется алгебраическим над  $F$ , если он является корнем некоторого многочлена с коэффициентами из  $F$ .

**ТЕОРЕМА 3.1.** *Для любого поля  $F$  существует алгебраически замкнутое поле  $\bar{F}$ , которое содержит  $F$ , а каждый его элемент алгебраичен над  $F$ . Такое поле единственно с точностью до изоморфизма.*

Поле  $\bar{F}$  из формулировки теоремы называется *алгебраическим замыканием* поля  $F$ .

Поле  $F$  называется *совершенным*, если любой неприводимый многочлен из  $F[t]$  не имеет кратных корней в алгебраическом замыкании поля  $F$ . Вспомнив, что кратные корни – это общие корни многочлена и его производной, нетрудно видеть, что поле совершенно, если производная неприводимого многочлена не может быть равна нулю. Действительно, неприводимый многочлен взаимно прост с любым ненулевым многочленом меньшей степени. Отсюда сразу следует, что любое поле характеристики 0 совершенно. В поле  $F$  характеристики  $p$  отображение  $F \rightarrow F$ ,  $x \mapsto x^p$ , сохраняет не только операцию умножения, но и сложения (так как  $\binom{p}{n}$  делится на  $p$  при любом  $n$  от 1 до  $p-1$ ). Оно называется *эндоморфизмом Фробениуса*. Ясно, что эндоморфизм Фробениуса инъективен ( $x^p = y^p \iff (x-y)^p = 0 \iff x = y$ ). Нетрудно доказать, что поле  $F$  совершенно тогда и только тогда, когда эндоморфизм Фробениуса биективен. В частности, любое конечное поле совершенно. Простейший пример несовершенного поля дает поле рациональных функций  $\mathbb{F}_p[t]$ , где неприводимый многочлен  $t^p - 1$  над алгебраическим замыканием имеет один корень кратности  $p$ .

Группа Галуа расширения  $K/F$  – это группа автоморфизмов поля  $K$  действующих тождественно на  $F$ . Следующая лемма является ключевой для перехода от случая замкнутого поля к любому совершенному во многих ситуациях.

**ТЕОРЕМА 3.2.** *Пусть  $F$  – совершенное поле, а  $\bar{F}$  – его алгебраическое замыкание. Тогда множество элементов, неподвижных под действием любого элемента группы Галуа расширения  $\bar{F}/F$ , совпадает с  $F$ .*

Квадратная матрица называется *полупростой*, если оператор умножения на нее диагонализуем.

**ТЕОРЕМА 3.3** (аддитивное разложение Жордана). *Предположим, что поле  $F$  совершенно. Тогда для любой матрицы  $A \in M_n(F)$  существуют единственные матрицы  $A^{(s)}, A^{(n)} \in M_n(F)$  такие, что:*

- (1)  $A^{(s)}$  – полупростая,  $A^{(n)}$  – нильпотентная;
- (2)  $A = A^{(s)} + A^{(n)}$ ;
- (3)  $A^{(s)}A^{(n)} = A^{(n)}A^{(s)}$ .

При этом матрицы  $A^{(s)}$  и  $A^{(n)}$  выражаются, как многочлены от матрицы  $A$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть сначала  $F$  алгебраически замкнуто. Тогда по теореме 2.2 существует обратимая матрица  $C$  такая, что

$$C^{-1}AC = \text{diag}(\mu_1 E, \dots, \mu_m E) + \text{diag}(N_1, \dots, N_m),$$

где  $\mu_1, \dots, \mu_m$  – все различные собственные числа матрицы  $A$ , а  $N_i$  – матрица с некоторым количеством единиц непосредственно над главной диагональю и нулями в остальных местах. Обозначим первое слагаемое (диагональную матрицу) через  $S$ , а второе – через  $N$ . Ясно, что  $\mu_i E$  коммутирует с  $N_i$ , поэтому  $SN = NS$ . Очевидно также, что  $S$  полупроста, а  $N$  нильпотентна. Таким образом,

$$A = CSC^{-1} + CNC^{-1}$$

является аддитивным разложением Жордана.

**Второй шаг** доказательства – утверждение о том, что полупростая и нильпотентная части матрицы  $A$  являются многочленами от  $A$ . Так как сопряжение при помощи  $C$  является автоморфизмом матричного кольца, достаточно доказать, что  $S$  – многочлен от  $B = C^{-1}AC$  (тогда  $N = B - S$  – тоже многочлен от  $B$ ). Докажем, что  $\text{diag}(0, \dots, 0, \mu_i E, 0, \dots, 0)$  является многочленом от  $B$ , этого достаточно, так как  $S$  равно сумме этих матриц. Утверждение не требует доказательства при  $\mu_i = 0$ . Пусть  $\mu_i \neq 0$ . Рассмотрим многочлен  $f(t) = \prod_{j \neq i} (t - \mu_j)^{k_j}$ , где  $k_j$  – размер  $j$ -го блока. Тогда

$$f(B) = \text{diag}(f(\mu_1 E + N_1), \dots, f(\mu_m E + N_m))$$

Так как  $N_j^{k_j} = 0$ , то для любого  $j \neq i$  в произведении  $f(\mu_j E + N_j)$  есть нулевой сомножитель. С другой стороны, матрица  $f(\mu_i E + N_i)$  является верхнетреугольной с числом  $\mu = \prod_{j \neq i} (\mu_i - \mu_j)$  на диагонали. Так как  $\mu_i \neq \mu_j$  при  $i \neq j$ , то  $\mu \neq 0$ . Получаем,

$$f(\mu_i E + N_i) = \mu E + U,$$

где  $U$  – верхнетреугольная матрица с 0 на главной диагонали. Нетрудно видеть, что  $U^{k_i} = 0$ . Положим  $g(t) = (\mu - t)^{k_i} - \mu^{k_i}$ . Тогда  $g(0) = 0$  и  $g(\mu E + U) = -\mu^{k_i} E$ . Следовательно,

$$g(f(B)) = g(\text{diag}(0, \dots, 0, \mu E + U, 0, \dots, 0)) = \text{diag}(0, \dots, 0, -\mu^{k_i} E, 0, \dots, 0).$$

Таким образом, многочлен  $\frac{\mu_i}{-\mu^{k_i}} g \circ f$  отображает  $B$  в требуемую диагональную матрицу.

**Третий шаг** – доказательство единственности разложения. Снова достаточно доказать это для матрицы  $B$ . Заметим сначала, что любая матрица, коммутирующая с  $B$ , коммутирует также и с любым многочленом от  $B$ , в частности, с  $N$  и  $S$ . Пусть  $B = S' + N'$ , где  $S'$  полупростая,  $N'$  нильпотентная, и  $S'N' = N'S'$ . Из последнего равенства следует, что  $S'$  и  $N'$  коммутируют с  $B$ , следовательно, все 4 матрицы  $N, S, N'$  и  $S'$  коммутируют друг с другом.

Так как  $S = \text{diag}(\mu_1 E, \dots, \mu_m E)$ , где все  $\mu_i$  различны, а  $SS' = S'S$ , то простое матричное вычисление показывает, что  $S' = \text{diag}(S^{(1)}, \dots, S^{(m)})$ , где размеры диагональных блоков равны размерам диагональных блоков, на которые разбита матрица  $S$ . Заметим, что сумма коммутирующих между собой нильпотентных элементов кольца нильпотентна. Действительно, если  $y^k = z^r = 0$ , то в сумме

$$(y + z)^{k+r-1} = \sum_{i=0}^{k+r-1} \binom{k+r-1}{i} y^i z^{k+r-1-i},$$



каждое слагаемое равно нулю, потому что либо  $i \geq k$ , либо  $k + r - 1 - i \geq r$ . Таким образом, матрица  $S' - S = N - N'$  нильпотентна.

Пусть  $J^{(i)} = (C^{(i)})^{-1}S^{(i)}C^{(i)}$  – жорданова форма матрицы  $S^{(i)}$ . Положим

$$C' = \text{diag}(C^{(1)}, \dots, C^{(m)}) \text{ и } J' = \text{diag}(J^{(1)}, \dots, J^{(m)}).$$

Тогда  $(C')^{-1}S'C' = J'$ . Так как  $S'$  диагонализуема, то этим свойством обладает и матрица  $J'$ . Но  $J'$  – блочно диагональная матрица с жордановыми блоками по диагонали. Если не все эти блоки имеют размер 1 на 1, то алгебраическая кратность какого-то собственного числа не совпадает с геометрической, что противоречит диагонализуемости. Таким образом, матрица  $J'$  диагональна. Заметим, что  $C'$  коммутирует с  $S$ , потому что  $S$  коммутирует с любой блочно диагональной матрицей с такими размерами блоков. Следовательно, матрица  $S - J' = (C')^{-1}(S - S')C$  диагональна и нильпотентна. Легко видеть, что она нулевая. Таким образом,  $S = S'$ , откуда следует единственность.

**Четвертый шаг** доказательства – существование аддитивного разложения Жордана над незамкнутым полем. Пусть  $\bar{F}$  – алгебраическое замыкание поля  $F$ . Тогда по доказанному существуют единственные матрицы  $A^{(s)}, A^{(n)} \in M_n(\bar{F})$ , удовлетворяющие условиям теоремы. Необходимо показать, что все элементы матриц  $A^{(s)}$  и  $A^{(n)}$  лежат в исходном поле  $F$ . Пусть  $\sigma$  – элемент группы Галуа расширения  $\bar{F}/F$ , т.е. автоморфизм поля  $\bar{F}$ , тождественный на  $F$ . Нетрудно видеть, что он индуцирует автоморфизм матричного кольца  $M_n(\bar{F})$ , тождественный на  $M_n(F)$ , который мы, допуская вольность записи, будем также обозначать через  $\sigma$ . А именно, для матрицы  $X \in M_n(\bar{F})$  положим  $\sigma(X)_{ij} = \sigma(x_{ij})$ . Очевидно, что любой автоморфизм матричного кольца сохраняет свойства коммутирования, нильпотентности и диагонализуемости. Следовательно,  $A = \sigma(A) = \sigma(A^{(s)}) + \sigma(A^{(n)})$  является аддитивным разложением Жордана матрицы  $A$ . Из единственности разложения следует, что  $\sigma(A^{(s)}) = A^{(s)}$  и  $\sigma(A^{(n)}) = A^{(n)}$ . Таким образом, все элементы матриц  $A^{(s)}$  и  $A^{(n)}$  неподвижны под действием любого элемента  $\sigma$  группы Галуа  $\bar{F}/F$ . По теореме 3.2 все эти элементы принадлежат  $F$ .

Наконец, последний **пятый шаг** – доказать, что коэффициенты многочленов  $p$  и  $q$ , для которых  $A^{(s)} = p(A)$  и  $A^{(n)} = q(A)$ , лежат в  $F$ . По доказанному на втором шаге такие многочлены существуют в  $\bar{F}[t]$ . Давайте считать, что они имеют минимально возможную степень, тогда они определены единственным образом, см. текст перед леммой 2.7. Элемент  $\sigma$  группы Галуа  $\bar{F}/F$  индуцирует автоморфизм кольца многочленов  $\sum \alpha_i t^i \mapsto \sum \sigma(\alpha_i) t^i$ , который мы будем снова обозначать через  $\sigma$ . Ясно, что

$$p(A) = A^{(s)} = \sigma(A^{(s)}) = \sigma(p(A)) = \sigma(p)(\sigma(A)) = \sigma(p)(A).$$

Так как  $\sigma$  не меняет степень многочлена, а  $p(A) = \sigma(p)(A)$ , то  $\sigma(p) = p$ . По теореме 3.2 все коэффициенты многочлена  $p$  лежат в  $F$ , т.е.  $p \in F[t]$   $\square$

Элемент  $r$  кольца с 1 называется унитарным, если  $r - 1$  нильпотентен.

**СЛЕДСТВИЕ 3.4** (мультипликативное разложение Жордана). *Для любой матрицы  $A \in \text{GL}_n(F)$  над совершенным полем  $F$  существуют матрицы  $S, U \in M_n(F)$  такие, что  $S$  – полупростая,  $U$  – унитарная,  $A = SU$ , и  $SU = US$ .*

*При этом матрицы  $S$  и  $U$  выражаются, как многочлены от матрицы  $A$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $A = S + N$  – аддитивное разложение Жордана матрицы  $A$ . Так как  $A$  – обратимая матрица, то и  $S = A - N$  обратима. Действительно,  $(A - N)A^{-1} = E - NA^{-1}$ , матрица  $\tilde{N} = NA^{-1}$  нильпотентна, так как  $N$  нильпотентна и коммутирует с  $A^{-1}$ , а  $(E - \tilde{N})(E + \tilde{N} + \dots + \tilde{N}^{k-1}) = E - \tilde{N}^k = E$  для достаточно большого  $k$ . Таким образом,  $A = SU$ , где  $U = (E + S^{-1}N)$  и есть мультипликативное разложение Жордана.

Осталось доказать, что  $U$  – многочлен от  $A$ . Пусть  $S = p(A)$ , где  $p \in F[t]$  – многочлен, существование которого утверждается в предыдущей теореме, а  $x$  – собственный вектор матрицы  $A$ , соответствующий собственному числу  $\lambda \in \bar{F}$ . Тогда  $Sx = p(A)x = p(\lambda)x$  (последнее равенство

достаточно проверить на одночленах, для которых оно очевидно). Так как  $S$  обратима, а  $x \neq 0$ , то  $p(\lambda) \neq 0$ . Так как только собственные числа являются корнями минимального многочлена  $\varphi_A$  матрицы  $A$ , то  $p$  взаимно прост с  $\varphi_A$ . Напишем линейное представление НОД:  $1 = pf + \varphi_A g$  и подставим туда  $A$ . Получим  $E = p(A)f(A) + \varphi_A(A)g(A) = Sf(A)$ . Таким образом,  $S^{-1} = f(A)$ , и  $U = AS^{-1} = Af(A)$ .  $\square$

#### 4. Функции от матриц

Пусть  $f : D \rightarrow \mathbb{C}$  – дифференцируемая функция комплексной переменной, где  $D$  – открытый круг в  $\mathbb{C}$ . Из теории функций комплексной переменной следует, что она раскладывается в степенной ряд в окрестности любой точки  $\mu \in D$ :

$$f(z) = \sum_{k=0}^{\infty} \alpha_k(\mu)(z - \mu)^k.$$

При этом радиус сходимости этого ряда не меньше, чем расстояние от  $\mu$  до границы круга. Как и в случае числового ряда, для матрицы  $A \in M_n(\mathbb{C})$  положим по определению,

$$f(A) = \lim_{m \rightarrow \infty} \sum_{k=0}^m \alpha_k(\mu)(A - \mu E)^k,$$

где предел берется поэлементно (впрочем, можно брать предел по любой норме на векторном пространстве  $M_n(\mathbb{C})$  так как в конечномерном пространстве предел не зависит от выбора нормы). Естественно, этот предел не всегда существует. Вскоре мы докажем, что при некоторых предположениях он не зависит от точки  $\mu$ .

Умножение матриц задается многочленами и, поэтому, непрерывно, как функция  $\mathbb{C}^{2n^2} \rightarrow \mathbb{C}^{n^2}$ . Для  $A \in M_n(\mathbb{C})$  и  $C \in GL_n(\mathbb{C})$  имеем:

$$f(C^{-1}AC) = \lim_{m \rightarrow \infty} \sum_{k=0}^m \alpha_k(C^{-1}AC - \mu E)^k \stackrel{2.4}{=} \lim_{m \rightarrow \infty} C^{-1} \left( \sum_{k=0}^m \alpha_k(A - \mu E)^k \right) C \stackrel{\text{непр.}}{=} C^{-1} f(A) C.$$

Равенство означает, что либо ряды в обеих частях расходятся, либо эти выражения равны. Предположим, что  $C^{-1}AC = \text{diag}(\lambda_1 E + J_{k_1}, \dots, \lambda_l E + J_{k_l})$  – жорданова форма матрицы  $A$ . По лемме 2.5 для вычисления многочлена от блочно диагональной матрицы достаточно вычислить его от каждого диагонального блока. Аналогичное утверждение очевидно верно и с заменой слова “многочлен” на слово “предел”. Докажем, что для жорданова блока результат применения функции не зависит от того, в окрестности какой точки мы раскладываем эту функцию в ряд.

**ЛЕММА 4.1.** Пусть  $\lambda, \mu \in D$ , а  $J = J_s$  – жорданов блок размера  $s \times s$  с собственным числом 0. Тогда

$$f(\lambda E + J) = \sum_{k=0}^{\infty} \alpha_k(\mu)((\lambda - \mu)E + J)^k = \sum_{k=0}^{s-1} \alpha_k(\lambda) J^k$$

не зависит от выбора точки  $\mu \in D$ .

ДОКАЗАТЕЛЬСТВО. Раскладывая  $f(z)$  в ряд в окрестностях точек  $\lambda$  и  $\mu$  получаем

$$\begin{aligned} f(z) &= \sum_{k=0}^{\infty} \alpha_k(\lambda)(z - \lambda)^k = \sum_{j=0}^{\infty} \alpha_j(\mu)((z - \lambda) + (\lambda - \mu))^j = \\ &= \sum_{j=0}^{\infty} \alpha_j(\mu) \left( \sum_{k=0}^j \binom{j}{k} (z - \lambda)^k (\lambda - \mu)^{j-k} \right) = \sum_{k=0}^{\infty} \left( \sum_{j=k}^{\infty} \alpha_j(\mu) \binom{j}{k} (\lambda - \mu)^{j-k} \right) (z - \lambda)^k \end{aligned}$$

(так как внутри круга сходимости ряд сходится абсолютно, мы имеем право менять порядок суммирования). Нетрудно доказать, что коэффициенты при соответствующих степенях  $z - \lambda$  должны быть равны. Следовательно,

$$\alpha_k(\lambda) = \sum_{j=k}^{\infty} \alpha_j(\mu) \binom{j}{k} (\lambda - \mu)^{j-k}.$$

Подставляя  $\lambda E + J$  вместо  $z$  в предыдущее вычисление, получим<sup>3</sup>

$$f(\lambda E + J) = \sum_{k=0}^{\infty} \alpha_k(\mu) ((\lambda - \mu)E + J)^k = \cdots = \sum_{k=0}^{s-1} \alpha_k(\lambda) J^k.$$

□

**ТЕОРЕМА 4.2.** Пусть  $A \in M_n(\mathbb{C})$  имеет собственные числа  $\lambda_1, \dots, \lambda_l \in D$  (не обязательно различные), а  $C = C_{e \rightarrow u}$  – матрица перехода от стандартного базиса  $\mathbb{C}^n$  к жорданову базису матрицы  $A$ . Тогда ряд для  $f(A)$  сходится и

$$f(A) = C \operatorname{diag}(f(\lambda_1 E + J_{s_1}), \dots, f(\lambda_l E + J_{s_l})) C^{-1},$$

а значение  $f$  на жордановом блоке вычисляется по формуле

$$f(\lambda E + J_s) = \sum_{k=0}^{s-1} \alpha_k(\lambda) J_s^k.$$

Вычисление экспоненты от матрицы применяется при решении системы дифференциальных уравнений  $y' = Ay$ , где  $y = (y_1, \dots, y_n)^T$ ,  $y_k$  – дифференцируемые функции  $\mathbb{C} \rightarrow \mathbb{C}$ , а  $A \in M_n(\mathbb{C})$ . Общее решение этой системы имеет вид  $y = e^{At}c$ , где  $c$  пробегает множество столбцов  $\mathbb{C}^n$ .

## 5. Другое доказательство жордановой формы

Основным доказательством теоремы о жордановой форме в нашем курсе будет доказательство, использующее строение конечнопорожденных модулей над кольцом многочленов. Это будет сделано в параграфе 9. А сейчас мы приведем набросок другого доказательства. Первым шагом является теорема о ядре произведения многочленов от оператора. Напомним, что умножение в алгебре операторов на векторном пространстве – это композиция.

**ТЕОРЕМА 5.1.** Пусть  $L : V \rightarrow V$  – линейный оператор на векторном пространстве  $V$  над полем  $F$  ( $V$  не предполагается конечномерным), а  $p, q \in F[t]$  – взаимно простые многочлены. Тогда

$$\operatorname{Ker}(p(L)q(L)) = \operatorname{Ker} p(L) \oplus \operatorname{Ker} q(L).$$

**ДОКАЗАТЕЛЬСТВО.** Так как  $p$  и  $q$  взаимно просты, существуют многочлены  $f, h \in F[t]$  такие, что  $pf + qh = 1$ . Подставляя в это равенство оператор  $L$ , получим  $f(L)p(L) + h(L)q(L) = \operatorname{id}$ . Действуя на вектор  $x \in V$ , получим  $f(L)p(L)(x) + h(L)q(L)(x) = x$ . Если  $x \in \operatorname{Ker}(p(L)q(L))$ , то первое слагаемое лежит в ядре оператора  $q(L)$ , так как  $q(L)f(L)p(L)(x) = f(L)(p(L)q(L))(x) = f(L)(0) = 0$ . Аналогично второе слагаемое лежит в ядре оператора  $p(L)$ . Таким образом,  $\operatorname{Ker}(p(L)q(L)) = \operatorname{Ker} p(L) + \operatorname{Ker} q(L)$ . Если же  $x \in \operatorname{Ker} p(L) \cap \operatorname{Ker} q(L)$ , то  $x = f(L)p(L)(x) + h(L)q(L)(x) = 0$ , следовательно, сумма прямая. □

<sup>3</sup>Доказательство выглядит, как жульничество, но смысл его таков. Кольцо  $R$  дифференцируемых функций в некотором открытом круге вкладывается в кольцо формальных степенных рядов  $\mathbb{C}[[t]]$  (определения этого кольца нет в конспекте, но этот пример был в лекциях первого семестра). Подкольцо  $\mathbb{C}[J_s]$  матричного кольца  $M_s(\mathbb{C})$  изоморфно кольцу усеченных многочленов  $\mathbb{C}[t]/(t^s)$ , потому что  $t^s$  – минимальный многочлен матрицы  $J^s$ . Любой элемент из  $\mathbb{C}[[t]]$  единственным образом представляется в виде суммы многочлена степени, меньшей  $s$ , и ряда, делящегося на  $t^s$ . Поэтому  $\mathbb{C}[[t]]/(t^s) \cong \mathbb{C}[t]/(t^s) \cong \mathbb{C}[J_s]$ . Поэтому равенство в  $\mathbb{C}[[t]]$  выполнено и для образов левой и правой части в  $\mathbb{C}[J_s]$ .

Пусть теперь поле алгебраически замкнуто. Используя теорему Гамильтона–Кэли (или минимальный многочлен оператора вместо характеристического) и последнюю теорему, разложим пространство в прямую сумму подпространств

$$V = \text{Ker } \varphi_L(L) = \bigoplus_{i=1}^m \text{Ker}(L - \lambda_i \text{id})^{k_i}.$$

Подпространство  $\text{Ker}(L - \lambda_i \text{id})^{k_i}$  называется корневым подпространством оператора  $L$ , соответствующим собственному числу  $\lambda_i$ .

Обозначим через  $A$  сужение оператора  $L - \lambda_i \text{id}$  на корневое подпространство  $U = \text{Ker}(L - \lambda_i \text{id})^{k_i}$ . Для окончания доказательства теоремы о жордановой форме достаточно научиться выбирать базис  $u$  пространства  $U$  такой, что  $A_u$  состоит из жордановых блоков. Так как оператор  $A$  нильпотентен, то его собственные числа равны 0. Таким образом, необходимо выбрать базис, удовлетворяющий условиям  $A(u_j) = u_{j-1}$  или  $A(u_j) = 0$  для всех  $j = 1, \dots, k_j$ . Набор векторов  $v_1, \dots, v_k$  таких, что  $A(v_1) = 0$ , а  $A(v_j) = v_{j-1}$  при  $j = 2, \dots, k$  называется жордановой цепочкой. Следующее утверждение заканчивает доказательство.

**ТЕОРЕМА 5.2.** *Для любого нильпотентного оператора существует базис, состоящий из жордановых цепочек (это верно над любым полем).*

Доказательство этой теоремы не очень сложно, но требует аккуратной организации индукции по размерности пространства.

## 6. Дифференциальные и рекуррентные уравнения

Приведем еще одно приложение теоремы 5.1. Пусть дано линейное однородное уравнение с постоянными коэффициентами

$$(6) \quad y^{(n)} + a_{n-1}y^{(n-1)} + \dots + a_0y = 0.$$

Это уравнение можно записать в виде  $p(D)(y) = 0$ , где  $D$  – оператор дифференцирования на множестве дифференцируемых функций  $\mathbb{C} \rightarrow \mathbb{C}$ , а  $p = t^n + a_{n-1}t^{n-1} + \dots + a_0$ . Другими словами, нам надо найти ядро дифференциального оператора  $p(D)$ .

Аналогично, пусть  $F^\infty$  обозначает векторное пространство бесконечных последовательностей  $x : \mathbb{N}_0 \rightarrow F$ , где  $F$  алгебраически замкнутое поле. Рекуррентное уравнение

$$(7) \quad x_{m+n} + a_{n-1}x_{m+n-1} + \dots + a_0x_m = 0 \text{ при любом } m \in \mathbb{N}_0$$

сводится к нахождению ядра оператора  $p(S)$ , где  $S$  – оператор сдвига номеров, т. е.  $S(x)_k = x_{k+1}$  при всех  $k \in \mathbb{N}_0$ .

По теореме 5.1 для решения обеих задач над замкнутым полем (в случае дифференциальных уравнений над  $\mathbb{C}$ ) достаточно рассмотреть случай  $p(t) = (t - \lambda)^k$ . При  $\lambda = 0$  мы умеем решать такую задачу: решение дифференциального уравнения  $y^{(k)} = 0$  – множество многочленов степени  $\leq k - 1$ , а для рекуррентного уравнения  $x_{m+k} = 0$  при любом  $m \in \mathbb{N}$  – множество конечных последовательностей длины  $k$ , дополненных нулями. Общий случай для дифференциальных уравнений следует из теоремы сдвига.

**ТЕОРЕМА 6.1.** *Пусть  $D$  – оператор дифференцирования, определенный выше, а  $p$  – многочлен. Тогда*

$$\text{Ker } p(D - \lambda \text{id}) = e^{\lambda t} \text{Ker } p(D).$$

Для рекуррентного уравнения теорему сдвига написать не удастся.

Решение дифференциального уравнения (6) можно найти и с помощью вычисления экспоненты от матрицы. Для этого надо переписать это уравнение в виде системы

$$y'_0 = y_1; \quad y'_1 = y_2; \quad \dots \quad y'_{n-1} = y_n; \quad y'_n = - \sum_{k=0}^{n-1} a_k y_k$$

и решить ее помощью экспоненты от матрицы, как было описано в параграфе 4.

Аналогично, решение рекуррентного уравнения (7) можно найти возводя некоторую матрицу в степень, что делается с помощью жордановой формы. А именно, уравнение (7) можно записать в виде

$$\begin{pmatrix} x_{m+1} \\ x_{m+2} \\ \vdots \\ x_{m+n-1} \\ x_{m+n} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & 0 \\ \dots & \dots & \dots & \ddots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix} \cdot \begin{pmatrix} x_m \\ x_{m+1} \\ \vdots \\ x_{m+n-2} \\ x_{m+n-1} \end{pmatrix},$$

или короче  $x^{(m+1)} = Ax^{(m)}$ . Тогда для нахождения формулы для  $x^{(m)}$  надо просто возвести матрицу  $A$  в степень  $m$  и умножить на произвольный столбец  $x^{(0)}$ .

## 7. Модули над кольцами

**ОПРЕДЕЛЕНИЕ 7.1.** Пусть  $R$  – (не обязательно коммутативное) кольцо с 1. Аддитивная абелева группа  $M$  с заданной операцией “умножения”  $M \times R \rightarrow M$  называется правым  $R$ -модулем, если для любых  $\alpha, \beta \in R$  и  $u, v \in M$ :

- (1)  $v(\alpha\beta) = (v\alpha)\beta$ ;
- (2)  $v(\alpha + \beta) = v\alpha + v\beta$ ;
- (3)  $(u + v)\alpha = u\alpha + v\alpha$ ;

Аналогично определяется левый  $R$ -модуль.

Модуль называется унитарным, если  $v \cdot 1 = v$  для любого  $v \in M$ . В нашем курсе все модули по умолчанию считаются унитарными.

Гомоморфизмом (или  $R$ -линейным отображением)  $R$ -модулей называется отображение  $L : M \rightarrow M'$ , удовлетворяющее условиям  $L(v + v') = L(v) + L(v')$  и  $L(v\alpha) = L(v)\alpha$ .

### Примеры.

- (1) Идеал является модулем.
- (2) Абелева группа –  $\mathbb{Z}$ -модуль, векторное пространство –  $F$ -модуль.
- (3) Кольцо является модулем над самим собой. Этот модуль называется регулярным. Это аналог одномерного векторного пространства.
- (4) Если  $\varphi : R \rightarrow A$  – гомоморфизм колец, то  $A$  является (левым)  $R$ -модулем относительно действия:  $r * a = \varphi(r)a$ .
- (5) Если  $\varphi : R \rightarrow A$  – гомоморфизм колец, а  $M$  –  $A$ -модуль, то  $M$  является  $R$ -модулем относительно действия:  $r * m = \varphi(r)m$ .
- (6) Множество  $R^n$  является правым  $R$ -модулем и левым  $M_n(R)$ -модулем.

Подмодуль, фактормодуль (по подмодулю), прямая сумма модулей, ядро и образ гомоморфизма, линейная комбинация, линейная оболочка, линейная независимость, система образующих определяется так же, как для векторных пространств. Имеет место теорема о гомоморфизме. Базис – это линейно независимая система образующих. Далеко не любой модуль имеет базис.

**ОПРЕДЕЛЕНИЕ 7.2.** Модуль называется свободным, если он имеет базис.

Свободный модуль  $F(X)$  с базисом  $X$  обладает следующим универсальным свойством.

**ПРЕДЛОЖЕНИЕ 7.3.** Для любого  $R$ -модуля  $M$  и функции  $X \rightarrow M$  существует единственный гомоморфизм модулей  $F(X) \rightarrow M$  такой, что диаграмма

$$\begin{array}{ccc} X & \longrightarrow & F(X) \\ & \searrow & \downarrow \\ & & M \end{array}$$

коммутативна.

**ДОКАЗАТЕЛЬСТВО.** Из условия коммутативности диаграммы мы знаем образы базисных элементов. Так как любой элемент  $F(X)$  является линейной комбинацией базисных, а гомоморфизм модулей переводит линейные комбинации в линейные комбинации, то образы всех элементов  $F(X)$  определены однозначно. Проверка того, что таким образом мы действительно получим гомоморфизм модулей тривиальна.  $\square$

Следующее утверждение – конструкция свободного модуля.

**ПРЕДЛОЖЕНИЕ 7.4.** Пусть  $F(X)$  – множество финитных функций  $X \rightarrow R$ , т. е. множество тех функций, значения которых равны нулю везде, кроме конечного множества. Они образуют модуль над  $R$  относительно поточечных операций. Зададим функцию  $i : X \rightarrow F(X)$

формулой  $i(x) = \mathbb{1}_x$  – характеристическая функция множества  $\{x\}$ , т. е.  $\mathbb{1}_x(y) = \begin{cases} 1, & y = x \\ 0, & y \neq x \end{cases}$ .

Тогда  $F(X)$  вместе с отображением  $i$  – свободный модуль с базисом  $X$ .

**ПРЕДЛОЖЕНИЕ 7.5.** Если  $X$  конечно, то  $F(X) \cong R^{|X|} \cong \underbrace{R \oplus \dots \oplus R}_{|X| \text{ раз}}$ .

**ДОКАЗАТЕЛЬСТВО.** Фактически множество столбцов высоты  $n = |X|$  – это и есть множество функций  $X \rightarrow R$ , или множество кортежей длины  $n$ , которое совпадает с прямой суммой. Легко проверить, что после отождествления окажется, что операции определены одинаково.  $\square$

**ЗАМЕЧАНИЕ 7.6.** Для бесконечного множества  $X$  утверждение тоже верно, если правильно определить прямую сумму бесконечного набора модулей.

## 8. Подмодули свободного модуля над ОГИ

Следующие два параграфа лежат на стыке теории коммутативных колец и линейной алгебры. Мы докажем теорему классификации конечнопорожденных модулей над кольцами главных идеалов, из которой затем выведем теорему о Жордановой форме оператора. В качестве бесплатного приложения мы получим теорему о строении конечнопорожденных абелевых групп.

Пусть  $R$  – коммутативное кольцо, а  $M$  – конечнопорожденный  $R$ -модуль, т. е. в  $M$  существует конечная система образующих  $X = \{x_1, \dots, x_k\}$ . По универсальному свойству свободного модуля существует единственный гомоморфизм свободного модуля  $F(X)$  в  $M$ , тождественный на  $X$ . Так как  $X$  – система образующих, то этот гомоморфизм сюръективен. По теореме о гомоморфизме  $M \cong F(X)/N$  для некоторого подмодуля  $N$  в  $F(X)$ . Учитывая, что  $F(X) \cong R^{|X|}$ , для описания произвольного конечнопорожденного  $R$ -модуля достаточно описать подмодули в  $R^k$  для произвольного натурального  $k$ .

Прежде, чем перейти к классификации подмодулей, определим аналог размерности векторных пространств для конечнопорожденных свободных модулей. Если  $u$  и  $v$  – конечные базисы свободного модуля, то, также как и для векторных пространств, существуют взаимно обратные матрицы перехода  $C_{u \rightarrow v}$  и  $C_{v \rightarrow u}$ . Неквадратная матрица над коммутативным кольцом не может быть двусторонне обратима. Действительно, если бы она была двусторонне обратима, то ее образ над любым факторкольцом обладал бы тем же свойством. С другой стороны, в любом коммутативном кольце существует максимальный идеал, фактор по которому – поле, а для поля результат

известен из линейной алгебры. Поэтому любой базис свободного модуля имеет одинаковое число элементов, которое называется рангом этого модуля.<sup>4</sup>

Специфика области главных идеалов, необходимая для классификации подмодулей конечно-порожденного свободного модуля, выражена в следующей лемме.

**ЛЕММА 8.1.** *Пусть  $R$  – область главных идеалов. Для любого столбца  $x \in R^k$  существует матрица  $A \in \text{GL}_k(R)$  такая, что  $Ax = e_{*1}\alpha$ . При этом  $\alpha$  является наибольшим общим делителем элементов столбца  $x$ .*

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство индукцией по  $k$ . Для  $k = 1$  доказывать нечего. При  $k > 1$  положим  $d = \gcd(x_{k-1}, x_k)$ ,  $a = \frac{x_{k-1}}{d}$  и  $b = \frac{x_k}{d}$ . По теореме о линейном представлении НОД существуют  $r, s \in R$  такие, что  $x_{k-1}r + x_k s = d$ , откуда  $ar + bs = 1$ . Тогда

$$\begin{pmatrix} E & 0 & 0 \\ 0 & r & s \\ 0 & -b & a \end{pmatrix} \begin{pmatrix} x' \\ x_{k-1} \\ x_k \end{pmatrix} = \begin{pmatrix} x' \\ d \\ 0 \end{pmatrix},$$

где  $x' = (x_1, \dots, x_{k-2})^\top$ . Заметим, что определитель первого сомножителя равен 1, следовательно, эта матрица обратима. По индукционному предположению существует обратимая матрица  $A'$  такая, что  $A' \begin{pmatrix} x' \\ d \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}$ , где  $\alpha = \gcd(x_1, \dots, x_{k-2}, d) = \gcd(x_1, \dots, x_k)$ .  $\square$

Если  $R$  – нетерова область целостности, то свойство из предыдущей леммы равносильно тому, что любой идеал в  $R$  является главным.

**ТЕОРЕМА 8.2** (классификации подмодулей конечнопорожденного свободного модуля). *Пусть  $R$  – кольцо главных идеалов, а  $N$  – подмодуль свободного модуля  $R^k$ . Существует базис  $u = (u_1, \dots, u_k)$  модуля  $R^k$  и элементы  $\alpha_1, \dots, \alpha_k \in R$  такие, что*

- (1) *элементы  $u_1\alpha_1, \dots, u_k\alpha_k$  лежат в  $N$  и порождают его;*
- (2)  *$\alpha_{i+1}$  делится на  $\alpha_i$  при всех  $i = 1, \dots, k-1$  (мы считаем, что 0 делится на 0).*

**СХЕМА ДОКАЗАТЕЛЬСТВА.**

$$\begin{pmatrix} n_1 & * \\ n_2 & * \\ \vdots & * \\ n_k & * \end{pmatrix} \rightarrow \begin{pmatrix} \alpha & y_1 & * \\ 0 & y_2 & * \\ \vdots & \vdots & * \\ 0 & y_k & * \end{pmatrix} = \begin{pmatrix} \alpha & y_1 & \gcd(\alpha, y_1) & * \\ 0 & y_2 & * & * \\ \vdots & \vdots & * & * \\ 0 & y_k & * & * \end{pmatrix} \rightarrow \begin{pmatrix} \alpha & 0 & \dots \\ 0 & * & * \\ \vdots & * & * \\ 0 & * & * \end{pmatrix} \rightarrow \dots \rightarrow \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \alpha_k \end{pmatrix}.$$

$\square$

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство индукцией по рангу  $k$  свободного модуля, в котором лежит изучаемый подмодуль. При  $k = 1$  подмодуль в  $R^1$  – это идеал кольца  $R$ , а любой идеал в  $R$  – главный. Таким образом, достаточно взять  $u_1 = 1$ , а  $\alpha_1$  – образующая этого идеала.<sup>5</sup>

Пусть  $k > 1$ . Обозначим через  $I(x)$  идеал, порожденный элементами столбца  $x$ . Положим  $S = \{I(x) \mid x \in N\}$ . Пусть  $I(n) = \alpha R$  максимальный из идеалов множества  $S$ . Можно считать, что  $\alpha \neq 0$ , иначе  $N = 0$  и утверждение очевидно. По лемме 8.1 существует  $A \in \text{GL}_k(R)$  такая,

<sup>4</sup>Для некоммутативных колец это утверждение неверно, т. е. существует некоммутативное кольцо  $\Lambda$  для которого модули  $\Lambda^n$  и  $\Lambda^m$  изоморфны при  $m \neq n$ . Простейший пример такого кольца – кольцо эндоморфизмов бесконечномерного векторного пространства. Кольца, для которых ранг свободного модуля определен однозначно, называются ИБЧ или IBN-кольцами (Invariant Basis Number). Нетрудно доказать, что из не-ИБЧ-кольца не существует ни одного гомоморфизма ни в одно ИБЧ-кольцо, т. е. в каком-то смысле класс не-ИБЧ-колец – это черная дыра: попав туда, выбраться уже невозможно.

<sup>5</sup>На самом деле можно было бы начинать индукцию с  $k = 0$ , при котором утверждение пусто, так как нулевой модуль порожден пустым множеством.

что  $An = e_{*1}\alpha$ . Возьмем  $x \in N$ , обозначим  $y = Ax$  и докажем, что  $y_1$  делится на  $\alpha$ . Пусть  $\gamma = \gcd(y_1, \alpha)$ . Существуют элементы  $\lambda, \mu \in R$  такие, что  $y_1\lambda + \alpha\mu = \gamma$ . Тогда первый элемент столбца  $Ax\lambda + An\mu$  равен  $\gamma$ . Имеем

$$\alpha R \leq \gamma R \leq I(Ax\lambda + An\mu) = I(x\lambda + n\mu).$$

Так как  $x\lambda + n\mu \in N$ , то идеал  $I(x\lambda + n\mu)$  принадлежит  $S$ . Максимальность идеала  $\alpha R$  влечет равенство  $\alpha R = I(x\lambda + n\mu)$ , откуда  $y_1 \in \gamma R = \alpha R$ .

Таким образом,  $y_1 = \alpha\beta$  для некоторого  $\beta \in R$ , и

$$Ax = An\beta + \sum_{i=2}^k e_{*i}y_i = e_{*1}\alpha\beta + \sum_{i=2}^k e_{*i}y_i.$$

Домножая на  $A^{-1}$  получаем

$$x = u'_1\alpha\beta + \sum_{i=2}^k u'_iy_i \in \langle u'_1\alpha, u'_2, \dots, u'_k \rangle,$$

где  $u'_i = a'_{i*}$  – столбцы матрицы  $A^{-1}$ . Так как  $x$  – произвольный элемент из  $N$ , то мы доказали, что  $N \leq \langle u'_1\alpha, u'_2, \dots, u'_k \rangle$ . Более того, из формулы для  $x$  следует, что  $\sum_{i=2}^k u'_iy_i = x - u'_1\alpha\beta \in N$ , откуда

$$N = \langle u'_1\alpha \rangle \oplus (\langle u'_2, \dots, u'_k \rangle \cap N)$$

(сумма прямая, потому что уже  $\langle u'_1 \rangle \cap \langle u'_2, \dots, u'_k \rangle = \{0\}$ ).

Модуль  $N' = N \cap \langle u'_2, \dots, u'_k \rangle$  содержится в свободном модуле  $\langle u'_2, \dots, u'_k \rangle$  ранга  $k-1$ , поэтому к нему можно применить индукционное предположение. Другими словами, существует базис  $u_2, \dots, u_k$  модуля  $\langle u'_2, \dots, u'_k \rangle$  и элементы  $\alpha_2, \dots, \alpha_k \in R$  такие, что  $N'$  порожден элементами  $u_2\alpha_2, \dots, u_k\alpha_k$  и  $\alpha_{i+1}$  делится на  $\alpha_i$  при всех  $i = 2, \dots, k-1$ . Положим  $\alpha_1 = \alpha$  и  $u_1 = u'_1$ . Легко проверить, что  $u_1, \dots, u_k$  – базис модуля  $R^k$ , а  $u_1\alpha_1, \dots, u_k\alpha_k$  порождает  $N$ .

Осталось доказать, что  $\alpha_2$  делится на  $\alpha_1$ . Обозначим через  $C = C_{e \rightarrow u}$  матрицу, составленную из столбцов  $u_1, \dots, u_n$ . Элемент  $u_1\alpha_1 + u_2\alpha_2$  принадлежит  $N$ , поэтому

$$I(u_1\alpha_1 + u_2\alpha_2) = I(C^{-1}u_1\alpha_1 + C^{-1}u_2\alpha_2) = \alpha_1 R + \alpha_2 R \in S.$$

Так как  $\alpha_1 R$  – максимальный среди идеалов из  $S$ , то  $\alpha_1 R + \alpha_2 R = \alpha_1 R$ , откуда следует, что  $\alpha_2 \in \alpha_1 R$ , т. е.  $\alpha_2$  делится на  $\alpha_1$ .  $\square$

**СЛЕДСТВИЕ 8.3.** *Любой подмодуль конечнопорожденного свободного модуля над областью главных идеалов является свободным, причем ранг подмодуля не превосходит ранга модуля.*

**СЛЕДСТВИЕ 8.4** (Нормальная форма Смита). *Для любой матрицы  $A \in M_{k,l}(R)$  над областью главных идеалов  $R$  существуют матрицы  $B \in GL_k(R)$  и  $C \in GL_l(R)$  такие, что все недиагональные элементы матрицы  $BAC$  равны нулю, а каждый диагональный элемент делится на предыдущий.*

Формально это утверждение не следует из теоремы, так как “матрица перехода” от одной системы образующих к другой не обязана быть обратимой. Для доказательства достаточно повторить рассуждения из доказательства теоремы с  $N$  равным линейной оболочке столбцов матрицы  $A$ , с необходимыми уточнениями.

## 9. Конечнопорожденные модули над кольцами главных идеалов

Модуль  $M$  над кольцом  $R$  называется циклическим, если он порожден одним элементом. Любой циклический модуль изоморфен  $R/I$  для некоторого идеала  $I$  кольца  $R$ . Действительно, если  $M = \langle m \rangle$ , то отображение  $\pi : R \rightarrow M$ , заданное формулой  $\pi(r) = mr$  является эпиморфизмом модулей, следовательно,  $M \cong R/\text{Кер } \pi$ .

Циклический модуль  $R/I$  называется примарным, если  $I$  – степень простого идеала (если  $R$  – область целостности, то  $I$  может быть равен 0).



**ТЕОРЕМА 9.1** (Классификация конечнопорожденных модулей). *Любой конечнопорожденный модуль над областью главных идеалов изоморфен прямой сумме примарных модулей. При этом набор примарных модулей определен однозначно.*

**ДОКАЗАТЕЛЬСТВО.** В этом параграфе мы докажем только существование такого разложения и выведем несколько следствий. Единственность будет доказана в следующем разделе.

Пусть  $M$  – конечнопорожденный модуль над областью главных идеалов  $R$ . Как уже говорилось, существует эпиморфизм  $R^k \rightarrow M$ . Обозначим его ядро через  $N$ . По теореме 8.2 существует базис  $u_1, \dots, u_k$  модуля  $R^k$  и элементы  $\alpha_1, \dots, \alpha_k \in R$  такие, что  $N = \langle u_1\alpha_1, \dots, u_k\alpha_k \rangle$ . Зададим гомоморфизм  $\rho: R^k \rightarrow \bigoplus_{i=1}^k R/\alpha_i R$  формулой

$$\rho(u_1\beta_1 + \dots + u_k\beta_k) = (\beta_1 \bmod \alpha_1, \dots, \beta_k \bmod \alpha_k)$$

(так как  $u$  – базис, то эта формула однозначно задает отображение). Легко видеть, что  $\rho$  – эпиморфизм, а его ядро равно  $N$ . По теореме о единственности эпиморфизма с данным ядром  $M \cong \bigoplus_{i=1}^k R/\alpha_i R$ , т.е.  $M$  является прямой суммой циклических модулей. С другой стороны, по китайской теореме об остатках любой циклический модуль равен прямой сумме примарных.  $\square$

**СЛЕДСТВИЕ 9.2** (Классификация конечнопорожденных абелевых групп). *Любая конечнопорожденная абелева группа изоморфна прямой сумме циклических групп бесконечного порядка и порядка  $p^n$ , где  $p$  – простое число. При этом такое разложение единственно с точностью до перестановки прямых слагаемых.*

В частности, если порядок абелевой группы делится на простое число  $p$ , то среди прямых слагаемых обязательно должна быть циклическая группа порядка  $p^n$ , следовательно, в ней есть элемент порядка  $p$  – утверждение, которое будет использовано при доказательстве первой теоремы Силова.

Из теоремы о строении конечнопорожденных модулей, примененной к кольцу многочленов, получаем доказательство существования нормальных форм матрицы оператора. Клеткой Фробениуса называется матрица  $A \in M_n(F)$  с элементами  $a_{i+1,i} = 1$  при  $i = 1, \dots, n-1$ , произвольными  $a_{in}$ ,  $i = 1, \dots, n$ , и остальными нулями.

**ТЕОРЕМА 9.3** (нормальная форма Фробениуса). *Для любого линейного оператора  $L: V \rightarrow V$  существует базис  $u$  пространства  $V$  такой, что матрица  $L_u$  клеточно диагональная с клетками Фробениуса по диагонали.*

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим  $V$  как  $F[t]$ -модуль, полагая  $t^k v = L^k(v)$  и продолжая это определение по линейности на все кольцо  $F[t]$ . Так как  $F[t]$  – кольцо главных идеалов, то по теореме 9.1  $V$  изоморфно прямой сумме циклических модулей (допуская вольность речи будем считать, что  $V$  равно прямой сумме циклических модулей). Заметим, что  $F[t]$  не может встречаться в прямой сумме, потому что  $V$  конечномерно над  $F$ , а  $F[t]$  – нет.

Каждый из циклических модулей является  $L$ -инвариантным подпространством, поэтому в  $F$ -базисе  $V$ , состоящем из  $F$ -базисов циклических модулей, матрица оператора  $L$  будет клеточно диагональной. В каждом циклическом модуле  $F[t]/pF[t]$  выберем базис из смежных классов  $\bar{t}^k = t^k + pF[t]$ . Тогда  $L(\bar{t}^k) = t \cdot \bar{t}^k = \bar{t}^{k+1}$ . Если  $k < \deg p - 1$ , то оператор  $L$  отображает базисный вектор в следующий. Следовательно, в соответствующих столбцах матрицы оператора  $L$  появляются единицы под главной диагональю и остальные нули. Таким образом, в диагональных блоках стоят клетки Фробениуса.  $\square$

В предыдущей теореме единственности не было, потому что клетки Фробениуса соответствуют циклическим модулям, которые не обязательно примарны. Заметим, что характеристический многочлен фробениусовой клетки  $A$  равен  $\pm(t^n + a_{nn}t^{n-1} + \dots + a_{2n}t + a_{1n})$ .

**ДОКАЗАТЕЛЬСТВО СУЩЕСТВОВАНИЯ ЖОРДАНОВОЙ ФОРМЫ.** Пусть  $F$  – алгебраически замкнутое поле,  $V$  – векторное пространство над  $F$ ,  $L : V \rightarrow V$  – линейное отображение, а  $R = F[t]$ . Рассмотрим  $V$  как  $R$ -модуль, полагая  $t^k v = L^k(v)$  и продолжая это определение по линейности на все кольцо  $R$ . Так как  $R$  – область главных идеалов, то по теореме 9.1  $V$  изоморфно прямой сумме примарных модулей. Заметим, что  $R$  не может встречаться в прямой сумме, потому что  $V$  конечномерно над  $F$ , а  $R$  – нет.

Так как  $F$  замкнуто, то неприводимыми элементами кольца  $R$  являются только многочлены  $t - \lambda$ . Таким образом, осталось изучить модули  $M = R/(t - \lambda)^k R$ . Элементы этого модуля взаимно однозначно соответствуют многочленам степени, меньшей  $k$ . Поэтому любой элемент  $M$  может быть единственным образом представлен в виде  $F$ -линейной комбинации  $\sum_{i=0}^{k-1} \alpha_i (t - \lambda)^i$ , где  $\alpha_i \in F$ . Таким образом, элементы  $(t - \lambda)^i$ ,  $i = 0, \dots, k-1$ , образуют базис  $M$ , как векторного пространства над  $F$ . Если  $v_0, \dots, v_{k-1}$  – элементы  $V$ , соответствующие  $(t - \lambda)^0, \dots, (t - \lambda)^{k-1}$  при изоморфизме, то ясно, что  $(t - \lambda)v_i = v_{i+1}$  при  $i < k-1$ , а  $(t - \lambda)v_{k-1} = 0$ . По определению действия  $t$  на  $V$  получаем:

$$L(v_i) = v_{i+1} + \lambda v_i \text{ при } i < k-1, \text{ и } L(v_{k-1}) = \lambda v_{k-1}.$$

Другими словами, матрица сужения оператора  $L$  на подпространство  $\langle v_0, \dots, v_{k-1} \rangle$  в выбранном базисе – это жорданова клетка. Таким образом, пространство  $V$  разбилось в прямую сумму подпространств, в каждом из которых матрица сужения  $L$  в подходящем базисе является жордановой клеткой. Объединение базисов прямых слагаемых является базисом пространства. Ясно, что в объединении подходящих базисов матрица оператора  $L$  будет клеточно-диагональной с жордановыми блоками по диагонали.

Утверждение о единственности следует из единственности разложения конечнопорожденного модуля в прямую сумму примарных модулей.  $\square$

## 10. Единственность разложения на примарные

Пусть  $R$  – область целостности, а  $M$  –  $R$ -модуль. Множество элементов из  $M$ , которые при умножении на какой-нибудь ненулевой элемент кольца обращаются в 0, называется подмодулем кручения. Это действительно подмодуль, потому что если  $m_1 r_1 = 0$  и  $m_2 r_2 = 0$ , то  $(m_1 + m_2) r_1 r_2 = 0$  (здесь  $m_1, m_2 \in M$ , а  $r_1, r_2 \in R \setminus \{0\}$ ). Говорят, что  $M$  – модуль без кручения, если его подмодуль кручения нулевой. Фактормодуль по подмодулю кручения является модулем без кручения. Действительно, Обозначим через  $T = T(M)$  подмодуль кручения. Тогда  $x + T$  содержится в  $T(M/T)$  тогда и только тогда, когда  $xr \in T$  для некоторого ненулевого  $r \in R$ . Но тогда по определению подмодуля кручения  $xrr' = 0$  для какого-то  $r' \in R \setminus \{0\}$ , при этом  $rr' \neq 0$ , так как  $R$  – область целостности. Следовательно,  $x \in T$ , т. е.  $x + T = 0_{M/T}$ .

Пусть теперь  $R$  – область главных идеалов, а  $p \in R$  – неприводимый элемент. Тогда  $R/pR$  – поле. Для натурального числа  $k$  рассмотрим фактормодуль  $p^{k-1}M/p^kM$ . Так как умножение на  $p$  аннулирует любой элемент этого модуля, то можно естественным образом определить на этом модуле структуру  $R/pR$ -векторного пространства:  $(r + pR)(p^{k-1}m + p^kM) = p^{k-1}rm + p^kM$ . Оказывается числа  $l_{p,k} = l_{p,k}(M) = \dim_{R/pR} p^{k-1}M/p^kM$  по всем неприводимым  $p \in R$  и всем  $k \in \mathbb{N}$  полностью определяют строение подмодуля кручения  $T(M)$ .

**ЛЕММА 10.1.** Пусть  $M = R/p^n R$  – примарный модуль, а  $q \neq p$  – неприводимый элемент в  $R$ . Тогда  $l_{q,k} = 0$ ,  $l_{p,k} = 1$  при  $n \geq k$ , и  $l_{p,k} = 0$  в противном случае.

$$l_{p,k}(M_1 \oplus M_2) = l_{p,k}(M_1) + l_{p,k}(M_2).$$

Если  $M$  – прямая сумма примарных модулей не изоморфных  $R$ , то  $l_{p,k}(M)$  равно количеству прямых слагаемых в разложении  $M$ , изоморфных  $R/p^h R$  с  $h \geq k$ .

<sup>6</sup>Здесь мы отождествляем многочлен степени, меньшей  $k$ , с его смежным классом, также как мы часто делаем в группе  $\mathbb{Z}/k\mathbb{Z}$ , отождествляя смежный класс целого числа с остатком от деления на  $k$ .

ДОКАЗАТЕЛЬСТВО. Так как  $q$  обратим в кольце  $R/p^n R$ , то умножение на  $q$  является автоморфизмом модуля  $M$ , откуда  $q^k M = q^{k-1} M$ . Фактормодуль циклического модуля циклический, поэтому если он ненулевой, то он порожден 1 элементом. При  $n \geq k$  модуль  $p^{k-1}(R/p^n R)$  порожден элементом  $p^{k-1}$ , отсюда первое утверждение.

Ясно, что  $p^k(M_1 \oplus M_2) = p^k M_1 \oplus p^k M_2$ . Следовательно,

$$p^{k-1}(M_1 \oplus M_2)/p^k(M_1 \oplus M_2) \cong p^{k-1}M_1/p^k M_1 \oplus p^{k-1}M_2/p^k M_2,$$

откуда вытекает второе утверждение леммы. Третье утверждение сразу вытекает из двух первых.  $\square$

**ЗАМЕЧАНИЕ 10.2.** В предыдущей лемме можно заменить идеалы вида  $p^n R$  на  $\mathfrak{m}^n$ , где  $\mathfrak{m}$  – максимальный идеал. Тогда можно не накладывать никаких ограничений на коммутативное кольцо  $R$ .

ДОКАЗАТЕЛЬСТВО ЕДИНСТВЕННОСТИ РАЗЛОЖЕНИЯ ИЗ ТЕОРЕМЫ 9.1. Пусть  $R$  – область главных идеалов, а

$$M = R^k \oplus M_1 \oplus \cdots \oplus M_s, \text{ где } M_i = \bigoplus_{j=1}^{t_i} R/p_i^{h_{ij}} R \text{ при всех } i = 1, \dots, s,$$

а  $p_1, \dots, p_s$  – различные неприводимые элементы  $R$ . Мы хотим доказать, что набор  $p_1, \dots, p_s$ , а также числа  $k, s, t_i$  и  $h_{ij}$  зависят только от самого модуля  $M$ , а не от разложения в прямую сумму.

Ясно, что  $T(M) = M_1 \oplus \cdots \oplus M_s$  является подмодулем кручения в  $M$ , а  $R^k \cong M/T(M)$ . Так как ранг свободного модуля определен однозначно, то  $k$  определено однозначно.

Числа  $l_{q,k} = l_{q,k}(T(M))$  также не зависят от разложения. Количество прямых слагаемых в разложении модуля  $M$  на примарные, изоморфных  $R/p^h R$ , равно  $l_{p,h} - l_{p,h+1}$ . Действительно, по предыдущей лемме  $l_{p,h+1}$  – количество слагаемых  $R/p^n R$ , где  $n \geq h+1$ , а  $l_{p,h}$  количество слагаемых  $R/p^n R$ , где  $n \geq h$ . Таким образом, количество слагаемых изоморфных  $R/p^h R$  также определяется модулем  $M$  однозначно, что завершает доказательство.  $\square$

## Билинейные и квадратичные формы

Везде в этой главе мы считаем, что характеристика основного поля не равна 2. Изучение квадратичных форм в характеристике 2 – это существенно более сложная задача, даже на уровне определений.

### 1. Формы и их матрицы

Пусть  $V$  – векторное пространство над полем  $F$ .

Напомним, что функция  $B : V \times V \rightarrow F$  называется билинейной формой, если для любых  $x, y, z \in V$  и  $\alpha, \beta \in F$  имеют место равенства:

$$B(x\alpha + y\beta, z) = B(x, z)\alpha + B(y, z)\beta \text{ и } B(z, x\alpha + y\beta) = B(z, x)\alpha + B(z, y)\beta.$$

Билинейная форма  $B$  называется симметричной (антисимметричной), если  $B(x, y) = B(y, x)$  (соотв.  $B(x, y) = -B(y, x)$ ) для любых  $x, y \in V$ .

Обозначим через  $\text{Bil}(V)$  – множество всех билинейных форм на  $V$ , а через  $\text{Bil}^{(s)}(V)$  и  $\text{Bil}^{(a)}(V)$  – множества симметричных и антисимметричных билинейных форм. Ясно, что все 3 множества являются подпространствами пространства всех функций  $V \times V \rightarrow F$  (с поточечными операциями).

**ЛЕММА 1.1.**  $\text{Bil}(V) = \text{Bil}^{(s)}(V) \oplus \text{Bil}^{(a)}(V)$ .

**ДОКАЗАТЕЛЬСТВО.** Положим  $B^{(s)}(x, y) = \frac{1}{2}(B(x, y) + B(y, x))$  и  $B^{(a)}(x, y) = \frac{1}{2}(B(x, y) - B(y, x))$ . Ясно, что  $B^{(s)}$  является симметричной билинейной формой,  $B^{(a)}$  антисимметричной, а  $B = B^{(s)} + B^{(a)}$ . Тот факт, что  $\text{Bil}^{(s)}(V) \cap \text{Bil}^{(a)}(V) = \{0\}$  очевиден (и тоже использует условие, что  $2 \neq 0$  в поле  $F$ ).  $\square$

**ОПРЕДЕЛЕНИЕ 1.2.** Функция  $Q : V \rightarrow F$  называется квадратичной формой, если существует билинейная форма  $B : V \times V \rightarrow F$  такая, что  $Q(x) = B(x, x)$ .

**ТЕОРЕМА 1.3** (поляризация квадратичной формы). Пусть  $Q$  – квадратичная форма на  $V$ , соответствующая билинейной форме  $B$ . Положим

$$B^{(s)}(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)).$$

Тогда  $B^{(s)}$  является симметризацией формы  $B$ , и  $Q(x) = B^{(s)}(x, x)$ .

Таким образом, мы имеем биекцию между множеством квадратичных и симметричных билинейных форм, которая на самом деле является изоморфизмом векторных пространств.

В некоторых ситуациях приходится рассматривать чуть более общий случай. Пусть  $\bar{\cdot} : F \rightarrow F$  – инволюция, т.е. автоморфизм поля порядка 2. Иными словами, для любых  $\alpha, \beta \in F$  выполнены равенства

- (1)  $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$ ;
- (2)  $\overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}$  и
- (3)  $\bar{\bar{\alpha}} = \alpha$ .

**ОПРЕДЕЛЕНИЕ 1.4.** Функция  $B : V \times V \rightarrow F$  называется полуторалинейной формой, если для любых  $x, y, z \in V$  и  $\alpha, \beta \in F$  имеют место равенства:

$$B(x\alpha + y\beta, z) = B(x, z)\bar{\alpha} + B(y, z)\bar{\beta} \text{ и } B(z, x\alpha + y\beta) = B(z, x)\alpha + B(z, y)\beta.$$

Полуторалинейная форма  $B$  называется эрмитовой, если  $B(x, y) = \overline{B(y, x)}$  для любых  $x, y \in V$ .

Симметричная билинейная форма является частным случаем эрмитовой формы, если инволюция тривиальна. Поэтому в дальнейшем, везде где можно, мы будем рассматривать эрмитовы формы вместо симметричных билинейных.

Для матрицы  $A \in M_{m,n}(F)$  обозначим  $A^* = \overline{A}^\top$ . Другими словами,  $a_{ij}^* = \overline{a_{ji}}$ .

**ПРЕДЛОЖЕНИЕ 1.5.** Пусть  $B$  полуторалинейная форма на  $V$ , а  $v = (v_1, \dots, v_n)$  – базис  $V$ . Тогда существует матрица  $A \in M_n(F)$  такая, что  $B(x, y) = x_v^* A y_v$  для любых  $x, y \in V$ . При этом  $a_{ij} = B(v_i, v_j)$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $x_v = (x_1, \dots, x_n)^\top$  и  $y_v = (y_1, \dots, y_n)^\top$ . Тогда

$$B(x, y) = B\left(\sum_{i=1}^n v_i x_i, \sum_{j=1}^n v_j y_j\right) = \sum_{i,j=1}^n \overline{x_i} B(v_i, v_j) y_j = x_v^* A y_v.$$

□

**ОПРЕДЕЛЕНИЕ 1.6.** Матрица  $A$ , построенная в предыдущей лемме, называется матрицей формы  $B$  в базисе  $v$  и обозначается через  $B_v$ . Матрицей квадратичной формы называется матрица ассоциированной с ней симметричной билинейной формы.

**ОПРЕДЕЛЕНИЕ 1.7.** Полуторалинейная форма называется вырожденной, если существует  $y \in V \setminus \{0\}$  такой, что  $B(y, x) = 0$  при всех  $x \in V$ .

Если форма вырождена, то  $y_v^* B_v x_v = 0$  для любого столбца  $x_v \in F^n$ , откуда система линейных уравнений  $z B_v = 0$  имеет ненулевое решение. Таким образом, вырожденность формы равносильна вырожденности матрицы этой формы (в любом базисе). Следовательно, вырожденность “слева” эквивалентна вырожденности “справа”:

$$\exists y \in V \setminus \{0\} \forall x \in V : B(x, y) = 0.$$

Ясно, что матрица квадратичной формы симметрична, т.е.  $B_v^\top = B_v$ , а матрица эрмитовой формы эрмитова, т.е.  $B_v^* = B_v$  (другое название такой матрицы самосопряженная).

**ЗАМЕЧАНИЕ 1.8.** Пусть  $F$  – поле с инволюцией, а  $K = \{\alpha \in F \mid \overline{\alpha} = \alpha\}$ . Нетрудно проверить, что  $K$  – подполе в  $F$ . Диагональные элементы и определитель любой эрмитовой матрицы  $A$  лежит в  $K$ . Действительно,  $A = A^* \implies \det A = \det A^* = \det \overline{A} = \overline{\det A}$ , а утверждение про диагональные элементы очевидно.

**ПРЕДЛОЖЕНИЕ 1.9.** Пусть  $B$  полуторалинейная форма на  $V$ , а  $u$  и  $v$  – базисы пространства  $V$ . Тогда  $B_v = C_{u \rightarrow v}^* B_u C_{u \rightarrow v}$ .

## 2. Диагонализация эрмитовой формы

В этом параграфе мы начинаем классификацию эрмитовых (квадратичных) форм. Сначала для этого надо определить, какие формы мы считаем одинаковыми. Вместо квадратичной формы можно всегда рассматривать соответствующую симметричную билинейную форму, являющуюся эрмитовой формой с тривиальной инволюцией поля. Поэтому в дальнейшем мы в основном формулируем все для эрмитовых форм.

**ОПРЕДЕЛЕНИЕ 2.1.** Если  $B$  – квадратичная (эрмитова) форма на векторном пространстве  $V$ , то пара  $(V, B)$  называется квадратичным (соотв. эрмитовым) пространством. Квадратичное или эрмитово пространство называется невырожденным, если форма  $B$  невырождена.

Изометрией эрмитовых пространств  $(V, B) \rightarrow (V', B')$  называется биективное линейное отображение  $L : V \rightarrow V'$ , обладающее свойством  $B'(L(x), L(y)) = B(x, y)$  для всех  $x, y \in V$ .

**ПРЕДЛОЖЕНИЕ 2.2.** Пусть  $B$  эрмитова форма на  $V$ . Положим

$$V^\perp = \{x \in V \mid B(x, y) = 0 \forall y \in V\}.$$

Если  $V = V^\perp \oplus U$  (заметим, что такое  $U$  всегда существует), то сужение формы  $B$  на  $U \times U$  невырождено. При этом, если  $V = V^\perp \oplus U'$ , то  $U$  и  $U'$  изометричны.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $x \in U$  такой, что  $B(x, y) = 0$  для любого  $y \in U$ . Любой вектор  $z \in V$  представляется в виде суммы  $z = y + w$  для некоторых  $y \in U$  и  $w \in V^\perp$ . Тогда  $B(x, z) = B(x, y) + B(x, w) = 0$ . Таким образом,  $x \in U \cap V^\perp = \{0\}$ , следовательно, сужение  $B$  на  $U \times U$  невырождено.

Пусть  $V^\perp \oplus U = V^\perp \oplus U' = V$ . Тогда для любого  $x' \in U'$  существует единственный  $x \in U$  такой, что  $x' \in x + V^\perp$  (такой  $x$  называется проекцией  $x'$  на  $U$  параллельно  $V^\perp$ ). Нетрудно проверить, что такое проектирование (т. е. сопоставление  $x' \mapsto x$ ) является линейным отображением, а обратным к нему является проектирование  $U$  на  $U'$  параллельно  $V^\perp$ . Так что это изоморфизм векторных пространств и

$$B(x', x') = B(x + w, x + w) = B(x, x) + B(w, x) + B(x, w) + B(w, w) = B(x, x),$$

откуда следует, что этот изоморфизм – изометрия.  $\square$

Задача теории эрмитовых форм – классификация всех конечномерных эрмитовых пространств над данным полем с точностью до изометрии. Ясно, что пространства разной размерности не могут быть изометричными. Очевидно также, что изометрия сохраняет подпространство  $V^\perp$  из предложения 2.2. Таким образом, достаточно классифицировать невырожденные эрмитовы пространства любой фиксированной размерности.

**ЛЕММА 2.3.** Эрмитовы пространства  $(V, B)$  и  $(V', B')$  изометричны тогда и только тогда, когда существуют такие базисы  $v$  и  $v'$  пространств  $V$  и  $V'$  соответственно, что  $B_v = B'_{v'}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $L : V \rightarrow V'$  – изометрия эрмитовых пространств, а  $v = (v_1, \dots, v_n)$  – базис пространства  $V$ . Тогда  $v' = (L(v_1), \dots, L(v_n))$  является базисом  $V'$ . По определению изометрии  $B'(L(x), L(y)) = B(x, y)$  для любых  $x, y \in V$ , откуда  $B_v = B'_{v'}$ .

Обратно, если  $B_v = B'_{v'}$ , то отображение  $L(x) = v'x_v$  является изометрией эрмитовых пространств. Действительно,  $L(x)_{v'} = x_v$ , поэтому

$$B'(L(x), L(y)) = L(x)_{v'}^* B'_{v'} L(y)_{v'} = x_v^* B_v y_v.$$

$\square$

**ЛЕММА 2.4.** Пусть  $B$  – ненулевая эрмитова форма на  $V$ . Тогда существует вектор  $x \in V$  такой, что  $B(x, x) \neq 0$ .

**ДОКАЗАТЕЛЬСТВО.** Так как форма ненулевая, существует пара векторов  $y, z \in V$  таких, что  $B(y, z) \neq 0$ . Если  $B(y, y)$  или  $B(z, z)$  не равно нулю, то все доказано. Иначе

$$B(y + \lambda z, y + \lambda z) = B(y, y) + B(z, z) + B(y, \lambda z) + B(\lambda z, y) = B(y, z)\lambda + \bar{\lambda} \cdot \overline{B(y, z)}$$

При  $\lambda = \overline{B(y, z)}$  получим  $B(y + \lambda z, y + \lambda z) = 2B(y, z)\overline{B(y, z)} \neq 0$ .  $\square$

**ТЕОРЕМА 2.5** (диагонализация матрицы эрмитовой формы). Для любой эрмитовой формы существует базис, в котором ее матрица диагональна.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $B$  – эрмитова форма на  $V$ . Мы должны доказать, что существует базис  $v$  пространства  $V$  ортогональный относительно формы  $B$ . По предложению 2.2  $V = V^\perp \oplus U$ , и сужение формы  $B$  на  $U \times U$  невырождено. Для доказательства достаточно найти  $B$ -ортогональный базис пространства  $U$  (вектора из  $V_0$  по определению ортогональны всем векторам).

Проведем доказательство индукцией по  $n = \dim U$ . Если  $n = 1$ , то доказывать нечего. Пусть  $n > 1$ . По предыдущей лемме существует  $u_1 \in U$  такой, что  $B(u_1, u_1) \neq 0$ . Дополним  $u_1$  до базиса  $u = (u_1, \dots, u_n)$  пространства  $U$ . Положим  $w_k = u_k - \frac{B(u_k, u_1)}{B(u_1, u_1)}u_1$  при  $2 \leq k \leq n$ . Тогда

$$B(w_k, u_1) = B\left(u_k - \frac{B(u_k, u_1)}{B(u_1, u_1)}u_1, u_1\right) = B(u_k, u_1) - \frac{B(u_k, u_1)}{B(u_1, u_1)}B(u_1, u_1) = 0.$$

Таким образом,  $u_1$   $B$ -ортогонален всем векторам  $w_k$  при  $2 \leq k \leq n$ , а, следовательно, и всему подпространству  $W = \langle w_2, \dots, w_n \rangle$ . По индукционному предположению существует  $B$ -ортогональный базис  $(v_2, \dots, v_n)$  подпространства  $W$ . Положив  $v_1 = u_1$ , получим ортогональный базис  $(v_1, \dots, v_n)$  пространства  $U$ .  $\square$

Покажем, как алгоритм диагонализации, приведенный в доказательстве теоремы, работает на практике. Пусть  $u$  – произвольный базис пространства  $V$ , и  $A = B_u$ . При переходе к другому базису матрица  $A$  меняется на  $C^*AC$ . Если  $C$  – трансвекция, то умножение справа на  $C$  производит преобразование Гаусса со столбцами, а умножение слева на  $C^*$  – такое же преобразование со строками, но с сопряженными коэффициентами. Если  $a_{11} = B(u_1, u_1) \neq 0$ , то

$$\begin{pmatrix} a_{11} & c \\ c^* & \star \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ -c^*/a_{11} & E \end{pmatrix} \begin{pmatrix} a_{11} & c \\ c^* & \star \end{pmatrix} \begin{pmatrix} 1 & -c/a_{11} \\ 0 & E \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ 0 & \star \end{pmatrix},$$

где  $c = (a_{12}, \dots, a_{1n})$ , а знак “ $\approx$ ” стоит между матрицами одной и той же формы в разных базисах. После этого мы работаем с получившейся матрицей  $(n-1) \times (n-1)$ , обозначенной звездочкой.

Если  $a_{11} = 0$ , но какой-нибудь другой диагональный элемент матрицы  $A$  не равен нулю, то проделываем аналогичные преобразования используя этот элемент вместо  $a_{11}$ . Если же все диагональные элементы равны нулю, но  $a_{ij} = \alpha \neq 0$  (такой элемент всегда найдется в ненулевой матрице), то по лемме 2.4 сумма  $u_i + u_j\bar{\alpha}$  не аннулируется квадратичной формой, ассоциированной с  $B$ . Значит достаточно прибавить  $u_j\bar{\alpha}$  к  $u_i$  и проделать операции, как в вынесенной формуле. Матрица перехода между такими базисами отличается от единичной только в позиции  $(j, i)$ , в которой стоит  $\bar{\alpha}$ . Проиллюстрируем сказанное на примере матрицы  $2 \times 2$  с  $a_{11} = a_{22} = 0$ .

$$\begin{pmatrix} 0 & \alpha \\ \bar{\alpha} & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ \bar{\alpha} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \bar{\alpha} & 1 \end{pmatrix} = \begin{pmatrix} 2\alpha\bar{\alpha} & \alpha \\ \bar{\alpha} & 0 \end{pmatrix} \approx \begin{pmatrix} 2\alpha\bar{\alpha} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix}.$$

Пусть  $Q$  – квадратичная форма. Если матрица  $Q_v$  диагональна, а  $u_k = v_k\lambda_k$ , то матрица  $Q_u$  также диагональна, причем ее диагональные элементы отличаются от диагональных элементов  $Q_v$  умножением на  $\lambda_k^2$ . Таким образом, для невырожденных форм, играют роль только классы вычетов диагональных элементов  $Q_v$  в  $F^*/(F^*)^2$ . В частности, если из любого элемента поля  $F$  можно извлечь квадратный корень, то классификация совсем простая.

**ОПРЕДЕЛЕНИЕ 2.6.** Поле  $F$  называется квадратично замкнутым, если для любого  $\alpha \in F$  уравнение  $x^2 = \alpha$  имеет хотя бы одно решение. В частности, алгебраически замкнутое поле является квадратично замкнутым.

**СЛЕДСТВИЕ 2.7.** Любые два невырожденных квадратичных пространства одинаковой размерности над квадратично замкнутым полем изоморфны.

### 3. Вещественные квадратичные формы

В этом параграфе  $V$  обозначает вещественное векторное пространство размерности  $m$ . В общем случае неверно, что любые две диагональные матрицы  $Q_u$  и  $Q_v$  квадратичной формы  $Q$  отличаются только перестановкой диагональных элементов и умножением их на квадраты. Однако, для поля вещественных чисел это так, и роль играют только знаки диагональных элементов.

**ОПРЕДЕЛЕНИЕ 3.1.** Сигнатурой последовательности вещественных чисел называется пара чисел  $(p, n)$ , где  $p$  – количество положительных среди этих чисел, а  $n$  – отрицательных.

Сигнатурой вещественной диагональной матрицы называется сигнатура последовательности ее диагональных элементов.

**ЛЕММА 3.2.** Пусть  $B$  – симметричная билинейная форма на  $V$ , а  $v_1, \dots, v_k \in V$ . Если  $B(v_i, v_i) > 0$  при всех  $i$ , а  $B(v_i, v_j) = 0$  при всех  $j \neq i$ , то форма  $B$  положительно определена на подпространстве  $\langle v_1, \dots, v_k \rangle$ .

**ТЕОРЕМА 3.3** (закон инерции квадратичных форм). Пусть  $Q$  – квадратичная форма на вещественном векторном пространстве  $V$ , а  $u, v$  – базисы  $V$  такие, что матрицы  $Q_u$  и  $Q_v$  диагональны. Тогда сигнатуры матриц  $Q_u$  и  $Q_v$  равны.

**ДОКАЗАТЕЛЬСТВО.** По предложению 2.2 можно считать, что форма  $Q$  невырождена. Пусть  $(p_u, n_u)$  – сигнатура матрицы  $Q_u$ , а  $(p_v, n_v)$  – сигнатура матрицы  $Q_v$ . Перенумеровав при необходимости базисные элементы, можно считать, что положительные диагональные элементы матриц  $Q_u$  и  $Q_v$  стоят выше (и левее) отрицательных.

Предположим, что  $p_u > p_v$ . По предыдущей лемме форма  $Q$  положительно определена на подпространстве  $U = \langle u_1, \dots, u_{p_u} \rangle$ . Аналогично,  $Q$  отрицательно определена на  $W = \langle v_{p_v+1}, \dots, v_m \rangle$ . Но по теореме о размерности суммы и пересечения

$$\dim U \cap W = p_u + (m - p_v) - \dim(U + W) \geq p_u + (m - p_v) - m = p_u - p_v > 0.$$

Следовательно,  $U \cap W \neq \{0\}$ , но форма  $Q$  одновременно положительно и отрицательно определена на этом подпространстве. Противоречие показывает, что неравенство  $p_u > p_v$  невозможно. По аналогичным причинам невозможно и обратное неравенство, следовательно,  $p_u = p_v$ .  $\square$

В соответствие с законом инерции можно дать следующее определение. Сигнатурой квадратичной формы называется сигнатура ее матрицы в таком базисе, в котором эта матрица диагональна. Сигнатуру квадратичной формы  $Q$  будем обозначать через  $\text{Sign } Q$ .

**СЛЕДСТВИЕ 3.4** (классификация вещественных квадратичных форм). Два вещественных квадратичных пространства  $(V, Q)$  и  $(V', Q')$  изометричны тогда и только тогда, когда  $\dim V = \dim V'$ , а  $\text{Sign } Q = \text{Sign } Q'$ .

Пусть  $A$  – квадратная матрица. Определитель главной подматрицы

$$\begin{vmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{vmatrix}$$

называется

главным минором  $k$ -ого порядка матрицы  $A$ . Обозначим его для краткости  $\Delta_k$ . По определению положим  $\Delta_0 = 1$ . Напомним, что матрица называется унитарной, если она треугольна с 1 на главной диагонали.

**ТЕОРЕМА 3.5** (критерий Сильвестра). Пусть  $Q$  – квадратичная форма на  $V$ , а  $A$  – матрица формы  $Q$ . Предположим, что главные миноры  $\Delta_1, \dots, \Delta_m$  матрицы  $A$  не равны нулю. Тогда сигнатура формы  $Q$  равна сигнатуре последовательности  $(\frac{\Delta_1}{\Delta_0}, \dots, \frac{\Delta_m}{\Delta_{m-1}})$ .

В частности, форма положительно определена тогда и только тогда, когда все ее главные миноры больше 0.

**ДОКАЗАТЕЛЬСТВО.** По лемме 12.6 главы 2 матрица  $A$  лежит в главной клетке Гаусса, т.е.  $A = BDC$ , где  $B$  – нижняя унитарная матрица,  $C$  – верхняя унитарная, а  $D$  – диагональная. Так как  $A$  симметрична, то  $BDC = (BDC)^T = C^T D B^T$ , откуда  $B^{-1} C^T D = DC (B^T)^{-1}$ . Но последняя матрица одновременно нижняя и верхняя треугольная, следовательно  $B^{-1} C^T = E$ , т.е.  $B = C^T$ . Это означает, что  $D$  – матрица той же квадратичной формы  $Q$  в другом базисе, а ее сигнатура совпадает с сигнатурой формы  $Q$ .



Аналогично лемме 12.5 главы 2 главные миноры матриц  $A$  и  $D$  совпадают. Действительно, при умножении матрицы слева на унитарную главные подматрицы также умножаются на унитарные (это просто блочное умножение матриц) и, значит, их определители не меняются. Следовательно,  $\Delta_k = d_{11} \dots d_{kk}$ , откуда  $d_{kk} = \Delta_k / \Delta_{k-1}$ . Таким образом, последовательность из формулировке равна последовательности диагональных элементов матрицы  $D$ .

Если все главные миноры положительны, то в любой диагонализации формы  $Q$  все диагональные элементы положительны. По лемме 3.2 из этого следует, что форма положительно определена. Обратно, если  $Q$  положительно определена, то все диагональные элементы матрицы этой формы в любом базисе положительны.  $\square$

**ЗАМЕЧАНИЕ 3.6.** Рассмотрим эрмитову форму  $B$  на комплексном векторном пространстве (инволюция – комплексное сопряжение). В соответствии с замечанием 1.8 диагональные элементы и главные миноры любой матрицы этой формы лежат в  $\mathbb{R}$ , поэтому для этой формы имеют смысл все утверждения настоящего параграфа. На самом деле все эти утверждения верны, а доказательства повторяют доказательства для вещественного случая с необходимыми уточнениями.

#### 4. Пространства со скалярным произведением

В этом параграфе мы рассмотрим случай вещественных (комплексных) векторных пространств с положительно определенной симметричной билинейной (соотв. эрмитовой) формой, при этом инволюция на поле комплексных чисел – это обычное комплексное сопряжение. Можно рассматривать эти 2 случая одновременно, считая, что  $V$  – векторное пространство над полем  $F = \mathbb{R}$  или  $\mathbb{C}$ , а в вещественном случае инволюция тривиальна. Для эрмитовой формы  $B$  и  $x \in V$  имеем  $B(x, x) = \overline{B(x, x)}$ , откуда  $B(x, x) \in \mathbb{R}$ .

**ОПРЕДЕЛЕНИЕ 4.1.** Эрмитова форма называется положительно определенной, если  $B(x, x) > 0$  для любого вектора  $x \neq 0$ . Положительно определенная эрмитова форма называется (эрмитовым) скалярным произведением. В вещественном случае эрмитовость означает симметричность и билинейность, а скалярное произведение называется евклидовым. Конечномерное векторное пространство со скалярным произведением называется евклидовым или (классическим) эрмитовым пространством.

Квадратичная форма  $Q$  над произвольным полем называется анизотропной, если  $Q(x) \neq 0$  при  $x \neq 0$ . Аналогично, мы будем говорить, что эрмитова форма  $B$  анизотропна, если  $B(x, x) \neq 0$  при  $x \neq 0$ . В частности, скалярное произведение, является анизотропной формой. Позже мы узнаем, что для классификации квадратичных форм достаточно классифицировать анизотропные формы, так что они занимают особое место в теории квадратичных форм. По определению скалярное произведение является анизотропной формой, поэтому все утверждения, в которых не используется специфика поля вещественных или комплексных чисел<sup>1</sup> будут доказаны для произвольных анизотропных форм.

В дальнейшем скалярное произведение будет обозначаться просто  $(x, y)$  вместо  $B(x, y)$ , а матрица этой формы будет называться матрицей Грама и обозначаться через  $\Gamma$  или  $\Gamma_v$ , где  $v$  – базис. Соответствующая квадратичная форма будет обозначаться через  $\|x\|^2 = (x, x)$ . Другими словами,  $\|x\| = \sqrt{(x, x)}$ , что имеет смысл за счет положительной определенности.

Как следует из предложения 1.5, любое скалярное произведение на  $F^n$  имеет вид  $(x, y) = x^* \Gamma y$ , где  $\Gamma \in M_n(F)$  – матрица Грама в стандартном базисе. Эта формула всегда задает полуторалинейную форму, эрмитовость такой формы равносильна эрмитовости матрицы  $\Gamma$ , а положительная определенность, как мы узнаем чуть позже, – положительности собственных чисел  $\Gamma$ . В случае  $\Gamma = E$  такое скалярное произведение называется стандартным.

**ТЕОРЕМА 4.2.** Пусть  $V$  – векторное пространство (не обязательно конечномерное) со скалярным произведением. Тогда для любых  $x, y \in V$  имеют место неравенства:

<sup>1</sup>Эта специфика чаще всего проявляется в наличии неравенств.

- (1)  $|(x, y)|^2 \leq \|x\|^2 \|y\|^2$  (неравенство Коши–Буняковского–Шварца – КБШ);  
 (2)  $\|x + y\| \leq \|x\| + \|y\|$  (неравенство треугольника).

ДОКАЗАТЕЛЬСТВО. (1). Если  $y = 0$ , то обе части равенства равны 0, поэтому можно считать, что  $y \neq 0$ .  $0 \leq \|x + y\lambda\|^2 = \|x\|^2 + (x, y)\lambda + \bar{\lambda}(y, x) + \|y\|^2|\lambda|^2$ . Положим  $\lambda = -\frac{(y, x)}{(y, y)}$ . Тогда последнее выражение равно  $\|x\|^2 - \frac{(x, y)(y, x) + \overline{(y, x)}(y, x)}{(y, y)} + \frac{\|y\|^2|(y, x)|^2}{\|y\|^4} = \|x\|^2 - \frac{|(y, x)|^2}{\|y\|^2} \geq 0$ . После домножения на знаменатель (который больше 0) получаем неравенство КБШ.

(2). Возводя неравенство треугольника в квадрат, получаем  $(x + y, x + y) \leq \|x\|^2 + \|y\|^2 + 2\|x\|\|y\|$ . Раскрывая скобки в левой части и сокращая  $\|x\|^2 + \|y\|^2$  имеем  $(x, y) + (y, x) \leq 2\|x\|\|y\|$ . Так как  $(y, x) = \overline{(x, y)}$ , левая часть равна  $2\operatorname{Re}(x, y)$ . Но  $\operatorname{Re}(x, y) \leq |(x, y)| \leq \|x\| \cdot \|y\|$  по неравенству КБШ, откуда следует последнее неравенство.  $\square$

Следующие несколько утверждений верны для произвольной анизотропной эрмитовой формы  $B$ .

**ЛЕММА 4.3.** *Набор ненулевых попарно  $B$ -ортогональных векторов линейно независим.*

**ТЕОРЕМА 4.4** (ортогонализация Грама–Шмидта). *Пусть  $B$  – анизотропная форма на  $V$ ,  $u_1, \dots, u_n \in V$ . Положим*

$$\begin{aligned} v_1 &= u_1 \\ v_2 &= u_2 - v_1 \frac{B(v_1, u_2)}{B(v_1, v_1)} \\ &\dots\dots\dots \\ v_n &= u_n - \sum_{i=1}^{n-1} v_i \frac{B(v_i, u_n)}{B(v_i, v_i)} \end{aligned}$$

(если  $v_i = 0$ , то соответствующее слагаемое отсутствует; строго говоря, надо было бы писать, что коэффициент при  $v_i$  в формуле для  $v_k$  равен 0, в случае  $v_i = 0$ , и  $\frac{B(v_i, u_k)}{B(v_i, v_i)}$  в противном случае). Тогда для любых  $i, j, k \in \{1, \dots, n\}$ ,  $i \neq j$  выполнены следующие утверждения.

- (1)  $B(v_i, v_j) = 0$ .
- (2)  $\langle u_1, \dots, u_k \rangle = \langle v_1, \dots, v_k \rangle$ .
- (3) Если  $u_1, \dots, u_k$  линейно независимы, то и  $v_1, \dots, v_k$  линейно независимы, в частности,  $v_m \neq 0$  при всех  $m = 1, \dots, k$ .
- (4) Если  $u_k \in \langle u_1, \dots, u_{k-1} \rangle$ , то  $v_k = 0$ .
- (5) Если  $(u_1, \dots, u_n)$  – система образующих  $V$ , то ненулевые из векторов  $v_1, \dots, v_n$  образуют базис.
- (6) Если  $(u_1, \dots, u_n)$  – базис  $V$ , то  $(v_1, \dots, v_n)$  –  $B$ -ортогональный базис  $V$ .

Процесс ортогонализации – конструктивный способ построения ортогонального базиса пространства, существование которого мы уже доказали для произвольной эрмитовой формы в теореме 2.5. На самом деле доказательство теоремы 2.5 для анизотропной формы совпадает с процессом ортогонализации. В случае скалярного произведения можно сделать нормы всех базисных векторов равными 1. Такой базис будет называться ортонормированным.

В следующем утверждении в качестве  $B$  традиционно рассматривается стандартное скалярное произведение на  $F^m$ , хотя на самом деле это не имеет никакого значения. Для доказательства достаточно применить процесс ортогонализации к столбцам матрицы  $A$ .

**СЛЕДСТВИЕ 4.5** (QR-разложение). *Пусть  $B$  – анизотропная эрмитова форма на  $F^m$ . Для любой матрицы  $A \in M_{m,n}(F)$  существует матрица  $Q \in M_{m,n}(F)$  с  $B$ -ортогональными столбцами и верхняя унитарная матрица  $R \in M_n(F)$  такие, что  $A = QR$ .*

Для подпространства  $U \leq V$  определим ортогональное дополнение  $U$  формулой

$$U^{\perp} = U^{\perp} = \{x \in V \mid B(y, x) = 0 \forall y \in U\}.$$

Нетрудно видеть, что сужение формы  $B$  на  $U$  невырождено тогда и только тогда, когда  $U \cap U^{\perp} = \{0\}$ . В конечномерном пространстве из подсчета размерностей сразу следует, что в этом случае ортогональное дополнение является и прямым дополнением.

**ПРЕДЛОЖЕНИЕ 4.6.** Пусть  $B$  невырожденная эрмитова форма на конечномерном пространстве  $V$ , а  $U \leq V$ . Тогда  $\dim U^{\perp} = \dim V - \dim U$  и  $(U^{\perp})^{\perp} = U$ .

Если сужение  $B$  на  $U$  невырождено, то  $V = U \oplus U^{\perp}$ . В частности, если  $B$  анизотропна, то равенства выполнены для любого подпространства  $U$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $u = (u_1, \dots, u_k)$  – базис  $U$ , а  $L : V \rightarrow F^k$  – линейное отображение, заданное формулой  $L(x) = (B(u_1, x), \dots, B(u_k, x))^T$ . Ясно, что  $U^{\perp} = \text{Ker } L$ . Если  $v$  – базис  $V$ , то можно записать наше отображение в координатной форме:  $L(x) = CB_v x_v$ , где  $C = ((u_1)_v, \dots, (u_k)_v)^T$ . Так как набор  $u$  линейно независим, ранг матрицы  $C$  равен  $k$ . Так как  $B$  невырождена, матрица  $B_v$  обратима и умножение на нее не меняет ранга матрицы. Следовательно, размерность образа оператора  $L$  равна  $k$ , а по теореме о размерности ядра и образа  $\dim \text{Ker } L = \dim V - k$ .

Очевидно, что  $U \leq (U^{\perp})^{\perp}$ . С другой стороны, из доказанного следует, что их размерности равны, откуда вытекает второе равенство.

Если  $B|_U$  невырождена, то  $U \cap U^{\perp} = \{0\}$ , откуда  $U \oplus U^{\perp} \leq V$ . Но мы уже доказали, что  $\dim U + \dim U^{\perp} = \dim V$ , следовательно,  $U \oplus U^{\perp} = V$ .  $\square$

Вернемся к ситуации, когда форма анизотропна. Тогда другое доказательство того, что  $V = U + U^{\perp}$  дает процесс ортогонализации, примененный к последовательности  $(u_1, \dots, u_k, x)$ , где  $x$  произвольный элемент из  $V$ . Действительно, на последнем шаге мы получим вектор  $y \in x + U$ , ортогональный  $U$ , откуда  $x \in y + U \subseteq U^{\perp} + U$ .

Из последнего предложения следует, что каждый вектор  $x \in V$  единственным образом представляется в виде  $x = z + y$ , где  $z \in U$ , а  $y \in U^{\perp}$ . В этом случае элемент  $z$  называется ортогональной проекцией  $x$  на  $U$ . Мы будем обозначать его  $\text{pr}_U x$ . Проекция на вектор – это проекция на подпространство, порожденное этим вектором. Легко видеть, что

$$\text{pr}_z x = \frac{(z, x)}{(z, z)} z.$$

В этих терминах формулу процесса ортогонализации можно произнести следующим образом: новый вектор  $v_k$  равен разности старого  $u_k$  и его проекций на все вектора, найденные на предыдущих шагах.

Обратите внимание, что если  $u$  является ортогональным базисом подпространства  $U$ , то  $\text{pr}_U x = \sum_{j=1}^k \text{pr}_{u_j} x$ , если же базис  $u$  не ортогонален, то такое равенство может выполняться только случайно.<sup>2</sup>

**ПРЕДЛОЖЕНИЕ 4.7** (равенство Парсеваля и неравенство Бесселя). Пусть  $u_1, \dots, u_k$  – ортогональный набор ненулевых векторов пространства  $V$  со скалярным произведением, а  $x \in V$ . Обозначим через  $U$  линейную оболочку векторов  $u_1, \dots, u_k$ . Тогда

$$(1) \text{pr}_U x = \sum_{j=1}^k \text{pr}_{u_j} x = \sum_{j=1}^k \frac{(u_j, x)}{(u_j, u_j)} u_j;$$

$$(2) \|x\|^2 \geq \|\text{pr}_U x\|^2 = \sum_{j=1}^k \frac{|(u_j, x)|^2}{(u_j, u_j)} \text{ (неравенство Бесселя);}$$

$$(3) \text{ равенство в последней формуле имеет место тогда и только тогда, когда } x \in U \text{ (равенство Парсеваля).}$$

<sup>2</sup> Упражнение. Найдите условие на  $u$  равносильное существованию ненулевого  $x$ , для которого равенство верно.

ДОКАЗАТЕЛЬСТВО. Пусть  $z = \text{pr}_U x = \sum_{j=1}^k u_j \alpha_j$ . Тогда  $x = z + y = \sum_{j=1}^k u_j \alpha_j + y$  для некоторого  $y \in U^\perp$ . Домножая выражение для  $x$  скалярно (слева) на  $u_l$ , получаем формулу для  $\alpha_l$ , откуда следует первый пункт предложения.

Так как набор  $u_1, \dots, u_k$  ортогонален, то скалярный квадрат правой части выражения для  $z$  равен сумме скалярных квадратов слагаемых. Следовательно, правая часть неравенства Бесселя равна  $\|z\|^2$ . Но  $\|x\|^2 = \|z + y\|^2 = \|z\|^2 + \|y\|^2 \geq \|z\|^2$ , причем равенство достигается, только если  $y = 0$ .  $\square$

Неравенство Бесселя является всего лишь выражением того факта, что длина гипотенузы не меньше длины катета. Следующее утверждение сравнивает длину гипотенузы того же прямоугольного треугольника с длиной другого катета.

**ПРЕДЛОЖЕНИЕ 4.8.** Для любого  $u \in U$  выполнено неравенство  $\|x - u\| \geq \|x - \text{pr}_U x\|$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $x = z + y$ , где  $z = \text{pr}_U x$ , а  $y \in U^\perp$ . Тогда для любого  $u \in U$ :

$$\|x - u\|^2 = \|y + (z - u)\|^2 = \|y\|^2 + \|z - u\|^2 \geq \|y\|^2 = \|x - \text{pr}_U x\|^2.$$

$\square$

До конца параграфа  $V = F^m$  пространство со стандартным скалярным произведением.

**ЛЕММА 4.9.** Пусть  $A \in M_{m,n}(F)$  – матрица с линейно независимыми столбцами. Тогда матрица  $A^*A$  невырождена.

ДОКАЗАТЕЛЬСТВО. Если  $U \leq V$  – подпространство, порожденное столбцами матрицы  $A$ , то  $A^*A$  – матрица Грама сужения скалярного произведения на  $U \times U$ . Так как наше скалярное произведение невырождено на любом подпространстве, то эта матрица невырождена.  $\square$

**ТЕОРЕМА 4.10** (метод наименьших квадратов). Пусть  $A \in M_{m,n}(F)$  – матрица с линейно независимыми столбцами, а  $b \in F^m$ . Тогда  $\|Ax - b\|$  минимальна, если  $x \in F^n$  удовлетворяет уравнению  $A^*Ax = A^*b$ . (заметим, что по предыдущей лемме такой вектор  $x$  всегда существует и единственный).

ДОКАЗАТЕЛЬСТВО. Для любого  $y \in F^n$

$$(Ay, Ax - b) = y^*(A^*Ax - A^*b) = 0.$$

Таким образом, вектор  $Ax - b$  ортогонален подпространству, порожденному столбцами матрицы  $A$ , т. е.  $Ax$  является ортогональной проекцией  $b$  на это подпространство. Теперь результат следует из предложения 4.8.  $\square$

## 5. Нормальные операторы

**ОПРЕДЕЛЕНИЕ 5.1.** Пусть  $V$  – векторное пространство над произвольным полем  $F$ . Множество линейных отображений из  $V$  в  $F$

$$V^* := \text{Hom}_F(V, F)$$

с поточечными операциями называется пространством, двойственным к  $V$  (dual space).

Пусть  $U$  и  $V$  – векторные пространства, а  $L : U \rightarrow V$  – линейное отображение. Тогда сопряженное отображение  $L^* : V^* \rightarrow U^*$  задается формулой  $L^*(\varphi) = \varphi \circ L$ .

Если  $V$  конечномерно, то при помощи выбора базиса его можно отождествить с  $F^n$ . Тогда любое линейное отображение  $V \rightarrow F$  – это умножение слева на строку длины  $n$ , следовательно,  $V^*$

отождествляется с  ${}^nF$ . Так как эти пространства имеют одинаковую размерность, то они изоморфны.<sup>3</sup> В случае бесконечномерных пространств это совсем не так, например базис пространства, двойственного к счетномерному, имеет мощность континуум.

Далее на протяжении этого параграфа пространство  $V$  конечномерно. Любая невырожденная полуторалинейная форма  $B$  задает полулинейную биекцию пространства на его сопряженное. А именно, для  $x \in V$  положим  $\varphi_x(y) = B(x, y)$ . Тогда  $\varphi_x \in V^*$ , а  $x \mapsto \varphi_x$  — искомая биекция. Действительно, невырожденность формы  $B$  равносильна тривиальности ядра этого отображения; ясно, что отображение полулинейно, т. е.  $\varphi_{x+z} = \varphi_x + \varphi_z$  и  $\varphi_{\alpha x} = \bar{\alpha}\varphi_x$ ; а сюръективность следует из теоремы о размерности ядра и образа, которая верна и для полулинейных отображений. Большую часть утверждений настоящего параграфа можно сформулировать для эрмитовых пространств над произвольным полем. Мы, однако, оставим эти обобщения в качестве упражнения и будем рассматривать только евклидовы и классические эрмитовы пространства.

Если  $U$  и  $V$  эрмитовы пространства, то мы можем отождествить их со своими двойственными при помощи полулинейной биекции, определенной в предыдущем абзаце. Тогда  $L^*$  отождествляется с линейным отображением  $L^* : V \rightarrow U$ , для которого следующая диаграмма коммутативна.

$$\begin{array}{ccc} V & \xrightarrow{L^*} & U \\ x \mapsto \varphi_x \downarrow & & \downarrow y \mapsto \varphi_y \\ V^* & \xrightarrow{L^*} & U^* \end{array}$$

Обратите внимание, что пока мы различаем  $L^* : V^* \rightarrow U^*$  и  $L^* : V \rightarrow U$  (у них разные символы “звездочка”).

**ЛЕММА 5.2.** *Определенное выше отображение  $L^*$  удовлетворяет равенству*

$$(8) \quad (L^*(x), y)_U = (x, L(y))_V$$

и  $L^{**} = L$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $x \in V$ . Тогда коммутативность диаграммы говорит, что  $L^*(\varphi_x) = \varphi_{L^*(x)}$ . Применяя обе части равенства к элементу  $y \in U$  получим

$$L^*(\varphi_x)(y) = \varphi_x(L(y)) = (x, L(y))_V = \varphi_{L^*(x)}(y) = (L^*(x), y)_U.$$

Далее,

$$(x, L(y))_V = (L^*(x), y)_U = \overline{(y, L^*(x))_U} = \overline{(L^{**}(y), x)_V} = (x, L^{**}(y))_V.$$

Так как последнее равенство выполнено для любого  $x \in V$ , а скалярное произведение невырождено, то  $L(y) = L^{**}(y)$  для любого  $y \in U$ , что и означает  $L^{**} = L$ .  $\square$

Последняя лемма говорит в частности, что отображение  $L^*$ , удовлетворяющее равенству (8) существует. Единственность такого отображения очевидна (см. конец доказательства предыдущей леммы). Таким образом, мы получаем 2 равносильных определения оператора  $L^*$ , ни одно из которых не выглядит конструктивным, так как в каждом из них надо искать вектор, скалярное умножение на который реализует данный линейный функционал. В действительности же, для нахождения такого вектора надо просто решить систему линейных уравнений.

В дальнейшем, мы меняем обозначение  $L^*$  на общепринятое  $L^*$ . Какой из операторов имеется в виду  $V \rightarrow U$  или  $V^* \rightarrow U^*$ , всегда будет ясно из контекста. Обратите внимание, что первая версия  $L^*$  употребляется, только если зафиксированы изоморфизмы между пространствами и сопряженными к ним, в частности, если  $U$  и  $V$  — эрмитовы (квадратичные) пространства или если там зафиксированы базисы. В этом и следующем параграфах  $L^*$  обозначает оператор  $V \rightarrow U$ .

**ЛЕММА 5.3.** *Пусть  $u$  — ортонормированный базис эрмитова пространства  $V$ , а  $L : V \rightarrow V$ . Тогда  $(L^*)_u = (L_u)^*$ .*

<sup>3</sup>Это первый пример в нашем курсе неканонического изоморфизма, т. е. изоморфизма, который зависит от какого-то выбора.

**ДОКАЗАТЕЛЬСТВО.**  $(y, L^*(x)) = (L(y), x)$ . Так как базис  $u$  ортонормирован, то  $(z, t) = z_u^* t_u$ . Используя это и определение матрицы оператора получим  $y_u^*(L^*)_u x_u = (L_u y_u)^* x_u = y_u^*(L_u)^* x_u$ . Так как  $x_u$  и  $y_u$  – произвольные столбцы, получаем требуемое равенство матриц.  $\square$

**ОПРЕДЕЛЕНИЕ 5.4.** Оператор  $L : V \rightarrow V$  называется самосопряженным или эрмитовым, если  $L^* = L$ .

Изоморфизм  $L : U \rightarrow V$  называется унитарным или изометрией, если  $L^* = L^{-1}$ .

Оператор  $L : V \rightarrow V$  называется нормальным, если  $L^* L = L L^*$ .

Таким образом, нормальные операторы являются одновременным обобщением таких важных типов, как самосопряженные и унитарные операторы (а на самом деле еще и косоэрмитовы, т.е. те, для которых  $L^* = -L$ ). Следующее утверждение говорит о связи эрмитовых форм и самосопряженных операторов.

**ЛЕММА 5.5.** Пусть  $L : V \rightarrow V$  – линейный оператор, а  $B = B_L$  – полуторалинейная форма, заданная равенством  $B(x, y) = (x, L(y))$ . Оператор  $L$  является самосопряженным тогда и только тогда, когда форма  $B$  эрмитова. При этом  $B_u = L_u$  в любом ортонормированном базисе  $u$ .

**ТЕОРЕМА 5.6.** Для любого нормального оператора существует ортонормированный базис из собственных векторов.

Собственные вектора нормального оператора, соответствующие различным собственным числам, ортогональны.

Собственные числа самосопряженного оператора вещественны.

Собственные числа унитарного оператора по модулю равны 1.

Доказательство первого утверждения опирается на 2 леммы.

**ЛЕММА 5.7.** Если  $AB = BA$ , то собственное подпространство оператора  $A$  инвариантно относительно  $B$ .

**ДОКАЗАТЕЛЬСТВО.** Если  $Ax = \lambda x$ , то  $A(Bx) = B(Ax) = B(\lambda x) = \lambda Bx$ , т.е.  $Bx$  принадлежит тому же собственному подпространству, что и  $x$ .  $\square$

**ЛЕММА 5.8.** Если  $U \leq V$  инвариантно относительно оператора  $L : V \rightarrow V$ , то  $U^\perp$  инвариантно относительно  $L^*$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $x \in U^\perp$ , а  $y$  – произвольный вектор из  $U$ . Так как  $L(y) \in U$ , то  $(L^*(x), y) = (x, L(y)) = 0$ . Таким образом,  $L^*(x) \in U^\perp$ .  $\square$

**ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5.6.** Пусть  $L$  – нормальный оператор в эрмитовом пространстве  $V$ . Проведем доказательство индукцией по  $\dim V$ . Так как  $\mathbb{C}$  алгебраически замкнуто, то существует хотя бы один корень характеристического многочлена, следовательно, хотя бы одно ненулевое собственное подпространство  $V_\lambda$ . Так как  $LL^* = L^*L$ , то по лемме 5.7  $V_\lambda$  инвариантно относительно  $L^*$ . Теперь по лемме 5.8  $V_\lambda^\perp$  инвариантно относительно  $L^{**} = L$ . Размерность пространства  $V_\lambda^\perp$  строго меньше  $\dim V$ , поэтому к нему можно применить индукционное предположение. Выберем ортогональный базис  $(v_1, \dots, v_k)$  подпространства  $V_\lambda^\perp$  из собственных векторов оператора  $L$  и ортогональный базис  $(v_{k+1}, \dots, v_n)$  подпространства  $V_\lambda$ . Тогда  $(v_1, \dots, v_n)$  – искомый базис пространства  $V$ .

Из доказанного следует, что собственные подпространства нормального оператора попарно ортогональны, откуда вытекает второе утверждение.

Пусть  $L(x) = \lambda x$  для некоторого  $x \neq 0$ . Если  $L = L^*$ , то

$$\bar{\lambda}(x, x) = (L(x), x) = (x, L(x)) = \lambda(x, x),$$

откуда  $\bar{\lambda} = \lambda$ , т.е.  $\lambda \in \mathbb{R}$ .

Аналогично, если  $L^{-1} = L^*$ , то

$$\bar{\lambda}\lambda(x, x) = (L(x), L(x)) = (x, x).$$

Сокращая на  $(x, x)$ , получаем  $|\lambda|^2 = \bar{\lambda}\lambda = 1$ .  $\square$

На самом деле условия, собранные в теореме 5.6 являются характеристизациями соответствующих типов операторов. Следствие в одну сторону доказано в теореме, а обратное сразу следует из леммы 5.3.

**СЛЕДСТВИЕ 5.9.** *Оператор  $L$  является нормальным тогда и только тогда, когда существует ортогональный базис из его собственных векторов. При этом он самосопряжен тогда и только тогда, когда его собственные числа вещественные, и является унитарным тогда и только тогда, когда его собственные числа по модулю равны 1.*

Следующее утверждение является частным случаем спектральной теоремы, которая говорит о строении самосопряженных операторов в гильбертовых пространствах. Она формулируется в терминах ортогональных проекторов.

**ОПРЕДЕЛЕНИЕ 5.10.** Оператор  $P : V \rightarrow V$  называется проектором, если  $P^2 = P$ . Если  $\text{Ker } P \perp \text{Im } P$ , то проектор  $P$  называется ортогональным.

Если  $P$  – проектор в произвольном векторном пространстве  $V$ , то  $V = \text{Ker } P \oplus \text{Im } P$ . Действительно,  $P(x - P(x)) = 0$ , т. е.  $x - P(x) \in \text{Ker } P$ , следовательно,  $x = x - P(x) + P(x) \in \text{Ker } P + \text{Im } P$ ; с другой стороны,  $P(x) \in \text{Ker } P \implies P(x) = P^2(x) = 0$ , откуда  $\text{Im } P \cap \text{Ker } P = \{0\}$ . Отсюда следует, что для ортогонального проектора  $P$  имеет место равенство  $\text{Ker } P = (\text{Im } P)^\perp$ . Нетрудно видеть, что ортогональный проектор является самосопряженным оператором.

**СЛЕДСТВИЕ 5.11** (спектральная теорема). *Оператор  $L$  в евклидовом (эрмитовом) пространстве  $V$  является самосопряженным тогда и только тогда, когда он представляется в виде линейной комбинации ортогональных проекторов на попарно ортогональные подпространства с вещественными коэффициентами.*

Эти ортогональные подпространства можно считать одномерными, порожденными собственными векторами  $u_1, \dots, u_n$  оператора  $L$ . Тогда

$$L = \sum_{k=1}^n \lambda_k P_k, \text{ где } P_k(x) = \text{pr}_{u_k} x = \frac{(u_k, x)}{(u_k, u_k)} u_k.$$

**ДОКАЗАТЕЛЬСТВО.** Очевидно, что линейная комбинация самосопряженных операторов с вещественными коэффициентами является самосопряженным оператором. Обратно, по теореме 5.6 существует ортогональный базис из собственных векторов  $u_1, \dots, u_n$  оператора  $L$ . По формуле “координаты в ортогональном базисе” (теорема 4.7(1))  $x = \sum_{k=1}^n \frac{(u_k, x)}{(u_k, u_k)} u_k$ , откуда

$$L(x) = \sum_{k=1}^n \frac{(u_k, x)}{(u_k, u_k)} L(u_k) = \sum_{k=1}^n \lambda_k \frac{(u_k, x)}{(u_k, u_k)} u_k.$$

При этом мы уже доказывали, что формула  $P_k(x) = \text{pr}_{u_k} x = \frac{(u_k, x)}{(u_k, u_k)} u_k$  задает ортогональный проектор на  $\langle u_k \rangle$ , что доказывает оба утверждения.  $\square$

Проекторы на собственные вектора, соответствующие одному и тому же собственному числу, можно собрать в один проектор на собственное подпространство. Так что можно выразить самосопряженный оператор через линейную комбинацию проекторов на его собственные подпространства.

**СЛЕДСТВИЕ 5.12.** *Для любой эрмитовой формы в эрмитовом пространстве  $V$  существует ортонормированный базис, в котором матрица этой формы диагональна.*

*Для любой квадратичной формы в евклидовом пространстве  $V$  существует ортонормированный базис, в котором матрица этой формы диагональна.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $L : V \rightarrow V$  – самосопряженный оператор, соответствующий данной форме. По теореме 5.6 существует ортогональный базис из собственных векторов этого оператора. Нормируя эти вектора (что не портит их ортогональности и “собственности”) получаем ортонормированный базис из собственных векторов. В этом базисе из собственных векторов матрица оператора диагональна, а по лемме 5.5 она равна матрице исходной формы.

В евклидовом пространстве надо только заметить, что, так как собственные числа оператора  $L$  вещественны, то и у него существуют собственные вектора в исходном пространстве, а дальше повторить доказательство теоремы 5.6 для евклидова случая.  $\square$

## 6. Матричные разложения

В этом параграфе снова  $F$  – это поле вещественных или комплексных чисел.

**ОПРЕДЕЛЕНИЕ 6.1.** Самосопряженный оператор называется положительно (неотрицательно) определенным, если все его собственные числа положительны (неотрицательны). Это равносильно тому, что эрмитова форма, заданная этим оператором, положительно (неотрицательно) определена.

Эрмитова матрица  $A \in M_n(\mathbb{C})$  называется положительно (неотрицательно) определенной, если эрмитова форма  $B(x, y) = x^*Ay$  положительно (неотрицательно) определена.

Для диагональной матрицы  $D \in M_n(\mathbb{R})$  с неотрицательными диагональными элементами положим  $\sqrt{D} = \text{diag}(\sqrt{d_{11}}, \dots, \sqrt{d_{nn}})$  (берутся арифметические квадратные корни). Сейчас мы определим, точнее, докажем корректность определения квадратного корня из произвольной неотрицательно определенной эрмитовой матрицы. Это утверждение понадобится для доказательства единственности полярного разложения. Обобщение этого утверждения на другие полиномиальные матричные уравнения (вместо  $X^2 = A$ ) оставляется читателю в качестве упражнения.

**ЛЕММА 6.2.** Пусть  $A \in M_n(\mathbb{C})$  – неотрицательно определенная эрмитова матрица. Тогда существует единственная неотрицательно определенная эрмитова матрица  $H \in M_n(\mathbb{C})$  такая, что  $H^2 = A$ .

**ДОКАЗАТЕЛЬСТВО.** По теореме 5.6 существует матрица  $C \in GL_n(\mathbb{C})$  такая, что  $A = C^{-1}DC$ , где  $D$  диагональна с неотрицательными диагональными элементами. Тогда  $H = C^{-1}\sqrt{D}C$  удовлетворяет условиям леммы.

Обратно, если  $H$  удовлетворяет условиям леммы, то  $H = G^{-1}\bar{D}G$  для некоторой матрицы  $G \in GL_n(\mathbb{C})$  и диагональной  $\bar{D}$  с неотрицательными элементами по диагонали. Тогда  $H^2 = G^{-1}\bar{D}^2G = C^{-1}DC$ . Поэтому собственные числа матриц  $\bar{D}^2$  и  $D$  и их кратности совпадают. Меняя при необходимости порядок собственных векторов матриц  $A$  и  $H$  можно считать, что  $\bar{D}^2 = D = \text{diag}(\lambda_1 E, \dots, \lambda_k E)$ , где  $\lambda_j \neq \lambda_l$  при  $j \neq l$ . Из выражения для  $H^2$  получаем  $(CG^{-1})D = D(CG^{-1})$ . Вычисление показывает, что  $CG^{-1}$  – блочно диагональная матрица с блоками тех же размеров, что и диагональные блоки матрицы  $D$ . Заметим, что  $\bar{D} = \text{diag}(\sqrt{\lambda_1} E, \dots, \sqrt{\lambda_k} E)$  также коммутирует с любой такой блочно диагональной матрицей, откуда  $H = G^{-1}\bar{D}G = C^{-1}\bar{D}C$  – единственная матрица с неотрицательными собственными числами, удовлетворяющая равенству  $H^2 = A$ .  $\square$

**ТЕОРЕМА 6.3** (разложение Холецкого). Любая положительно определенная эрмитова матрица  $A \in M_n(\mathbb{C})$  представляется в виде произведения  $A = C^*C$ , для некоторой верхнетреугольной матрицы  $C$  с положительными диагональными элементами. При этом матрица  $C$  определена единственным образом.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $B(x, y) = x^*Ay$  – эрмитова форма на  $\mathbb{C}^n$ . Ее матрица в стандартном базисе  $B_e = A$ . По определению положительная определенность  $A$  равносильна положительной определенности  $B$ . По теореме 2.5 существует базис, в котором эта форма диагональна, а так как она положительно определена, то диагональные элементы вещественны и положительны. Домножая базисные вектора на соответствующие вещественные константы можно



добиться того, чтобы эта матрица стала единичной. Если  $u$  такой базис  $\mathbb{C}^n$ , что  $B_u = E$ , то  $A = B_e = C_{u \rightarrow e}^* B_u C_{u \rightarrow e} = C_{u \rightarrow e}^* C_{u \rightarrow e}$ . По QR-разложению  $C_{u \rightarrow e} = QC$  для некоторой матрицы  $Q$  с ортонормированными столбцами и верхнетреугольной матрицы  $C$  с положительными элементами по диагонали. Тогда  $A = (QC)^* QC = C^* Q^* QC = C^* C$ .

На самом деле, это доказательство равносильно применению процесса ортогонализации Грама–Шмидта относительно скалярного произведения  $B$  к векторам стандартного базиса. Действительно, процесс ортогонализации (вместе с нормированием) говорит, что умножая стандартный базис на верхнетреугольную матрицу с положительными диагональными элементами, можно получить базис  $v$ , ортонормированный относительно  $B$ . Это означает, что  $B_v = E$ , а  $C_{e \rightarrow v}$  верхнетреугольная, откуда  $A = B_e = C_{e \rightarrow v}^* C_{e \rightarrow v}$ .

Другое доказательство существования вытекает из разложения Гаусса и совпадает с началом доказательства критерия Сильвестра. А именно, так как форма  $B(x, y) = x^* A y$  положительно определена, то все главные миноры ее матрицы в любом базисе положительны. Следовательно, по лемме 12.6 главы 2  $A$  лежит в главной клетке Гаусса, т. е.  $A = GDH$  для некоторой верхней унитреугольной матрицы  $H$ , диагональной матрицы  $D$  и нижней унитреугольной матрицы  $G$ . Так как  $A = A^*$ , то  $GDH = H^* D^* G^*$  откуда  $(H^*)^{-1} G D = D^* G^* H^{-1}$ . Последняя матрица является одновременно верхней и нижней треугольной, следовательно,  $G = H^*$  и  $D = D^*$ . Из положительной определенности сразу следует, что диагональные элементы матрицы  $D$  положительны. Следовательно,  $A = (H^* \sqrt{D})(\sqrt{D} H)$  – искомое разложение.

Единственность следует из единственности разложения Гаусса. Если  $C^* C = \bar{C}^* \bar{C}$  для некоторых верхнетреугольных матриц  $C, \bar{C}$  с положительными диагональными элементами, то матрица  $(C^*)^{-1} C^* = \bar{C} C^{-1}$  верхнетреугольна и нижнетреугольна одновременно, следовательно, она диагональна. То есть  $\bar{C} = LC$  для некоторой диагональной матрицы  $L$ . Так как диагональные элементы  $C$  и  $\bar{C}$  положительны, то  $L$  обладает тем же свойством. Кроме того,  $C^* C = \bar{C}^* \bar{C} = (LC)^* LC = C^* (L^* L) C$ , откуда  $L^* L = L^2 = E$ . Таким образом,  $L = E$  и  $\bar{C} = C$ .  $\square$

**ТЕОРЕМА 6.4** (сингулярное разложение). *Любая матрица  $A \in M_{m,n}(\mathbb{C})$  представляется в виде произведения  $A = BDC$ , где  $B$  и  $C$  – квадратные унитарные матрицы, а  $D \in M_{m,n}(\mathbb{C})$  диагональна (т. е.  $d_{ij} = 0$  при всех  $i \neq j$ ) с неотрицательными элементами по диагонали.*

*На языке линейных отображений это же утверждение звучит следующим образом.*

*Для любого линейного отображения  $L : U \rightarrow V$ , где  $U$  и  $V$  – классические эрмитовы пространства, существуют ортонормированные базисы  $u$  и  $v$  пространств  $U$  и  $V$  соответственно, в которых матрица  $D = L_v^u$  оператора  $L$  диагональна с неотрицательными элементами по диагонали.*

*При этом диагональные элементы матрицы  $D$  определены однозначно с точностью до перестановки и равны корням из собственных чисел матрицы  $A^* A$  (соотв. оператора  $L^* L$ ) или 0.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $u$  и  $v$  ортонормированные базисы пространств  $U$  и  $V$  соответственно. Матрица  $L_v^u$  диагональна с элементами  $\alpha_i$  по диагонали тогда и только тогда, когда  $L(u_i) = \alpha_i v_i$  или  $L(u_i) = 0$  (последнее существенно, если  $\dim U > \dim V$ ). Ортогональность базиса  $v$  влечет  $(L(u_i), L(u_j)) = 0$  при всех  $i \neq j$ . Перепишем последнее равенство в виде  $(L^* L(u_i), u_j) = 0$ , т. е. вектор  $L^* L(u_i)$  лежит в ортогональном дополнении подпространства, порожденного всеми  $u_j$  при  $j \neq i$ . Заметим, что это ортогональное дополнение одномерно и содержит  $u_i$ . Следовательно,  $L^* L(u_i) = \lambda_i u_i$ . Таким образом, если сингулярное разложение оператора существует, то  $u_i$  – собственные вектора оператора  $L^* L$ . Этот оператор самосопряженный и неотрицательно определенный, поэтому все  $\lambda_i$  – вещественные неотрицательные числа. Так как  $\|v_i\| = 1$ , а  $\alpha_i > 0$ , то  $\alpha_i = \|L(u_i)\|$ . Имеем

$$\alpha_i^2 = (L(u_i), L(u_i)) = (L^* L(u_i), u_i) = \lambda_i (u_i, u_i) = \lambda_i.$$

Мы доказали, что если сингулярное разложение существует, то матрица  $D$  определена единственным образом с точностью до перестановки диагональных элементов.

По теореме 5.6 существует ортонормированный базис из собственных векторов оператора  $L^*L$ . Расположим эти вектора так, чтобы  $u_1, \dots, u_k$  соответствовали ненулевым собственным числам, а остальные – собственному числу 0. Тогда при  $i > k$  имеем  $0 = (L^*L(u_i), u_i) = (L(u_i), L(u_i))$ , откуда  $L(u_i) = 0$ . Вектора  $v_j = \frac{L(u_j)}{\|L(u_j)\|}$  при  $j \leq k$  образуют базис образа оператора  $L$ . Как было показано выше,  $L(u_j) \perp L(u_h)$  при  $j \neq h$ , поэтому этот базис образа ортонормированный. Дополним его до ортонормированного базиса  $v$  пространства  $V$  (это можно сделать, дополнив до произвольного базиса, применив процесс ортогонализации и нормировав полученные вектора). Таким образом, в ортонормированных базисах  $u$  и  $v$  матрица оператора  $L$  диагональна, что завершает доказательство.  $\square$

**СЛЕДСТВИЕ 6.5** (полярное разложение). *Любая матрица  $A \in M_n(\mathbb{C})$  представляется в виде произведения  $A = GH$ , где  $G$  – унитарная матрица, а  $H \in M_n(\mathbb{C})$  – неотрицательно определенная эрмитова. При этом матрица  $H$  определена единственным образом, а если  $A$  обратима, то и  $G$  единственна.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $A = BDC$  – сингулярное разложение матрицы  $A$ . Тогда  $A = (BC)(C^{-1}DC)$  – ее полярное разложение. Действительно, произведение унитарных матриц унитарно, а  $C^{-1}DC = C^*DC$  – эрмитова.

Если  $A = GH$ , где  $G$  унитарная, а  $H$  эрмитова, то  $A^*A = H^*G^*GH = H^2$ . Но по лемме 6.2 такая положительно определенная матрица  $H$  единственна. Если же  $A$  обратима, то обратима и  $H$ , поэтому  $G = AH^{-1}$  единственна.  $\square$

Очевидно, что унитарность (самосопряженность) оператора равносильна унитарности (самосопряженности) его матрицы в ортонормированном базисе. Таким образом, можно говорить о полярном разложении оператора.

**СЛЕДСТВИЕ 6.6.** *Пусть  $V$  – евклидово или эрмитово пространство. Линейный оператор  $L : V \rightarrow V$  является нормальным тогда и только тогда, когда унитарный и эрмитов операторы в его полярном разложении коммутируют.*

**ДОКАЗАТЕЛЬСТВО.** Если  $L = GH$ , где  $G$  – унитарный, а  $H$  – эрмитов, то  $L^*L = H^*G^*GH = H^2$ , а  $LL^* = GHH^*G^* = GH^2G^{-1}$ . Таким образом,  $L^*L = LL^*$  тогда и только тогда, когда  $G$  коммутирует с  $H^2$ . В этом случае  $(GHG^{-1})^2 = H^2$ , и по лемме 6.2  $GHG^{-1} = H$ , т.е.  $G$  и  $H$  коммутируют. Обратная импликация очевидна.  $\square$

## 7. Гильбертово пространство

Не вдаваясь в подробности, в этом параграфе мы обсудим, какие утверждения этой главы про евклидовы (эрмитовы) пространства выживают в бесконечномерных пространствах со скалярным произведением. Мы будем рассматривать только одно (с точностью до изометрии) бесконечномерное пространство, а именно то, которым в основном интересуется функциональный анализ – сепарабельное гильбертово пространство.

Пусть  $V$  – (бесконечномерное) векторное пространство над  $\mathbb{R}$  или  $\mathbb{C}$  с евклидовым (соотв. эрмитовым) скалярным произведением. Также как в предыдущих параграфах мы будем обозначать основное поле буквой  $F$ , а в вещественном случае черта будет тождественной инволюцией. Скалярное произведение задает норму в пространстве  $V$ , которая в соответствии с неравенством треугольника превращает его в нормированное, а, следовательно, и топологическое пространство. Оно называется полным, если любая фундаментальная последовательность имеет предел. Оно называется сепарабельным, если в нем существует плотное счетномерное подпространство. Гильбертово пространство – это полное пространство со скалярным произведением. Для простоты мы считаем наше гильбертово пространство сепарабельным. Все сепарабельные гильбертовы пространства над  $F$  изометричны.

Моделью сепарабельного гильбертова пространства является множество  $\ell_2$  бесконечных последовательностей  $x = (x_n)_{n=0}^\infty$ , для которых ряд  $\sum_{n=0}^\infty |x_n|^2$  сходится, с естественными операциями

сложения и умножения на число и со скалярным произведением

$$(x, y) = \sum_{n=0}^{\infty} \overline{y_n} x_n.$$

Другой пример (приведем только вещественную версию) –  $L_2([a, b])$ . Пусть  $V$  – множество измеримых функций  $f : [a, b] \rightarrow \mathbb{R}$  таких, что интеграл Лебега  $\int_a^b f(t)^2 dt$  сходится, с поточечными операциями. Зададим симметричную билинейную форму  $B$  на  $V$  формулой

$$B(f, g) = \int_a^b f(t)g(t) dt.$$

Ясно, что эта форма неотрицательно определена, но вырождена, скажем, функция, отличающаяся от нуля на множестве меры 0 (например, в конечном числе точек), ортогональна всему пространству. Положим  $L_2([a, b]) = V/V^{\perp B}$ . Тогда  $B$  индуцирует скалярное произведение на этом пространстве. Можно доказать, что набор функций  $1, \sin nt, \cos nt$  ( $n \in \mathbb{N}$ ) являются ортогональным базисом плотного подпространства в  $L_2([-\pi, \pi])$ , поэтому  $L_2([a, b])$  является сепарабельным (чтобы перевести  $[-\pi, \pi]$  в  $[a, b]$  достаточно сделать линейную замену переменных).

В анализе базисом гильбертова пространства называют базис плотного подпространства, т. е. базис – это набор  $v$  такой, что любой вектор представляется в виде бесконечной линейной комбинации базисных векторов  $\sum_{n=0}^{\infty} v_n \alpha_n$  единственным образом (как обычно, сумма ряда – это предел последовательности частичных сумм, а понятие предела в нормированном пространстве существует). Тот базис, который изучается в курсе линейной алгебре, в гильбертовом пространстве, конечно же, также существует. Он называется алгебраическим базисом или базисом Гамеля. Заметим, что счетного базиса Гамеля в гильбертовом пространстве не существует.

Неравенство треугольника, КБШ, и процесс ортогонализации естественно имеют место и в гильбертовом пространстве, так как работают с конечномерными подпространствами. Процесс ортогонализации работает и с бесконечными базисами.

А вот дальше начинаются неожиданности, связанные с наличием незамкнутых линейных подпространств, не непрерывных линейных отображений и инъективных, но не сюръективных эндоморфизмов. В  $\ell_2$  незамкнутым линейным подпространством является множество  $\ell_2^{fin}$  финитных последовательностей. Оно как раз является счетномерным плотным подпространством, наличие которого доказывает сепарабельность. Базис этого подпространства можно дополнить до алгебраического базиса всего гильбертова пространства, следовательно,  $\ell_2 = \ell_2^{fin} \oplus U$  для некоторого подпространства  $U$ . Отображение  $L : \ell_2 \rightarrow F$ , заданное равенствами  $L(x + y) = \sum_{n=0}^{\infty} nx_n$ , где  $x \in \ell_2^{fin}$ , а  $y \in U$ , не является непрерывным. Инъективным, но не сюръективным является сдвиг  $S(x)_1 = 0, S(x)_n = x_{n-1}$ . Сдвиг в обратную сторону:  $S'(x)_n = x_{n+1}$  является примером сюръективного, но не инъективного оператора в  $\ell_2$ . Заметим, что  $S' \circ S = \text{id} \neq S \circ S'$ , то есть в алгебре операторов существуют односторонне обратимые элементы.

В анализе под подпространством гильбертова пространства по умолчанию считают *замкнутое* подпространство, а под линейным оператором – непрерывный линейный оператор. С такой оговоркой разложение в прямую сумму подпространства и его ортогонального дополнения и равенство  $(U^{\perp})^{\perp} = U$  имеют место и в гильбертовых пространствах (для незамкнутого подпространства  $(U^{\perp})^{\perp}$  является замыканием  $U$ ).

Формула для координат в ортогональном базисе, неравенство Бесселя и равенство Парсеваля имеют место в гильбертовых пространствах и для бесконечных ортогональных наборов. Выполнена также лемма о расстоянии от точки до (замкнутого) подпространства.

Двойственное пространство к гильбертову пространству  $H$  – это пространство *непрерывных* линейных функционалов, т. е. непрерывных линейных отображений  $H \rightarrow F$ . С таким соглашением можно доказать, что  $H^*$  канонически изоморфно  $H$  (это называется теоремой Рисса). Оба определения сопряженного оператора теперь переносятся и на гильбертовы пространства.

Изучение собственных чисел операторов становится существенно сложнее из-за наличия инъективных, но не сюръективных операторов. Далее  $F = \mathbb{C}$ , потому что даже в конечномерных пространствах над  $\mathbb{R}$  все доказательства проходят через  $\mathbb{C}$ . Множество тех чисел  $\lambda \in \mathbb{C}$ , для которых оператор  $L - \lambda \text{id}$  не обратим, называется спектром оператора  $L$ . При этом  $\lambda$  называется собственным числом, если (также как и в конечномерном случае) этот оператор не инъективен. Множество собственных чисел называется точечным спектром. Для компактного самосопряженного оператора верен аналог следствия 5.11 (с бесконечной линейной комбинацией проекторов). Если же самосопряженный оператор не компактен, то он может вообще не иметь собственных чисел и теорема о его строении гораздо сложнее.

Некоторые из матричных разложений имеют место и для операторов в гильбертовых пространствах с соответствующими оговорками. Таково, например, полярное разложение.

## 8. Кватернионы и движения трехмерного пространства

К теории квадратичных и эрмитовых форм примыкает теория конечномерных алгебр с делением. Алгебра  $A$  над полем  $F$  называется телом или алгеброй с делением, если любой ее ненулевой элемент обратим. Она называется центральной, если  $F$  является ее центром, т. е. множеством элементов, коммутирующих со всеми элементами  $A$ . Легко доказать, что над замкнутым полем любая такая алгебра совпадает с самим полем. Действительно, для любого элемента  $a \in A$  алгебра  $F[a]$  изоморфна  $F[t]/(f)$  для некоторого многочлена  $f$ . Если  $f$  приводим, то  $F[a]$  содержит делители нуля, что невозможно. В противном случае, так как  $F$  замкнуто, то  $\deg f = 1$ , откуда  $a \in F$ .

Над полем вещественных чисел существует ровно одна центральная алгебра с делением. Она называется алгеброй кватернионов. Алгебра кватернионов  $\mathbb{H}$  – это 4-мерное векторное пространство над  $\mathbb{R}$  с базисом  $e = (1, \mathbf{i}, \mathbf{j}, \mathbf{k})$  и таблицей умножения

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Легко проверить, что эта алгебра ассоциативна (достаточно проверить это на базисных элементах).

Кватернион  $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$  можно представить как сумму скалярной части  $a$  и векторной части  $v = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ . Если отождествить векторную часть с трехмерным вектором, то умножение векторных частей выглядит следующим образом:

$$uv = u \times v - (u, v),$$

где  $\times$  обозначает векторное произведение. Кватернион с нулевой скалярной частью называется чистым кватернионом.

Отображение  $\bar{\cdot} : \mathbb{H} \rightarrow \mathbb{H}$ ,  $a + v \rightarrow a - v$ , называется сопряжением и является антиинволюцией на  $\mathbb{H}$ . Действительно,

$$(b+u)(a+v) = ba - (u, v) + (u \times v + au + bv), \quad \text{а} \quad (a-v)(b-u) = ab - (v, u) + (v \times u - au - bv) = \overline{(b+u)(a+v)},$$

а остальные свойства антиинволюции очевидны. Кроме того

$$(a+v)(a-v) = a^2 - vv = a^2 - v \times v + (v, v) = a^2 + (v, v).$$

Для ненулевого кватерниона это число является положительным вещественным числом и квадратный корень из него называется модулем кватерниона. Таким образом, мы видим, что  $h \frac{\bar{h}}{|h|^2} = 1$ , т. е.  $\mathbb{H}$  – алгебра с делением.

Легко видеть, что модуль является гомоморфизмом мультипликативной группы кватернионов в мультипликативную группу положительных вещественных чисел. Действительно,

$$|h|^2 |g|^2 = h \bar{h} g \bar{g} = g h \bar{h} \bar{g} = g h \bar{g} \bar{h} = |gh|^2.$$

Сопоставление кватерниону  $a + bi + cj + dk$  матрицы умножения на этот кватернион в стандартном базисе  $(1, i, j, k)$

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

задает гомоморфизм алгебры кватернионов в алгебру матриц  $M_4(\mathbb{R})$ , а определитель этой матрицы – гомоморфизм мультипликативной группы кватернионов в  $\mathbb{R}^*$ , который является нормой<sup>4</sup> из  $\mathbb{H}$  в  $\mathbb{R}$ . Вычисление показывает, что этот определитель равен  $(a^2 + b^2 + c^2 + d^2)^2$ , т. е. четвертой степени модуля кватерниона.

Другое матричное представление кватернионов получается при рассмотрении  $\mathbb{H}$ , как векторного пространства над  $\mathbb{C}$  с умножением  $h(a + bi) = h(a + bi)$ , где  $h \in \mathbb{H}$ , а  $a, b \in \mathbb{R}$ . Тогда  $\mathbb{H}$  будет 2-мерным векторным пространством над  $\mathbb{C}$  с базисом  $(1, j)$ : любой кватернион единственным образом представляется в виде  $a + bi + cj + dk = 1 \cdot (a + bi) + j \cdot (c - di)$ . Умножение на кватернион  $a + bi + cj + dk$  слева является линейным оператором на этом векторном пространстве, матрица которого равна

$$\begin{pmatrix} a + bi & -c - di \\ c - di & a - bi \end{pmatrix}.$$

Нетрудно проверить, что это отображение задает вложение мультипликативной группы кватернионов в группу  $GL_2(\mathbb{C})$ . Определитель указанной матрицы равен  $a^2 + b^2 + c^2 + d^2$  и называется редуцированной нормой  $\text{prd}(a + bi + cj + dk)$ . Заметим, что кватернионы с модулем 1 отображаются в унитарные матрицы с определителем 1. Это совершенно не удивительно, потому что умножение на кватернион с модулем 1 является изометрией 4-мерного пространства кватернионов, норма кватерниона равна норме столбца его координат в выбранном базисе (относительно стандартного скалярного произведения в  $\mathbb{C}^2$ ), а умножение на матрицу сохраняет нормы столбцов тогда и только тогда, когда она унитарна. Более удивительно, что это отображение биективно, чуть позже мы сформулируем это в виде изоморфизма групп. Заметим, что это не все изометрии 4-мерного вещественного пространства  $\mathbb{H}$ , а только  $\mathbb{C}$ -линейные изометрии.

Интересно также рассмотреть операцию сопряжения кватернионом:  $c_h(z) = hzh^{-1}$ . Эта операция тоже не меняет модуль кватерниона  $z$ , а кроме того оставляет инвариантным пространство чистых кватернионов. Это можно доказать вычислением, а можно воспользоваться идеями параграфа 5. Действительно, множество вещественных чисел инвариантно относительно оператора сопряжения любым кватернионом, а подпространство чистых кватернионов является его ортогональным дополнением (относительно евклидова скалярного произведения, ассоциированного с выбранной нормой). По лемме 5.8 оно инвариантно относительно сопряженного оператора. Так как оператор сопряжения является унитарным, то сопряженный с ним равен обратному. Таким образом, подпространство чистых кватернионов инвариантно относительно сопряжения обратным к любому кватерниону.

Если  $h = a + v$  – разложение кватерниона на вещественную часть и чистый кватернион, то  $c_h(v) = v$ , и нетрудно видеть, что  $\langle 1, v \rangle_{\mathbb{R}}$  – собственное подпространство оператора  $c_h$ , соответствующее 1. По леммам 5.7 и 5.8 ортогональное дополнение этого подпространства (плоскость в пространстве чистых кватернионов)  $c_h$ -инвариантно. Непосредственное вычисление показывает, что любой поворот в этой плоскости реализуется, а отношение  $a/|v|$  определяет угол этого поворота,

<sup>4</sup>Понятие нормы в алгебре отличается от понятия нормы в анализе. В алгебре нормой называют определитель матрицы умножения на элемент  $F$ -алгебры.

Действительно, можно считать, что  $|h| = 1$ , а тогда

$$(a + v)w(a - v) = a^2w + a(vw - wv) + v w v = a^2w + 2av \times w - (v \times w - (v, w))v = \\ a^2w + 2av \times w - v \times w \times v + (v, w)v = a^2w + 2av \times w - (v, v)w + 2(v, w)v.$$

Пусть  $a = \cos \frac{\alpha}{2}$ ,  $|v| = \sin \frac{\alpha}{2}$ , а  $e_1 = w - \text{pr}_v w$ ,  $e_2 = \frac{v \times w}{|v|}$ ,  $e_3 = \text{pr}_v w$  – ортогональный базис. Тогда

$$(a + v)w(a - v) = w(\cos^2 \frac{\alpha}{2} - \sin^2 \frac{\alpha}{2}) + 2 \text{pr}_v w \cdot \sin^2 \frac{\alpha}{2} + 2e_2 \cdot \cos \frac{\alpha}{2} \sin \frac{\alpha}{2} = \\ w \cos \alpha - \text{pr}_v w \cdot \cos \alpha + \text{pr}_v w + e_2 \cdot \sin \alpha = e_1 \cos \alpha + e_2 \sin \alpha + e_3.$$

Заметим, что третья координата  $w$  в этом базисе не изменилась, а длины векторов  $e_1$  и  $e_2$  равны. Следовательно,  $(a + v)w(a - v)$  – вектор, полученный поворотом  $w$  на угол  $\alpha$  вокруг прямой, натянутой на вектор  $v$ . Таким образом, сопряжение кватернионом реализует любой поворот трехмерного пространства.

Несколько слов об обозначениях групп изометрий эрмитова пространства. В общем виде, если  $F$  – поле с инволюцией,  $V$  – конечномерное векторное пространство над  $F$ , а  $B$  – невырожденная эрмитова форма на  $V$ , то группа изометрий формы  $B$  называется унитарной группой и обозначается  $U(B)$  или  $U_n(F)$ , где  $n = \dim V$ , если инволюция и форма известны из контекста. Если инволюция тривиальна, то эта группа называется ортогональной группой и обозначается через  $O(B)$  или  $O_n(F)$ . Подгруппы этих групп, состоящие из преобразований с определителем 1, называются специальной унитарной и специальной ортогональной группой и обозначаются через  $SU$  и  $SO$ , соответственно.

Для стандартных скалярных произведений в  $\mathbb{C}^n$  и  $\mathbb{R}^n$  соответствующие группы обычно обозначаются просто через  $U_n$ ,  $SU_n$ ,  $O_n$  и  $SO_n$ . Как мы видели, определитель унитарной матрицы по модулю равен 1. Следовательно, определитель вещественной ортогональной матрицы равен  $\pm 1$ . Поэтому группа  $O_{2k+1}$  раскладывается в прямое произведение  $SO_{2k+1} \times \{\pm E\}$ .

Собственные числа матрицы из  $SO_3$  по модулю равны 1, одно из них вещественно, а два других комплексно сопряженные (если все 3 вещественны, то одно равно 1, а два других равны между собой). Так как произведение комплексно сопряженных чисел равно 1, то одно из собственных чисел должно быть равно 1, т.е. ортогональное преобразование действует на некоторой прямой тривиально. Ортогональное дополнение этой прямой инвариантно. Легко видеть, что ортогональная матрица  $2 \times 2$  с определителем 1 – это матрица поворота. Если же определитель преобразования из  $O_3$  равен  $-1$ , то композиция его с любым зеркальным отражением будет лежать в  $SO_3$ , т.е. будет вращением. Таким образом, мы доказали хорошо известный из геометрии факт.

**ПРЕДЛОЖЕНИЕ 8.1.** Любое движение трехмерного пространства с неподвижной точкой является поворотом или композицией поворота с (любой) зеркальной симметрией.

Повороты называются собственными движениями, а композиция поворота и симметрии – несобственными. Таким образом,  $SO_3$  – это группа собственных движений трехмерного пространства.

Теперь можно сформулировать связь кватернионов с унитарными и ортогональными группами.

**ПРЕДЛОЖЕНИЕ 8.2.** Мультипликативная группа кватернионов с модулем 1 изоморфна группе  $SU_2$ , а всех кватернионов  $\mathbb{H}^* \cong \mathbb{R}_{>0}^* \times SU_2$ .

Факторгруппа  $\mathbb{H}^*/\mathbb{R} \cong SU_2/\{\pm E\} \cong SO_3$ .

Модуль кватерниона задает на  $\mathbb{H}^*$  структуру нормированного топологического пространства, которая индуцирует топологию на  $\mathbb{H}^*/\mathbb{R}$ . Ясно, что  $\mathbb{H}^*/\mathbb{R}$  с этой топологией гомеоморфно проективному пространству  $\mathbb{RP}^3$ . Изоморфизм  $\mathbb{H}^*/\mathbb{R} \rightarrow SO_3$  является гомеоморфизмом и, следовательно,  $SO_3$  гомеоморфно  $\mathbb{RP}^3$ .

## 9. Теоремы Витта

Этот параграф посвящен основам классификации квадратичных пространств над произвольным полем  $F$  характеристики не 2. Мы увидим, что любая квадратичная форма является суммой нескольких экземпляров гиперболической плоскости и анизотропной формы. Начнем с определения суммы форм и гиперболической плоскости.

Будем говорить, что две формы изоморфны, если соответствующие квадратичные пространства изометричны. Пусть  $(V, Q)$  и  $(V', Q')$  – квадратичные пространства. Обозначим через  $Q \oplus Q'$  квадратичную форму на  $V \oplus V'$ , действующую по правилу  $Q \oplus Q'(x, x') = Q(x) + Q'(x')$  (проверьте, что это действительно квадратичная форма). Если подпространства  $V$  и  $V'$  невырождены, то в пространствах  $V \oplus V'$  они являются ортогональными дополнениями друг друга относительно формы  $Q \oplus Q'$ . Поэтому в текстах про квадратичные формы чаще используют обозначение  $Q \perp Q'$  вместо  $Q \oplus Q'$  и называют такую форму ортогональной суммой форм  $Q$  и  $Q'$ .

Обозначим через  $\langle \alpha_1 \rangle \oplus \dots \oplus \langle \alpha_n \rangle = \langle \alpha_1, \dots, \alpha_n \rangle$  форму, которая в некотором базисе имеет матрицу  $\text{diag}(\alpha_1, \dots, \alpha_n)$ . Форма  $\mathbb{H} \cong \langle 1, -1 \rangle$  (точнее двумерное пространство с этой формой) называется гиперболической плоскостью. Ненулевой вектор  $x$  называется изотропным относительно формы  $Q$ , если  $Q(x) = 0$ , в противном случае  $x$  называется анизотропным. Напомним, что форма  $Q$  называется изотропной, если существует  $Q$ -изотропный вектор, и анизотропной в противном случае.

**ЛЕММА 9.1.** *Любая невырожденная изотропная квадратичная форма  $Q$  изоморфна  $\mathbb{H} \oplus Q'$  для некоторой невырожденной формы  $Q'$ .*

**ДОКАЗАТЕЛЬСТВО.** Так как  $Q$  изотропна, существует  $x \in V \setminus \{0\}$  такой, что  $Q(x) = 0$ . Обозначим через  $B$  симметричную билинейную форму, ассоциированную с  $Q$ . Поскольку  $Q$  невырождена, найдется  $y \in V$  такой, что  $B(x, y) \neq 0$ . Домножая  $y$  на подходящий скаляр, можно считать, что  $B(x, y) = 2$ . Для любого  $\lambda \in F$  вектора  $x$  и  $z = y + \lambda x$  линейно независимы, причем  $B(x, z) = B(x, y) + \lambda B(x, x) = 2$ . Наконец,  $Q(z) = B(y + \lambda x, y + \lambda x) = B(y, y) + 2\lambda B(x, y) + B(x, x) = Q(y) + 4\lambda$ . Значит, если положить  $\lambda = -Q(y)/4$ , получим  $Q(z) = 0$ . Возьмем теперь  $v_1 = (x + z)/2$ , а  $v_2 = (x - z)/2$ . Тогда  $B(v_1, v_2) = 0$ , а  $Q(v_1) = -Q(v_2) = 1$ .

Дополнив  $v_1, v_2$  до базиса  $(v_1, v_2, u_3, \dots, u_n)$  при  $i \geq 3$  положим

$$v_i = u_i - B(v_1, u_i)v_1 + B(v_2, u_i)v_2.$$

Так как  $B(v_1, v_i) = B(v_2, v_i) = 0$ , то  $Q \cong \mathbb{H} \oplus Q'$ , где  $Q'$  – сужение формы  $Q$  на подпространство, порожденное векторами  $v_3, \dots, v_n$ .  $\square$

Из леммы следует в частности, что все невырожденные изотропные двумерные формы изоморфны  $\mathbb{H}$ . Большая часть алгебраистов предпочитает выбирать базис  $\mathbb{H}$  так, чтобы матрица квадратичной формы была равна  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , а не  $\text{diag}(1, -1)$ , то есть в координатах:  $Q(x) = 2x_1x_2$ , а не  $Q(x) = x_1^2 - x_2^2$ .

Из леммы следует также, что любое квадратичное пространство представляется в виде суммы нескольких экземпляров гиперболической плоскости и анизотропного подпространства. Наша следующая цель – доказать, что анизотропное подпространство определено единственным образом с точностью до изометрии. Для этого мы докажем теорему о сокращении, которая говорит о том, что изометрию  $U \oplus V \cong U \oplus W$  можно сокращать на  $U$ .

Пусть  $Q$  – квадратичная форма на  $V$ , соответствующая симметричной билинейной форме  $B$ , а  $x$  –  $Q$ -анизотропный вектор. Определим отражение  $S_x$  относительно вектора<sup>5</sup>  $x$  формулой

$$S_x(y) = y - 2 \frac{B(x, y)}{Q(x)} x.$$

Простое вычисление показывает, что отражение является изометрией, а  $S_x^2 = \text{id}$ .

<sup>5</sup>Геометрически, это является отражением относительно гиперплоскости, ортогональной  $x$ .

**ЛЕММА 9.2.** Пусть  $x_1, x_2 \in V$  и  $Q(x_1) = Q(x_2) \neq 0$ . Тогда существует композиция отражений, переводящая  $x_1$  в  $x_2$ .

ДОКАЗАТЕЛЬСТВО. Если  $Q(x_1 - x_2) \neq 0$ , то подойдет отражение относительно этого вектора:

$$\begin{aligned} S_{x_1-x_2}(x_1) &= x_1 - 2 \frac{B(x_1 - x_2, x_1)}{Q(x_1 - x_2)}(x_1 - x_2) = \\ &= x_1 - 2 \frac{Q(x_1) - B(x_2, x_1)}{Q(x_1) + Q(x_2) - 2B(x_2, x_1)}(x_1 - x_2) = x_1 - (x_1 - x_2) = x_2. \end{aligned}$$

Если  $Q(x_1 + x_2) \neq 0$ , то  $S_{x_1+x_2}(x_1) = -x_2$ , а  $S_{x_2}(-x_2) = x_2$ . Если же  $Q(x_1 - x_2) = Q(x_1 + x_2) = 0$ , то

$$0 = Q(x_1 - x_2) + Q(x_1 + x_2) = Q(x_1) + Q(x_2) + Q(x_1) + Q(x_2) = 4Q(x_1),$$

что противоречит предположению.  $\square$

**СЛЕДСТВИЕ 9.3.** Любая изометрия невырожденного пространства есть композиция отражений.

ДОКАЗАТЕЛЬСТВО. Пусть  $L : V \rightarrow V$  – изометрия невырожденного квадратичного пространства  $(V, Q)$ . Доказываем индукцией по  $n = \dim V$ ; база  $n = 1$  очевидна. Пусть  $n > 1$ . Возьмем  $x \in V$  такой, что  $Q(L(x)) = Q(x) \neq 0$ . По лемме найдется композиция отражений  $S : V \rightarrow V$  такая, что  $S(x) = L(x)$ . Отображение  $S^{-1}L$ , таким образом, является изометрией и оставляет  $x$  на месте; значит,  $S^{-1}L$  оставляет на месте и  $W = x^\perp$  – подпространство размерности  $n - 1$ . По предположению индукции изометрия  $S^{-1}L|_W$  является композицией отражений (относительно векторов из  $W$ ). Заметим, что любое отражение относительно вектора из  $W$  оставляет на месте  $x$ , поскольку  $x \perp W$ . Значит, изометрия  $S^{-1}L$  является композицией тех же самых отражений, рассматриваемых уже как преобразований всего пространства  $V$ . Переносим  $S$  в другую часть, получаем, что и  $L$  является композицией отражений.  $\square$

**ТЕОРЕМА 9.4** (Витта о сокращении). Если  $Q \oplus Q_1 \cong Q \oplus Q_2$ , то  $Q_1 \cong Q_2$ .

ДОКАЗАТЕЛЬСТВО. Предложение 2.2 дает возможность сокращать на ортогональное дополнение ко всему пространству, поэтому можно считать, что форма  $Q$  невырождена. Докажем сначала, что из  $\langle \alpha \rangle \oplus Q_1 \cong \langle \alpha \rangle \oplus Q_2$  следует, что  $Q_1 \cong Q_2$ . Пусть при  $i = 1, 2$  форма  $Q'_i = \langle \alpha \rangle \oplus Q_i$  задана на пространстве  $\langle x_i \rangle \oplus W_i$ , причем  $Q'_i(x_i) = \alpha$ . Изометричность этих форм означает, что существует линейное отображение  $L : \langle x_1 \rangle \oplus W_1 \rightarrow \langle x_2 \rangle \oplus W_2$ , для которого  $Q'_2(L(x)) = Q'_1(x)$ . Так как  $Q'_2(L(x_1)) = Q'_1(x_1) = \alpha$ , то по лемме 9.2 найдется изометрия  $S : \langle x_2 \rangle \oplus W_2 \rightarrow \langle x_2 \rangle \oplus W_2$  такая, что  $S(x_2) = L(x_1)$ . Ясно, что  $S^{-1}L$  является изометрией  $\langle x_1 \rangle \oplus W_1 \rightarrow \langle x_2 \rangle \oplus W_2$  и  $S^{-1}L(x_1) = x_2$ . Так как изометрия сохраняет ортогональность векторов, то она сохраняет и ортогональные дополнения. Поэтому  $S^{-1}L$  отображает  $W_1 = x_1^\perp$  на  $W_2 = x_2^\perp$ . Это означает, что ограничение  $S^{-1}L$  на  $W_1$  и дает нужную изометрию между  $Q_1$  и  $Q_2$ .

В общем случае по теореме 2.5  $Q \cong \langle \alpha_1 \rangle \oplus \dots \oplus \langle \alpha_n \rangle$ , и доказательство проводится очевидной индукцией по  $n$ .  $\square$

**СЛЕДСТВИЕ 9.5.** Любая невырожденная форма  $Q$  представляется в виде

$$Q \cong \underbrace{\mathbb{H} \oplus \dots \oplus \mathbb{H}}_{r \text{ раз}} \oplus Q_{an},$$

где анизотропная часть  $Q_{an}$  определена однозначно с точностью до изометрии, и индекс Витта  $i(Q) := r$  определен однозначно.

ДОКАЗАТЕЛЬСТВО. По лемме 9.1 если форма изотропна, из нее можно выделить  $\mathbb{H}$ . Продолжая этот процесс, дойдем до какой-то анизотропной формы (потому что размерность все время убывает). Единственность легко выводится из теоремы о сокращении.  $\square$



Для доказательства теоремы о продолжении изометрии в случае, когда мы продолжаем изометрию с вырожденного подпространства, нам понадобится следующее утверждение.

**ЛЕММА 9.6.** Пусть  $B$  невырожденная симметричная билинейная форма на  $V$ , а  $W$  вырожденное подпространство в  $V$ . Пусть  $w = (w_1, \dots, w_k)$  – базис пространства  $W \cap W^\perp$ , а  $v = (v_1, \dots, v_m)$  – дополнение  $w$  до базиса пространства  $W$ . Тогда существует набор векторов  $u = (u_1, \dots, u_k)$  пространства  $V$  таких, что подпространство  $U = \langle w \cup u \rangle$  ортогонально подпространству  $\langle v \rangle$ , а матрица сужения  $B$  на  $U$  в базисе  $w \cup u$  равна  $\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}$ .

Заметим, что тогда подпространство  $\langle w \cup u \cup v \rangle$  невырождено.

**ДОКАЗАТЕЛЬСТВО.** Так как  $B$  невырождена, то по лемме 4.6 размерность ортогонального дополнения подпространства  $W$  строго меньше, чем размерность ортогонального дополнения подпространства  $W' = \langle w_1, \dots, w_{k-1}, v_1, \dots, v_m \rangle$ . Поэтому существует вектор  $x \in V$ , ортогональный всем векторам из набора  $w \cup v$ , кроме  $w_k$ . Таким образом, подпространство, порожденное  $w_k$  и  $x$  двумерно, изотропно и ортогонально  $W'$ . Также как в доказательстве леммы 9.1, найдем в этом подпространстве изотропный вектор  $u_k$  такой, что  $B(u_k, w_k) = 1$ .

Теперь в пространстве  $\bar{W} = W + \langle u_k \rangle$  имеем:  $\bar{W} \cap \bar{W}^\perp = \langle w_1, \dots, w_{k-1} \rangle$ . Индукцией по  $k$  найдем изотропные вектора  $u_1, \dots, u_k$  такие, что  $u_i$  ортогонален  $w_j$  при всех  $j \neq i$ , всем  $u_j$  и всем  $v_j$ . При этом  $B(u_i, w_i) = 1$ , а это и означает, что  $u$  – искомый набор.

По лемме 2.2 подпространство  $\langle v \rangle$  невырождено. Подпространство  $\langle w \cup u \rangle$  невырождено, так как матрица сужения формы  $B$  на него невырождена. Наконец ортогональная сумма двух невырожденных подпространств невырождена.  $\square$

**СЛЕДСТВИЕ 9.7** (Теорема о продолжении изометрии). Пусть  $(V, Q)$  – невырожденное квадратичное пространство,  $W_1, W_2$  – подпространства в  $V$  такие, что существует изометрия  $L: W_1 \rightarrow W_2$ . Тогда существует изометрия  $M: V \rightarrow V$  такая, что  $M|_{W_1} = L$ .

**ДОКАЗАТЕЛЬСТВО.** В случае, когда  $W_1$  невырождено, утверждение следует из теоремы Витта о сокращении. Действительно, в этом случае по предложению 4.6  $V$  раскладывается в прямую сумму  $W_i$  и его ортогонального дополнения ( $i = 1, 2$ ). По теореме о сокращении существует изометрия  $L': W_1^\perp \rightarrow W_2^\perp$ . Тогда изометрия  $M: V = W_1 \oplus W_1^\perp \rightarrow W_2 \oplus W_2^\perp = V$  задается формулой  $M(x + y) = L(x) + L'(y)$  при  $x \in W_1, y \in W_1^\perp$ .

Пусть теперь  $W_1$  – вырожденное подпространство в невырожденном пространстве  $V$ . Выберем базис  $w = (w_1, \dots, w_k)$  пространства  $W_1 \cap W_1^\perp$  и дополним его до базиса  $w \cup v$  пространства  $W_1$ . Выберем набор  $u = (u_1, \dots, u_k)$ , удовлетворяющий условиям леммы 9.6. Так как  $L$  изометрия, то  $L(w)$  является базисом пространства  $W_2 \cap W_2^\perp$ , а  $L(w) \cup L(v)$  – базисом  $W_2$ . Выберем набор  $u' = (u'_1, \dots, u'_k)$ , удовлетворяющий условиям леммы 9.6 с  $W = W_2$ . Продолжим  $L$  на пространство  $W'_1 = W_1 + \langle u \rangle$ , положив  $L(u) = u'$  и продолжив по линейности. Так как матрицы сужений формы  $Q$  на  $\langle w \cup u \rangle$  и  $\langle L(w) \cup L(u) \rangle$  в базисах  $w \cup u$  и  $L(w) \cup L(u)$  совпадают, то сужение  $L$  на эти подпространства является изометрией. С другой стороны, сужение  $L$  на  $\langle v \rangle$  и было изометрией этого пространства на  $\langle L(v) \rangle$ . Так как  $\langle w \cup u \rangle \perp \langle v \rangle$ , а  $\langle L(w) \cup L(u) \rangle \perp \langle L(v) \rangle$ , то определенное выше продолжение  $L$  является изометрией  $W'_1 \rightarrow W'_2 = W_2 + \langle u' \rangle$ . Наконец, по той же самой лемме 9.6 пространство  $W'_1$  невырождено, и по первому абзацу доказательства  $L$  можно продолжить с него на все пространство  $V$ .  $\square$

**СЛЕДСТВИЕ 9.8.** Индекс Витта равен размерности максимального полностью изотропного подпространства (т. е. подпространства, сужение формы на которое нулевое). Более того, все максимальные изотропные подпространства переводятся друг в друга изометриями.

## 10. Симплектические формы

Симплектическая форма – это билинейная антисимметричная форма. В отличие от квадратичных форм, определение симплектической формы не зависит от характеристики поля, надо только

правильно определять понятие антисимметричности, см. параграф 1. Некоторая часть теории эрмитовых форм переносится и на симплектические формы,<sup>6</sup> основным же отличием является то, что любой вектор изотропен и, следовательно, нет никаких шансов диагонализировать матрицу симплектической формы. К счастью, любая симплектическая форма приводится к очень простому каноническому виду, причем все симплектические пространства (т. е. пространства с симплектической формой) одной размерности изометричны. Группа линейных преобразований, сохраняющих симплектическую форму, называется симплектической группой. Наряду с полной линейной, унитарной, ортогональной группами и некоторыми их модификациями, симплектическая группа является *классической группой*. Классические группы являются примерами полупростых групп Ли (над  $\mathbb{R}$  или  $\mathbb{C}$ ) и алгебраических групп (над произвольным полем), и играют огромную роль во многих отраслях математики от чистой алгебры до механики. В частности, из классических групп над конечными полями строится большая часть простых конечных групп (обычно, факторгруппа коммутанта классической группы по центру проста), а симплектические многообразия (нечто, склеенное из кусков симплектических пространств) и симплектическая группа являются чуть ли не основой гамильтоновой механики.

В этом параграфе мы докажем только классификацию конечномерных невырожденных симплектических пространств. Заметим сначала, что матрица симплектической формы в любом базисе кососимметрическая, т. е.  $A^T = -A$ . Пусть  $V$  – двумерное пространство с ненулевой симплектической формой  $B$ . Существует пара векторов  $v_1, v_2$  для которых  $B(v_1, v_2) \neq 0$ . Домножая  $v_2$  на подходящую константу, можно считать, что  $B(v_1, v_2) = 1$ . Так как  $B(v_1, v_1) = 0$ , то отсюда сразу следует линейная независимость  $v_1$  и  $v_2$ . В базисе  $v = (v_1, v_2)$  матрица формы  $B$  имеет вид

$$B_v = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Таким образом, все двумерные невырожденные симплектические пространства изометричны между собой. Такое пространство будем называть симплектической плоскостью.

**ТЕОРЕМА 10.1.** *Любое невырожденное симплектическое пространство имеет четную размерность и изометрично ортогональной сумме симплектических плоскостей.*

**ДОКАЗАТЕЛЬСТВО.** Из сказанного выше следует, что любая пара векторов пространства  $V$ , на которых симплектическая форма  $B$  не равна нулю, порождают симплектическую плоскость  $S$ . Также как в доказательстве леммы 4.6 легко видеть, что  $\dim S^{\perp_B} = \dim V - 2$  и  $S \cap S^{\perp_B} = \{0\}$ . Поэтому  $V = S \oplus S^{\perp_B}$  и  $(S^{\perp_B})^{\perp_B} = S$ . Так как  $S^{\perp_B} \cap (S^{\perp_B})^{\perp_B} = \{0\}$ , то подпространство  $S^{\perp_B}$  невырождено, можно применить индукцию по размерности пространства  $V$ . Так как размерность падает на 2, то база индукции – случай размерности 0 или 1. Первый из них тривиален, а во втором надо только заметить, что любая симплектическая форма на одномерном пространстве нулевая, откуда следует, что невырожденных симплектических форм нечетной размерности не бывает.  $\square$

<sup>6</sup>Кусок теории эрмитовых форм переносится на полуторалинейные формы с довольно слабым условием симметрии:  $B(x, y) = 0 \iff B(y, x) = 0$ .

## Теория групп

Мы возвращаемся к изучению теории групп и рассмотрим в этой главе несколько базовых конструкций.

### 1. Свободные группы, задание группы образующими и соотношениями

Универсальное свойство свободной группы аналогично определению свободного модуля. Пусть  $X$  – множество. Группа  $F_X$  вместе с отображением  $i : X \rightarrow F_X$  называется *свободной группой с множеством образующих  $X$*  (или порожденной  $X$ , или свободной группой множества  $X$ ), если для любой функции  $f$  из  $X$  в группу  $G$  существует единственный гомоморфизм групп  $\tilde{f} : F_X \rightarrow G$  такой, что диаграмма

$$\begin{array}{ccc} X & \xrightarrow{i} & F_X \\ & \searrow f & \downarrow \tilde{f} \\ & & G \end{array}$$

коммутативна.

Как обычно, это определение ничего не говорит о существовании универсального объекта. Сейчас мы построим свободную группу и покажем, что она удовлетворяет сформулированному универсальному свойству. Пусть  $\bar{X} = \{\bar{x} \mid x \in X\}$  – множество символов. Для  $x \in X$  положим  $\bar{\bar{x}} = x$ . Рассмотрим множество  $W = W_X$ , состоящее из слов (включая пустое слово) в алфавите  $X \cup \bar{X}$ . Пусть  $Q$  – подмножество в  $W \times W$ , состоящее из всех пар  $(w_1 x \bar{x} w_2, w_1 w_2)$ ,  $w_1, w_2 \in W$ ,  $x \in X \cup \bar{X}$ . Обозначим через  $\sim$  наименьшее отношение эквивалентности на  $W$ , содержащее  $Q$ . Другими словами,  $u \sim v$  тогда и только тогда, когда  $u$  приводится к  $v$  при помощи вставки и стирания фрагментов вида  $x\bar{x}$ .

Пусть  $F_X = W / \sim$  – множество классов эквивалентности  $\sim$ . Определим операцию на  $F(X)$ , как конкатенацию слов. Точнее,  $[w_1] \cdot [w_2] = [w_1 w_2]$ , где  $w_1, w_2 \in W$ , а квадратные скобки означают класс эквивалентности, содержащий данное слово. Нетрудно проверить, что результат операции не зависит от выбора представителей классов эквивалентности. Очевидно, что операция ассоциативна, а нейтральным элементом является класс эквивалентности пустого слова. Обратный к  $[x_1 \dots x_n]$  – это элемент  $[\bar{x}_n \dots \bar{x}_1]$ , где  $x_1, \dots, x_n \in X \cup \bar{X}$ . Таким образом,  $F_X$  – группа.

**ТЕОРЕМА 1.1.** *Группа  $F_X$  вместе с отображением  $X \rightarrow F_X$ ,  $x \mapsto [x]$  является свободной группой с множеством образующих  $X$ .*

**ДОКАЗАТЕЛЬСТВО.** Заметим, что по определению умножения в  $F_X$  для  $x \in X$  имеем  $[x]^{-1} = [\bar{x}]$ . Для удобства обозначений, допуская вольность речи, будем писать  $x^{-1}$  вместо  $\bar{x}$ . Пусть  $f : X \rightarrow G$  – функция из  $X$  в группу  $G$ . Зададим отображение  $f' : W \rightarrow G$  формулой

$$f'(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} \cdot \dots \cdot f(x_n)^{\varepsilon_n}, \text{ где } x_1, \dots, x_n \in X, \varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}.$$

Так как  $f'(w_1 x \bar{x} w_2) = f'(w_1 w_2)$ , то отношение  $u \sim_{f'} v \iff f'(u) = f'(v)$  на  $W$  содержит  $Q$ . А так как оно является отношением эквивалентности, то оно содержит и отношение  $\sim$  на  $W$ , определенное выше. Другими словами,  $f'(u) = f'(v)$  при любых  $u \sim v$ . Поэтому функция

$$\tilde{f} : F_X \rightarrow G, \quad \tilde{f}([w]) = f'(w)$$

задана корректно. Теперь очевидно, что  $\tilde{f}$  является гомоморфизмом, причем  $\tilde{f}([x]) = f(x)$  для любого  $x \in X$ , что равносильно коммутативности диаграммы. Так как любой гомоморфизм  $F_X \rightarrow$

$G$ , делающий диаграмму коммутативной, должен отображать  $[x]$  в  $f(x)$ , а множество  $\{[x] \mid x \in X\}$  порождает  $F_X$ , то это отображение должно совпадать с  $\tilde{f}$ .  $\square$

Обычно элементы множества  $X$  отождествляют с их образами в  $F_X$ , т.е. с классами эквивалентности однобуквенных слов. Слово из  $W$  называется редуцированным, если оно не содержит вхождений  $x\bar{x}$  при  $x \in X \cup \bar{X}$ . Нетрудно выбрать редуцированного представителя в каждом классе эквивалентности.<sup>1</sup>

**ПРЕДЛОЖЕНИЕ 1.2.** *В каждом классе эквивалентности  $W/\sim$  есть ровно одно редуцированное слово. Оно имеет наименьшую длину среди всех слов из этого класса.*

**ДОКАЗАТЕЛЬСТВО.** Возьмем произвольное слово из фиксированного класса эквивалентности. Если оно не редуцированное, то выкинув из него вхождение  $x\bar{x}$  получим более короткое слово из того же класса. Доказательство существования заканчивает индукция по длине слова.

Доказательству единственности мешает неоднозначность алгоритма удаления вхождений  $x\bar{x}$  из нередуцированного слова. Значит, для однозначности надо придумать детерминированный алгоритм, который является проекцией на множество редуцированных слов, т.е. редуцированное слово переводит в себя, а нередуцированное – в редуцированное. Кроме того, надо доказать, что применение этого алгоритма к эквивалентным словам возвращает одно и то же. Так как эквивалентные слова связаны цепочкой вставок и удалений фрагментов  $x\bar{x}$ , то достаточно доказывать, что алгоритм возвращает одинаковые значения на словах  $w_1w_2$  и  $w_1x\bar{x}w_2$ , где  $w_1, w_2 \in W$ , а  $x \in X \cup \bar{X}$ .<sup>2</sup>

Определим функцию  $f : W \times W \rightarrow W \times W$  следующими равенствами:

$$\begin{aligned} f(w, \emptyset) &= (w, \emptyset); \\ f(\emptyset, xw) &= (x, w); \\ f(vy, xw) &= (vyx, w), \text{ если } y \neq \bar{x}; \\ f(v\bar{x}, xw) &= (v, w), \end{aligned}$$

где  $v, w \in W$ , а  $x, y \in X \cup \bar{X}$ . Так как длина второго слова под действием  $f$  убывает ровно на 1, пока оно не пустое, то  $f^k(\emptyset, w) = (w', \emptyset)$  для достаточно большого  $k$  (здесь  $f^k$  обозначает композицию  $f$  с собой  $k$  раз). В этом случае положим  $g(w) = w'$ . Это и есть наш алгоритм, он называется  $W$ -процессом. Легко проверить, что если  $v$  редуцированное слово, то первое слово в  $f(v, w)$  также является редуцированным. Поэтому  $g$  всегда возвращает редуцированное слово. Также очевидно, что редуцированное слово отображается в себя под действием  $g$ , потому что последнее правило из определения  $f$  ни разу не применяется.

Осталось доказать, что  $g(w_1w_2) = g(w_1x\bar{x}w_2)$ . Ясно, что

$$f^k(\emptyset, w_1w_2) = (g(w_1), w_2) \text{ и } f^k(\emptyset, w_1x\bar{x}w_2) = (g(w_1), x\bar{x}w_2),$$

где  $k$  – длина слова  $w_1$ . Далее, если  $g(w_1) = \emptyset$  или  $g(w_1) = vy$  при  $y \neq \bar{x}$ , то  $f^2(g(w_1), x\bar{x}w_2) = f(g(w_1)x, \bar{x}w_2) = (g(w_1), w_2)$ . В случае  $g(w_1) = v\bar{x}$ ,  $f^2(v\bar{x}, x\bar{x}w_2) = f(v, \bar{x}w_2) = (g(w_1), w_2)$ . Итак, в любом случае  $f^{k+2}(\emptyset, w_1x\bar{x}w_2) = f^k(\emptyset, w_1w_2)$ , следовательно,  $g(w_1w_2) = g(w_1x\bar{x}w_2)$ .  $\square$

Соотношением в группе называется равенство  $w = 1$ , где  $w$  элемент свободной группы на некотором множестве  $X$ . В дальнейшем мы иногда будем говорить “соотношение  $w$ ” вместо “соотношение  $w = 1$ ”. Если соотношение выполняется в группе для всех элементов (как, например,

<sup>1</sup>Следующее утверждение – из серии “очевидно, потому что очевидно”. Доказывать такие утверждения бывает, однако, нелегко, а главное, очень противно. Зачем доказывать то, что и так понятно? К сожалению уровень абстракции современной математики таков, что некоторые утверждения из этой серии оказываются неверными. Почти любой математик испытал это на себе, найдя контрпример к “очевидному” утверждению в начале своего доказательства какой-нибудь классной теоремы.

<sup>2</sup>Другими словами, если  $g(v) = g(w)$  при всех  $(v, w) \in Q$ , то эквивалентность  $v \stackrel{g}{\sim} w \iff g(v) = g(w)$  содержит эквивалентность  $\sim$ . Это соображение мы уже использовали выше.

$x^{-1}y^{-1}xy = 1$  в абелевой группе), то оно называется групповым тождеством. Мы же сейчас рассмотрим соотношения, которые выполнены для конкретных элементов. Пусть  $R$  – подмножество свободной группы на множестве  $X$ ,  $G$  группа, а  $f : X \rightarrow G$  – функция. Говорят, что в  $G$  выполняются соотношения  $R$ , если при подстановке в элементы из  $R$  вместо элементов множества  $X$  их образов в  $G$  получается верное равенство. Более строго, по универсальному свойству свободной группы существует единственный гомоморфизм  $\tilde{f} : F_X \rightarrow G$  такой, что  $\tilde{f} = f \circ i$ , где  $i$  – вложение  $X$  в  $F_X$ . Говорят, что в  $G$  выполняются соотношения  $R$ , если  $R \subseteq \text{Ker } \tilde{f}$ .<sup>3</sup>

Универсальная группа, удовлетворяющая соотношениям  $R$ , называется группой, заданной образующими  $X$  и соотношениями  $R$ , и обозначается через  $\langle X \mid R \rangle$ . Точнее, группа  $U = \langle X \mid R \rangle$  вместе с функцией  $X \rightarrow U$  называется группой заданной образующими  $X$  и соотношениями  $R$ , если в ней выполнены соотношения  $R$  и для любой группы  $G$  с соотношениями  $R$  существует единственный гомоморфизм  $U \rightarrow G$ , для которого диаграмма

$$\begin{array}{ccc} X & \longrightarrow & U \\ & \searrow & \downarrow \\ & & G \end{array}$$

коммутативна.

Пусть  $P \leq Q$  – группы, а  $S$  – подмножество в  $Q$ . Напомним, что подгруппа, порожденная  $S$ , – это наименьшая подгруппа  $\langle S \rangle$  в  $Q$ , содержащая  $S$ . Наименьшая нормальная подгруппа группы  $Q$ , содержащая подгруппу  $P$  называется нормальным замыканием  $P$  в  $Q$  и обозначается  $P^Q$ . Нетрудно видеть, что она порождена всеми элементами вида  $p^q$ ,  $p \in P$ ,  $q \in Q$ .

**ТЕОРЕМА 1.3.**  $\langle X \mid R \rangle \cong F_X / \langle R \rangle^{F_X}$ . Отображение из  $X$  в эту группу – это композиция канонического отображения  $X \rightarrow F_X$  с канонической проекцией  $F_X \rightarrow F_X / \langle R \rangle^{F_X}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $G$  – группа с соотношениями  $R$ . Функция  $X \rightarrow G$  индуцирует единственный гомоморфизм  $F_X \rightarrow G$ . По определению  $R$  лежит в ядре этого гомоморфизма. Так как ядро – это нормальная подгруппа, то подгруппа  $\langle R \rangle$  и ее нормальное замыкание также лежат в ядре. По универсальному свойству факторгруппы (теорема 5.3 главы 3) существует единственный гомоморфизм  $F_X / \langle R \rangle^{F_X} \rightarrow G$ , делающий следующую диаграмму коммутативной:

$$\begin{array}{ccccc} X & \longrightarrow & F_X & \longrightarrow & F_X / \langle R \rangle^{F_X} \\ & \searrow & \searrow & & \downarrow \\ & & & & G \end{array}$$

Таким образом, группа  $F_X / \langle R \rangle^{F_X}$  вместе с указанным отображением из множества  $X$  удовлетворяет определению группы, заданной образующими  $X$  и соотношениями  $R$ .  $\square$

Примеры групп, заданных образующими и соотношениями.

- (1)  $\mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid [x, y] \rangle = \langle x, y \mid [x, y] = 1 \rangle = \langle x, y \mid xy = yx \rangle$ .
- (2)  $D_n \cong \langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle$ .

## 2. Подгруппы свободной группы

**ТЕОРЕМА 2.1** (теорема Нильсена–Шрайера). *Любая подгруппа свободной группы свободна.*

**ЗАМЕЧАНИЕ 2.2.** При этом количество образующих подгруппы свободной группы с двумя образующими может быть любым от 1 до (счетной) бесконечности.

<sup>3</sup>Второе определение, в отличие от первого, не апеллирует к конструкции свободной группы, а только к ее универсальному свойству. Также как и для многочленов, подстановка значений вместо переменных – это образ элемента свободной группы, являющегося аналогом многочлена, под действием некоторого канонического гомоморфизма.

Существует несколько доказательств теоремы Нильсена–Шрайера. Мы приведем идеи двух геометрических доказательств и полностью изучим алгебраическое доказательство Шрайера, в котором явно строятся свободные образующие.

**ТОПОЛОГИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ НИЛЬСЕНА–ШРАЙЕРА.** Рассмотрим свободную группу  $F$  со свободной системой образующих  $X$ . Пусть, далее,  $Y$  – букет окружностей, занумерованных элементами множества  $X$ . Тогда  $F$  является фундаментальной группой  $Y$ . Каждая подгруппа  $H \leq F$  является фундаментальной группой какого-то накрытия пространства  $Y$ . Однако каждое накрытие  $Y$  само гомотопно букету окружностей. Но это и значит, что  $H$  свободна.  $\square$

Комбинаторно-геометрическое доказательство, приведенное в книге J.-P. Serre “Trees”, сразу следует из теоремы о свободном действии группы на дереве. Представим граф, как множество вершин  $V$ , множество ребер  $E$ , и функции  $s, t : E \rightarrow V$ , сопоставляющие ребру его начало (source) и конец (target). Говорят, что группа  $G$  действует на графе  $(V, E, s, t)$ , если задан гомоморфизм из  $G$  в группу автоморфизмов графа. Другими словами, задано действие  $G$  на множествах  $V$  и  $E$ , удовлетворяющие условиям:

$$gs(v) = s(gv) \text{ и } gt(v) = t(gv) \text{ для любых } g \in G \text{ и } v \in V.$$

Граф называется неориентированным, если задан автоморфизм  $\bar{\cdot}$  этого графа порядка 2 такой, что  $s(\bar{v}) = t(v)$  для любого ребра  $v \in V$  (в этом случае ребра  $v$  и  $\bar{v}$  рассматриваются как одно неориентированное ребро. Будем говорить, что группа  $G$  действует свободно на неориентированном графе  $(V, E, s, t, \bar{\cdot})$ , если она действует свободно на множестве вершин и  $gv \neq \bar{v}$  для всех  $g \in G$  и  $v \in V$ . Неориентированный граф без циклов называется деревом.

Графом Кэли группы  $G$  относительно системы образующих  $S$  называется неориентированный граф, вершинами которого являются элементы группы, а неориентированные ребра соответствуют парам  $(g, gs)$  по всем  $g \in G$  и  $s \in S$ . Группа очевидным образом действует на своем графе Кэли: действие на вершинах – это левое умножение, при этом ребро  $(g, gs)$  переходит в ребро  $(hg, hgs)$  под действием элемента  $h$ . Заметим, что это действие свободно тогда и только тогда, когда  $S$  не содержит инволюций (т. е. элементов порядка 2).

**ЛЕММА 2.3.** *Граф Кэли группы  $G$  является деревом, на котором группа действует свободно, тогда и только тогда, когда  $S$  свободно порождает  $G$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $s_1, \dots, s_n \in S \cup S^{-1}$ , а  $w = s_1 \dots s_n \in F_S$  – редуцированное слово. Канонический образ  $w$  в  $G$  равен  $e_G$  тогда и только тогда, когда ребра, соединяющие вершины  $e_G, s_1, s_1 s_2, \dots, s_1 \dots s_n = e_G$  образуют цикл. Условие свободы действия необходимо для того, чтобы исключить образующие порядка 2, которые по нашему соглашению образуют не цикл, а определяют неориентированное ребро.  $\square$

Таким образом, свободная группа свободно действует на некотором дереве. Оказывается, верно и обратное.

**ТЕОРЕМА 2.4.** *Группа свободно действует на дереве тогда и только тогда, когда она свободна.*

Отсюда сразу следует теорема Нильсена–Шрайера, потому что любая подгруппа свободной группы свободно действует на том же дереве, на котором свободно действует вся группа.

Третье доказательство теоремы Нильсена–Шрайера основано на следующих двух утверждениях. Пусть  $X \subseteq G$  – порождающее множество группы  $G$ ,  $H \leq G$ , а  $Y$  – система представителей левых смежных классов  $G$  по  $H$ , т. е.  $G = HY$ , причем, если  $Hu_1 = Hu_2$  для  $u_1, u_2 \in Y$ , то  $u_1 = u_2$ . Будем считать, что  $H \cap Y = \{1\}$ . Рассмотрим проекцию  $G \rightarrow Y$ ,  $g \mapsto \bar{g}$ , которая каждому  $g \in G$  сопоставляет тот единственный  $\bar{g} \in Y$ , для которого  $H\bar{g} = Hg$ . По нашему соглашению относительно представителя  $H$  для любого  $h \in H$  имеем  $\bar{h} = 1$ .

**ТЕОРЕМА 2.5** (Теорема Шрайера). *Подгруппа  $H$  порождается множеством*

$$Z = \{yx \cdot (\overline{yx})^{-1} \mid y \in Y, x \in X\}.$$

**ДОКАЗАТЕЛЬСТВО.** Так как  $Hux = H\overline{ux}$ , все элементы из  $Z$  действительно лежат в  $H$ . Для доказательства того, что они порождают  $H$ , воспользуемся “трюком накопления”. Запишем элемент  $h \in H$  в виде произведения образующих:  $h = x_1 \dots x_l$ , где  $x_1, \dots, x_l \in X \cup X^{-1}$ . Так как  $\overline{x_1 \dots x_l} = \overline{h} = 1$ , то можно переписать выражение для  $h$  в виде

$$h = (1 \cdot x_1(\overline{1 \cdot x_1})^{-1})(\overline{x_1 x_2}(\overline{x_1 x_2})^{-1})(\overline{x_1 x_2 x_3}(\overline{x_1 x_2 x_3})^{-1}) \dots (\overline{x_1 \dots x_{l-1} x_l}(\overline{x_1 \dots x_l})^{-1}),$$

Докажем, что все сомножители в правой части лежат в  $Z \cup Z^{-1}$ . Прежде всего, заметим, что, так как  $H\overline{g_1} = Hg_1$ , то  $H\overline{g_1 g_2} = Hg_1 g_2$ , откуда  $\overline{g_1 g_2} = \overline{g_1} \overline{g_2}$  для любых  $g_1, g_2 \in G$ . Если  $x_k \in X$ , то

$$\overline{x_1 \dots x_{k-1} x_k}(\overline{x_1 \dots x_k})^{-1} = yx_k \cdot (\overline{yx_k})^{-1} \in Z,$$

где  $y = \overline{x_1 \dots x_{k-1}} \in Y$ .

Пусть теперь  $x_k = x^{-1}$  для некоторого  $x \in X$ , а  $y \in Y$ . Положим  $\tilde{y} = \overline{yx^{-1}}$ . Тогда  $\tilde{y}x = \overline{yx^{-1}x} = y$ . Следовательно,

$$(yx^{-1} \cdot (\overline{yx^{-1}})^{-1})^{-1} = \tilde{y}x \cdot y^{-1} = \tilde{y}x \cdot (\tilde{y}x)^{-1} \in Z.$$

Таким образом,  $yx_k \cdot (\overline{yx_k})^{-1} \in Z^{-1}$ , что завершает доказательство.  $\square$

**СЛЕДСТВИЕ 2.6.** *Подгруппа конечного индекса в конечнопорожденной группе конечно порождена.*

Следующее утверждение, также принадлежащее Шрайеру, говорит о выборе “хорошего” множества представителей смежных классов по подгруппе  $H$  свободной группы  $F_X$ . Пусть  $U \subseteq F_X$ , а  $g \in F_X$ . Обозначим через  $l(g)$  длину редуцированного слова в алфавите  $X \cup X^{-1}$  равного  $g$  и положим  $l(U) = \min_{g \in U} l(g)$ . Система представителей  $Y$  смежных классов  $F_X$  по  $H$  называется минимальной, если для любого  $g \in F_X$  длина представителя  $\bar{g}$  смежного класса  $Hg$  равна  $l(Hg)$ . Система  $Y$  называется шрайеровской трансверсалью, если любой начальный отрезок редуцированного слова из  $Y$  принадлежит  $Y$  (в частности, пустое слово принадлежит  $Y$ ). Ясно, что достаточно требовать, чтобы для каждого редуцированного слова  $x_1 \dots x_n \in Y$  слово  $x_1 \dots x_{n-1}$  также лежало бы в  $Y$  (т. е. брать отрезки на 1 меньшей длины).

**ЛЕММА 2.7.** *Для любой подгруппы  $H \leq F_X$  существует минимальная шрайеровская трансверсаль  $Y$ .*

**ДОКАЗАТЕЛЬСТВО.** Строим представитель  $Y \cap Hg$  индукцией по  $n = l(Hg)$ . При  $n = 0$  выбираем нейтральный элемент (пустое слово). Пусть теперь  $n > 0$ , а  $h = x_1 \dots x_n$ ,  $x_i \in X \cup X^{-1}$ , – слово наименьшей длины в  $Hg$ . Пусть  $u = x_1 \dots x_{n-1}$  – начальный отрезок этого слова. Так как  $l(Hu) < n$ , то по индукционному предположению мы уже выбрали представителя  $Hu$  в  $Y$ . Пусть, скажем,  $H\bar{u} = Hu$ , где  $\bar{u}$  – такой представитель,  $l(\bar{u}) = m \leq n - 1$ , а  $\bar{u} = t_1 \dots t_m$ ,  $t_i \in X \cup X^{-1}$ , – его приведенное разложение. Тогда  $H\bar{u}x_n = Hux_n = Hh = Hg$ . Так как  $h$  – элемент наименьшей длины в своем смежном классе, то  $m + 1 \geq l(\bar{u}x_n) \geq l(h) = n$ . Таким образом,  $m = n - 1$  и значит,  $y = \bar{u}x_n = t_1 \dots t_{n-1}x_n$  является приведенным разложением  $y$ . Выберем  $y$  в качестве представителя смежного класса  $Hg$ . Очевидно, что для него выполняется условие, фигурирующее в определении минимальной шрайеровской системы.  $\square$

Пусть  $H$  произвольная группа, а  $Z$  – произвольная система образующих  $H$  такая, что  $Z \cap Z^{-1} = \emptyset$ . Для того чтобы доказать, что  $H \cong F_Z$ , достаточно проверить, что непустое редуцированное слово в алфавите  $Z \cup Z^{-1}$  не равно 1 в  $H$ . Действительно, по универсальному свойству свободной группы существует единственный гомоморфизм  $\varphi : F_Z \rightarrow H$ , отображающий однобуквенные слова в соответствующие элементы множества  $Z$ . Так как система образующих группы  $H$  лежит в образе  $\varphi$ , то  $\varphi$  сюръективно. Ядро  $\varphi$  – это множество редуцированных слов (точнее, их классов эквивалентности), которые отображаются в  $1_H$ , а приведенное выше условие как раз и говорит,

что таких непустых слов не существует. Это простое соображение вместе с двумя предыдущими леммами лежит в основе нашего доказательства теоремы Нильсена–Шрайера.

**ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ НИЛЬСЕНА–ШРАЙЕРА.** Пусть  $H$  – подгруппа свободной группы  $F_X$ ,  $Y$  – шрайеровская трансверсаль к  $H$  (не обязательно минимальная), существование которой обеспечивает предыдущая лемма, а  $\pi : F_X \rightarrow Y$  – проекция из теоремы 2.5. Также как в теореме 2.5 возьмем систему образующих

$$Z = Z(X) = \{yx(\overline{yx})^{-1} \mid y \in Y, x \in X\} \setminus \{1\}$$

группы  $H$  (естественно, единичный элемент можно выбросить из системы образующих) и докажем, что множество  $Z$  свободно порождает  $H$ .

Легко видеть (это уже было в доказательстве теоремы Шрайера), что  $Z(X)^{-1} \subseteq Z(X^{-1})$ . Аналогично,  $Z(X^{-1})^{-1} \subseteq Z(X)$ , откуда  $Z(X)^{-1} = Z(X^{-1})$ . Таким образом,  $Z \cup Z^{-1} = Z(X \cup X^{-1})$ .

Начнем с доказательства того, что естественное представление элемента из  $Z(X \cup X^{-1})$  несократимо. Пусть  $x \in X \cup X^{-1}$ , а  $y \in Y$ . Ясно, что

$$yx \in Y \iff yx = \overline{yx} \iff yx(\overline{yx})^{-1} = 1.$$

Пусть  $y = x_1 \dots x_n$  и  $\tilde{y} = \overline{yx} = t_1 \dots t_m$  представлены редуцированными словами, где  $x_i, t_i \in X \cup X^{-1}$ . Если  $yx \notin Y$ , то слово  $x_1 \dots x_n x t_m^{-1} \dots t_1^{-1}$ , представляющее элемент  $yx\tilde{y}^{-1}$  из  $Z(X \cup X^{-1})$ , также редуцировано. Действительно, если  $x = x_n^{-1}$ , то  $yx = x_1 \dots x_{n-1} \in Y$ , так как система представителей шрайеровская, а если  $x = t_m$ , то  $\tilde{y}x^{-1} = t_1 \dots t_{m-1} \in Y$ , по той же причине. Но тогда  $\tilde{y}x^{-1} = \tilde{y}x^{-1} = \overline{yx}x^{-1} = y$ , откуда опять  $yx = \tilde{y} \in Y$ , что противоречит предположению. В других же местах сокращения не могут произойти.

Далее рассмотрим произведения двух элементов  $z = yx(\overline{yx})^{-1}$  и  $z' = uv(\overline{uv})^{-1}$  из  $Z \cup Z^{-1}$  (т. е.  $x, v \in X \cup X^{-1}$ , а  $y, u \in Y$ ). Положим,  $\tilde{u} = \overline{uv}$  и предположим, что  $z' \neq z^{-1}$ . Докажем, что при этом условии

$$v\tilde{u}^{-1}yx = vwx, \quad \text{т. е.} \quad z'z = uvwx(\overline{yx})^{-1},$$

где  $w$  и  $vwx$  несократимые слова (при этом  $w$  может быть пустым). Пусть  $\tilde{u} = t_1 \dots t_k$  и  $y = x_1 \dots x_m$  – редуцированные слова (здесь  $x_i, t_i \in X \cup X^{-1}$ ). Так как  $z$  и  $z'$  не равны 1, то их естественные представления несократимы, т. е.  $v \neq t_k$ , а  $x \neq x_m^{-1}$ . Для определенности предположим, что  $k \geq m$  (ситуация  $m < k$  аналогична случаю  $m > k$ ). Если  $y \neq t_1 \dots t_m$ , то  $v\tilde{u}^{-1}yx = vwx$ , где  $w$  – несократимое слово начинающееся с  $t_k^{-1}$  и заканчивающееся  $x_m$ . Следовательно, слово  $vwx$  также редуцировано.

Пусть теперь  $y = t_1 \dots t_m$ . Если  $k = m$ , то  $v\tilde{u}^{-1}yx = vx$ . Если  $v = x^{-1}$ , то  $(\overline{yx})^{-1} = (\overline{uv^{-1}})^{-1} = u^{-1}$ , следовательно,  $z' = z^{-1}$ , что противоречит предположению. В противном случае возьмем в качестве  $w$  пустое слово. Наконец, если  $k > m$ , то  $v\tilde{u}^{-1}yx = vt_k^{-1} \dots t_{m+1}^{-1}x$ . Если  $x \neq t_{m+1}$ , то последнее слово несократимо. В противном случае  $yx = t_1 \dots t_{m+1}$ , что лежит в  $Y$ , так как это начало слова  $v \in Y$ , а  $Y$  шрайеровская. Но это противоречит предположению о том, что  $z \neq 1$ .

Из доказательства следует, что если  $z' = z^{-1}$ , то  $v = x^{-1}$ , а это невозможно при  $v, x \in X$ . Поэтому пересечение  $Z(X) \cap Z(X)^{-1}$  пусто.

Доказательство заканчивает индукция по длине произведения элементов из  $Z \cup Z^{-1}$ . Пусть  $z_i = y_i x_i (\overline{y_i x_i})^{-1} \in Z \cup Z^{-1}$ . Индукцией по  $n$  докажем, что редуцированная форма элемента  $z_1 \dots z_n$  оканчивается на  $x_n (\overline{y_n x_n})^{-1}$  и, следовательно, это произведение не равно 1. База  $n = 1$  уже доказана там, где говорится, что  $xy(\overline{yx})^{-1}$  либо равно 1, либо несократимо (естественно, везде предполагается, что  $(\overline{yx})^{-1}$  записано редуцированным словом).

По индукционному предположению  $z_1 \dots z_{n-1} = tx_{n-1}(\overline{y_{n-1}x_{n-1}})^{-1}$ . По доказанному ранее  $x_{n-1}(\overline{y_{n-1}x_{n-1}})^{-1}y_n x_n = x_{n-1}wx_n$ , причем последняя запись несократима. Следовательно,

$$z_1 \dots z_n = tx_{n-1}(\overline{y_{n-1}x_{n-1}})^{-1}y_n x_n (\overline{y_n x_n})^{-1} = tx_{n-1}wx_n (\overline{y_n x_n})^{-1}.$$

□



Рассмотрим следующий пример. Пусть  $X = \{t, x\}$  и  $F = F_X$  – свободная группа с двумя образующими. Построим множество шрайеровских образующих коммутанта группы  $F$ . Ясно, что факторгруппа по коммутанту – это свободная абелева группа (т.е. свободный  $\mathbb{Z}$ -модуль) с двумя образующими. Короче,  $F/[F, F] \cong \mathbb{Z} \oplus \mathbb{Z}$ . Естественный представитель класса эквивалентности, отображающегося в  $(n, k)$  – элемент  $t^n x^k$ . Ясно, что трансверсаль  $Y = \{t^n x^k \mid n, k \in \mathbb{Z}\}$  является шрайеровской. Далее,  $(t^n x^k)x \in Y$ , поэтому из таких произведений не возникают элементы шрайеровской системы образующих. Зато  $(t^n x^k)t \notin Y \iff k \neq 0$ , и  $(t^n x^k)t = t^{n+1}x^k$ . Таким образом,

$$(t^n x^k)t(t^{n+1}x^k)^{-1} = t^n x^k t x^{-k} t^{-n-1} \in Z$$

(заметим, что последний элемент является коммутатором  $[t^n x^k t^{-n}, t]$ ). Легко видеть, что все такие слова являются редуцированными и, следовательно, различны в  $F$ . По доказательству теоремы Нильсена–Шрайера получаем, что подгруппа  $[F, F]$  свободно порождена множеством  $Z = \{t^n x^k t x^{-k} t^{-n-1} \mid k, n \in \mathbb{Z}, k \neq 0\}$  и является свободной группой со счетным числом образующих.

### 3. Действие группы на множестве и лемма Бернсайда

**ОПРЕДЕЛЕНИЕ 3.1.** Пусть  $G$  – группа, а  $X$  – множество. Будем говорить, что  $G$  действует на  $X$  и писать  $G \curvearrowright X$ , если задана операция  $G \times X \rightarrow X$  (образ пары  $(g, x)$  обозначается обычно просто  $gx$ ), обладающая для любого  $x \in X$  и  $g, h \in G$  следующими свойствами:

- (1)  $g(hx) = (gh)x$  (внешняя ассоциативность);
- (2)  $1 \cdot x = x$  (унитальность).

Напомним, что для множества  $X$  множество всех биективных функций  $X \rightarrow X$  с операцией композиции называется *симметрической группой* на множестве  $X$  и обозначается через  $S_X$ . Заметим, что любой гомоморфизм  $\theta : G \rightarrow S_X$  задает действие группы  $G$  на множестве  $X$  по правилу  $gx = \theta(g)(x)$  (проверьте, что эта операция действительно удовлетворяет условиям определения 3.1). Обратно, если задано действие  $G$  на  $X$ , то можно задать гомоморфизм  $\theta : G \rightarrow S_X$  формулой  $\theta(g)(x) = gx$  (проверьте, что  $\theta(g)$  – биекция, и что  $\theta$  – гомоморфизм). Таким образом, можно считать, что действие группы на множестве – это гомоморфизм  $G \rightarrow S_X$ , что является равносильным определением действия группы на множестве.

На самом деле мы определили левое действие  $G \curvearrowright X$ . Правое действие  $X \curvearrowleft G$  определяется аналогично.

**ОПРЕДЕЛЕНИЕ 3.2.** Будем говорить, что  $G$  действует справа на  $X$  и писать  $X \curvearrowleft G$ , если задана операция  $X \times G \rightarrow X$  (образ пары  $(x, g)$  обычно обозначается через  $xg$ ), обладающая для любого  $x \in X$  и  $g, h \in G$  следующими свойствами:

- (1)  $(xg)h = x(gh)$ ;
- (2)  $x \cdot 1 = x$ .

Правому действию соответствует антигомоморфизм  $\eta_X : G \rightarrow S_X$ . Из правого действия довольно просто сделать левое действие, взяв композицию

$$G \xrightarrow{inv} G \xrightarrow{\eta_X} S_X, \text{ где } inv(g) = g^{-1}.$$

**Пример.** Пусть  $X, Y$  – множества,  $G$  – группа, а  $Y^X$  – множество функций из  $X$  в  $Y$ . Если  $G \curvearrowright X$ , то  $Y^X \curvearrowleft G$  по правилу:  $fg = f \circ \theta_X(g)$ . Но тогда формула  $gf = f \circ \theta_X(g^{-1})$  задает левое действие. Другими словами,  $(gf)(x) := f(g^{-1}x)$ .

Введем теперь некоторые понятия, связанные с действием группы  $G$  на множестве  $X$ .

**ОПРЕДЕЛЕНИЕ 3.3.** Орбитой элемента  $x \in X$  под действием  $G$  называется множество  $Gx = \{gx \mid g \in G\}$ . Количество элементов в данной орбите называется *длиной орбиты* (в разных орбитах может быть разное количество элементов).

**ЛЕММА 3.4.** Любые две орбиты либо не пересекаются, либо совпадают. Таким образом, множество  $X$  разбивается в дизъюнктное объединение орбит.

Доказательство этого утверждения практически совпадает с доказательством аналогичного утверждения для смежных классов.

**ОПРЕДЕЛЕНИЕ 3.5.** Неподвижными точками элемента  $g \in G$  называются те  $x \in X$ , для которых  $gx = x$ . Множество неподвижных точек элемента  $g$  мы будем обозначать через  $\text{Fix}_X(g)$ .

**ОПРЕДЕЛЕНИЕ 3.6.** Множество элементов группы  $G$ , оставляющих на месте данный элемент  $x \in X$  называется стабилизатором элемента  $x$  и обозначается через  $G_x$ . Другими словами,  $G_x = \{g \in G \mid gx = x\}$ . Очевидно, что стабилизатор является подгруппой в  $G$ .

**ЗАМЕЧАНИЕ 3.7.** Обратите внимание на то, что количество пар  $(g, x) \in G \times X$ , для которых  $gx = x$  можно вычислить двумя способами, которые указаны в разных частях следующего равенства:

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |\text{Fix}_X(g)|.$$

Последнее равенство, несмотря на свою очевидность, играет важную роль при доказательстве важного комбинаторного приложения теории групп, леммы Бернсайда. Второе ключевое соображение приведено в следующей лемме. Здесь  $G/G_x$  обозначает множество левых смежных классов (оно не обязано быть подгруппой, потому что  $G_x$ , вообще говоря, не является нормальной подгруппой).

**ЛЕММА 3.8.** Отображение  $f : G/G_x \rightarrow Gx$ , заданное формулой  $f(gG_x) = gx$ , является биекцией. В частности, длина орбиты элемента  $x$  равна индексу стабилизатора этого элемента:  $|Gx| = |G : G_x|$ .

**ДОКАЗАТЕЛЬСТВО.** Очевидно,  $gx = gg'x$  для любого  $g' \in G_x$ , поэтому  $f$  задана корректно (определение не зависит от выбора представителя смежного класса). Сюръективность  $f$  сразу следует из определения орбиты. Предположим, что  $f(gG_x) = f(hG_x)$ , т.е.  $gx = hx$ . Но тогда  $h^{-1}gx = x$ , откуда  $h^{-1}g \in G_x$ , а из этого сразу следует, что  $gG_x = hG_x$ .  $\square$

**ОПРЕДЕЛЕНИЕ 3.9.** Пусть  $G \curvearrowright X$ .

- Действие называется точным, если  $\text{Ker}(\theta_X) = \{1\}$ , другими словами, если из того что  $\forall x \in X : gx = x$  следует, что  $g = 1$ .
- Действие называется свободным, если  $gx = x \implies g = 1$ , другими словами, если  $\forall x \in X : G_x = \{1\}$ .
- Действие называется транзитивным, если  $\forall x, y \in X \exists g \in G : gx = y$ , другими словами,  $\forall x \in X : Gx = X$  (квантор не имеет значения, равносильно можно написать  $\exists x \in X : Gx = X$ ).

**Примеры.**

- $S_n \curvearrowright \{1, \dots, n\}$ .
- $\text{GL}_n(R) \curvearrowright R^n$ .
- $G \curvearrowright G$ ,  $gx$  – умножение в группе (регулярное действие или действие левыми трансляциями) Оно является свободным и транзитивным.
- $G \curvearrowright G$ ,  ${}_gx := gxg^{-1}$  – действие левым сопряжением.

$\text{Ker}(G \rightarrow S_G) = C(G)$  – центр группы  $G$ . Орбита называется классом сопряженных элементов.

- $G \curvearrowright G$ ,  $x^g := g^{-1}xg$  – действие правым сопряжением. Это правое действие.
- $G \times G \curvearrowright G : (g, h)x := gxh^{-1}$ .
- $G \curvearrowright X$ ,  $H \leq G \implies H \curvearrowright X$ .

Если  $H \curvearrowright G$  левыми трансляциями, то орбиты – правые смежные классы.

Лемма Бернсайда вычисляет количество орбит действия группы на множестве с помощью суммы по всем элементам группы. Она применяется в том случае, когда порядок множества  $X$  намного больше, чем порядок группы  $G$ .

**ТЕОРЕМА 3.10** (лемма Бернсайда). *Количество орбит действия группы  $G$  на множестве  $X$  равно*

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}_X(g)|.$$

**ДОКАЗАТЕЛЬСТВО.** Обозначим число орбит через  $N$ . Каждый элемент  $x \in X$  лежит в орбите  $Gx$ . Сопоставим ему число  $\frac{1}{|Gx|}$ . Сумма этих чисел по всем  $x$  из данной орбиты  $\mathcal{O}$  очевидно равна 1 (мы просто  $|\mathcal{O}|$  раз складываем число  $\frac{1}{|\mathcal{O}|}$  с самим собой). Поэтому количество орбит можно вычислить по формуле  $N = \sum_{x \in X} \frac{1}{|Gx|}$ . Подставляя сюда формулу для длины орбиты из леммы 3.8 получим  $N = \sum_{x \in X} \frac{|Gx|}{|G|} = \frac{1}{|G|} \sum_{x \in X} |Gx|$ . Используя формулу из замечания 3.7 получим  $N = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}_X(g)|$ , что и требовалось доказать.  $\square$

#### 4. Классификация $G$ -множеств

Перейдем теперь к классификации действий данной группы  $G$  на множестве. При этом удобно будет говорить, что если  $G$  действует на множестве  $X$ , то  $X$  является  $G$ -множеством (по аналогии с  $R$ -модулем). Во-первых, надо понять, с точностью до чего будет происходить классификация, т. е. что такое изоморфизм  $G$ -множеств.

**ОПРЕДЕЛЕНИЕ 4.1.** Пусть  $X, Y$  –  $G$ -множества. Функция  $f : X \rightarrow Y$  называется  $G$ -эквивариантной, если  $f(gx) = g f(x)$  для любых  $x \in X$  и  $g \in G$ .

Изоморфизмами  $G$ -множеств являются  $G$ -эквивариантные биекции.

В этом параграфе мы дадим классификацию  $G$ -множеств с точностью до изоморфизма.

**ЛЕММА 4.2.** *Стабилизаторы точек из одной орбиты сопряжены.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $x \in X$ , а  $y \in Gx$ , т. е. существует  $g \in G$  такое, что  $y = gx$ . Тогда

$$h \in G_y \iff hy = y \iff hgx = gx \iff g^{-1}hgx = x \iff g^{-1}hg \in G_x.$$

Таким образом,  $G_x = g^{-1}G_yg$ , что и требовалось.  $\square$

**ОПРЕДЕЛЕНИЕ 4.3.** Если  $G \curvearrowright X$  транзитивно, то  $X$  называется однородным  $G$ -множеством.

Если  $H$  – подгруппа в  $G$ , то  $G$  действует на множестве левых смежных классов  $G/H$  по формуле  $g(xH) = (gx)H$ ,  $g, x \in G$ . Такое действие называется стандартным однородным  $G$ -множеством.

**ТЕОРЕМА 4.4.** *Любое однородное  $G$ -множество  $X$  изоморфно стандартному однородному  $G$ -множеству. Точнее,  $X \cong G/G_x$  для любой точки  $x \in X$ .*

*$G$ -множества  $G/H$  и  $G/F$  изоморфны тогда и только тогда, когда подгруппы  $H$  и  $F$  сопряжены.*

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим функцию  $\varphi : G/G_x \rightarrow Gx = X$ ,  $\varphi(gG_x) = gx$ , заданную в лемме 3.8, где проверено, что это отображение биективно. Проверка того, что это отображение  $G$ -эквивариантно, не составляет труда.

Пусть  $F = gHg^{-1}$ . Докажем, что  $F = G_{gH}$  – стабилизатор элемента  $gH$  при действии  $G$  на  $G/H$ . Действительно,

$$f(gH) = gH \iff g^{-1}fgH = H \iff g^{-1}fg \in H \iff f \in gHg^{-1} = F.$$

Следовательно, по первой части доказательства  $G/H \cong G/F$ .

Обратно, пусть  $\varphi$  – изоморфизм  $G$ -множеств  $G/H \xrightarrow{\sim} G/F$ , а  $\varphi(H) = gF$ . Для любого  $h \in H$  имеем:  $gF = \varphi(H) = \varphi(hH) = h\varphi(H) = hgF$ , откуда  $g^{-1}hg \in F$ . Таким образом,  $g^{-1}Hg \subseteq F$ .

Для доказательства обратного включения заметим, что  $\varphi(H) = gF \iff F = \varphi(g^{-1}H) \iff \varphi^{-1}(F) = g^{-1}H$ . Следовательно, для любого  $f \in F$  имеем  $g^{-1}H = \varphi^{-1}(fF) = f\varphi^{-1}(F) = fg^{-1}H$ , откуда  $fgf^{-1} \in H$ .  $\square$

**СЛЕДСТВИЕ 4.5** (классификация  $G$ -множеств). Любое  $G$ -множество изоморфно  $\bigsqcup_{i \in \mathcal{I}} G/H_i$ , где  $\mathcal{I}$  – некоторое множество индексов, а  $H_i$  – подгруппа в  $G$ . Такое представление единственно, с точностью до перестановки элементов множества  $\mathcal{I}$  и замены каждой  $H_i$  на сопряженную. Точнее, если

$$\bigsqcup_{i \in \mathcal{I}} G/H_i \cong \bigsqcup_{j \in \mathcal{J}} G/F_j,$$

то существует биекция  $\sigma : \mathcal{I} \rightarrow \mathcal{J}$  и элементы  $g_i \in G$  такие, что  $g_i H_i g_i^{-1} = F_{\sigma(i)}$ .

## 5. Несколько приложений действия группы на множестве

Естественное приложение леммы Бернсайда – задачи о раскрасках. Оно подробно описаны в моем тексте <http://alexei.stefanov.spb.ru/students/algebra3/Bernside.pdf>. Такие задачи естественно разбирать на практических занятиях. В этом же параграфе мы рассмотрим менее очевидные приложения действия групп на множествах. На самом деле, все утверждения этого параграфа являются несложными задачами, которые показывают, как можно использовать изученный в предыдущих двух параграфах материал.

Пусть  $H \leq G$ . Сердцевинной подгруппы  $H$  называется наибольшая нормальная подгруппа в  $G$ , содержащаяся в  $H$ . Сердцевина  $H$  равна

$$\text{Core } H = \bigcap_{g \in G} H^g.$$

**ПРЕДЛОЖЕНИЕ 5.1.** Ядро транзитивного действия  $G \curvearrowright X$  равно  $\text{Core } G_x = \bigcap_{y \in X} G_y$ , где  $x \in X$ .

**ДОКАЗАТЕЛЬСТВО.** Ядро действия по определению есть пересечение стабилизаторов всех точек из  $X$ . По лемме 4.2 все эти стабилизаторы сопряжены в  $G$ . Легко проверить также, что  $gG_xg^{-1} = G_{gx}$ , т. е. все подгруппы, сопряженные с  $G_x$  являются стабилизаторами точек.  $\square$

**ТЕОРЕМА 5.2.** Пусть  $H$  – подгруппа индекса  $n$  в  $G$ . Тогда индекс  $\text{Core } H$  конечен и делит  $n!$ . В частности, если в бесконечной группе есть подгруппа конечного индекса, то есть и нормальная подгруппа конечного индекса.

**ДОКАЗАТЕЛЬСТВО.** Стандартное однородное пространство  $G/H$  задает гомоморфизм  $\theta : G \rightarrow S_n$ . Порядок образа этого гомоморфизма равен индексу ядра, т. е.  $|G : \text{Core } H|$ .  $\square$

Следующее утверждение – задача, которую я услышал от А. С. Меркурьева, показывает еще один трюк, связанный с гомоморфизмом  $G \rightarrow S_n$ , который возникает при действии  $G$  на  $n$ -элементном множестве.

**УПРАЖНЕНИЕ 5.3.** Пусть  $G$  – группа четного порядка. Зададим функцию  $\varphi : G \rightarrow \mathbb{Z}_2$  формулой  $\varphi(g) = |G|/\text{ord } g \pmod 2$ . Докажите, что эта функция – гомоморфизм.

**РЕШЕНИЕ.** Пусть  $|G| = 2n$ . Рассмотрим действие  $G$  на себе левыми трансляциями, соответствующее отображение  $\theta : G \rightarrow S_{2n}$  и его композицию с четностью перестановки  $\varepsilon : S_{2n} \rightarrow \mathbb{Z}_2$ . Если  $k = \text{ord } g$ , то  $g$  отображается в перестановку, состоящую из  $k$ -циклов (эти циклы – соответствуют правым смежным классам по  $\langle g \rangle$ ). Четность такой перестановки равна  $(k-1) \cdot \frac{2n}{k} = 2n - \frac{2n}{k} \equiv \frac{2n}{k} \pmod 2$ . Таким образом, функция из условия задачи – это и есть гомоморфизм  $\varepsilon \circ \theta$ .  $\square$

Вот еще одна задача, которую в разных вариациях любят давать на мат-меховских экзаменах.

**УПРАЖНЕНИЕ 5.4.** Пусть  $p$  – наименьшее простое число, делящее порядок группы  $G$ . Тогда подгруппа индекса  $p$  нормальна в  $G$ . В частности, подгруппа индекса 2 всегда нормальна, подгруппа индекса 3 нормальна в группе нечетного порядка и т. п.

РЕШЕНИЕ. Пусть  $|G : H| = p$  – простое, а  $|G|$  не делится на простые, меньшие  $p$ . Тогда  $|G|$  взаимно просто с  $(p-1)!$ , а индекс  $|G : \text{Core } H|$  делит  $|G|$  и  $p!$ . Так как  $\gcd(|G|, p!) = p$ , то  $|G : H| \leq |G : \text{Core } H| = p$ , откуда  $\text{Core } H = H$ .  $\square$

## 6. Теоремы о гомоморфизме и лемма о бабочке

В этом параграфе мы докажем несколько технических утверждений, несложно вытекающих из теоремы о гомоморфизме. В следующем утверждении сформулирован наиболее общий факт типа второй теоремы о гомоморфизме. Сама теорема, также как и чуть более сложное утверждение, лемма о бабочке, являются его простыми следствиями.

Будем говорить, что подгруппа  $A$  нормализует подгруппу  $B$ , если  $a^{-1}Ba = B$  для любого  $a \in A$ . Другими словами,  $A$  нормализует  $B$ , если она содержится в нормализаторе

$$N_G(B) := \{g \in G \mid B^g = B\}$$

подгруппы  $B$  в группе  $G$ . В этом случае  $AB = \{ab \mid a \in A, b \in B\}$  является подгруппой в  $G$ , в которой  $B$  нормальна.

**ЛЕММА 6.1.** Пусть  $C \leq B$  и  $A$  – подгруппы группы  $G$  такие, что  $B \leq \langle A \cup C \rangle$ . Тогда

$$\frac{\langle A \cup C \rangle}{B} \cong \frac{A}{A \cap B}.$$

ДОКАЗАТЕЛЬСТВО. Обозначим  $D = \langle A \cup C \rangle$ . Из условия  $B \leq D$  следует, что  $A$  нормализует  $B$ , и, следовательно,  $D \leq \langle A \cup B \rangle = AB$ . Рассмотрим гомоморфизм  $\varphi : A \rightarrow D/B$ , являющийся композицией вложения и канонической проекции  $A \hookrightarrow D \twoheadrightarrow D/B$ . Любой элемент  $d \in D$  представляется в виде  $d = ab$  для некоторых  $a \in A$  и  $b \in B$ . Тогда  $\varphi(a) = dB$ , откуда следует сюръективность  $\varphi$ . Условие  $\varphi(a) = 1_{D/B} = B$  равносильно тому, что  $a \in A \cap B$ , т.е. ядро  $\varphi$  равно  $A \cap B$ . По теореме о гомоморфизме получаем искомый изоморфизм.  $\square$

При  $C = B$  из предыдущей леммы получаем следующее утверждение.

**ТЕОРЕМА 6.2** (2-я теорема о гомоморфизме). Если  $A$  нормализует  $B$ , то

$$\frac{AB}{B} \cong \frac{A}{A \cap B}.$$

**ТЕОРЕМА 6.3** (3-я теорема о гомоморфизме). Пусть  $K \leq G$ , а  $\pi : G \rightarrow G/K$  – канонический гомоморфизм. Тогда отображение  $H \mapsto \pi(H)$  является биекцией множества подгрупп в  $G$ , содержащих  $K$ , на множество подгрупп в  $G/K$ . При этом  $H$  нормальна в  $G$  тогда и только тогда, когда  $\pi(H)$  нормальна в  $G/K$  и

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

(здесь  $\pi(H)$  обозначена за  $H/K$ , так как эти группы даже не просто изоморфны, а равны).

ДОКАЗАТЕЛЬСТВО. Обратным к заданному отображению будет взятие полного прообраза. Очевидно, что  $\pi(\pi^{-1}(F)) = F$  и  $\pi^{-1}(\pi(H)) \supseteq H$ . Если  $g \in \pi^{-1}(\pi(H))$ , т.е.  $\pi(g) = \pi(h)$  для некоторого  $h \in H$ , то  $gh^{-1} \in \text{Ker } \pi = K \leq H$ , откуда  $g \in hH = H$ .

Так как при нашей биекции сопряженные подгруппы переходят в сопряженные, утверждение о нормальности очевидно. Для доказательства изоморфизма зададим гомоморфизм  $\pi' : G \rightarrow \frac{G/K}{H/K}$  как композицию двух канонических проекций. Композиция сюръекций сюръективна, с другой стороны  $\text{Ker } \pi' = \pi^{-1}(H/K) = H$ . Теперь результат следует из первой теоремы о гомоморфизме.  $\square$

**ТЕОРЕМА 6.4** (лемма о бабочке). Пусть  $A' \leq A$  и  $B' \leq B$  – подгруппы некоторой группы  $G$ . Тогда

$$\frac{A \cap B}{(A \cap B')(B \cap A')} \cong \frac{A'(A \cap B)}{A'(A \cap B')} \cong \frac{B'(B \cap A)}{B'(B \cap A')}.$$

**ДОКАЗАТЕЛЬСТВО.** Легко видеть, что  $A \cap B$  нормализует  $A'$ ,  $B'$ ,  $A \cap B'$  и  $B \cap A'$ , поэтому все произведения подгрупп в формуле, которую требуется доказать, корректно определены. По лемме 6.1  $\frac{A'(A \cap B)}{A'(A \cap B')} \cong \frac{A \cap B}{F}$ , где  $F = (A'(A \cap B')) \cap A \cap B$ . Так как  $A'(A \cap B') \subseteq A$ , то  $F = (A'(A \cap B')) \cap B$ . Любой элемент из  $A'(A \cap B')$  записывается в виде  $ab$ , где  $a \in A'$ , а  $b \in A \cap B' \subseteq B$ . Если этот элемент лежит в  $F \subseteq B$ , то  $a \in A' \cap B$ . Таким образом,  $F \subseteq (A' \cap B)(A \cap B')$ . Обратное включение очевидно. Итак, мы доказали, что первая факторгруппа в формуле изоморфна второй. Аналогично доказывается, что первая факторгруппа изоморфна третьей.  $\square$

## 7. Теоремы Силова

Далее в этом параграфе  $G$  – конечная группа, а  $p$  – простое число. Группа порядка  $p^k$  называется  $p$ -группой.

**ОПРЕДЕЛЕНИЕ 7.1.**  $p$ -Подгруппа  $S \leq G$  называется силовской  $p$ -подгруппой, если ее индекс взаимно прост с  $p$ .

Целью этого параграфа является доказательство существования силовских подгрупп и их основных свойств. Для этого нам потребуется несколько вспомогательных утверждений.

**ЛЕММА 7.2.** Если  $A, B$  –  $p$ -подгруппы в  $G$ , причем  $A$  нормализует  $B$ , то  $AB$  также является  $p$ -подгруппой.

**ДОКАЗАТЕЛЬСТВО.** По второй теореме об изоморфизме 6.2  $\frac{AB}{B} \cong \frac{A}{A \cap B}$ , откуда  $|AB| = |B| \cdot |\frac{A}{A \cap B}|$ , что очевидно является степенью числа  $p$ .  $\square$

**ЛЕММА 7.3.** Пусть  $G \curvearrowright X$ . Предположим, что индекс любой собственной подгруппы  $G$  делится на  $p$ . Тогда количество неподвижных точек под действием  $G$  сравнимо с  $|X|$  по модулю  $p$ .

**ДОКАЗАТЕЛЬСТВО.** Длина орбиты равна индексу стабилизатора точки. Если этот стабилизатор – собственная подгруппа, т.е. если точка не является неподвижной, то по условию длина ее орбиты делится на  $p$ . Количество элементов в  $X$  равно сумме длин орбит, следовательно, по модулю  $p$  оно сравнимо с суммой длин одноэлементных орбит, т.е. с количеством неподвижных точек.  $\square$

Напомним, что центром группы  $G$  называется множество элементов, коммутирующих со всеми элементами группы  $G$ :

$$\text{Center}(G) = \{c \in G \mid cg = gc \forall g \in G\}.$$

**СЛЕДСТВИЕ 7.4.** Любая  $p$ -группа имеет нетривиальный центр.

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим действие  $p$ -группы  $G$  на себе сопряжениями. По лемме 7.3 количество неподвижных точек сравнимо с порядком группы по модулю  $p$ , а значит, делится на  $p$ . Но оно ненулевое, так как одна из неподвижных точек – нейтральный элемент группы.  $\square$

**ТЕОРЕМА 7.5** (теоремы Силова).

$E_p$ : В  $G$  существует силовская  $p$ -подгруппа.

$S_p$ : Все силовские  $p$ -подгруппы в  $G$  сопряжены.

$D_p$ : Любая  $p$ -подгруппа содержится в силовской  $p$ -подгруппе.

$F_p$ : Количество силовских  $p$ -подгрупп сравнимо с 1 по модулю  $p$ .

**ДОКАЗАТЕЛЬСТВО.**  $E_p$ . Индукция по  $|G|$ . База тривиальна. Если  $|G|$  не делится на  $p$ , то доказывать нечего. Поэтому считаем, что  $|G| = p^n t$ , где  $t$  не делится на  $p$ .

Пусть существует собственная подгруппа  $H$  в  $G$ , индекс которой взаимно прост с  $p$ . Тогда по индукционному предположению в  $H$  существует силовская  $p$ -подгруппа, которая будет силовской  $p$ -подгруппой в  $G$ . В противном случае рассмотрим действие  $G$  на себе сопряжениями. По лемме 7.3 количество неподвижных точек этого действия делится на  $p$ , т.е. порядок центра группы  $G$

делится на  $p$ . Предположим, что он равен  $p^k l$ , где  $l$  не делится на  $p$ . По теореме о строении конечнороджденных абелевых групп в центре существует подгруппа  $C$  порядка  $p^k$ . По индукционному предположению в группе  $G/C$ , имеющей порядок  $p^{n-k}m$ , существует силовская  $p$ -подгруппа  $\bar{P}$ , которая имеет порядок  $p^{n-k}$ . Обозначим через  $P$  полный прообраз группы  $\bar{P}$  под действием гомоморфизма редукции  $\rho : G \rightarrow G/C$ . Пусть  $\pi : P \rightarrow \bar{P}$  – сужение  $\rho$  на  $P$ . Тогда  $|\text{Ker } \pi| = |C| = p^k$ , а  $|\text{Im } \pi| = |\bar{P}| = p^{n-k}$ . Следовательно,  $|P| = p^n$ , и  $P$  является силовской  $p$ -подгруппой в  $G$ .

**$\mathbf{C}_p + \mathbf{D}_p$ .** Пусть  $H$  –  $p$ -подгруппа, а  $S$  – силовская  $p$ -подгруппа. Рассмотрим действие  $H$  на  $G/S$  левыми трансляциями. По лемме существует неподвижная точка этого действия, скажем,  $HxS = xS$ . Тогда  $x^{-1}Hx \subseteq S$ , что доказывает, что  $H$  содержится в силовской  $p$ -подгруппе  $xSx^{-1}$ . С другой стороны, если  $H$  была силовской, то мы доказали, что  $H$  и  $S$  сопряжены.

**$\mathbf{F}_p$ .** Рассмотрим действие силовской  $p$ -подгруппы  $S$  на множестве  $X$  всех силовских  $p$ -подгрупп сопряжением. Если  $\{P\}$  – неподвижный элемент этого действия, то  $S$  нормализует  $P$ . Тогда по лемме 7.2  $PS$  является  $p$ -подгруппой и, следовательно, совпадает с  $S$ . Таким образом, у этого действия ровно одна неподвижная точка. Теперь, по лемме 7.3  $1 \equiv |X| \pmod{p}$ , что и требовалось доказать.  $\square$

**ЛЕММА 7.6** (аргумент Фраттини). Пусть  $H$  – конечная нормальная подгруппа группы  $G$ , а  $P$  – силовская подгруппа в  $H$ . Тогда  $G = N_G(P) \cdot H$ .

**ДОКАЗАТЕЛЬСТВО.** Для любого  $g \in G$  рассмотрим подгруппу  $P^g$ . Так как  $P \leq H \trianglelefteq G$ , то  $P^g \leq H$ , и, следовательно, является силовской подгруппой в  $H$ . Так как силовские подгруппы сопряжены, существует элемент  $h \in H$  такой, что  $P^h = P^g$ , откуда  $P^{gh^{-1}} = P$ , т.е.  $gh^{-1} \in N_G(P)$ . Таким образом,  $g \in N_G(P)h \subseteq N_G(P) \cdot H$ .  $\square$

**СЛЕДСТВИЕ 7.7.** Любая подгруппа, содержащая нормализатор силовской подгруппы, самонормализуема.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $P$  – силовская подгруппа группы  $F$ . Пусть  $H$  содержит ее нормализатор  $N_F(P)$ , и положим  $G = N_F(H)$ . Заметим, что силовская подгруппа  $P$  группы  $F$  является силовской подгруппой и в любой промежуточной между  $P$  и  $F$  подгруппой, в частности,  $P$  – силовская в  $H$ . В соответствии с аргументом Фраттини  $G = N_G(P) \cdot H \leq N_F(P) \cdot H = H$ .  $\square$

**УПРАЖНЕНИЕ 7.8.** Для подгруппы  $B$  группы  $G$  следующие условия эквивалентны.

- (1) Любая надгруппа группы  $B$  самонормализуема, и никакие 2 различные надгруппы не сопряжены.
- (2)  $x \in \langle B, B^x \rangle$  для любого  $x \in G$ .
- (3)  $B \not\leq H^x$  для любых  $B \leq H \leq G$  и  $x \in G \setminus H$ .

Подгруппа  $B$ , удовлетворяющая условиям последнего упражнения, называется абнормальной.

**УПРАЖНЕНИЕ 7.9.** Докажите, что нормализатор силовской подгруппы абнормален.

**УПРАЖНЕНИЕ 7.10.** Докажите, что в полной линейной группе  $\text{GL}_n(F)$  над конечным полем  $F$  характеристики  $p$  одна из силовских  $p$ -подгрупп – это группа верхних унитреугольных матриц  $U_n(F)$ ,<sup>4</sup> а ее нормализатор – это группа всех обратимых верхнетреугольных матриц  $B_n(F)$ .

Из двух последних утверждений следует, что  $B_n(F)$  абнормальна. Оказывается, что это верно над любым полем.

**УПРАЖНЕНИЕ 7.11.** Пусть  $K$  – произвольное поле. Докажите, что  $B_n(K)$  абнормальна в  $\text{GL}_n(K)$ .

<sup>4</sup>Все остальные силовские  $p$ -подгруппы с ней сопряжены, т.е. становятся группой верхних унитреугольных матриц после замены базиса.

## 8. Полупрямое произведение

В категории  $\mathcal{C}$  рассмотрим морфизмы  $A \xrightarrow{\varphi} B \xrightarrow{\psi} A$ , композиция которых равна  $\text{id}_A$ . В этом случае морфизм  $\psi$  называется ретракцией, а  $\varphi$  называется сечением морфизма  $\psi$ . Заметим, что в этом случае  $\varphi$  обязано быть мономорфизмом, а  $\psi$  – эпиморфизмом.

Приведенная ситуация очень хороша тем, что сохраняется под действием любого функтора. Например, рассмотрим гомоморфизмы коммутативных колец  $R \hookrightarrow R[t] \twoheadrightarrow R$  (при втором отображении  $t$  переходит в 0) и применим к этой диаграмме функтор  $GL_n$ . Получим ретракцию групп  $GL_n(R[t]) \twoheadrightarrow GL_n(R)$ . В настоящем параграфе мы выясним, как устроена любая ретракция групп.

**ПРЕДЛОЖЕНИЕ 8.1.** Пусть  $H, K$  – подгруппы в  $G$ , причем  $K$  нормальна. Следующие условия эквивалентны.

- (1) Существует ретракция  $\psi : G \rightarrow H$  группы  $G$  на подгруппу  $H$  (сечение – это вложение  $H$  в  $G$ ), а  $K = \text{Ker } \psi$ .
- (2)  $G = KH$  и  $H \cap K = \{1\}$  (заметим, что  $HK$  – подгруппа по теореме 6.2).
- (3) Любой элемент группы  $G$  единственным образом представляется в виде произведения  $kh$ ,  $h \in H$ ,  $k \in K$ .

**ДОКАЗАТЕЛЬСТВО.** (1)  $\implies$  (2). По условию композиция вложения  $H \hookrightarrow G$  и  $\psi$  – тождественное отображение. Другими словами,  $\psi(h) = h$  для любого  $h \in H$ , в частности,  $\psi(\psi(g)) = \psi(g)$ . Для любого  $g \in G$  имеем:  $g = g\psi(g)^{-1} \cdot \psi(g)$ , причем  $\psi(g\psi(g)^{-1}) = \psi(g)\psi(g)^{-1} = 1$ , т.е.  $g\psi(g)^{-1} \in K$ , откуда  $g \in KH$ . Если  $g \in H \cap K$ , то  $g = \psi(g) = 1$ , следовательно, пересечение тривиально.

(2)  $\implies$  (3). Существование очевидно. Если  $hk = h'k'$  для некоторых  $h, h' \in H$  и  $k, k' \in K$ , то  $hh'^{-1} = k^{-1}k' \in H \cap K = \{1\}$ , откуда  $h = h'$  и  $k = k'$ .

(3)  $\implies$  (1). Для любого  $g = kh \in G$ , где  $k \in K$ ,  $h \in H$ , положим  $\psi(g) = \psi(kh) = h$ . При  $h, h' \in H$  и  $k, k' \in K$  имеем  $khk'h' = k(hk'h^{-1}) \cdot hh'$ ,  $k(hk'h^{-1}) \in K$  и  $hh' \in H$ . Поэтому  $\psi(khk'h') = hh' = \psi(kh)\psi(k'h')$ , т.е.  $\psi$  – гомоморфизм. Так как  $\psi(kh) = 1 \iff h = 1$ , то  $\text{Ker } \psi = K$ . С другой стороны,  $\psi(h) = h$  для любого  $h \in H$ , т.е. композиция вложения  $H \hookrightarrow G$  и  $\psi$  тождественна.  $\square$

**ОПРЕДЕЛЕНИЕ 8.2.** Если выполнены условия предложения 8.1, то  $G$  называется (внутренним) полупрямым произведением подгрупп  $H$  и  $K$ ; это обозначается через  $G = K \rtimes H$ .

Пусть  $G = K \rtimes H$ , а  $\theta : H \rightarrow S_K$  – гомоморфизм, определяющий действие  $H$  на  $K$  левым сопряжением, т.е.  $\theta(h)(k) = hkh^{-1}$ . Легко проверить, что сопряжение является автоморфизмом, т.е. образ  $\theta$  лежит в группе автоморфизмов  $\text{Aut}(K)$  группы  $K$ . При этом, для  $h, h' \in H$  и  $k, k' \in K$  имеем  $khk'h' = k(hk'h^{-1}) \cdot hh' = k\theta(h)(k') \cdot hh'$ . В соответствии с последним равенством мы определим внешнее полупрямое произведение произвольных групп  $A$  и  $B$ , соответствующее гомоморфизму  $\theta : B \rightarrow \text{Aut}(A)$ .

**ОПРЕДЕЛЕНИЕ 8.3.** Пусть  $G$  – декартово произведение множеств  $A$  и  $B$ . Определим умножение на  $G$  формулой

$$(a, b) \cdot (a', b') = (a\theta(b)(a'), bb').$$

Тогда  $G$  называется (внешним) полупрямым произведением групп  $A$  и  $B$ , соответствующим  $\theta$  и обозначается  $G = A \rtimes_\theta B$ .

Также как и в случае прямого произведения, внешнее полупрямое произведение после некоторых отождествлений становится внутренним.

**ПРЕДЛОЖЕНИЕ 8.4.** Пусть  $G = A \rtimes_\theta B$ . Положим  $A' = A \times \{1_B\}$  и  $B' = \{1_A\} \times B$ . Тогда  $G$  является внутренним полупрямым произведением  $A' \rtimes B'$ .

Обратно, если  $G$  – внутреннее полупрямое произведение своих подгрупп  $K \rtimes H$ , а  $\theta : H \rightarrow \text{Aut}(K)$  – действие  $H$  на  $K$  левыми сопряжениями, то  $G \cong K \rtimes_\theta H$ .



Одним из простых геометрических примеров полупрямого произведения является группа автоморфизмов аффинного пространства.

**ОПРЕДЕЛЕНИЕ 8.5.** Пусть  $V$  – векторное пространство над произвольным полем  $F$ . Если аддитивная группа  $V$  свободно и транзитивно действует на множестве  $A$ , то пара  $(A, V)$  называется аффинным пространством над  $F$ . Действие  $V$  на  $A$  обычно обозначается сложением:  $(a, v) \mapsto a + v$ .

Аффинным отображением  $\varphi : (A, V) \rightarrow (A', V')$  называется пара  $(\varphi_v, \varphi_a)$ , состоящая из линейного отображения  $\varphi_v : V \rightarrow V'$  и функции  $\varphi_a : A \rightarrow A'$ , для которых имеет место тождество  $\varphi_a(a + v) = \varphi_a(a) + \varphi_v(v)$ . Нетрудно видеть, что  $\varphi_a$  однозначно определяется заданием образа одной точки  $a \in A$  и линейным отображением  $\varphi_v$ . Действительно, по условию для любой  $b \in A$  существует единственный вектор  $v \in V$  такой, что  $b = a + v$ , следовательно,  $\varphi_a(b) = \varphi_a(a) + \varphi_v(v)$ . Аффинное отображение  $\varphi$  называется изоморфизмом, если  $\varphi_v$  изоморфизм (тогда  $\varphi_a$  автоматически является биекцией).

Пара  $(B, W)$  называется аффинным подпространством пространства  $(A, V)$ , если  $B \subseteq A$ ,  $W \leq V$ , и эта пара сама является аффинным пространством относительно той же операции. Пара  $(B, W)$ ,  $B \subseteq A$ ,  $W \leq V$ , является аффинным подпространством тогда и только тогда, когда  $b + w \in B$  для любых  $b \in B$  и  $w \in W$  и  $W$  действует транзитивно на  $B$ .

Если мы рассмотрим регулярное действие  $V$  на себе, то получим *стандартное* аффинное пространство  $(V, V)$ .<sup>5</sup> Нетрудно видеть, что любое аффинное пространство изоморфно стандартному. Если  $\varphi_v : V \rightarrow V$  тождественное отображение, то изоморфизм  $\varphi$  однозначно определяется выбором базовой точки множества  $A$ , т.е. образом нуля при отображении  $\varphi_a$ . Давайте изучим строение группы автоморфизмов стандартного аффинного пространства.

**ПРЕДЛОЖЕНИЕ 8.6.** *Группа автоморфизмов аффинного пространства  $(V, V)$  изоморфна полупрямому произведению  $V \rtimes \text{Aut}(V)$ . Если  $\dim V = n < \infty$ , то эта группа изоморфна подгруппе в  $\text{GL}_{n+1}(F)$ , состоящей из всех матриц, у которых последняя строка совпадает с последней строкой единичной матрицы.*

**ДОКАЗАТЕЛЬСТВО.** Сопоставим автоморфизму  $\varphi$  его векторную часть  $\varphi_v$ . Ясно, что это гомоморфизм групп  $\pi : \text{Aut}(V, V) \rightarrow \text{Aut}(V)$ . Ядро этого гомоморфизма состоит из аффинных изоморфизмов вида  $(\psi, \text{id})$ , которые, как мы заметили выше, однозначно определяются образом нуля. Так как  $\psi(v) = \psi(0 + v) = \psi(0) + v$  (здесь  $v$  в выражении  $\psi(v)$  играет роль точки, а в остальных – роль вектора), то  $\psi$  – это сдвиг на  $\psi(0)$ . Поэтому отображение  $(\psi, \text{id}) \mapsto \psi(0)$  задает изоморфизм  $\text{Ker } \pi \cong V$ .

С другой стороны,  $\text{Aut}(V)$  вкладывается в  $\text{Aut}(V, V)$  по правилу  $\theta \mapsto (\theta, \theta)$ . Таким образом, имеем последовательность гомоморфизмов  $\text{Aut}(V) \rightarrow \text{Aut}(V, V) \rightarrow \text{Aut}(V)$ , композиция которых тождественная. Кроме того,

$$(\theta, \theta) \circ (\psi, \text{id}) \circ (\theta^{-1}, \theta^{-1}) = (\theta \circ \psi \circ \theta^{-1}, \text{id}), \text{ а } \theta \circ \psi \circ \theta^{-1}(0) = \theta(\psi(0)),$$

так что образ автоморфизма  $\theta$  действует на сдвиг, соответствующий вектору  $\psi(0)$  естественным образом.

□

На основании теорем Силова и строения полупрямого произведения можно классифицировать все группы порядка  $pq$ , где  $p$  и  $q$  – простые числа. Напомним, что  $C_k \cong \mathbb{Z}/k\mathbb{Z}$  обозначает циклическую группу порядка  $k$ . Докажем сначала две простые леммы.

**ЛЕММА 8.7.** *Группа автоморфизмов аддитивной группы  $\mathbb{Z}/p\mathbb{Z}$  равна  $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$ .*

**ДОКАЗАТЕЛЬСТВО.** Автоморфизм  $\varphi$  аддитивной группы  $\mathbb{Z}/p\mathbb{Z}$  однозначно определен образом 1: если  $\varphi(1) = t + p\mathbb{Z}$ , то  $\varphi(x) = tx + p\mathbb{Z}$ . Для того чтобы заданный таким образом гомоморфизм

<sup>5</sup>Рассмотрение стандартного аффинного пространства вместо векторного пространства – это способ формализовать отождествление точек и векторов.

$\varphi$  был автоморфизмом, необходимо и достаточно, чтобы  $t$  было взаимно просто с  $p$ , т.е.  $t \in (\mathbb{Z}/p\mathbb{Z})^*$  (таким образом, элемент группы  $(\mathbb{Z}/p\mathbb{Z})^*$  отождествляется с автоморфизмом умножения на этот элемент). В этой части доказательства  $p$  не обязательно простое число. Если же  $p$  простое, то кольцо  $\mathbb{Z}/p\mathbb{Z}$  является полем, следовательно, группа  $(\mathbb{Z}/p\mathbb{Z})^*$  циклическая.  $\square$

**ЛЕММА 8.8.** *Множество элементов циклической группы, порядок которых делит фиксированное число  $q$ , является циклической подгруппой, порядок которой делит  $q$ .*

*Если  $q$  простое число, то любой неединичный элемент порождает эту подгруппу.*

**ДОКАЗАТЕЛЬСТВО.** Возведение в степень  $q$  является эндоморфизмом абелевой группы, а рассматриваемая подгруппа – его ядро. Любая подгруппа циклической группы циклическая. Порядок циклической группы равен порядку образующей, который по условию делит  $q$ .  $\square$

**ПРЕДЛОЖЕНИЕ 8.9.** *Пусть  $p > q$  – простые числа, а  $G$  – группа порядка  $pq$ . Тогда  $G \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\theta} (\mathbb{Z}/q\mathbb{Z})$ .*

*Если гомоморфизм  $\theta$  тривиален, то  $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$ . В частности, если  $p-1$  не делится на  $q$ , то существует единственная группа порядка  $pq$  (с точностью до изоморфизма).*

*Если гомоморфизмы  $\theta, \eta$  оба нетривиальны, то  $(\mathbb{Z}/p\mathbb{Z}) \rtimes_{\theta} (\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\eta} (\mathbb{Z}/q\mathbb{Z})$ . В частности, если  $p-1$  делится на  $q$ , то существует ровно 2 группы порядка  $pq$  (с точностью до изоморфизма).*

**ДОКАЗАТЕЛЬСТВО.** По теореме Силова количество силовских  $p$ -подгрупп равно  $pk+1$  для некоторого целого неотрицательного  $k$ . Так как в группе порядка  $p$  нет собственных подгрупп, две различных силовских  $p$ -подгруппы пересекаются по нейтральному элементу. Тогда количество элементов во всех силовских  $p$ -подгруппах равно  $1 + (p-1)(pk+1) = p(pk-k+1) \leq pq$ , откуда  $k(p-1) \leq q-1$ . Но по условию  $q < p$ , поэтому это неравенство возможно только при  $k=0$ . Таким образом, существует только одна силовская  $p$ -подгруппа  $P \cong \mathbb{Z}/p\mathbb{Z}$ . Так как  $P^g$  является силовской  $p$ -подгруппой, то  $P^g = P$  для любого  $g \in G$ . Следовательно,  $P$  нормальна в  $G$ . Если  $S \cong \mathbb{Z}/q\mathbb{Z}$  – силовская  $q$ -подгруппа, то  $SP$  является группой, а  $S \cap P = \{1_G\}$ . Легко видеть (например, по второй теореме об изоморфизме), что  $SP/P \cong S$ , откуда  $|SP| = pq$  и  $SP = G$ . Таким образом,  $G = P \rtimes S \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/q\mathbb{Z})$ .

По предложению 8.4  $G \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\theta} (\mathbb{Z}/q\mathbb{Z})$ . Если  $\theta$  отображает любой элемент  $\mathbb{Z}/q\mathbb{Z}$  в тождественный автоморфизм, то полупрямые сомножители поэлементно коммутируют, т.е. произведение прямое. В случае, если  $p-1$  не делится на  $q$ , никаких других гомоморфизмов из  $\mathbb{Z}/q\mathbb{Z}$  в  $\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong C_{p-1}$  нет, что доказывает второе утверждение нашего предложения.

Пусть теперь  $p-1 \vdots q$ , а  $\theta, \eta : \mathbb{Z}/q\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$  – два нетривиальных гомоморфизма. Так как группа  $(\mathbb{Z}/p\mathbb{Z})^*$  циклическая, то по лемме 8.8 существует  $k \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$  такое, что  $\eta(k) = \eta(1)^k = \theta(1)$ . Тогда  $\theta(y) = \eta(ky)$  при любом  $y \in \mathbb{Z}/q\mathbb{Z}$ . Зададим отображение

$$\varphi : (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\theta} (\mathbb{Z}/q\mathbb{Z}) \rightarrow (\mathbb{Z}/p\mathbb{Z}) \rtimes_{\eta} (\mathbb{Z}/q\mathbb{Z}) \text{ по формуле } \varphi(x, y) = (x, ky).$$

Тогда

$$\begin{aligned} \varphi((x_1, y_1)(x_2, y_2)) &= \varphi(x_1 + x_2 \cdot \theta(y_1), y_1 + y_2) = (x_1 + x_2 \cdot \theta(y_1), k(y_1 + y_2)) \\ \varphi(x_1, y_1)\varphi(x_2, y_2) &= (x_1, ky_1)(x_2, ky_2) = (x_1 + x_2 \cdot \eta(ky_1), ky_1 + ky_2) \end{aligned}$$

Эта выкладка доказывает, что  $\varphi$  – гомоморфизм, а его биективность очевидна.  $\square$

## 9. Субнормальные ряды

**ОПРЕДЕЛЕНИЕ 9.1.** Цепочка подгрупп  $\{1\} = H_0 \leq H_1 \leq \dots \leq H_{n-1} \leq H_n = G$  называется нормальным (субнормальным) рядом, если  $H_i$  нормально в  $G$  (соответственно в  $H_{i+1}$ ) для любого  $i = 1, \dots, n-1$ . Длиной ряда называется количество включений (в данном случае  $n$ ). Факторгруппы  $H_{i+1}/H_i$  называются факторгруппами ряда.

Два ряда называются эквивалентными, если их длины равны, а факторгруппы изоморфны с точностью до перестановки, т.е. существует перестановка  $\sigma \in S_n$  такая, что факторгруппа первого ряда с номером  $i$  изоморфна факторгруппе второго ряда с номером  $\sigma(i)$ .

Ряд не имеет повторов, если  $H_i \neq H_{i+1}$  при всех  $i = 1, \dots, n-1$ .

Уплотнение ряда подгрупп – это другой ряд подгрупп, содержащий каждый элемент первоначального ряда.

Субнормальный ряд без повторов, для которого любое его уплотнение без повторов совпадает с ним самим, называется композиционным рядом.

Напомним, что группа называется простой, если она не содержит нетривиальных нормальных подгрупп (т.е. нормальных подгрупп, не совпадающих с самой группой и с единицей). Эквивалентное определение композиционного ряда – это ряд без повторов, у которого все факторгруппы просты.

Ясно, что композиционный ряд существует не для любой группы, но для конечных групп он, конечно, существует. Более общо, композиционный ряд существует тогда и только тогда, когда выполнены условия обрыва возрастающих и убывающих цепей подгрупп данной группы. Сейчас мы докажем, что любые 2 композиционных ряда изоморфны (если существуют). Этот факт легко следует из теоремы Шрайера о том, что любые 2 субнормальных ряда имеют эквивалентные уплотнения.

**ТЕОРЕМА 9.2** (теорема Шрайера об уплотнении). *Любые 2 субнормальных ряда имеют эквивалентные уплотнения.*

ДОКАЗАТЕЛЬСТВО. Пусть

$$\{1\} = H_0 \leq H_1 \leq \dots \leq H_n = G \text{ и } \{1\} = K_0 \leq K_1 \leq \dots \leq K_m = G$$

субнормальные ряды группы  $G$ . Для всех допустимых  $i, j$  положим

$$H_{ij} = H_i(H_{i+1} \cap K_j) \text{ и } K_{ji} = K_j(K_{j+1} \cap H_i)$$

(так как  $H_i \trianglelefteq H_{i+1}$  и  $K_j \trianglelefteq K_{j+1}$ , произведения являются подгруппами). Получаем композиционные ряды

$$\begin{aligned} \{1\} &= H_{00} \leq H_{01} \leq \dots \leq H_{0m-1} \leq \dots \\ &\leq H_{i-1m} = H_i = H_{i0} \leq H_{i1} \leq \dots \leq H_{im-1} \leq \dots \\ &\leq H_{n-2m} = H_{n-1} = H_{n-10} \leq H_{n-11} \leq \dots \leq H_{n-1m-1} \leq H_{n-1m} = G \end{aligned}$$

и аналогично

$$\begin{aligned} \{1\} &= K_{00} \leq K_{01} \leq \dots \leq K_{0n-1} \leq \dots \\ &\leq K_{j-1n} = K_j = K_{j0} \leq K_{j1} \leq \dots \leq K_{jn-1} \leq \dots \\ &\leq K_{m-2n} = K_{m-1} = K_{m-10} \leq K_{m-11} \leq \dots \leq K_{m-1n-1} \leq K_{m-1n} = G \end{aligned}$$

Очевидно, эти ряды являются уплотнениями исходных рядов. Для доказательства того, что они эквивалентны, докажем изоморфизм  $H_{ij+1}/H_{ij} \cong K_{j+1}/K_{ji}$ , другими словами,

$$\frac{H_i(H_{i+1} \cap K_{j+1})}{H_i(H_{i+1} \cap K_j)} \cong \frac{K_j(K_{j+1} \cap H_{i+1})}{K_j(K_{j+1} \cap H_i)}.$$

Но последний изоморфизм – это в точности лемма о бабочке. □

Из теоремы следует, что любые 2 композиционных ряда имеют эквивалентные уплотнения. Если из этих уплотнений выкинуть повторения, то получатся исходные композиционные ряды, которые, естественно, также будут эквивалентны.

**СЛЕДСТВИЕ 9.3.** *Любые 2 композиционных ряда группы эквивалентны.*

Факторы композиционного ряда называются композиционными факторами группы. Как мы только что доказали, набор (но не последовательность!) композиционных факторов определен однозначно. Это и означает, что любая конечная группа строится из кирпичиков, которыми являются простые группы. При этом набор кирпичиков, но не их порядок, определен группой однозначно. И, как мы уже видели при изучении групп порядка  $pq$ , из одного набора кирпичиков, даже сложенного в одном порядке, можно получить разные группы.

Простейшими примерами простых групп являются группы  $A_n$ ,  $n \geq 5$ , и  $\text{PSL}_n(F)$ , где  $n \geq 3$  или  $n = 2$ , а поле  $F$  содержит больше 3 элементов.

## 10. Примеры простых групп

Исторически первым примером простой неабелевой группы была знакопеременная группа  $A_n$ ,  $n \geq 5$ .

Назовем элемент  $i$  подвижным под действием перестановки  $\sigma$ , если  $\sigma(i) \neq i$ . Использование стандартного термина: “ $i$  неподвижная точка  $\iff \sigma(i) = i$ ” привело бы к необходимости произносить “не неподвижная точка”, что явно неблагозвучно.

**ЛЕММА 10.1.** *Группа  $A_n$  порождена 3-циклами.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\sigma \in A_n$ . Докажем, что  $\sigma$  раскладывается в произведение 3-циклов индукцией по количеству элементов, подвижных под действием  $\sigma$ . Если это количество равно 0, то  $\sigma$  – тождественная перестановка, и доказывать нечего. Ясно, что это количество не может быть равно 1, а если оно было бы равно 2, то  $\sigma$  была бы транспозицией, которая не лежит в  $A_n$ . Поэтому можно считать, что  $\sigma(i_1) \neq i_1$ ,  $\sigma(i_2) \neq i_2$ ,  $\sigma(i_3) \neq i_3$  для некоторых различных  $1 \leq i_1, i_2, i_3 \leq n$ . Заметим, что  $\sigma^{\pm 1}(i_k)$  также подвижны под действием  $\sigma$ . Предположим для определенности, что  $\sigma(i_2) \neq i_1$  (иначе заменим  $i_2$  на  $i_3$ ). Положим  $\tau = (\sigma(i_1) i_1 \sigma(i_2))\sigma$ . Тогда  $\tau(m) = \sigma(m)$  для любого  $m \neq i_1, \sigma^{-1}(i_1), i_2$ . Следовательно, любая неподвижная точка перестановки  $\sigma$  осталась неподвижной точкой перестановки  $\tau$ , а кроме того  $\tau(i_1) = i_1$ . Таким образом, неподвижных точек у  $\tau$  строго больше, чем у  $\sigma$  и можно воспользоваться индукционным предположением.  $\square$

**СЛЕДСТВИЕ 10.2.** *Если подгруппа  $H \trianglelefteq A_n$  содержит 3-цикл, то она совпадает с  $A_n$ .*

**ДОКАЗАТЕЛЬСТВО.** При  $n = 3$  утверждение очевидно. Пусть  $n \geq 4$  и  $(i j k) \in H$ . Возьмем  $l \neq i, j, k$  и рассмотрим перестановку  $\tau(i j k)\tau^{-1} = (\tau(i) \tau(j) \tau(k)) \in H$  при  $\tau = (i j l)$ . Получим  $(j l k) \in H$  и  $(j k l) = (j l k)^{-1} \in H$ . Таким образом, мы можем заменить один любой индекс в 3-цикле на любой другой. Ясно, что делая так несколько раз, мы докажем, что любой 3-цикл лежит в  $H$ . Доказательство заканчивает лемма 10.1.  $\square$

**ЛЕММА 10.3.** *Пусть  $n > 3$ . Для любой  $\sigma \in S_n \setminus \{\text{id}\}$  существует  $\tau \in A_n$  такая, что  $[\sigma, \tau] \neq \text{id}$  и имеет не более 5 подвижных точек.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\sigma(i) \neq i$ . Возьмем  $k \neq i, \sigma(i), \sigma^2(i)$ . Тогда

$$\rho := [\sigma, (i \sigma(i) k)] = {}^{\sigma}(i \sigma(i) k) \cdot (i \sigma(i) k)^{-1} = (\sigma(i) \sigma^2(i) \sigma(k))(i k \sigma(i)),$$

а эта перестановка двигает максимум 5 элементов  $i, \sigma(i), \sigma^2(i), k, \sigma(k)$ . Если  $\rho = \text{id}$ , то  $(\sigma(i) \sigma^2(i) \sigma(k)) = (\sigma(i) k i)$ , что противоречит неравенству  $k \neq \sigma^2(i)$ .  $\square$

**ТЕОРЕМА 10.4.** *Группа  $A_n$  является простой при  $n \geq 5$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $H$  – нетривиальная нормальная подгруппа в  $A_n$ . По лемме 10.3 она содержит нетождественную перестановку,двигающую не более 5 элементов. Есть всего 3 циклических типа таких четных перестановок: 3,  $2 + 2$ , и 5. Далее считаем, что  $i_1, i_2, i_3, i_4, i_5$  – различные индексы от 1 до  $n$ . Если  $(i_1 i_2)(i_3 i_4) \in H$ , то

$$[(i_1 i_2)(i_3 i_4), (i_1 i_2)(i_3 i_5)] = [(i_3 i_4), (i_3 i_5)] = (i_3 i_4 i_5) \in H$$

Если же 5-цикл  $\sigma = (i_1 i_2 i_3 i_4 i_5) \in H$ , то

$$[(i_1 i_2)(i_3 i_4), (i_1 i_2 i_3 i_4 i_5)] = (i_2 i_1 i_4 i_3 i_5)(i_1 i_2 i_3 i_4 i_5) = (i_2 i_5 i_4) \in H$$

Как видно, в любом случае наша нормальная подгруппа содержит 3-цикл и следствие 10.2 заканчивает доказательство.  $\square$

Другой пример простой группы – проективная специальная линейная группа. Напомним, что  $\mathrm{PSL}_n(F)$  обозначает факторгруппу группы  $\mathrm{SL}_n(F)$ , состоящей из матриц с определителем 1, по центру, т. е. по подгруппе скалярных матриц.

**ТЕОРЕМА 10.5.** Пусть  $F$  – поле, а  $n \geq 2$ . При  $n = 2$  предположим дополнительно, что  $|F| > 3$ . Тогда группа  $\mathrm{PSL}_n(F)$  проста.

Если поле конечно, то  $\mathrm{PSL}_n(F)$  – конечная простая группа. Большая часть конечных простых групп – это проективные линейные группы, т. е. факторгруппы по центру матричных групп над конечными полями. Они называются группами типа Ли, потому что в каком-то смысле они похожи на группы Ли. Группы типа Ли классифицируются некоторыми комбинаторными структурами, называемыми системами корней (система корней – это конечный набор точек в евклидовом пространстве, обладающий большой группой симметрий). Теорема классификации простых конечных групп утверждает, что кроме знакопеременных групп и групп типа Ли существует ровно 26 простых конечных групп, которые называются спорадическими группами.

## 11. Разрешимые и нильпотентные группы

**ОПРЕДЕЛЕНИЕ 11.1.** Разрешимая группа – группа, обладающая субнормальным рядом подгрупп с абелевыми факторами.

Как видно из следующего утверждения, разрешимая группа всегда обладает нормальным рядом с абелевыми факторами. Определим производный ряд группы  $G$  следующим образом:

$$D^0 G = G, \quad D^1 G = [G, G], \quad D^{k+1} G = [D^k G, D^k G].$$

Ясно, что производный ряд является нормальным рядом с абелевыми факторами.

**ПРЕДЛОЖЕНИЕ 11.2.** Группа разрешима тогда и только тогда, когда ее производный ряд обрывается на  $\{1\}$ .

**ДОКАЗАТЕЛЬСТВО.** Если производный ряд конечен, то он и является субнормальным (и даже нормальным) рядом с абелевыми факторами. Обратно, если  $\{1\} = H_0 \leq H_1 \leq \dots \leq H_{n-1} \leq H_n = G$  – субнормальный ряд с абелевыми факторами, то  $[H_k, H_k] \leq H_{k-1}$ . По индукции легко получаем, что  $D^k G \leq H_{n-k}$ , откуда  $D^n G = \{1\}$ .  $\square$

Длина производного ряда, т. е. наименьшее  $n$ , для которого  $D^n G = \{1\}$ , называется степенью разрешимости группы.

**ТЕОРЕМА 11.3.** Пусть  $H \triangleleft G$ . Группа  $G$  разрешима тогда и только тогда, когда разрешимы  $H$  и  $G/H$ .

**ДОКАЗАТЕЛЬСТВО.** Ясно, что  $D^k H \leq D^k G$  а  $D^k G/H$  является образом  $D^k G$  под действием канонической проекции  $G \rightarrow G/H$ . Следовательно разрешимость  $G$  влечет разрешимость  $H$  и  $G/H$ . Обратно, если  $D^k G/H = \{1\}$ , то  $D^k G \leq H$ . Теперь, если  $D^m H = \{1\}$ , то  $D^{m+k} G = D^m(D^k G) = \{1\}$ .  $\square$

**СЛЕДСТВИЕ 11.4.** Пусть  $H_1$  и  $H_2$  – разрешимые подгруппы в  $G$ , и  $H_1$  нормализует  $H_2$ . Тогда  $H_1 H_2$  разрешима.

**ДОКАЗАТЕЛЬСТВО.** По второй теореме о гомоморфизме 6.2 произведение  $H_1 H_2$  является подгруппой,  $H_2$  нормальна в этой подгруппе, и  $\frac{H_1 H_2}{H_2} \cong \frac{H_1}{H_1 \cap H_2}$ . Так как  $H_1$  разрешима, то правая часть последнего изоморфизма разрешима. Следовательно, разрешима факторгруппа  $H_1 H_2/H_2$  и, по условию, подгруппа  $H_2$ . Теперь результат следует из теоремы.  $\square$

Разрешимость группы Галуа поля разложения неприводимого сепарабельного многочлена  $p$  равносильно разрешимости уравнения  $p(t) = 0$  в радикалах. Это одна из основных теорем теории Галуа, которая дала название разрешимым группам. Исходя из этих соображений интересно изучать разрешимость конечных групп. Из последнего следствия вытекает, что в конечной группе существует наибольшая разрешимая нормальная подгруппа – произведение всех разрешимых подгрупп данной группы. Она называется разрешимым радикалом группы. Фактор по разрешимому радикалу уже не содержит разрешимых подгрупп.

Для группы, обладающей композиционным рядом, например конечной, существует альтернатива: либо группа разрешима, либо хотя бы один из факторов ее композиционного ряда является неабелевой простой группой. Самая маленькая неабелева простая группа – знакопеременная группа  $A_5$ , порядок которой равен 60. Поэтому все группы меньших порядков разрешимы.

**ОПРЕДЕЛЕНИЕ 11.5.** Цепочка нормальных подгрупп  $\{1\} = H_0 \leq H_1 \leq \dots \leq H_{n-1} \leq H_n = G$  называется *центральной цепочкой*, если  $H_{i+1}/H_i$  лежит в центре  $G/H_i$  (равносильно:  $[G, H_{i+1}] \leq H_i$ ) для любого  $i = 1, \dots, n$ .

*Нильпотентная группа* – группа, обладающая центральной цепочкой подгрупп.

Определим *нижний центральный ряд* группы  $G$  по индукции следующим образом. Положим  $C_0(G) = G$  и  $C_n(G) = [C_{n-1}(G), G]$  для  $n \geq 1$ . Из определения сразу вытекает, что

$$G = C_0(G) \geq C_1(G) \geq C_2(G) \geq \dots \geq C_n(G) \geq \dots$$

Ясно, что этот ряд действительно является центральным. Нижний центральный ряд известен также под именем *убывающий* центральный ряд. Очень часто эпитет “нижний” или “убывающий” здесь опускается и говорят просто о центральном ряде.

**УПРАЖНЕНИЕ 11.6.** Докажите, что  $[C_m(G), C_n(G)] \leq C_{m+n+1}(G)$ .

Определим теперь *верхний центральный ряд* группы  $G$  по индукции следующим образом. Положим  $C^0(G) = 1$ , а для  $n \geq 1$  обозначим через  $C^n(G)$  полный прообраз центра факторгруппы  $G/C^{n-1}(G)$  по предыдущему члену ряда, относительно канонической проекции. Иными словами,  $C^n(G)$  это такая подгруппа  $C^{n-1}(G) \leq C^n(G) \leq G$ , что ее факторгруппа по  $C^{n-1}(G)$  совпадает с центром факторгруппы  $G/C^{n-1}(G)$ :

$$C^n(G)/C^{n-1}(G) = C(G/C^{n-1}(G)).$$

Таким образом,  $C^1(G) = C(G)$  – центр группы  $G$ ,  $C^2(G)$  – *гиперцентр*, т. е. такая подгруппа в  $G$ , что  $C^2(G)/C(G) = C(G/C(G))$  и так далее. Верхний центральный ряд часто называется также *возрастающим* центральным рядом, а его член  $C^n(G)$  обычно называется также  *$n$ -м гиперцентром* группы  $G$ .

Приведем классический пример вычисления центральных рядов, часто встречающийся в приложениях. Напомним, что

$$U_n^{(k)} = U_n^{(k)}(F) = \{a \in M_n(F) \mid a_{ii} = 1, a_{ij} = 0 \text{ при всех } i \neq j, j - i < k\},$$

см. параграф 7 главы 3.

**УПРАЖНЕНИЕ 11.7.** Докажите, что  $C_m(U(n, F)) = U_n^{(m)}(F) = C^{n-1-m}(G)$ .

**ТЕОРЕМА 11.8.** Пусть  $\{1\} = H_0 \leq H_1 \leq \dots \leq H_{n-1} \leq H_n = G$  – центральный ряд группы  $G$ . Тогда  $C_{n-k}(G) \leq H_k \leq C^k(G)$ .

*Длины нижнего и верхнего центральных рядов нильпотентной группы равны.*

**ДОКАЗАТЕЛЬСТВО.** По определению центрального ряда  $[G, H_k] \leq H_{k-1}$ . Теперь простая индукция по  $n - k$  показывает, что  $C_{n-k}(G) = [G, C_{n-k-1}(G)] \leq [G, H_{k+1}] \leq H_k$ . Таким образом, длина любого центрального ряда не меньше длины нижнего.

Докажем теперь второе включение индукцией по  $k$ . База  $k = 0$  очевидна. Далее,  $[G, H_{k+1}] \leq H_k \leq C^k$  по индукционному предположению. Следовательно,  $H_{k+1}/C^k$  лежит в центре  $G/C^k$ .

Так как  $C_{k+1}$  – полный прообраз этого центра, то  $H_{k+1} \leq C_{k+1}$ . В частности, длина любого центрального ряда не меньше длины верхнего. Таким образом и нижний, и верхний центральные ряды имеют наименьшую возможную длину, следовательно их длины равны.  $\square$

Длина нижнего центрального ряда нильпотентной группы называется *классом* или *степенью нильпотентности*. Любая нильпотентная группа класса  $n$  удовлетворяет тождеству

$$[\dots [x_1, x_2], \dots], x_n] = 1,$$

Таким образом, имеется универсальный прием доказательства всех результатов о нильпотентных группах – индукция по классу нильпотентности. Классифицировать нильпотентные группы невозможно, но индивидуально каждая из них устроена чрезвычайно незатейливо.

Далее мы докажем, что класс нильпотентных групп замкнут относительно перехода к подгруппам, фактор-группам и прямым произведениям.

**ПРЕДЛОЖЕНИЕ 11.9.** *Класс нильпотентных групп обладает следующими свойствами:*

- Подгруппа нильпотентной группы класса  $n$  нильпотентна класса  $\leq n$ ;
- Фактор-группа нильпотентной группы класса  $n$  нильпотентна класса  $\leq n$ ;
- Прямое произведение двух нильпотентных групп классов  $m$  и  $n$  нильпотентно класса  $\max(m, n)$ .

Доказательство абсолютно аналогично первой части доказательства теоремы 11.3.

В противоположность классу разрешимых групп, класс нильпотентных групп не замкнут относительно расширений. Иными словами, если  $H \trianglelefteq G$  нормальная подгруппа в  $G$ , причем как  $H$ , так и  $G/H$  нильпотентны, то отсюда еще совершенно не следует, что  $G$  тоже нильпотентна. Однако имеет место следующий результат.

**ТЕОРЕМА 11.10** (Холла). *Если  $H \trianglelefteq G$  нормальная подгруппа в  $G$ , причем как  $H$ , так и  $G/[H, H]$  нильпотентны, то  $G$  тоже нильпотентна.*

Подгруппа  $H$  в  $G$  называется *субнормальной*, если существует субнормальный ряд  $H = H_0 \leq H_1 \leq \dots \leq H_d = G$ . Длина самого короткого такого ряда называется глубиной подгруппы  $H$ . Часто условие нильпотентности используется в следующей форме.

**ТЕОРЕМА 11.11.** *Каждая подгруппа  $H$  нильпотентной группы  $G$  субнормальна, причем глубина  $d$  подгруппы  $H$  не превосходит класс нильпотентности группы  $G$ .*

**ДОКАЗАТЕЛЬСТВО.** По определению гиперцентров имеем

$$[C^{i+1}(G), C^i(G) \cdot H] \leq [C^{i+1}(G), G] \leq C^i(G) \leq C^i(G) \cdot H,$$

так что  $C^{i+1}(G)$  нормализует  $C^i(G) \cdot H$ , откуда  $C^i(G) \cdot H \triangleleft C^{i+1}(G) \cdot H$ . Пусть  $k$  – наибольшее целое такое, что  $C^k(G) \leq H$ . Получаем субнормальный ряд

$$H = C^k(G) \cdot H \leq C^{i+1}(G) \cdot H \leq \dots \leq C^n(G) \cdot H = G,$$

длина которого не больше длины верхнего центрального ряда.  $\square$

Очевидно, что из этой теоремы сразу вытекает такое следствие, называемое *нормализаторным условием*.

**СЛЕДСТВИЕ 11.12.** *Если группа  $G$  нильпотентна, то  $H \not\leq N_G(H)$  для любой собственной подгруппы  $H \leq G$ .*

Группа унитарных матриц является самым важным и самым типичным примером нильпотентной группы. Во многих важных классах групп никаких других нильпотентных групп, кроме подгрупп в  $U(n, R)$ , не бывает. Приведем два примера.

Каждая конечная группа вкладывается в подходящую полную линейную группу  $GL(n, K)$  над произвольным полем  $K$ . Если  $\text{char } K = p$ , то группа  $U = U(n, K)$  является силовой  $p$ -подгруппой в  $GL(n, K)$ . Тем самым, каждая конечная  $p$ -группа вкладывается в группу  $U(n, K)$ . Из

доказанной ниже теоремы Бернсайда–Виландта вытекает, что каждая конечная нильпотентная группа изоморфна подгруппе в  $U(n, R)$ , где  $R = K_1 \oplus \dots \oplus K_s$ , где характеристики  $p_1, \dots, p_s$  полей  $K_1, \dots, K_s$  пробегают множество простых делителей порядка  $G$ .

Так как

$$\begin{pmatrix} 1 & * & * & * \\ 0 & 1 & x & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & nx & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

то группа  $U(n, \mathbb{Z})$  не имеет кручения. Как мы знаем, каждая подгруппа нильпотентной группы является нильпотентной. Среди конечно порожденных групп никаких других нильпотентных групп без кручения нет.

**ТЕОРЕМА 11.13** (Холла). *Конечно порожденная нильпотентная группа без кручения изоморфна подгруппе в  $U(n, \mathbb{Z})$  для достаточно большого  $n$ .*

Как утверждает следствие 7.4, центр конечной  $p$ -группы нетривиален. Поэтому любая конечная  $p$ -группа нильпотентна. Тем самым, нильпотентно и конечное прямое произведение конечных  $p$ -групп. В заключении параграфа мы докажем, что никаких других нильпотентных конечных групп не бывает.

Из сопряженности силовских подгрупп вытекает следующий результат.

**ЛЕММА 11.14.** *Если все силовские подгруппы группы  $G$  нормальны, то  $G$  является их декартовым произведением.*

Таким образом, в этом случае группа  $G$  нильпотентна.

**ДОКАЗАТЕЛЬСТВО.** Так как силовские  $p$ -подгруппы сопряжены, для каждого простого  $p$  существует ровно одна силовская подгруппа. Так как силовские  $p$ -подгруппы с разными  $p$  имеют тривиальное пересечение, то их произведение прямое. Из сравнения количества элементов в этом произведении с порядком группы следует, что оно равно всей группе.  $\square$

Оказывается, верно и обратное. Иными словами, конечная группа  $G$  тогда и только тогда нильпотентна, когда она раскладывается в прямое произведение силовских подгрупп по всем простым делителям  $p$  порядка  $G$ . Или, иначе, конечная группа  $G$  тогда и только тогда нильпотентна, когда все ее силовские подгруппы нормальны.

**ТЕОРЕМА 11.15** (Бернсайда–Виландта). *Для конечной группы  $G$  следующие условия эквивалентны.*

- (1)  $G$  нильпотентна.
- (2) любая подгруппа  $H \leq G$  субнормальна.
- (3)  $G$  является прямым произведением своих силовских  $p$ -подгрупп.
- (4)  $G$  изоморфно декартову произведению  $p$ -групп.

**ДОКАЗАТЕЛЬСТВО.** Выше мы доказали, что первое условие влечет второе для произвольных нильпотентных групп, а не только конечных. С другой стороны, мы уже убедились, что группа, являющаяся прямым произведением своих силовских  $p$ -подгрупп, нильпотентна. Эквивалентность последних двух условий очевидна.

Таким образом, нам остается только доказать, что второе условие влечет третье, причем согласно предыдущей лемме для этого нам достаточно проверить, что все силовские  $p$ -подгруппы нормальны в  $G$ . В самом деле, пусть  $P$  – какая-то силовская  $p$ -подгруппа. По следствию 7.7 из аргумента Фраттини ее нормализатор  $N_G(P)$  самонормализуем. Но по условию (2) он субнормален, следовательно,  $N_G(P) = G$ , что и требовалось.  $\square$



**СЛЕДСТВИЕ 11.16.** *Конечная группа нильпотентна в том и только том случае, когда любые два элемента взаимно простых порядков коммутируют.*

ДОКАЗАТЕЛЬСТВО. Если группа  $G$  нильпотентна, то она изоморфна (будем считать, что равна) прямому произведению  $p_i$ -подгрупп  $P_i$  по  $i = 1, \dots, n$ , где  $p_i$  – различные простые числа. Любой элемент  $g \in G$  имеет вид  $(g_1, \dots, g_n)$ , где  $g_i \in P_i$ . Тогда  $\text{ord } g = \text{ord } g_1 \cdot \dots \cdot \text{ord } g_n$ , причем  $\text{ord } g_i$  является степенью  $p_i$ . Пусть  $h = (h_1, \dots, h_n)$ . Порядки  $g$  и  $h$  взаимно просты тогда и только тогда, когда для любого  $k = 1, \dots, n$  либо  $g_k = 1$ , либо  $h_k = 1$  (иначе порядки обоих делятся на  $p_k$ ). В любом случае  $g_k$  и  $h_k$  коммутируют, следовательно,  $g$  коммутирует с  $h$ .

Обратно...

□

## Начала теории категорий

Чем раньше математик начинает пользоваться языком теории категорий, тем проще ему потом изучать любые области математики, хотя бы потому что он видит формальные взаимосвязи между ними. Весь курс алгебры буквально пронизан категориями, функторами, естественными (и неестественными!) преобразованиями, универсальными конструкциями и сопряженными функторами. Поэтому прочитав настоящую главу вы сможете лучше увидеть взаимосвязи между различными понятиями и утверждениями.

### 1. Категория, универсальные объекты, типы морфизмов

**ОПРЕДЕЛЕНИЕ 1.1.** Категорией  $\mathcal{C}$  называется набор следующих данных:

- класс объектов  $\text{Obj } \mathcal{C}$ ;
- для каждых двух объектов  $X, Y \in \text{Obj } \mathcal{C}$  множество  $\text{Mor}(X, Y)$ , называемое множеством морфизмов из  $X$  в  $Y$ ;
- для каждых трех объектов  $X, Y, Z \in \text{Obj } \mathcal{C}$  функция  $\text{Mor}(Y, Z) \times \text{Mor}(X, Y) \rightarrow \text{Mor}(X, Z)$ ,  $(\varphi, \psi) \mapsto \varphi \circ \psi$ , называемую законом композиции морфизмов;

удовлетворяющих следующим условиям:

- (1) Если  $X \neq U$  или  $Y \neq V$ , то  $\text{Mor}(X, Y) \cap \text{Mor}(U, V) = \emptyset$ .
- (2) закон композиции морфизмов ассоциативен;
- (3) для каждого объекта  $X \in \text{Obj } \mathcal{C}$  существует *тождественный морфизм*  $\text{id}_X \in \text{Mor}(X, X)$  такой, что для любых морфизмов  $\alpha \in \text{Mor}(X, Y)$  и  $\beta \in \text{Mor}(Y, X)$  выполнены равенства  $\text{id}_X \circ \beta = \beta$  и  $\alpha \circ \text{id}_X = \alpha$ .

Категория называется *малой*, если класс объектов является множеством.

Часто мы будем писать:

- $X \in \mathcal{C}$  вместо  $X \in \text{Obj } \mathcal{C}$ ;
- $\alpha\beta$  вместо  $\alpha \circ \beta$  для композиции морфизмов (в некоторых книгах изначально говорят о произведении морфизмов, в этом случае они обычно меняют порядок сомножителей по сравнению с нашим соглашением).
- $\text{Mor}_{\mathcal{C}}(X, Y)$  вместо  $\text{Mor}(X, Y)$ , если из контекста неясно, про какую категорию идет речь;
- $\varphi : X \rightarrow Y$  вместо  $\varphi \in \text{Mor}(X, Y)$ ;
- $\varphi \in \text{Mor } \mathcal{C}$  для любого морфизма категории  $\mathcal{C}$  (т.е.  $\text{Mor } \mathcal{C}$  – это класс всех морфизмов категории  $\mathcal{C}$ );
- $X = \text{source } \varphi$  и  $Y = \text{target } \varphi$  для морфизма  $\varphi : X \rightarrow Y$ .

**ОПРЕДЕЛЕНИЕ 1.2.** Категория  $\mathcal{B}$  называется подкатегорией категории  $\mathcal{C}$ , если  $\text{Obj } \mathcal{B} \subseteq \text{Obj } \mathcal{C}$  и  $\text{Mor}_{\mathcal{B}}(X, Y) \subseteq \text{Mor}_{\mathcal{C}}(X, Y)$  для любых  $X, Y \in \text{Obj } \mathcal{B}$ . Подкатегория  $\mathcal{B}$  называется полной, если последнее включение всегда является равенством.

**ОПРЕДЕЛЕНИЕ 1.3.** Пусть  $\mathcal{C}$  – категория. Противоположной категорией к  $\mathcal{C}$  называется категория  $\mathcal{C}^{\text{op}}$ :

- $\text{Obj } \mathcal{C}^{\text{op}} = \text{Obj } \mathcal{C}$ ;
- $\text{Mor}_{\mathcal{C}^{\text{op}}}(X, Y) = \text{Mor}_{\mathcal{C}}(Y, X)$  для каждых двух объектов  $X, Y \in \text{Obj } \mathcal{C}$ ;
- закон композиции в  $\mathcal{C}^{\text{op}}$  отличается от закона композиции в  $\mathcal{C}$  порядком, т.е.  $\alpha \circ_{\mathcal{C}^{\text{op}}} \beta = \beta \circ_{\mathcal{C}} \alpha$ .

**ОПРЕДЕЛЕНИЕ 1.4.** Декартовым произведением  $\mathcal{C} \times \mathcal{B}$  категорий  $\mathcal{C}$  и  $\mathcal{B}$  называется следующая категория:

- $\text{Obj}(\mathcal{C} \times \mathcal{B}) = \text{Obj } \mathcal{C} \times \text{Obj } \mathcal{B}$ ;
- $\text{Mor}((X, Y), (Z, W)) = \text{Mor}(X, Z) \times \text{Mor}(Y, W)$ ;
- $(\alpha, \beta) \circ (\gamma, \delta) = (\alpha \circ \gamma, \beta \circ \delta)$ .

**ОПРЕДЕЛЕНИЕ 1.5.** Морфизм  $\varphi$  называется *мономорфизмом*, если равенство  $\varphi \circ \alpha = \varphi \circ \beta$  влечет равенство  $\alpha = \beta$ , и *эпиморфизмом*, если  $\alpha \circ \varphi = \beta \circ \varphi \implies \alpha = \beta$ . Морфизм, являющийся одновременно мономорфизмом и эпиморфизмом называется *биморфизмом*. Морфизм  $\varphi \in \text{Mor}(X, Y)$  называется *изоморфизмом*, если существует  $\varphi^{-1} \in \text{Mor}(Y, X)$  такой, что  $\varphi \circ \varphi^{-1} = \text{id}_Y$  и  $\varphi^{-1} \circ \varphi = \text{id}_X$ .

**ЗАМЕЧАНИЕ 1.6.** Очевидно, что любой изоморфизм является биморфизмом. Обратное вообще говоря неверно.

**ОПРЕДЕЛЕНИЕ 1.7.** Объект  $*$  называется *инициальным*, если для любого объекта  $X$  множество  $\text{Mor}(*, X)$  состоит ровно из одного элемента. Объект  $*$  называется *финальным*, если для любого объекта  $X$  множество  $\text{Mor}(X, *)$  состоит ровно из одного элемента.

**ПРЕДЛОЖЕНИЕ 1.8.** Инициальный (финальный) объект категории определен единственным образом с точностью до единственного изоморфизма, т. е. между двумя инициальными (финальными) объектами есть единственный изоморфизм.

**ДОКАЗАТЕЛЬСТВО.** Если  $*$  и  $'$  – инициальные объекты категории  $\mathcal{C}$ , то существуют единственные морфизмы  $\alpha : * \rightarrow ' и  $\alpha' : ' \rightarrow *$ . Тогда композиции  $* \circ ' и  $' \circ *$  – это единственные эндоморфизмы  $' и  $*$  соответственно. Но этими единственными морфизмами по определению категории должны быть тождественные. Следовательно,  $*$  и  $'$  – взаимно обратные изоморфизмы.  $\square$$$$

### Примеры.

- (1) Категория множеств  $\mathbf{Set}$ , пунктированных множеств  $\mathbf{Set}_*$ .
- (2) Категория множеств с инъективными (сюръективными) отображениями.
- (3) Алгебраические и геометрические структуры.
  - Категория моноидов  $\mathbf{Mon}$ .
  - Категория групп  $\mathbf{Grp}$ .
  - Категория абелевых групп  $\mathbf{Ab}$ .
  - Категория  $F$ -векторных пространств  $\mathbf{Vect} = F\text{-}\mathbf{Vect}$ , конечномерных векторных пространств  $F\text{-}\mathbf{Vect}_{f.d.}$ .
  - Категория  $R$ -модулей  $R\text{-}\mathbf{Mod}$ .
  - Категория  $R$ -алгебр  $R\text{-}\mathbf{Alg}$ .
  - Категория колец с 1  $\mathbf{Ring}$ , без 1 –  $\mathbf{Ang}$ .
  - Категория коммутативных колец с 1  $\mathbf{CRing}$ , без 1  $\mathbf{CAng}$ .
  - Категория полей (автоматом все морфизмы – мономорфизмы).
  - Категория топологических пространств  $\mathbf{Top}$ , пунктированных топологических пространств  $\mathbf{Top}_*$ .
  - Гомотопическая категория: объекты – топологические пространства, иногда обладающие какими-то хорошими свойствами, например CW-комплексы, морфизм из  $A$  в  $B$  – последовательность отображений

$$A = A_0 \xrightarrow{\varphi_0} B_0 \xleftarrow{\psi_0} A_1 \longrightarrow \dots \longrightarrow B_n = B,$$

где  $\varphi_i$  – непрерывны, а  $\psi_i$  – гомотопические эквивалентности. При композиции таких морфизмов соответствующие последовательности пририсовываются друг к другу, а фрагменты  $X \xleftarrow{\psi} Y \xrightarrow{\varphi} X$  вычеркиваются.

- (4) Моноид – категория с одним объектом.
- (5) Gruppoид – малая категория, все морфизмы которой являются изоморфизмами. Обобщение понятия группы. Полезно, например, при изучении фундаментальной группы несвязных пространств. Строится фундаментальный группойд: объекты – точки данного топологического пространства, Морфизм из точки  $a$  в точку  $b$  – класс гомотопных путей из  $a$  в  $b$ . Композиция – конкатенация путей, как она определяется в топологии (с точности до гомотопии).
- (6) Категория матриц над ассоциативным кольцом  $R$  с 1: объекты – натуральные числа,  $\text{Mor}(m, n) = M_{n \times m}(R)$ . Композиция морфизмов – произведение матриц.
- (7) Частично упорядоченное множество, из  $a$  в  $b$  есть ровно 1 морфизм  $\iff a \leq b$ .
- (8) Категории, связанные с ориентированным графом:
- категория путей: объекты – вершины, морфизмы – пути, включая пустой путь из точки в себя, композиция – конкатенация.
  - категория достижимости: из  $a$  в  $b$  есть ровно 1 морфизм  $\iff$  из  $a$  существует путь в  $b$ .
- (9) Категория морфизмов  $\text{Mor } \mathcal{C}$ . Объекты – морфизмы в категории  $\mathcal{C}$ , морфизмы из  $\varphi : X \rightarrow Y$  в  $\varphi' : X' \rightarrow Y'$  – коммутативные квадраты

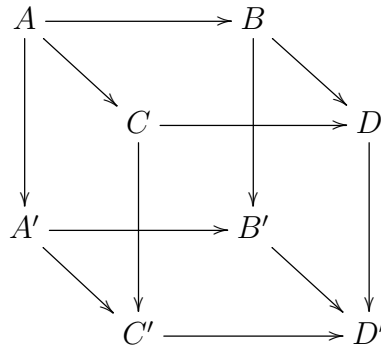
$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ \downarrow & & \downarrow \\ X' & \xrightarrow{\varphi'} & Y' \end{array}$$

- (10)  $\Gamma$  – ориентированный граф. Определим категорию коммутативных  $\mathcal{C}_\Gamma$  диаграмм в  $\mathcal{C}$  типа  $\Gamma$ . Диаграмма в  $\mathcal{C}$  типа  $\Gamma$  – это функция, сопоставляющая вершинам  $\Gamma$  объекты  $\mathcal{C}$ , а ребрам  $\Gamma$  – морфизмы  $\mathcal{C}$ . Диаграмма называется коммутативной, если для любых двух вершин и для любых двух путей, соединяющих эти вершины, композиции морфизмов вдоль этих путей совпадают.

Морфизм  $\eta$  диаграмм  $F$  и  $G$  – набор морфизмов  $\eta_a : F(a) \rightarrow G(a)$ , где  $a$  пробегает вершины графа  $\Gamma$ , такой что для любого ребра  $\alpha$  из вершины  $a$  в вершину  $b$  квадрат

$$\begin{array}{ccc} F(a) & \xrightarrow{F(\alpha)} & F(b) \\ \eta_a \downarrow & & \downarrow \eta_b \\ G(a) & \xrightarrow{G(\alpha)} & G(b) \end{array}$$

коммутативен. Например, если  $\Gamma$  – это квадрат со стрелками слева направо и сверху вниз, то морфизм диаграмм типа  $\Gamma$  – это коммутативный куб



- (11) Часто рассматривают подкатегорию в категории коммутативных диаграмм, состоящую из диаграмм, у которых объекты в нескольких вершинах и несколько морфизмов между ними фиксированы. В этом случае морфизмы – это морфизмы диаграмм, тождественные

на зафиксированных вершинах. Например, для данных объектов  $A, B, C \in \mathcal{C}$  и морфизмов  $C \leftarrow A \rightarrow B$  можно рассмотреть категорию квадратов вида

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ C & \longrightarrow & D \end{array}$$

морфизмами в которой являются коммутативные диаграммы

$$\begin{array}{ccccc} & & B & & \\ & \nearrow & & \searrow & \\ A & & & & D \longrightarrow D' \\ & \searrow & & \nearrow & \\ & & C & & \end{array}$$

Инициальный объект в этой категории называется пушаутом диаграммы  $C \leftarrow A \rightarrow B$  или копроизведением  $B$  и  $C$  над  $A$ . Позже мы рассмотрим несколько важных примеров пушаутов, а также двойственного понятия – пулбэка ([расслоенного] произведения).

## 2. Функторы

**ОПРЕДЕЛЕНИЕ 2.1.** Функтором  $\mathcal{F}$  из категории  $\mathcal{B}$  в категорию  $\mathcal{C}$  называется набор следующих отображений:

- $\mathcal{F} : \text{Obj } \mathcal{B} \rightarrow \text{Obj } \mathcal{C}$ ;
- $\mathcal{F}_{X,Y} : \text{Mor}(X, Y) \rightarrow \text{Mor}(\mathcal{F}(X), \mathcal{F}(Y))$  для каждой пары объектов  $X, Y \in \text{Obj } \mathcal{B}$ , удовлетворяющие свойствам  $\mathcal{F}_{X,Z}(\alpha \circ \beta) = \mathcal{F}_{Y,Z}(\alpha) \circ \mathcal{F}_{X,Y}(\beta)$  и  $\mathcal{F}_{X,X}(\text{id}_X) = \text{id}_{\mathcal{F}(X)}$ .

Индексы в обозначении отображения  $\mathcal{F}_{X,Y}$  обычно опускают, потому что они однозначно восстанавливаются по аргументу. В таких обозначениях свойства в определении означают, что  $\mathcal{F}$  сохраняет композицию морфизмов и тождественные морфизмы. Для функторов используется такое же обозначение, что и для функций: запись  $\mathcal{F} : \mathcal{B} \rightarrow \mathcal{C}$  означает, что  $\mathcal{F}$  является функтором из категории  $\mathcal{B}$  в категорию  $\mathcal{C}$ .

Функтор  $\mathcal{B}^{\text{op}} \rightarrow \mathcal{C}$  называется контравариантным функтором из  $\mathcal{B}$  в  $\mathcal{C}$  (обычный функтор, если хочется подчеркнуть, что он не меняет направление стрелок, называется ковариантным). Контравариантный функтор можно рассматривать и как функтор из  $\mathcal{B} \rightarrow \mathcal{C}^{\text{op}}$ .

Функтор называется строгим (полным), если он действует инъективно (сюръективно) на каждом множестве морфизмов. Образ полного функтора – полная подкатегория.

### Примеры.

- (1) Забывающие функторы – строгие функторы, “забывающие” часть структуры на объекте категории. Неформальное понятие.
- (2) Функтор вложения подкатегории в категорию. Очевидно он строгий. Он является полным  $\iff$  подкатегория полная. Как вы видите, строгий и полный функтор не обязан быть изоморфизмом и даже, как мы увидим позже, эквивалентностью категорий.
- (3)  $M_n$ ,  $GL_n$ , обратимые элементы моноида.
- (4) Центр группы  $Z(G) = \{a \in G \mid ag = ga \forall g \in G\}$  не определяет функтор, потому что образ центра не обязательно лежит в центре. Он будет функтором, если в качестве морфизмов в категории групп рассматривать только сюръективные гомоморфизмы.
- (5) Отображение, сопоставляющее группе ее коммутант, естественным образом определяет функтор, так как образ коммутанта очевидно содержится в коммутанте. Действие этого функтора на морфизмах – это просто сужение гомоморфизма групп на коммутанты (уменьшается как область определения, так и множество значений).

- (6) Отображение, которое множеству ставит в соответствие дискретное (антидискретное) топологическое пространство, свободную группу, свободный модуль над фиксированным кольцом.
- (7) Гомотопические группы:  $\pi_0 : \mathbf{Top}_* \rightarrow \mathbf{Set}_*$  – множество компонент связности,  $\pi_1 : \mathbf{Top}_* \rightarrow \mathbf{Grp}$  – фундаментальная группа,  $\pi_i : \mathbf{Top}_* \rightarrow \mathbf{Ab}$  – высшие гомотопические группы.
- (8) В произвольной категории  $\mathcal{C}$  отображение  $\text{Aut}$ , отображающее объект в множество (мономорфизм) его автоморфизмов, не является функтором, так как нет никакого разумного способа по морфизму  $\varphi : A \rightarrow B$  задать отображение  $\text{Aut } A \rightarrow \text{Aut } B$  или наоборот.
- (9) Пусть  $\Gamma$  – ориентированный граф, а  $\mathcal{C}_\Gamma$  – категория достижимости, связанная с этим графом. Функтор из  $\mathcal{C}_\Gamma$  в произвольную категорию  $\mathcal{B}$  называется коммутативной диаграммой типа  $\Gamma$  в категории  $\mathcal{B}$ .
- (10)  $\text{Mor} : \mathcal{C}^{op} \times \mathcal{C} \rightarrow \mathbf{Set}$ . Пусть задан морфизм  $(\alpha, \beta) \in \text{Mor}_{\mathcal{C}^{op} \times \mathcal{C}}((X, Y), (X', Y'))$ , т. е. пара морфизмов  $\alpha : X' \rightarrow X$  и  $\beta : Y \rightarrow Y'$  в категории  $\mathcal{C}$ . Тогда отображение

$$\text{Mor}(\alpha, \beta) : \text{Mor}(X, Y) \rightarrow \text{Mor}(X', Y')$$

отображает морфизм  $\varphi : X \rightarrow Y$  в композицию  $\beta \circ \varphi \circ \alpha : X' \rightarrow Y'$ .

Если  $\mathcal{C}$  – категория  $R$ -модулей, где  $R$  – кольцо, то вместо категории множеств можно написать категорию  $R$ -модулей. Можно зафиксировать первый или второй аргумент.

В частности,  $\text{Mor}(\_, F) : (R\text{-Mod})^{op} \rightarrow R\text{-Mod}$  – контравариантный функтор на категории  $R$ -модулей. Обычно его действие на объектах обозначается звездочкой. Модуль  $M^* = \text{Mor}(M, R)$  называется двойственным (или сопряженным) к  $M$ . Если  $R$  – поле, а  $V$  – векторное пространство над  $F$ , то элементы  $V^*$  часто называются ковекторами.

- (11) Предпучок на топологическом пространстве. Пусть  $X$  – топологическое пространство, а  $\Omega$  – множество его открытых подмножеств упорядоченное по включению. Обозначим через  $\mathcal{C}_X$  категорию, связанную с частично упорядоченным множеством  $\Omega$ . Тогда предпучком объектов категории  $\mathcal{B}$  на пространстве  $X$  называется контравариантный функтор из  $\mathcal{C}_X$  в  $\mathcal{B}$ .

Другими словами, каждому открытому множеству в  $X$  предпучок ставит в соответствие объект категории  $\mathcal{B}$ , а вложению открытых множеств – морфизм в категории  $\mathcal{B}$  в обратную сторону. Пучок – это предпучок, удовлетворяющий некоторым “условиям склейки”, которые выходят за рамки нашего беглого знакомства с теорией категорий.

Стандартный пример пучка множеств на топологическом пространстве  $X$  строится следующим образом. Каждому открытому множеству  $A$  сопоставим множество непрерывных функций  $\mathbb{R}^A$ . Если  $A \subseteq B$ , то отображение  $\mathbb{R}^B \rightarrow \mathbb{R}^A$  – это просто сужение функции  $B \rightarrow \mathbb{R}$  на подмножество  $A$ .

Множество непрерывных функций  $\mathbb{R}^A$  является коммутативным кольцом с 1 относительно поточечных операций. Обычно считают, что пучок из этого примера – это пучок коммутативных колец с 1. Естественно,  $\mathbb{R}$  можно заменить на  $\mathbb{C}$  или на что-то другое (правда тогда может оказаться, что множество функций не является кольцом), а свойство непрерывности на какое-нибудь другое свойство, скажем, дифференцируемость (если  $X$  – нормированное пространство).

Теперь мы можем привести еще один пример категории: категория категорий! Но, все же категории *всех* категорий не может быть, потому что мы не имеем право образовать класс всех категорий. Поэтому “категория категорий” – это на самом деле категория всех малых категорий. Морфизмами в этой категории являются функторы. Она обозначается  $\mathbf{Cat}$ .

Философски, тот факт, что  $\mathbf{Cat}$  знает только малые категории, не играет никакой роли, потому что категории из какого-то конкретного набора, который нас в данный момент интересует, всегда можно сделать малыми, изменив универсум, в котором мы работаем.

### 3. Естественные преобразования

**ОПРЕДЕЛЕНИЕ 3.1.** Пусть  $\mathcal{F}, \mathcal{G} : \mathcal{B} \rightarrow \mathcal{C}$  – функторы. Естественным преобразованием функторов  $\eta : \mathcal{F} \rightarrow \mathcal{G}$  называется набор морфизмов  $\eta_X \in \text{Mor}(\mathcal{F}(X), \mathcal{G}(X))$  по всем объектам  $X$  категории  $\mathcal{B}$ , удовлетворяющих условию

$$\eta_Y \circ \mathcal{F}(\alpha) = \mathcal{G}(\alpha) \circ \eta_X$$

для любых объектов  $X, Y \in \text{Obj } \mathcal{B}$  и любого морфизма  $\alpha \in \text{Mor}(X, Y)$ .

Последнее условие в определении означает коммутативность следующей диаграммы:

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\mathcal{F}(\alpha)} & \mathcal{F}(Y) \\ \eta_X \downarrow & & \downarrow \eta_Y \\ \mathcal{G}(X) & \xrightarrow{\mathcal{G}(\alpha)} & \mathcal{G}(Y). \end{array}$$

Функторы  $\mathcal{F}, \mathcal{G} : \mathcal{B} \rightarrow \mathcal{C}$  называются естественно изоморфными, если существует естественное преобразование  $\eta : \mathcal{F} \rightarrow \mathcal{G}$  такое, что  $\eta_X$  является изоморфизмом для любого  $X \in \text{Obj } \mathcal{B}$ . Очевидно, что в этом случае существует и обратное естественное преобразование  $\eta^{-1} : \mathcal{G} \rightarrow \mathcal{F}$ .

Категории  $\mathcal{B}$  и  $\mathcal{C}$  называются эквивалентными, если существуют функторы  $\mathcal{F} : \mathcal{B} \rightarrow \mathcal{C}$  и  $\mathcal{F}' : \mathcal{C} \rightarrow \mathcal{B}$  такие, что композиция  $\mathcal{F} \circ \mathcal{F}'$  естественно изоморфна  $\text{id}_{\mathcal{C}}$ , а  $\mathcal{F}' \circ \mathcal{F}$  естественно изоморфна  $\text{id}_{\mathcal{B}}$ . Другими словами, существуют естественные изоморфизмы  $X \cong \mathcal{F}'(\mathcal{F}(X))$  и  $Y \cong \mathcal{F}(\mathcal{F}'(Y))$ , где  $X \in \text{Obj } \mathcal{C}$ , а  $Y \in \text{Obj } \mathcal{B}$ . При этом функторы  $\mathcal{F}$  и  $\mathcal{F}'$  называются квазиобратными друг другу.

#### Примеры.

- (1) Вложение в тождественный функтор:  $M^* \hookrightarrow M$  (здесь  $M^*$  – моноид обратимых элементов), вложение коммутанта в группу и т.п.
- (2) Тривиальные естественные изоморфизмы, например  $(X \times Y) \times Z \cong X \times (Y \times Z)$ .
- (3)  $\det_n : \text{GL}_n \rightarrow \text{GL}_1, A \mapsto \det A$ .
- (4)  $\text{Mor}(X, \text{Mor}(Y, Z)) \cong \text{Mor}(X \times Y, Z)$  в категории множеств. Это называется “экспоненциальный закон для множеств” и обычно выражается формулой  $(Z^Y)^X = Z^{X \times Y}$ . При этом естественном отображении функция  $f : X \rightarrow Z^Y$  переходит в функцию  $g : X \times Y \rightarrow Z$ , заданную формулой  $g(x, y) = f(x)(y)$ .

Аналог этого естественного изоморфизма выполнен в разных других категориях  $\mathcal{C}$ , если множество  $\text{Mor}(Y, Z)$  естественным образом превращается в объект категории  $\mathcal{C}$ . При этом вместо прямого произведения возникают другие универсальные конструкции.

- (5) В категории векторных пространств над полем  $F$  множество  $\text{Mor}(Y, Z)$  имеет естественную структуру векторного пространства. Поэтому можно считать, что  $\text{Mor}_{F\text{-Vect}}(-, -)$  является функтором  $(F\text{-Vect})^{op} \times F\text{-Vect} \rightarrow F\text{-Vect}$ . Тогда  $\text{Mor}(X, \text{Mor}(Y, Z))$  естественно изоморфно пространству  $\text{Bil}(X \times Y, Z)$  билинейных отображений из  $X \times Y$  в  $Z$ . В следующем параграфе мы определим тензорное произведение  $X \otimes Y$  так, чтобы  $\text{Bil}(X \times Y, Z)$  было бы естественно изоморфно  $\text{Mor}(X \otimes Y, Z)$ .
- (6) Рассмотрим контравариантный функтор  $V \mapsto V^*$  на категории векторных пространств из примера 10. Ясно, что его композиция с самим собой будет ковариантным функтором. Построим естественное преобразование  $\eta$  тождественного функтора в функтор  $**$ . Для этого для любого векторного пространства  $V$  необходимо определить линейное отображение  $\eta_V : V \rightarrow V^{**}$ . Для  $x \in V$  положим  $\eta_V(x)(f) = f(x)$ . Проверка того, что такие отображения линейны, а  $\eta$  – естественное преобразование, является рутинной. Заметим, что отображение  $\eta_V$  является инъективным (нетрудно посчитать его ядро).

Пусть теперь  $\mathcal{V} = F\text{-Vect}_{f.d.}$  обозначает категорию конечномерных векторных пространств и их линейных отображений. Рассмотрим сужения функторов  $* : \mathcal{V} \rightarrow \mathcal{V}^{op}$  и  $** : \mathcal{V} \rightarrow \mathcal{V}$ . Так как размерности пространств  $V, V^*$  и  $V^{**}$  совпадают, то построенные

выше отображения  $\eta_V$  являются изоморфизмами векторных пространств. Это доказывает, что функтор  $** : \mathcal{V} \rightarrow \mathcal{V}$  естественно изоморфен тождественному, а функтор  $*$  – квазиобратен сам себе. В частности, категория конечномерных векторных пространств эквивалентна своей противоположной.

- (7) Пусть  $\Gamma$  – ориентированный граф,  $\mathcal{C}_\Gamma$  – категория достижимости в этом графе, а  $\mathcal{B}$  – произвольная категория. Тогда естественное преобразование функторов  $\mathcal{F} \rightarrow \mathcal{G}$ , где  $\mathcal{F}, \mathcal{G} : \mathcal{C}_\Gamma \rightarrow \mathcal{B}$ , – это просто морфизм соответствующих диаграмм (см. пример функторов номер 9).
- (8) Пусть  $\mathcal{F} : \mathcal{B} \rightarrow \mathcal{C}$  – функтор. Он определяет естественное преобразование функторов  $\eta^{\mathcal{F}} : \text{Mor}_{\mathcal{B}}(-, -) \rightarrow \text{Mor}_{\mathcal{C}}(\mathcal{F}(-), \mathcal{F}(-))$  по правилу:  $\eta_{(X,Y)}^{\mathcal{F}}(\alpha) = \mathcal{F}(\alpha)$ , где  $\alpha \in \text{Mor}(X, Y)$ .
- (9) Пусть  $\mathcal{M}$  – категория матриц, а  $\mathcal{V}$  – категория конечномерных векторных пространств (все над одним и тем же полем  $F$ ). Пусть  $\mathcal{F} : \mathcal{M} \rightarrow \mathcal{V}$  – функтор, который натуральному числу  $n$  ставит в соответствие пространство  $F^n$ , а матрице  $A \in M_{m \times n}(F) = \text{Mor}_{\mathcal{M}}(n, m)$  – линейное отображение  $L_A : F^n \rightarrow F^m$  умножения на матрицу  $A$ . Нетрудно проверить, что  $\mathcal{F}$  действительно является функтором.

Если мы верим в аксиому выбора для классов, то можно построить и квазиобратный функтор. Зафиксируем в каждом векторном пространстве  $V$  базис  $b_V$  (для простоты в пространстве  $F^n$  выберем стандартный базис) и зададим функтор  $\mathcal{G} : \mathcal{V} \rightarrow \mathcal{M}$ , который векторному пространству сопоставляет его размерность, а линейному отображению – его матрицу в выбранных базисах. Тогда композиция  $\mathcal{G} \circ \mathcal{F}$  просто тождественна (матрица отображения  $L_A$  в стандартных базисах равна  $A$ ), а композиция в обратном порядке естественно изоморфна тождественному. Действительно, зададим естественное отображение  $\eta : \mathcal{F} \circ \mathcal{G} \rightarrow \text{id}_{\mathcal{V}}$  по правилу  $\eta_V : F^{\dim V} \rightarrow V$  – это единственное линейное отображение, переводящее стандартный базис в выбранный базис пространства  $V$ . Условие естественности  $\eta$  – это коммутативность диаграммы:

$$\begin{array}{ccc} F^m & \longrightarrow & F^n \\ \eta_U \downarrow & & \downarrow \eta_V \\ U & \xrightarrow{L} & V \end{array}$$

где  $m = \dim U$ ,  $n = \dim V$ , а верхняя стрелка  $\mathcal{F}(\mathcal{G}(L))$  – умножение на матрицу оператора  $L$  в выбранных базисах. А коммутативность эта выполнена просто по определению матрицы линейного отображения.

Если мы не верим в аксиому выбора для классов,<sup>1</sup> то надо рассмотреть категорию конечномерных векторных пространств с выбранными базисами, морфизмами в которой являются любые линейные отображения никак не связанные с выбранными базисами.

Функторы можно применять к морфизмам, что наводит на мысль, что можно применять их и набору морфизмов, в частности, к естественному преобразованию.

**ПРЕДЛОЖЕНИЕ 3.2.** Пусть  $\eta$  – естественное преобразование функторов  $\mathcal{F}, \mathcal{G} : \mathcal{A} \rightarrow \mathcal{B}$ , а  $\mathcal{H} : \mathcal{B} \rightarrow \mathcal{C}$  – функтор. Тогда набор морфизмов  $(\mathcal{H}\eta)_X := \mathcal{H}(\eta_X)$  является естественным преобразованием  $\mathcal{H}\eta : \mathcal{H} \circ \mathcal{F} \rightarrow \mathcal{H} \circ \mathcal{G}$ .

Если  $\mathcal{E} : \mathcal{C} \rightarrow \mathcal{A}$ , то набор морфизмов  $(\eta^{\mathcal{E}})_X := \eta_{\mathcal{E}(X)}$  является естественным преобразованием  $\eta^{\mathcal{E}} : \mathcal{F} \circ \mathcal{E} \rightarrow \mathcal{G} \circ \mathcal{E}$ .

Если  $\eta$  изоморфизм, то  $\mathcal{H}\eta$  и  $\eta^{\mathcal{E}}$  – изоморфизмы.

<sup>1</sup>В отличие от аксиомы выбора для множеств, без которой никакой содержательной математики не получается, аксиома выбора для классов практически не используется, поэтому в некоторых аксиоматиках она отсутствует.



#### 4. Эквалайзеры, произведения и универсальные квадраты

В этом параграфе мы изучим несколько важных универсальных конструкций, являющихся частым случаем (ко)пределов. Пусть  $\alpha : A \rightarrow C$  и  $\beta : B \rightarrow C$  – морфизмы в категории  $\mathcal{C}$ . Говорят, что  $\beta$  пропускается через  $\alpha$ , если  $\beta = \alpha\gamma$  для некоторого морфизма  $\gamma : B \rightarrow A$ .

Пусть  $\varphi, \psi \in \text{Mor}(X, Y)$  – морфизмы в категории  $\mathcal{C}$ . Морфизм  $\varepsilon : E \rightarrow X$  называется *эквалайзером* пары  $(\varphi, \psi)$ , если  $\varphi\varepsilon = \psi\varepsilon$ , и для любой  $\varepsilon' : E' \rightarrow X$ , обладающий свойством  $\varphi\varepsilon' = \psi\varepsilon'$ , пропускается через  $\varepsilon$  единственным образом. Это определение можно выразить коммутативной диаграммой

$$\begin{array}{ccccc} E' & & & & \\ \downarrow & \searrow \varepsilon' & & & \\ E & \xrightarrow{\varepsilon} & X & \begin{array}{c} \xrightarrow{\varphi} \\ \xrightarrow{\psi} \end{array} & Y \end{array}$$

(обычно используется соглашение, что пути длины 1 из  $X$  в  $Y$  не должны быть равны на коммутативной диаграмме). Другими словами, рассмотрим категорию коммутативных диаграмм вида

$$E \xrightarrow{\varepsilon} X \begin{array}{c} \xrightarrow{\varphi} \\ \xrightarrow{\psi} \end{array} Y,$$

где  $X, Y, \varphi$  и  $\psi$  фиксированы, а  $E$  и  $\varepsilon$  меняются. Тогда эквалайзер – это финальный объект в этой категории. Как обычно, финальный объект единственный с точностью до единственного изоморфизма.

Двойственное понятие называется *коэквалайзером*. В категории множеств эквалайзер – это множество решений уравнения  $\varphi(x) = \psi(x)$  вместе с отображением вложения. Коэквалайзер – каноническая проекция  $Y$  на фактормножество по наименьшему отношению эквивалентности, содержащему все пары  $(\varphi(x), \psi(x))$ .

**ПРЕДЛОЖЕНИЕ 4.1.** *Эквалайзер всегда является мономорфизмом, а коэквалайзер – эпиморфизмом.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\varepsilon\alpha = \varepsilon\beta$  для некоторых морфизмов  $\alpha, \beta : A \rightarrow E$  и эквалайзера  $\varepsilon : E \rightarrow X$  морфизмов  $\varphi, \psi : X \rightarrow Y$ . Рассмотрим коммутативную диаграмму

$$\begin{array}{ccccc} A & & & & \\ \downarrow \beta & \searrow \alpha & \xrightarrow{\varepsilon\alpha=\varepsilon\beta} & & \\ E & \xrightarrow{\varepsilon} & X & \begin{array}{c} \xrightarrow{\varphi} \\ \xrightarrow{\psi} \end{array} & Y \end{array}$$

По утверждению о единственности из определения эквалайзера получим, что  $\alpha = \beta$ . Как обычно, двойственное утверждение можно не доказывать (принцип “2 по цене 1”).  $\square$

Нетрудно проверить, что в категории множеств любой мономорфизм является эквалайзером каких-то двух морфизмов. В общем случае это не так, свойство “быть эквалайзером” существенно сильнее свойства “быть мономорфизмом”, что видно, в частности, из следующего утверждения.

**ПРЕДЛОЖЕНИЕ 4.2.** *Эквалайзер, являющийся эпиморфизмом – изоморфизм. Двойственно: коэквалайзер, являющийся мономорфизмом – изоморфизм.*

**ДОКАЗАТЕЛЬСТВО.** Если  $\varepsilon$  является эквалайзером морфизмов  $\varphi, \psi : X \rightarrow Y$ , то  $\varphi\varepsilon = \psi\varepsilon$ , а если  $\varepsilon$  – эпиморфизм, то из этого равенства следует, что  $\varphi = \psi$ . Но в этом случае легко видеть, что  $\text{id}_X$  удовлетворяет определению эквалайзера. Так как два разных эквалайзера отличаются друг от друга на изоморфизм, то  $\varepsilon$  – изоморфизм.  $\square$

Следующие универсальные конструкции, которые мы изучим – произведение и копроизведение. Пусть  $A, B \in \mathcal{C}$ . Рассмотрим категорию диаграмм вида  $A \leftarrow C \rightarrow B$ . Финальный объект

в этой категории называется произведением объектов  $A, B$  и часто обозначается  $A \times B$ . Обратите внимание, что произведение – это объект вместе с морфизмами в  $A$  и в  $B$ , хотя, допуская вольность речи, про морфизмы часто забывают. В категории множеств, как и во многих других *конкретных* категориях<sup>2</sup>, произведение – это действительно декартово произведение (морфизмы – проекции).

**УПРАЖНЕНИЕ 4.3.** Пусть  $A, B, C \in \mathcal{C}$ . Докажите, что следующие условия эквивалентны.

- (1)  $C = A \times B$ .
- (2) Существует естественная биекция  $\text{Mor}(D, A) \times \text{Mor}(D, B) \rightarrow \text{Mor}(D, C)$ .

Двойственное понятие, копроизведение, – это инициальный объект в категории диаграмм вида  $A \rightarrow C \leftarrow B$  с фиксированными  $A$  и  $B$ . В категории множеств копроизведение – это дизъюнктное объединение, в других конкретных категориях – нечто, что “свободно” порождается  $A$  и  $B$ , конкретика в следующем параграфе.

Масса полезных конструкций в математике возникает, как универсальные объекты в категории квадратов с тремя фиксированными вершинами. Пусть  $\mathcal{C}$  – категория,  $A, B, C \in \text{Obj } \mathcal{C}$ ,  $\alpha \in \text{Mor}(A, C)$ ,  $\beta \in \text{Mor}(B, C)$ . Обозначим через  $\mathcal{S}$  категорию коммутативных квадратов вида

$$\begin{array}{ccc} \bullet & \longrightarrow & B \\ \downarrow & & \downarrow \beta \\ A & \xrightarrow{\alpha} & C \end{array}$$

(см. двойственный пример (11) из параграфа 1). Тогда финальный объект в этой категории называется пулбэком морфизмов  $\alpha$  и  $\beta$  или, чаще, пулбэком диаграммы

$$A \xrightarrow{\alpha} C \xleftarrow{\beta} B.$$

Двойственным образом определяется пушаут, т. е. пушаут в категории  $\mathcal{C}$  – это пулбэк в категории  $\mathcal{C}^{\text{op}}$ .

**ПРЕДЛОЖЕНИЕ 4.4.** Пулбэк диаграммы  $A \xrightarrow{\alpha} C \xleftarrow{\beta} B$  – это эквалайзер композиций  $A \times B \xrightarrow{\pi_A} A \xrightarrow{\alpha} C$  и  $A \times B \xrightarrow{\pi_B} B \xrightarrow{\beta} C$ .

Аналогично, пушаут диаграммы  $A \leftarrow C \rightarrow B$  – это коэквалайзер двух естественных морфизмов из  $C$  в копроизведение  $A$  и  $B$ .

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} D & \xrightarrow{\varphi} & B \\ \psi \downarrow & & \downarrow \beta \\ A & \xrightarrow{\alpha} & C \end{array}$$

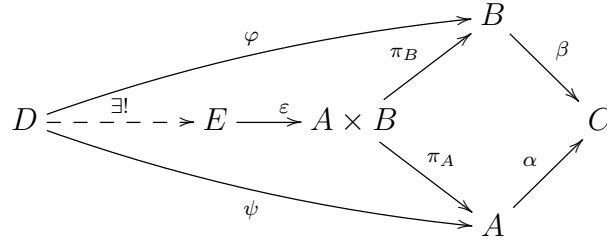
По универсальному свойству произведения существует единственный морфизм  $\theta : D \rightarrow A \times B$ , чьи композиции с проекциями  $\pi_A$  и  $\pi_B$  равны  $\psi$  и  $\varphi$  соответственно. Получаем диаграмму

$$D \xrightarrow{\theta} A \times B \xrightleftharpoons[\beta\pi_B]{\alpha\pi_A} C,$$

которая является коммутативной, так как  $\alpha\pi_A\theta = \alpha\psi = \beta\varphi = \beta\pi_B\theta$ . Следовательно, существует морфизм из  $D$  в эквалайзер  $(E, \varepsilon)$  морфизмов  $\alpha\pi_A$  и  $\beta\pi_B$ . Единственность морфизма из  $D$  в

<sup>2</sup>Категория называется конкретной, если из нее существует строгий “забывающий” функтор в категорию множеств.

эквалайзер сразу следует из единственности в определениях произведения и эквалайзера.



(на последней диаграмме правый квадрат некоммутативен!). □

**УПРАЖНЕНИЕ 4.5.** Рассмотрим коммутативную диаграмму

$$\begin{array}{ccccc} A & \longrightarrow & B & \longrightarrow & C \\ \downarrow & & \downarrow & & \downarrow \\ D & \longrightarrow & E & \longrightarrow & F \end{array}$$

Предположим, что квадрат  $BCFE$  является пулбэком. Докажите, что  $ABED$  – пулбэк тогда и только тогда, когда  $ACFD$  пулбэк. Приведите пример, когда  $ABED$  и  $ACFD$  – пулбэки, а  $BCFE$  – нет.

Следующее утверждение показывает, на каком универсальном примере можно проверять, является ли морфизм эпиморфизмом. Формулировка двойственного утверждения оставляется читателю в качестве упражнения.

**ПРЕДЛОЖЕНИЕ 4.6.** Предположим, что коммутативный квадрат

$$\begin{array}{ccc} A & \xrightarrow{\theta} & B \\ \theta \downarrow & & \psi \downarrow \\ B & \xrightarrow{\varphi} & C \end{array}$$

является пушаутом. Докажите, что следующие условия эквивалентны.

- (1)  $\theta$  – эпиморфизм.
- (2)  $\varphi$  – изоморфизм.
- (3)  $\psi$  – изоморфизм.
- (4)  $\varphi = \psi$ .

**ДОКАЗАТЕЛЬСТВО.** (1)  $\iff$  (4). Предположим, что  $\varphi = \psi$ . Пусть  $\alpha, \beta : B \rightarrow D$  такие морфизмы, что  $\alpha\theta = \beta\theta$ . По универсальному свойству пушаута существует единственный морфизм  $\gamma : C \rightarrow D$  такой, что  $\alpha = \gamma\varphi = \beta$ . Следовательно,  $\theta$  – эпиморфизм. Обратно,  $\varphi\theta = \psi\theta \implies \varphi = \psi$  просто по определению эпиморфизма.

(2)  $\implies$  (4). По определению пушаута для тождественного морфизма  $\text{id}_B$  существует  $\varepsilon : C \rightarrow B$  такой, что  $\varepsilon\varphi = \varepsilon\psi = \text{id}_B$ . Если  $\varphi$  – изоморфизм, то  $\varepsilon = \varphi^{-1}$  также является изоморфизмом (обратные слева и справа должны совпадать). Следовательно, на него можно сократить, откуда  $\varphi = \psi$ .

(1)  $\implies$  (2). Если  $\theta$  эпиморфизм, то для любого коммутативного квадрата

$$\begin{array}{ccc} A & \xrightarrow{\theta} & B \\ \theta \downarrow & & \beta \downarrow \\ B & \xrightarrow{\alpha} & D \end{array}$$

$\alpha = \beta$ . Поэтому  $C = B$ ,  $\varphi = \psi = \text{id}_B$  будут удовлетворять определению пушаута. Так как пушаут определен с точностью до изоморфизма, то  $\varphi = \psi$  – изоморфизмы.

Так как  $\varphi$  и  $\psi$  входят в условие симметрично, то импликации (1)  $\implies$  (3)  $\implies$  (4) доказывать не надо. □

Как это ни удивительно, но доказательство отрицательного результата, т. е. того, что морфизм не является эпиморфизмом, часто очень сложно доказать, пользуясь последним предложением. Проще оказывается построить не универсальный пример морфизмов  $\alpha \neq \beta$ , для которых  $\alpha\theta = \beta\theta$ . Так делается, например, для доказательства того, что **в категории групп несюръективное отображение не может быть эпиморфизмом**.

## 5. Универсальные алгебраические конструкции

**5.1. Универсальное свойство колец многочленов.** Пусть  $R$  – коммутативное кольцо с 1. Для начала обсудим категорию  $R$ -алгебр. Напомним, что  $R$ -алгебра – это  $R$ -модуль с  $R$ -билинейным умножением. Рассмотрим категорию ассоциативных  $R$ -алгебр с 1, обозначаемую  $R\text{-}\mathcal{Alg}$ . Морфизм в этой категории – это гомоморфизм  $R$ -алгебр, т. е.  $R$ -линейный гомоморфизм колец с 1. Так как 1 переходит в 1, то для любой  $R$ -алгебры  $A$  существует единственный гомоморфизм  $R \rightarrow A$ ,  $r \mapsto r \cdot 1_A$ . Так что  $R$  является инициальным объектом категории  $R\text{-}\mathcal{Alg}$ . В частности, инициальным объектом категории  $\mathbb{Z}\text{-}\mathcal{Alg} = \mathcal{Ring}$  является кольцо целых чисел. Заметим, что финальный объект в категории  $R\text{-}\mathcal{Alg}$  – это нулевая алгебра.

Более того, так как  $a(rb) = r \cdot 1_A \cdot (ab)$  для любых  $r \in R$  и  $a, b \in A$ , то при  $b = 1$  получаем  $a(r \cdot 1_A) = (r \cdot 1_A)a$ , т. е. образ  $R$  лежит в центре алгебры  $A$ .<sup>3</sup> Поэтому категория  $R\text{-}\mathcal{Alg}$  изоморфна (даже не просто эквивалентна, а именно изоморфна) категории морфизмов  $R \rightarrow A$  в категории  $\mathcal{Ring}$ , таких, что образ  $R$  содержится в центре  $A$ .

Пусть теперь  $R\text{-}\mathcal{Alg}_n$  обозначает категорию  $R$ -алгебр с  $n$  отмеченными точками. Точнее, объекты этой категории – это наборы  $(A, a_1, \dots, a_n)$ , где  $A$  –  $R$ -алгебра, а  $a_1, \dots, a_n$  – коммутирующие между собой элементы алгебры  $A$ , а морфизмы  $(A, a_1, \dots, a_n) \rightarrow (B, b_1, \dots, b_n)$  – это гомоморфизмы  $R$ -алгебр  $\varphi : A \rightarrow B$  такие, что  $\varphi(a_i) = b_i$  при всех  $i$ . Инициальным объектом в этой категории является алгебра многочленов  $(R[t_1, \dots, t_n], t_1, \dots, t_n)$ . Это и есть универсальное свойство кольца многочленов. Единственный морфизм  $(R[t_1, \dots, t_n], t_1, \dots, t_n) \rightarrow (A, a_1, \dots, a_n)$  – это гомоморфизм подстановки:  $p \mapsto p(a_1, \dots, a_n)$ .

**5.2. Локализация.** Пусть  $R$  – коммутативное кольцо с 1, а  $S$  – мультипликативное подмножество в  $R$ . Рассмотрим категорию  $\mathcal{C}$  морфизмов  $R \rightarrow A$  в категории  $\mathcal{C}\mathcal{Ring}$  таких, что образы всех элементов из  $S$  обратимы в  $A$ . По определению инициальным объектом этой категории является гомоморфизм локализации  $\lambda_S : R \rightarrow S^{-1}R$ .

То, что  $S$  замкнуто относительно умножения и содержит 1, не играет никакой роли при таком определении. Локализацией в произвольном подмножестве  $X \subseteq R$  будет локализация в мультипликативном подмножестве, порожденном  $X$ , т. е. в наименьшем мультипликативном подмоноиде  $R$ , содержащем  $X$ . Условие, что  $S$  мультипликативно, используется только для конструкции локализации.

Можно также отбросить и условие коммутативности  $R$  и  $A$ . В этом случае локализация все еще будет существовать, но конструкция ее будет намного сложнее. Она является частным случаем конструкции локализации категории.

**5.3. Локализация – эпиморфизм в категории  $\mathcal{C}\mathcal{Ring}$ .** Действительно, рассмотрим коммутативную диаграмму

$$R \xrightarrow{\lambda} S^{-1}R \begin{matrix} \xrightarrow{\varphi} \\ \xrightarrow{\psi} \end{matrix} X.$$

Так как при гомоморфизме колец с 1 обратимые элементы переходят в обратимые, то  $\varphi \circ \lambda = \psi \circ \lambda$  – морфизм в категории  $\mathcal{C}$ . Так как  $\lambda$  является инициальным объектом в этой категории, то существует единственный морфизм  $S^{-1}R \rightarrow X$ , делающий нашу диаграмму коммутативной, т. е.

<sup>3</sup>В частности, алгебра кватернионов не является алгеброй над  $\mathbb{C}$ : как бы вы не определили умножение кватерниона на комплексное число, оно будет линейным только по одному аргументу.

$\varphi = \psi$ . Нетрудно провести доказательство, пользуясь конструкцией локализации, а не ее универсальным свойством, но такое доказательство не будет работать для некоммутативных локализаций, а наше будет.

**5.4. Свободные объекты конкретных категорий.** Пусть  $X$  – множество, а  $R$  – коммутативное кольцо с 1. Пусть  $\mathcal{C} = \mathbf{Mon}, \mathbf{Grp}, R\text{-}\mathbf{Mod}$  или  $R\text{-}\mathbf{Alg}$  (в принципе можно рассмотреть любую конкретную категорию, просто конструкции будут разные, а постановка задачи одинаковая). Рассмотрим категорию, объектами которой будут *функции*  $X \rightarrow A$ , где  $A \in \mathcal{C}$ , а морфизмами – коммутативные треугольники

$$\begin{array}{ccc} & & A \\ & \nearrow & \downarrow \\ X & \longrightarrow & A' \end{array}$$

где вертикальная стрелка является морфизмом в категории  $\mathcal{C}$  (здесь мы используем, что морфизм в конкретной категории “является” отображением множеств, формально не он сам, а его образ под действием строгого функтора, входящего в определение конкретной категории). Инициальный объект такой категории называется *свободным объектом категории  $\mathcal{C}$ , порожденным  $X$* .

Конструкции свободной группы и свободного  $R$ -модуля мы изучали, сейчас мы (не вникая в детали) построим свободный моноид  $M_X$  и свободную  $R$ -алгебру, порожденные  $X$ . Алгебра обычно обозначается  $R\langle X \rangle$  и называется кольцом некоммутирующих многочленов от  $X$ .

Свободный моноид – это просто множество слов в алфавите  $X$ , включая пустое слово, с операцией конкатенации. Ясно, что как только мы знаем образы элементов множества  $X$ , то мы знаем и образы всех слов в алфавите  $X$  под действием гомоморфизма моноидов. Так строится единственный гомоморфизм из свободного моноида в произвольный моноид  $M$  по заданной функции  $X \rightarrow M$ .

Свободная  $R$ -алгебра  $R\langle X \rangle$  – это свободный  $R$ -модуль с базисом  $M_X$ , умножение на котором задано очевидным образом. Действительно, на базисе умножение уже задано, а дальше оно единственным образом продолжается по билинейности.

$$X \rightarrow R\langle X \rangle \implies M_X \rightarrow R\langle X \rangle \implies \langle M_X \rangle_R \rightarrow R\langle X \rangle.$$

**5.5. Тензорное произведение модулей.** Пусть  $R$  – коммутативное кольцо с 1, а  $M$  и  $N$  –  $R$ -модули. Рассмотрим категорию  $\mathcal{C}$ , объектами которой являются билинейные отображения  $M \times N \rightarrow P$ , где  $P$  также является  $R$ -модулем, а морфизмами –  $R$ -линейные отображения  $P \rightarrow P'$ , для которых диаграмма

$$\begin{array}{ccc} & & P \\ & \nearrow & \downarrow \\ M \times N & \longrightarrow & P' \end{array}$$

коммутативна (как диаграмма отображений множеств). Инициальный объект в такой категории называется тензорным произведением модулей  $M$  и  $N$  над  $R$  и обозначается через  $M \otimes_R N$ .

Формально, конструкция тензорного произведения чрезвычайно проста. Сначала мы забываем про билинейность отображений  $M \times N \rightarrow P$  и строим универсальный объект без учета билинейности. Такую задачу мы только что решили: это свободный  $R$ -модуль с базисом  $M \times N$ . Для того, чтобы превратить каноническое отображение  $M \times N \rightarrow \langle M \times N \rangle_R$  в билинейное, в свободном модуле должны быть выполнены условия

$$(m + m', n) = (m, n) + (m', n), \quad (m, n + n') = (m, n) + (m, n'), \quad r(m, n) = (rm, n) = (m, rn).$$

Универсальный модуль, в котором выполнены эти условия – фактормодуль

$$M \otimes_R N = \frac{\langle M \times N \rangle_R}{K},$$

где  $K$  – подмодуль в  $\langle M \times N \rangle_R$ , порожденный элементами  $(m, n) + (m', n) - (m + m', n)$ ,  $(m, n) + (m, n') - (m, n + n')$ ,  $r(m, n) - (rm, n)$ , и  $r(m, n) - (m, rn)$  по всем  $m, m' \in M$ ,  $n, n' \in N$ , и  $r \in R$ .

**ПРЕДЛОЖЕНИЕ 5.1.** *Модуль  $M \otimes_R N$ , определенный выше, действительно является тензорным произведением модулей  $M$  и  $N$  над  $R$ .*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\beta : M \times N \rightarrow P$  – билинейное отображение. По универсальному свойству свободного модуля существует единственный гомоморфизм  $R$ -модулей  $\alpha : \langle M \times N \rangle_R \rightarrow P$  такой, что  $\beta = \alpha \circ \iota$ , где  $\iota$  – каноническое вложение  $M \times N$  в  $\langle M \times N \rangle_R$ . Билинейность  $\beta$  равносильна 4 равенствам, первое из которых  $\beta(m + m', n) = \beta(m, n) + \beta(m', n)$ . Из этих равенств следуют такие же равенства с заменой  $\beta$  на  $\alpha$ , так как  $\iota$  – вложение. Следовательно,  $K$  лежит в ядре  $\alpha$ . По универсальному свойству факторгруппы (или фактормодуля)  $\alpha$  единственным образом пропускается через каноническую проекцию  $\langle M \times N \rangle_R \rightarrow \langle M \times N \rangle_R / K$ , что доказывает существование. Единственность вытекает из единственности в определениях свободного модуля и фактормодуля.

$$\begin{array}{ccc}
 & \langle M \times N \rangle_R & \longrightarrow \langle M \times N \rangle_R / K \\
 \iota \nearrow & \downarrow \alpha & \nwarrow \\
 M \times N & \xrightarrow{\beta} & P
 \end{array}$$

□

Если кольцо  $R$  известно из контекста, то часто пишут  $M \otimes N$  вместо  $M \otimes_R N$ . Канонический образ элемента  $(m, n) \in M \times N$  в  $M \otimes N$  обозначается  $m \otimes n$  и называется разложимым тензором. Если  $M$  и  $N$  свободные модули с базисами  $B$  и  $B'$  соответственно, то  $M \otimes N$  – свободный модуль с базисом  $\{b \otimes b' \mid b \in B, b' \in B'\}$ . Антиинтуитивный пример:  $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = 0$ . Действительно,

$$a \otimes b = \frac{a}{p} \cdot p \otimes b = \frac{a}{p} \otimes pb = \frac{a}{p} \otimes 0 = 0,$$

а тензорное произведение порождено разложимыми тензорами.

Как и любой универсальный объект, тензорное произведение определяет функтор. В данном случае это функтор  $\otimes : R\text{-Мод} \times R\text{-Мод} \rightarrow R\text{-Мод}$ ,  $(M, N) \mapsto M \otimes_R N$ , который действует на морфизмах следующим образом. Пусть  $\alpha : M \rightarrow M'$  и  $\beta : N \rightarrow N'$  –  $R$ -линейные отображения. Они индуцируют билинейное отображение  $M \times N \rightarrow M' \otimes_R N'$ ,  $(m, n) \mapsto \alpha(m) \otimes \beta(n)$ . Это билинейное отображение индуцирует линейное отображение  $M \otimes_R N \rightarrow M' \otimes_R N'$ , которое и называется  $\alpha \otimes \beta$ .

Более подробно тензорное произведение модулей будет изучаться в главе 10

**5.6. Алгебраическое замыкание.** Пусть  $F$  – поле, а  $\mathcal{C}$  – категория гомоморфизмов  $F \rightarrow K$ , где  $K$  – алгебраически замкнутое поле. По аналогии с определением локализации хочется сказать, что алгебраическим замыканием поля  $F$  называется инициальный объект категории  $\mathcal{C}$ . Однако это не так. К сожалению, единственность не может быть выполнена, что показывает пример алгебраического замыкания поля  $\mathbb{R}$ : существует 2 автоморфизма поля  $\mathbb{C}$ , тождественных на  $\mathbb{R}$ , тождественный и сопряжение. Таким образом, алгебраическое замыкание  $F$  – это такое поле  $\bar{F}$ , вместе с вложением  $\iota : F \rightarrow \bar{F}$ , что любое вложение  $F$  в замкнутое поле пропускается через  $\iota$  (мы говорим “вложение” вместо “гомоморфизм”, потому что любой гомоморфизм полей инъективен). То, что алгебраическое замыкание единственно с точностью до изоморфизма, уже не доказывается средствами теории категорий, хотя сам факт верен.

В такой ситуации иногда говорят “версальный объект” (универсальный без “уни”, т.е. без единственности). То есть можно сказать, что алгебраическое замыкание – это версальный объект категории  $\mathcal{C}$ .

**5.7. Образ ретракции под действием функтора.** Ретракцией называется морфизм, обратимый справа. Другими словами, если композиция морфизмов  $X \rightarrow Y \rightarrow X$  равна тождественному, то правая стрелка называется ретракцией, а левая – сечением этой ретракции (терминология пришла из топологии). В параграфе 8 главы 8 мы доказали, что ретракция в категории групп – это проекция полупрямого произведения на один из сомножителей. Следовательно, в категории абелевых групп ретракция – это проекция на сомножитель прямого произведения. Пример ретракции в категории  $\mathfrak{C}\mathfrak{X}\mathfrak{i}\mathfrak{n}\mathfrak{g}$ : гомоморфизм  $\varepsilon$  подстановки значения из кольца многочленов над  $R$  в  $R$ .

Так как любой функтор сохраняет тождественные морфизмы, то он сохраняет и ретракции. Таким образом, если у вас есть произвольный функтор  $\mathcal{F} : \mathfrak{C}\mathfrak{X}\mathfrak{i}\mathfrak{n}\mathfrak{g} \rightarrow \mathfrak{A}\mathfrak{b}$ , то  $\mathcal{F}(R[t]) \cong \mathcal{F}(R) \times K$  для некоторой абелевой группы  $K$ . Действительно, применяя  $\mathcal{F}$  к морфизмам  $R \rightarrow R[t] \rightarrow R$ , где правая стрелка – любой гомоморфизм подстановки, получаем гомоморфизмы  $\mathcal{F}(R) \rightarrow \mathcal{F}(R[t]) \rightarrow \mathcal{F}(R)$  с тождественной композицией. А это означает, что  $\mathcal{F}(R[t]) \cong \mathcal{F}(R) \oplus K$ , где  $K = \text{Ker}(\mathcal{F}(\varepsilon))$ .

**5.8. (ко)Ядро как (ко)эквалайзер или пулбэк (пушаут).** Предположим, что в некоторой категории  $\mathcal{C}$  инициальный объект  $*$  совпадает с финальным, как например в категории групп,  $R$ -модулей, колец без 1 или пунктированных множеств. В этом случае он обычно называется нулевым объектом. Тогда для любых двух объектов  $A, B \in \mathcal{C}$  существуют единственные морфизмы  $A \rightarrow * \rightarrow B$ . Композиция этих морфизмов называется нулевым морфизмом из  $A$  в  $B$ . Ядром морфизма  $\varphi : A \rightarrow B$  называется эквалайзер  $\varphi$  и нулевого морфизма. Как вы знаете, эквалайзер состоит из объекта и морфизма. Объект “ядро” будет обозначаться через  $\text{Ker}$ , а морфизм –  $\text{ker}$  (такая договоренность используется в литературе, но далеко не во всех текстах).

Другими словами, ядро – это пулбэк диаграммы  $A \xrightarrow{\varphi} B \leftarrow *$ . Действительно, нетрудно видеть, что  $A \times * \cong A$  и, следовательно, по предложению 4.4 пулбэк равен эквалайзеру из предыдущего абзаца.

Двойственно, коядро  $\text{coker } \varphi$  – это коэквалайзер  $\varphi$  и нулевого морфизма. В категории модулей коядро – это фактор по образу, в категории групп – фактор по нормальному замыканию образа, в категории пунктированных множеств – склейка образа функции  $\varphi$  в одну точку.

$$\begin{array}{ccc} \text{Ker } \varphi & \longrightarrow & * \\ \text{ker } \varphi \downarrow & & \downarrow \\ A & \xrightarrow{\varphi} & B \end{array} \qquad \begin{array}{ccc} A & \longrightarrow & * \\ \varphi \downarrow & & \downarrow \\ B & \xrightarrow{\text{coker } \varphi} & \text{Coker } \varphi \end{array}$$

**УПРАЖНЕНИЕ 5.2.** Определите образ морфизма в произвольной категории с помощью универсального свойства (для категории множеств он должен совпадать с вложением образа в множество значений функции). Сформулируйте двойственное определение.

**5.9. Удвоение кольца вдоль идеала, группы вдоль нормальной подгруппы.** Естественно, не любой идеал кольца является ядром ретракции. Следующая конструкция позволяет исправить это неудобство. Удвоением кольца  $R$  вдоль (двустороннего) идеала  $I$  называется пулбэк диаграммы  $R \rightarrow R/I \leftarrow R$ . Другими словами, удвоение кольца вдоль идеала – это подкольцо в прямой сумме  $R \oplus R$ , состоящее из пар  $(r, s)$ , где  $r \equiv s \pmod I$ . Удвоение  $R$  вдоль  $I$  обозначается  $R \ltimes I$ .

Теперь мы имеем гомоморфизмы колец  $R \rightarrow R \ltimes I$ ,  $r \mapsto (r, r)$  и  $\pi : R \ltimes I \rightarrow R$ ,  $(r, s) \mapsto r$  с тождественной композицией. Следовательно, для любого функтора  $\mathcal{F} : \mathfrak{X}\mathfrak{i}\mathfrak{n}\mathfrak{g} \rightarrow \mathfrak{G}\mathfrak{r}\mathfrak{p}$  имеем  $\mathcal{F}(R \ltimes I) \cong \mathcal{F}(R) \ltimes K$ , где  $K = \text{Ker } \mathcal{F}(\pi)$ . Стандартный прием: если функтор определен на категории колец, а хочется определить его значение на идеалах, то по определению полагают  $\mathcal{F}(R, I) = \text{Ker } \mathcal{F}(\pi)$ . При этом расширенное таким образом отображение становится функтором на категории пар  $(R, I)$ , где  $I$  – идеал в  $R$ . Морфизмами в категории пар являются гомоморфизмы колец, отображающие идеал в идеал.

Например, для функтора  $\mathcal{F} = \mathrm{GL}_n$  получим, что  $\mathrm{GL}_n(R, I)$  состоит из обратимых матриц, сравнимых с единичной по модулю  $I$ . Заметим, что  $\mathrm{GL}_n(R, I)$  не зависит от кольца  $R$ , потому что при вычислении произведения таких матриц используются только операции сложения и умножения внутри идеала  $I$ , рассматриваемого как кольцо без 1.

Аналогично можно определить удвоение группы вдоль нормальной подгруппы, как пулбэк диаграммы  $G \rightarrow G/H \leftarrow G$ . Это удвоение будет изоморфно полупрямому произведению  $G \ltimes H$ , где  $G$  действует на  $H$  сопряжениями.

**5.10. Копроизведение в категории множеств.** Для непересекающихся множеств копроизведение – это объединение. Однако, если  $A \cap B \neq \emptyset$ , то в объединении склеиваются элементы из  $A$  и  $B$ , чего, очевидно, не может быть в копроизведении. Так что копроизведение – это так называемое дизъюнктное объединение, которое может быть построено как подмножество в  $A \cup B \times \{0, 1\}$  состоящее из пар  $(a, 0)$  и  $(b, 1)$  по всем  $a \in A$  и  $b \in B$  с очевидными отображениями из  $A$  и  $B$ . Дизъюнктное объединение обозначается  $A \amalg B$ .

**5.11. Копроизведение в категории модулей.** Обычно, конструкция копроизведения в конкретных категориях сложнее, чем произведения. Но с модулями это не так. А именно, копроизведение в категории модулей, также как и произведение, равно прямой сумме (гомоморфизмы – канонические вложения). Действительно, задать диаграмму  $M \rightarrow P \leftarrow N$  это то же самое, что задать гомоморфизм  $M \oplus N \rightarrow P$ , при этом этот гомоморфизм делает соответствующую диаграмму коммутативной.

Соответственно, пушпаут диаграммы  $M \xleftarrow{\varphi} Q \xrightarrow{\psi} N$  – это фактормодуль прямой суммы  $M \oplus N$  по подмодулю  $\{(\varphi(q), -\psi(q)) \mid q \in Q\}$ .

**5.12. Копроизведение в категории групп.** Копроизведение в категории групп называется свободным произведением групп. Свободное произведение групп  $G$  и  $H$  обозначается  $G * H$  и строится следующим образом. На множестве  $W$  слов в алфавите  $G \amalg H$  определим отношение  $\sim$ , как наименьшее отношение эквивалентности, содержащее все пары вида  $(w_1 1_G w_2, w_1 w_2)$ ,  $(w_1 1_H w_2, w_1 w_2)$ ,  $(w_1 x y w_2, w_1 z w_2)$ , где  $w_1, w_2 \in W$ ,  $x, y, z \in G$  или  $x, y, z \in H$ , и  $xy = z$ . Множество  $W/\sim$  с операцией конкатенации слов – это и есть группа  $G * H$ . Также как и для свободной группы проверяется, что класс эквивалентности конкатенации не зависит от выбора представителей, а также, что в любом классе эквивалентности есть ровно одно самое короткое “редуцированное слово”. В редуцированном слове буквы из  $G$  и  $H$  чередуются и не равны 1. Отображения  $G \rightarrow G * H$  и  $H \rightarrow G * H$  очевидны: элементам сопоставляются соответствующие однобуквенные слова. Обычно считают, что  $G, H \subseteq G * H$ , а отображения являются вложениями. Заметим, что множество  $G \amalg H$  порождает группу  $G * H$ .

Для диаграммы

$$(9) \quad G \xrightarrow{\varphi} K \xleftarrow{\psi} H$$

определим отображение  $\theta : W \rightarrow K$  по правилу  $\theta(x_1 \dots x_n) = \varepsilon(x_1) \dots \varepsilon(x_n)$ , где  $x_i \in G \cup H$ , а  $\varepsilon : G \cup H \rightarrow K$  – отображение, совпадающее с  $\varphi$  на  $G$  и с  $\psi$  на  $H$ . Нетрудно видеть, что  $\theta$  отображает каждый класс эквивалентности в один элемент, и поэтому индуцирует отображение  $W/\sim = G * H \rightarrow K$ , которое очевидно является гомоморфизмом.

Из коммутативности диаграммы

$$\begin{array}{ccc} G * H & \longleftarrow & G \\ \uparrow & \searrow & \downarrow \varphi \\ H & \xrightarrow{\psi} & K \end{array}$$

следует, что этот гомоморфизм однозначно определен на  $G \amalg H$ . Но гомоморфизм однозначно определяется своими значениями на множестве образующих группы, откуда получаем единственность гомоморфизма  $G * H \rightarrow K$ .



Можно дать и другую конструкцию свободного произведения, с которой проще доказать, что она является свободным произведением, но сложнее работать в приложениях. А именно, определим  $G * H$  как факторгруппу свободной группы с образующими  $G \amalg H$  по наименьшей нормальной подгруппе  $N$ , содержащей все элементы вида  $xyz^{-1}$ , где  $x, y, z \in G$  или  $x, y, z \in H$ , и  $xy = z$ . Действительно, для диаграммы 9 по универсальному свойству свободной группы существует гомоморфизм групп  $\alpha : F_{G \amalg H} \rightarrow K$ . Так как  $\varphi$  и  $\psi$  – гомоморфизмы, то все упомянутые выше элементы лежат в ядре  $\alpha$ , следовательно,  $\alpha$  пропускается через факторизацию по  $N$ . Естественные отображения  $G, H \rightarrow F_{G \amalg H}/N$  теперь уже являются гомоморфизмами, так что существование доказано. Единственность следует из единственности выбранных отображений.

$$G, H \rightarrow K \implies G \amalg H \rightarrow K \implies F_{G \amalg H} \rightarrow K \implies F_{G \amalg H}/N = G * H \rightarrow K.$$

Пушаут в категории групп называется амальгамированным (свободным) произведением. Теперь, зная, что такое копроизведения и коэквиваленты, нетрудно его построить, пользуясь предложением 4.4. А именно, пушаут диаграммы  $G \xleftarrow{\lambda} A \xrightarrow{\mu} H$  – это факторгруппа свободного произведения  $G * H$  по наименьшей нормальной подгруппе, содержащей элементы  $\lambda(a)\mu(a)^{-1}$  по всем  $a \in A$ .

Амальгамированное произведение  $G$  и  $H$  над  $A$  (или свободное произведение  $G$  и  $H$  с амальгамированной подгруппой  $A$ , если отображения  $\lambda$  и  $\mu$  являются вложениями) обозначается через  $G *_A H$ . Как обычно, подразумевается, что гомоморфизмы  $\lambda$  и  $\mu$  известны из контекста.

**5.13. Копроизведение в категории коммутативных колец с 1.** В категории  $\mathfrak{C}\mathfrak{M}\mathfrak{i}\mathfrak{n}\mathfrak{g}$  для разнотензорности построим сразу пушаут диаграммы  $A \xleftarrow{\varphi} R \xrightarrow{\psi} B$ . Кольца  $A$  и  $B$  являются  $R$ -алгебрами, в частности,  $R$ -модулями. Поэтому существует тензорное произведение  $A \otimes_R B$ . Мы хотим превратить модуль  $A \otimes_R B$  в кольцо так, чтобы канонические отображения  $A, B \rightarrow A \otimes_R B$  стали бы гомоморфизмом алгебр. Это можно сделать конструктивно: на разложимых тензорах определить  $(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$ , а дальше продолжить по линейности. Но тогда надо проверять корректность, потому что элемент  $A \otimes_R B$  не единственным образом представляется в виде суммы разложимых.

Альтернативно, умножение в  $A$  является  $R$ -билинейным, следовательно индуцирует линейное отображение  $A \otimes_R A \rightarrow A$ . Аналогично получаем линейное отображение  $B \otimes_R B \rightarrow B$ . Так как тензорное произведение является функтором  $R\text{-Mod} \times R\text{-Mod} \rightarrow R\text{-Mod}$ , эти отображения индуцируют линейное отображение  $(A \otimes_R A) \otimes_R (B \otimes_R B) \rightarrow A \otimes_R B$ . Так как  $(A \otimes_R A) \otimes_R (B \otimes_R B)$  естественно изоморфно  $(A \otimes_R B) \otimes_R (A \otimes_R B)$ , то можно рассматривать последнее отображение, как отображение  $(A \otimes_R B) \otimes_R (A \otimes_R B) \rightarrow A \otimes_R B$ , которое соответствует билинейному отображению  $(A \otimes_R B) \times (A \otimes_R B) \rightarrow A \otimes_R B$ , а это и есть умножение в  $R$ -алгебре  $A \otimes_R B$ .

Пусть теперь

$$\begin{array}{ccc} R & \longrightarrow & A \\ \downarrow & & \downarrow \alpha \\ B & \xrightarrow{\beta} & C \end{array}$$

коммутативная диаграмма в категории колец (это то же самое, что и диаграмма  $A \xrightarrow{\alpha} C \xleftarrow{\beta} B$  в категории коммутативных  $R$ -алгебр). Пользуясь функториальностью тензорного произведения, зададим  $R$ -линейное отображение  $A \otimes_R B \rightarrow C \otimes_R C \rightarrow C$ , где вторая стрелка индуцирована умножением в  $C$ . Проверка того, что это отображение является гомоморфизмом  $R$ -алгебр и единственно оставляется в качестве упражнения.

## 6. Сопряженные функторы

**ОПРЕДЕЛЕНИЕ 6.1.** Пусть  $\mathcal{F} : \mathcal{B} \rightarrow \mathcal{C}$  и  $\mathcal{G} : \mathcal{C} \rightarrow \mathcal{B}$  – функторы.  $\mathcal{G}$  называется левым сопряженным к  $\mathcal{F}$ , если существует естественный изоморфизм между функторами  $\text{Mor}_{\mathcal{C}}(-, \mathcal{F}(-))$

и  $\text{Mor}_{\mathcal{B}}(\mathcal{G}(-), -)$  (как нетрудно заметить, эти функторы действуют из  $\mathcal{C}^{op} \times \mathcal{B}$  в  $\mathcal{Sets}$ ). При этом  $\mathcal{F}$  называется правым сопряженным к  $\mathcal{G}$ .

Прежде, чем изучать свойства сопряженных функторов, приведем несколько уже известных нам примеров.

### Примеры.

**6.1.** Левые сопряженные к забывающим функторам  $\mathcal{F} : \mathbf{Mon}, \mathbf{Grp}, R\text{-Mod}, R\text{-Alg} \rightarrow \mathbf{Set}$  – это сопоставление множеству  $X$  свободного объекта, построенного на этом множестве. На примере категории групп: каждой функции из множества  $X$  в  $\mathcal{F}(G)$  сопоставляется единственный гомоморфизм групп  $F_X \rightarrow G$ , и обратно: каждому гомоморфизму  $F_X \rightarrow G$  сопоставляется его композиция с вложением  $X \rightarrow F_X$ . Таким образом,

$$\text{Mor}_{\mathbf{Set}}(X, \mathcal{F}(G)) \cong \text{Mor}_{\mathbf{Grp}}(\mathcal{G}(X), G),$$

где  $\mathcal{G}$  – функтор, сопоставляющий множеству свободную группу, построенную на нем.

**6.2.** Левый сопряженный к забывающему функтору  $\mathcal{F} : R\text{-Alg} \rightarrow \mathbf{Mon}$ .

$$\text{Mor}_{\mathbf{Mon}}(M, \mathcal{F}(A)) \cong \text{Mor}_{R\text{-Alg}}(RM, A),$$

где  $RM$  – это то, что мы хотим построить. По аналогии с предыдущим пунктом, нам нужна  $R$ -алгебра, содержащая  $M$  с минимумом соотношений (чем больше соотношений в  $RM$ , тем меньше гомоморфизмов из  $RM$ ). Возьмем в качестве  $RM$  свободный  $R$ -модуль с базисом  $M$  и определим умножение при помощи умножения, заданного в  $M$ :

$$\left(\sum_i r_i m_i\right)\left(\sum_j s_j n_j\right) = \sum_{i,j} (r_i s_j)(m_i n_j).$$

Легко проверить, что  $RM$  теперь является  $R$ -алгеброй. Ясно, что у нас есть гомоморфизм моноидов  $M \rightarrow RM$ . Гомоморфизму  $R$ -алгебр  $RM \rightarrow A$  соответствует гомоморфизм моноидов  $M \rightarrow RM \rightarrow A$ . Обратно, если есть гомоморфизм моноидов  $M \rightarrow A$  то он единственным образом превращается в гомоморфизм  $R$ -модулей  $RM \rightarrow A$ , который при ближайшем рассмотрении оказывается гомоморфизмом  $R$ -алгебр.

Аналогично определяется левый сопряженный к функтору “группа обратимых элементов  $R$ -алгебры”. Группе  $G$  он сопоставляет *групповую алгебру*  $RG$  ( $G$  рассматривается как моноид, но так как это группа, то она отображается в группу обратимых элементов).

Можно заметить, что каждый раз у нас появляется (как бы ниоткуда) морфизм  $X \rightarrow \mathcal{G}(X)$  в категории с менее структурированными объектами, где  $\mathcal{G}$  – левый сопряженный к забывающему. Оказывается, что это совсем не случайно и имеет место для любой пары сопряженных функторов.

По определению сопряженных функторов

$$\text{Mor}_{\mathcal{C}}(X, \mathcal{F}(Y)) \cong \text{Mor}_{\mathcal{B}}(\mathcal{G}(X), Y).$$

Подставим  $Y = \mathcal{G}(X)$  и возьмем тождественный морфизм в правой части равенства. Ему будет соответствовать единственный морфизм  $f_X : X \rightarrow \mathcal{F}(\mathcal{G}(X))$  в левой части. Из естественности биекции в вынесенной формуле следует что набор морфизмов  $f_X$  по всем  $X \in \mathcal{C}$  является естественным преобразованием функторов  $\text{id} \rightarrow \mathcal{F} \circ \mathcal{G}$ . Это естественное преобразование называется *единицей сопряжения*.

Аналогично, подставляя  $X = \mathcal{F}(Y)$  и беря тождественный морфизм в левой части, получаем соответствующий ему естественный морфизм  $\mathcal{G}(\mathcal{F}(Y)) \rightarrow Y$ , который называется *коединицей сопряжения*.

**ТЕОРЕМА 6.2.** Для функтора  $\mathcal{F} : \mathcal{B} \rightarrow \mathcal{C}$  существует левый сопряженный тогда и только тогда, когда для любого  $X \in \mathcal{C}$  существует инициальный объект в категории  $\mathcal{M}_X$ , определенной следующим образом:

- $\text{Obj } \mathcal{M}_X = \{(Y, f) \mid Y \in \text{Obj } \mathcal{B}, f \in \text{Mor}_{\mathcal{C}}(X, \mathcal{F}(Y))\};$
- $\text{Mor}((Y, f), (Z, g)) = \{h \in \text{Mor}_{\mathcal{B}}(Y, Z) \mid \mathcal{F}(h) \circ f = g\};$

- композиция морфизмов – это их композиция в  $\mathcal{B}$ .

Этот инициальный объект и будет единицей сопряжения.

ДОКАЗАТЕЛЬСТВО. Пусть  $\mathcal{G}$  – левый сопряженный к  $\mathcal{F}$ ,  $f_X$  – единица сопряжения, а

$$\eta : \text{Mor}_{\mathcal{C}}(-, \mathcal{F}(-)) \longrightarrow \text{Mor}_{\mathcal{B}}(\mathcal{G}(-), -)$$

– естественный изоморфизм. Докажем, что пара  $(\mathcal{G}(X), f_X)$  является инициальным объектом в категории  $\mathcal{M}_X$ . Действительно, пусть  $(Y, f) \in \mathcal{M}_X$ . Положим  $g = \eta_{X,Y}(f) : \mathcal{G}(X) \rightarrow Y$ . Рассмотрим коммутативную диаграмму, связанную с естественным преобразованием  $\eta^{-1}$  и морфизмом  $(\text{id}_X, g) : (X, \mathcal{G}(X)) \rightarrow (X, Y)$ :

$$\begin{array}{ccc} \text{Mor}_{\mathcal{C}}(X, \mathcal{F}(\mathcal{G}(X))) & \xrightarrow{\varphi \mapsto \mathcal{F}(g) \circ \varphi} & \text{Mor}_{\mathcal{C}}(X, \mathcal{F}(Y)) \\ \eta_{X, \mathcal{G}(X)}^{-1} \uparrow & & \eta_{X,Y}^{-1} \uparrow \\ \text{Mor}_{\mathcal{B}}(\mathcal{G}(X), \mathcal{G}(X)) & \xrightarrow{\psi \mapsto g \circ \psi} & \text{Mor}_{\mathcal{B}}(\mathcal{G}(X), Y) \end{array}$$

Запишем условие коммутативности, примененное к тождественному морфизму  $\psi = \text{id}_{\mathcal{G}(X)}$ :

$$\eta_{X,Y}^{-1}(g) = \mathcal{F}(g) \circ \eta_{X, \mathcal{G}(X)}^{-1}(\text{id}_{\mathcal{G}(X)}).$$

Посмотрев на определение  $g$  видим, что в левой части стоит  $f$ . По определению  $f_X$  получаем

$$f = \mathcal{F}(g) \circ f_X,$$

что и означает, что  $g$  является морфизмом  $(\mathcal{G}(X), f_X) \rightarrow (Y, f)$  в категории  $\mathcal{M}_X$ .

Пусть  $g'$  другой морфизм  $(\mathcal{G}(X), f_X) \rightarrow (Y, f)$  в категории  $\mathcal{M}_X$ . Это означает, что  $f = \mathcal{F}(g') \circ f_X$ . Заменяя на коммутативном квадрате  $g$  на  $g'$ , получим

$$\eta_{X,Y}^{-1}(g') = \mathcal{F}(g') \circ \eta_{X, \mathcal{G}(X)}^{-1}(\text{id}_{\mathcal{G}(X)}) = \mathcal{F}(g') \circ f_X = f,$$

то есть  $g' = \eta_{X,Y}(f) = g$ .

Обратно, пусть  $(\mathcal{G}(X), f_X)$  – инициальный объект в категории  $\mathcal{M}_X$ . Здесь  $\mathcal{G}$  пока что просто отображение  $\text{Obj } \mathcal{C} \rightarrow \text{Obj } \mathcal{B}$ . Сейчас мы определим действие  $\mathcal{G}$  на морфизмах и докажем, что он и есть функтор, сопряженный к  $\mathcal{F}$ . Если  $\varphi \in \text{Mor}(X, X')$ , то  $f_{X'} \circ \varphi \in \text{Mor}(X, \mathcal{F}(\mathcal{G}(X')))$ . По универсальному свойству существует единственный морфизм  $\psi : \mathcal{G}(X) \rightarrow \mathcal{G}(X')$  такой, что  $f_{X'} \circ \varphi = \mathcal{F}(\psi) \circ f_X$ . Положим  $\mathcal{G}(\varphi) = \psi$ . Нетрудно видеть, что  $\mathcal{G}(\alpha \circ \beta) = \mathcal{G}(\alpha) \circ \mathcal{G}(\beta)$ , а  $\mathcal{G}(\text{id}) = \text{id}$ . Таким образом  $\mathcal{G}$  является функтором  $\mathcal{C} \rightarrow \mathcal{B}$ .

Определим функцию

$$\eta_{X,Y} : \text{Mor}_{\mathcal{C}}(X, \mathcal{F}(Y)) \rightarrow \text{Mor}_{\mathcal{B}}(\mathcal{G}(X), Y)$$

по правилу: для  $f : X \rightarrow \mathcal{F}(Y)$  морфизм  $\eta_{X,Y}(f)$  – это тот единственный морфизм, для которого  $f = \mathcal{F}(\eta_{X,Y}(f)) \circ f_X$ . Проверка того, что определенный класс функций задает естественный изоморфизм  $\eta$  является рутинной.  $\square$

**УПРАЖНЕНИЕ 6.3.** Сформулируйте аналогичное утверждение для правых сопряженных.

Теперь, зная, что для нахождения левого (правого) сопряженного нам надо найти соответствующий универсальный морфизм, продолжим приводить примеры.

**Примеры** (продолжение).

- (3) Топологические примеры. Левый сопряженный к забывающему функтору  $\mathbf{Top} \rightarrow \mathbf{Set}$  – дискретная топология на данном множестве. Правый сопряженный к тому же функтору – антидискретная топология.

- (4) Еще один пример левого сопряженного к забывающему. Пусть  $\mathcal{F} : \mathbf{Cat} \rightarrow \mathbf{Grph}$  – функтор, который забывает про композицию морфизмов в категории. Найти левый сопряженный к нему – значит построить универсальную категорию, в которую (точнее в  $\mathcal{F}$  от которой) вкладывается граф. Каждой вершине должен соответствовать объект категории, каждой стрелке – морфизм, каждому пути – композиция морфизмов. Следовательно, эта категория – категория путей графа, которая называется еще свободной категорией графа.
- (5) Левые сопряженные к функторам вложения. Первый пример – вложение  $\mathbf{Ab} \rightarrow \mathbf{Grp}$ . По гомоморфизму из группы  $G$  в абелеву группу  $A$  надо построить универсальный гомоморфизм  $G^{\text{ab}} \rightarrow A$ , где  $G^{\text{ab}}$  какая-то абелева группа. При любом гомоморфизме из  $G$  в абелеву группу  $[x, y]$  отображается в 1, следовательно, коммутант группы  $G$  лежит в ядре, и исходный гомоморфизм  $G \rightarrow A$  пропускается через  $G/[G, G]$ . Заметим, что последняя группа абелева. Таким образом,  $G^{\text{ab}} = G/[G, G]$ , а каноническая проекция  $G \rightarrow G^{\text{ab}}$  является единицей сопряжения.
- (6) Второй пример – вложение  $\mathbf{Grp} \rightarrow \mathbf{Mon}$ . Аналогично предыдущему примеру строим универсальную группу, в которую отображается моноид  $M$ . Можно сделать это совсем быстро, хотя при такой конструкции мы не много сможем сказать о реальном строении этой группы. Возьмем свободную группу  $F_M$  и профакторизуем по нормальному замыканию множества  $\{xyz^{-1} \mid x, y, z \in M, xy = z\}$ . Такая группа называется группой Гротендика моноида  $M$  и обозначается  $K(M)$ , хотя на самом деле Гротендик придумал эту конструкцию для абелевых групп и коммутативных моноидов.
- (7) Правый сопряженный к функтору вложения. Рассмотрим то же вложение, что и в предыдущем примере. Коединица – это универсальное отображение группы в данный моноид. При гомоморфизме моноидов обратимые элементы переходят в обратимые. Поэтому любая группа перейдет в множество обратимых элементов моноида  $M$ . Таким образом, достаточно взять  $\mathcal{G}(M) = M^*$ .
- (8) Пусть  $\mathcal{C}$  – категория с конечными произведениями, а  $\mathcal{F} : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$  – функтор, отображающий  $(A, B)$  в  $A \times B$  (универсальное свойство произведение индуцирует действие  $\mathcal{F}$  на морфизмах). Левый сопряженный к нему будет диагональный функтор  $\Delta$ , посылающий  $A$  в  $(A, A)$ . Действительно, элемент  $\text{Mor}(\Delta(C), (A, B))$  – это пара морфизмов  $C \rightarrow A$  и  $C \rightarrow B$ , которая однозначно соответствует морфизму  $C \rightarrow \mathcal{F}(A, B) = A \times B$  по определению произведения. Единица этого сопряжения – канонический морфизм  $C \rightarrow C \times C$ , соответствующий диаграмме  $C \xleftarrow{\text{id}} C \xrightarrow{\text{id}} C$ . Коединица – пара проекций  $A \times B \rightarrow A$  и  $A \times B \rightarrow B$ .
- (9) Левые сопряженные к функтору  $\text{Mor}$ . Пусть  $\mathcal{C} = \mathbf{Set}$  или  $R\text{-Mod}$ , а  $A \in \mathcal{C}$ . Рассмотрим функтор  $\text{Mor}(A, \_) : \mathcal{C} \rightarrow \mathcal{C}$  (множество гомоморфизмов  $R$ -модулей естественным образом превращается в  $R$ -модуль). Мы хотим найти функтор  $\mathcal{F}_A$  такой, что

$$\text{Mor}(X, \text{Mor}(A, Y)) \cong \text{Mor}(\mathcal{F}_A(X), Y).$$

Для множеств из экспоненциального закона мы знаем, что можно взять  $\mathcal{F}_A(X) = X \times A$ .

Для модулей  $\text{Mor}(X, \text{Mor}(A, Y))$  естественно изоморфно множеству билинейных отображений из  $X \times A \rightarrow Y$ . К счастью, определение тензорного произведения модулей говорит нам, что билинейные отображения из  $X \times A$  можно заменить на линейные отображения из  $X \otimes A$ . Таким образом, в категории  $R$ -модулей

$$\text{Mor}(X, \text{Mor}(A, Y)) \cong \text{Mor}(X \otimes A, Y),$$

т. е. левым сопряженным к функтору  $\text{Mor}(A, \_)$  является функтор  $\_ \otimes A$ .

Единицей этого сопряжения для множеств является функция  $X \rightarrow \text{Mor}(A, X \times A)$ , которая элементу  $x \in X$  сопоставляет функцию  $a \mapsto (x, a)$ . Коединица – это функция  $\text{Mor}(A, Y) \times A \rightarrow Y$ , которая паре  $(f, a)$  сопоставляет  $f(a)$ .

- (10) Правого сопряженного к функтору вложения  $\mathbf{Ab} \rightarrow \mathbf{Grp}$  не существует, потому что в произвольной группе невозможно универсальным образом выделить абелеву подгруппу.

Строгое доказательство этого утверждения оставляется читателю в качестве упражнения.

## 7. Пределы

Обобщим понятие диаграммы в категории  $\mathcal{C}$  на случай, когда индексирующим множеством является не граф, а категория.

**ОПРЕДЕЛЕНИЕ 7.1.** *Диаграммой* в категории  $\mathcal{C}$  называется ковариантный функтор  $\mathcal{F}: \mathcal{J} \rightarrow \mathcal{C}$ . Категория  $\mathcal{J}$  называется *индексирующей*.

В частности, если  $\mathcal{J}$  – дискретная категория (нет никаких морфизмов кроме тождественных), то это означает, что мы индексируем класс  $\text{Obj } \mathcal{C}$  другим классом  $\text{Obj } \mathcal{J}$ .

**ОПРЕДЕЛЕНИЕ 7.2.** *Конусом* над диаграммой  $\mathcal{F}: \mathcal{J} \rightarrow \mathcal{C}$  называется объект  $C \in \text{Obj } \mathcal{C}$  вместе с семейством морфизмов  $C \xrightarrow{\varphi_X} \mathcal{F}(X)$  для всех  $X \in \text{Obj}(\mathcal{J})$  таким, что для всякого морфизма  $X \xrightarrow{f} Y$  из  $\mathcal{J}$  следующая диаграмма в  $\mathcal{C}$  коммутативна:

$$(10) \quad \begin{array}{ccc} & C & \\ \varphi_X \swarrow & & \searrow \varphi_Y \\ \mathcal{F}(X) & \xrightarrow{\mathcal{F}(f)} & \mathcal{F}(Y) \end{array}$$

Конус часто обозначается  $C \rightarrow \mathcal{F}$ . Удобно представлять себе конус, как диаграмму, индексированную категорией  $\mathcal{J} \cup \{*\}$ . Последняя категория – это  $\mathcal{J}$  с присоединенным инициальным объектом  $\{*\}$  (при этом инициальный объект категории  $\mathcal{J}$ , если он существовал, перестает быть инициальным, так как из него нет морфизмов в  $*$ ). Скажем, если  $\mathcal{J} = (X \rightarrow Y \leftarrow Z)$ , то  $\mathcal{J} \cup \{*\}$  имеет вид

$$\begin{array}{ccc} & * & \\ \swarrow & \downarrow & \searrow \\ X & \longrightarrow Y & \longleftarrow Z \end{array}$$

(так как  $*$  – инициальный объект, то композиции стрелок по любому пути из  $*$  в  $Y$  равны). Определим морфизм между двумя конусами  $C \rightarrow \mathcal{F}$  и  $C' \rightarrow \mathcal{F}$  над  $\mathcal{F}$ , как морфизм  $C \rightarrow C'$ , для которого коммутативен любой треугольник

$$\begin{array}{ccc} C & \xrightarrow{\quad} & C' \\ & \searrow \quad \swarrow & \\ & \mathcal{F}(X) & \end{array}$$

Таким образом, получаем категорию конусов над  $\mathcal{F}$ .

**ОПРЕДЕЛЕНИЕ 7.3.** *Пределом* диаграммы  $\mathcal{F}: \mathcal{J} \rightarrow \mathcal{C}$  называется финальный объект в категории конусов.

Если индексирующая категория  $\mathcal{J}$  конечная (счетная, малая),<sup>4</sup> то и предел называют *конечным* (счетным, малым).

Понятие конуса и категории конусов можно сформулировать немного другими словами. Определим категорию диаграмм  $\text{Funct}(\mathcal{J}, \mathcal{C})$ , индексированных категорией  $\mathcal{J}$ . Объектами в ней являются диаграммы  $\mathcal{J} \rightarrow \mathcal{C}$ , а морфизмами – естественные преобразования диаграмм. Для  $C \in \mathcal{C}$  обозначим через  $\Delta C: \mathcal{J} \rightarrow \mathcal{C}$  постоянный функтор, отображающий любой объект категории  $\mathcal{J}$  в  $C$ , а любой морфизм – в тождественный. Тогда конус – это морфизм  $\Delta C \rightarrow \mathcal{F}$  в категории диаграмм (заметим, что естественность преобразования в точности означает коммутативность

<sup>4</sup>Учитывается мощность множества всех морфизмов в этой категории.

диаграммы (10)). Так как естественное преобразование  $\Delta C \rightarrow \Delta C'$  однозначно определяется морфизмом  $C \rightarrow C'$ , то морфизм конусов на  $\mathcal{F}$  – это морфизм в категории  $\text{Mor}_{\text{Funct}(\mathcal{J}, \mathcal{C})}$ . Таким образом, категория конусов становится подкатегорией в  $\text{Mor}_{\text{Funct}(\mathcal{J}, \mathcal{C})}$ .

### Примеры.

- (1) Если  $\mathcal{J}$  – категория без объектов, то для всякой категории  $\mathcal{C}$  существует единственная пустая диаграмма  $\mathcal{J} \rightarrow \mathcal{C}$ . Конус над такой диаграммой – это просто объект  $X \in \text{Obj}(\mathcal{C})$ . Предел пустой диаграммы – это финальный объект.
- (2) Если  $\mathcal{J}$  – дискретная категория (все стрелки – тождественные  $1_X$ ), то диаграмма  $\mathcal{J} \rightarrow \mathcal{C}$  – это набор (не обязательно всех) объектов в категории  $\mathcal{C}$ , индексруемых  $\mathcal{J}$ . Предел такой диаграммы называется *произведением* этого набора объектов (ясно, что от индексации ничего не зависит). В частности, если  $\mathcal{J}$  состоит из двух объектов, то получается определенное ранее произведение пары объектов из  $\mathcal{C}$ . Нетрудно доказать, что существует естественный изоморфизм

$$A_1 \times A_2 \times \cdots \times A_{n-1} \times A_n \cong (\cdots (A_1 \times A_2) \times \cdots \times A_{n-1}) \times A_n.$$

- (3) Возьмем теперь  $\mathcal{J} = (X \rightarrow Y \leftarrow Z)$ . Тогда диаграмма – эта пара морфизмов  $A \rightarrow B \leftarrow C$  в  $\mathcal{C}$ . Пределом этой диаграммы будет пулбэк  $A \times_B C$ .
- (4) Если  $\mathcal{J} = (X \rightrightarrows Y)$ , то диаграмма – это пара морфизмов  $\varphi, \psi \in \text{Mor}_{\mathcal{C}}(A, B)$  а ее предел – эквалайзер этих морфизмов.
- (5) Пусть  $\mathcal{C}_{\mathbb{N}}$  – категория, связанная с упорядоченным множеством  $\mathbb{N}$ . Тогда диаграмма типа  $\mathcal{C}_{\mathbb{N}}$  – это счетная последовательность морфизмов  $\cdots \rightarrow A_n \rightarrow A_{n-1} \rightarrow \cdots \rightarrow A_1$ . Предел такой диаграммы называется обратным пределом последовательности морфизмов и обозначается  $\varprojlim_{n \rightarrow \infty} A_n$ . Более общий случай прямых и обратных пределов мы рассмотрим чуть ниже, а сейчас приведем 2 важных алгебраических конструкции, являющихся обратными пределами.
- (6) Пусть  $R$  – коммутативное кольцо с 1. Рассмотрим диаграмму

$$\cdots \rightarrow R[t]/(t^n) \rightarrow R[t]/(t^{n-1}) \rightarrow \cdots \rightarrow R[t]/(t)$$

с очевидными морфизмами. Обратный предел этой диаграммы – это кольцо формальных степенных рядов  $R[[t]]$ . Если  $R$  – область целостности, то и  $R[[t]]$  обладает этим свойством. Поле частных кольца  $R[[t]]$  называют полем формальных степенных рядов и обозначают  $R((t))$  (термин обычно используется когда  $R$  – поле).

Заметим, что кольцо формальных степенных рядов над полем  $R$  является локальным кольцом с единственным максимальным идеалом, порожденным независимой переменной, любой ряд с ненулевым свободным членом обратим. Поэтому общий вид элемента поля формальных степенных рядов – формальный ряд Лорана  $\sum_{n=-k}^{\infty} r_n t^n$ , где  $k \in \mathbb{N}$ .

- (7) Пусть  $p \in \mathbb{Z}$ . Рассмотрим диаграмму

$$\cdots \rightarrow \mathbb{Z}/p^n \mathbb{Z} \rightarrow \mathbb{Z}/p^{n-1} \mathbb{Z} \rightarrow \cdots \rightarrow \mathbb{Z}/p \mathbb{Z}.$$

Обратный предел этой диаграммы называется кольцом целых  $p$ -адических чисел и обозначается  $\mathbb{Z}_p$  (именно поэтому в научных статьях не используется обозначение  $\mathbb{Z}_p$  для кольца вычетов по модулю  $p$ ; мы тоже начиная с этого места будем писать только  $\mathbb{Z}/p\mathbb{Z}$  или  $\mathbb{Z}/p$  для кольца вычетов). С помощью китайской теоремы об остатках легко доказать, что для взаимно простых  $a, b \in \mathbb{Z}$  имеем  $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$ . С другой стороны, если выкинуть часть диаграммы, оставив бесконечно много морфизмов, то предел не измениться (это несложное упражнение), так что  $\mathbb{Z}_{p^k} = \mathbb{Z}_p$ . Поэтому обычно считают, что  $p$  – простое число.

Целое  $p$ -адическое число – это последовательность чисел  $a_n$ ,  $0 \leq a_n \leq p^n - 1$ ,  $n \in \mathbb{N}$  такая, что  $a_{n+1} \equiv a_n \pmod{p^n}$ . Сложение определено следующим образом:  $(a_n) + (b_n) =$

$(a_n + b_n \bmod p^n)$ , аналогично определено умножение. Из этого описания ясно, что при простом  $p$  кольцо  $\mathbb{Z}_p$  является областью целостности, а его поле частных обозначается  $\mathbb{Q}_p$  и называется полем  $p$ -адических чисел.

- (8) Последние 2 примера можно обобщить, взяв произвольный идеал  $I$  коммутативного кольца  $R$  и рассмотрев обратный предел диаграммы

$$\cdots \rightarrow R/I^n \rightarrow R/I^{n-1} \rightarrow \cdots \rightarrow R/I$$

( $k$ -й степенью идеала называется наименьший идеал, содержащий всевозможные произведения  $k$  элементов идеала). Это кольцо называется пополнением кольца  $R$  в  $I$ -адической топологии и обозначается  $\hat{R}_I$ . Чаще  $I = sR$  – главный идеал, тогда говорят про  $s$ -адическую топологию.

Если теперь развернуть стрелки, то получатся *кочконусы* и *копределы*.

Предел или копредел произвольного функтора – вещь достаточно экзотическая. Чаще всего рассматриваются пределы диаграмм, индексированных направленными множествами.

**ОПРЕДЕЛЕНИЕ 7.4.** *Направленным множеством* называется непустое частично упорядоченное множество  $(J, \leq)$ , в котором для любых  $i, j \in J$  найдется  $k \in J$ , такой что  $i, j \leq k$ .

Если в качестве индексирующей категории  $\mathcal{J}$  выступает направленное множество  $(J, \leq)$ , то копредел диаграммы  $F: \mathcal{J} \rightarrow \mathcal{C}$  называется *прямым или инъективным пределом* и обозначается  $\varinjlim$ . Конструкцию прямого предела можно пересказать чуть подробнее. Пусть имеется направленное множество  $(J, \leq)$  и задано семейство  $\{X_i\}_{i \in J}$  объектов категории  $\mathcal{C}$ , так что выполняются следующие свойства:

- (1) Для всех  $i \leq j$  задан морфизм  $X_i \xrightarrow{f_i^j} X_j$ .
- (2) Для всех  $i \leq j \leq k$  выполнено  $f_j^k f_i^j = f_i^k$  и  $f_i^i = 1_{X_i}$ .

Тогда говорят, что морфизмы  $f_i^j$  образуют *направленное семейство*.

Если взять копредел по этому набору морфизмов, то получится объект

$$\varinjlim_{i \in J} X_i,$$

который называется *прямым пределом* соответствующего семейства объектов и морфизмов.

Простой пример: пусть  $X_i$  – множества, частично упорядоченные по включению, и пусть они образуют прямое семейство. Тогда  $\varinjlim X_i = \bigcup_i X_i$ . Прямые пределы обычно существуют в конкретных категориях и, если морфизмы инъективны, то равны объединению.

Вот еще один два полезных примера прямых пределов в категории коммутативных колец с 1.

- (1) Для кольца  $R$  рассмотрим диаграмму всех его конечнопорожденных  $\mathbb{Z}$ -подалгебр, отображения – включение меньших подалгебр в большие. Это направленное семейство морфизмов, потому что наименьшая подалгебра, содержащая две конечнопорожденные подалгебры, конечно порождена. Так как любой элемент содержится в какой-нибудь конечнопорожденной подалгебре, прямой предел этого набора морфизмов равен  $R$ . Это позволяет сводить некоторые вопросы о произвольных кольцах к конечнопорожденным, которые по теореме Гильберта о базисе являются нетеровыми.
- (2) Пусть  $S$  – мультипликативное подмножество кольца  $R$ . Главная локализация  $R_s$  имеет канонический гомоморфизм в  $R_{st}$ , где  $s, t \in S$ . Множество главных локализаций в элементах из  $S$  с каноническими гомоморфизмами является направленным множеством. Действительно, для  $s, t \in S$  имеем гомоморфизмы  $R_s \rightarrow R_{st}$  и  $R_t \rightarrow R_{st}$ . Прямой предел этого направленного множества – локализация  $S^{-1}R$ . Это наблюдение позволяет сводить некоторые вопросы о произвольных локализациях к главным.

Двойственно определяется обратный (проективный) предел (ко)направленного семейства морфизмов. Два примера проективных пределов мы уже рассмотрели выше.

**ОПРЕДЕЛЕНИЕ 7.5.** Категория называется полной (кополной), если в ней существуют все малые пределы (соотв. копределы).

Без доказательства сформулируем теорему о существовании конечных (ко)пределов.

**ТЕОРЕМА 7.6.** В категории существуют все конечные (ко)пределы, если в ней существуют (ко)произведения любых двух объектов, (ко)эквалайзеры и финальный (инициальный) объект. Равносильно: в ней существует финальный (инициальный) объект и пулбэки (пушауты).

Заметим, что даже в категориях, в которых конечные произведения совпадают с конечными копроизведениями, бесконечные произведения и копроизведения обычно отличаются. Например, в категории  $R$ -модулей  $\prod_{i=1}^{\infty} M_i$  – это множество всех последовательностей  $(a_i \in M_i \mid i \in \mathbb{N})$ , а  $\bigoplus_{i=1}^{\infty} M_i := \prod_{i=1}^{\infty} M_i$  – множество *финитных* последовательностей. В соответствии с этим и в других конкретных категориях декартовым (или прямым) произведением любого количества объектов называется множество всех последовательностей, а прямой суммой – множество финитных последовательностей. Заметим, что в категории колец с 1 бесконечных прямых сумм не существует, потому что в множестве финитных последовательностей нет 1 (последовательности, состоящей из 1).

## 8. Обзор других тем теории категорий

### 8.1. Скелет категории.

**ОПРЕДЕЛЕНИЕ 8.1.** Категория называется *скелетной*, если в ней нет различных изоморфных объектов. Скелетом данной категории называется скелетная категория, эквивалентная данной.

Скелет категории всегда существует, доказательство использует аксиому выбора для классов (или в формулировке надо говорить только про малые категории). При этом он единственный с точностью до изоморфизма. Пример: категория матриц является скелетом категории конечномерных векторных пространств.

### 8.2. Представимые функторы и лемма Йонеды.

**ОПРЕДЕЛЕНИЕ 8.2.** Функтор  $\mathcal{C} \rightarrow \mathbf{Set}$  называется представимым, если он естественно изоморфен функтору  $\mathrm{Mor}(A, -)$  для некоторого  $A \in \mathcal{C}$ .

В случае, когда  $\mathcal{C}$  – категория коммутативных  $R$ -алгебр, представимый функтор называется *аффинной схемой* над  $R$ . Если  $A = R[t_1, \dots, t_n]$ , то по универсальному свойству кольца многочленов гомоморфизмы  $A \rightarrow B$  находятся в биективном соответствии с наборами из  $n$  элементов алгебры  $B$ . Таким образом, функтор  $B \mapsto B^n \cong \mathrm{Mor}(A, B)$  является аффинной схемой над  $R$ . Эта схема называется аффинным пространством и обозначается через  $\mathbb{A}_R^n$ .

Если  $A$  – конечнопорожденная алгебра над  $R$ , то она изоморфна алгебре  $R[t_1, \dots, t_n]/I$  для некоторого идеала  $I$  кольца многочленов  $R[t_1, \dots, t_n]$ . Если  $R$  нетерово, то по теореме Гильберта о базисе  $I$  конечно порожден, скажем, многочленами  $f_1, \dots, f_m$ . Тогда множество  $\mathrm{Mor}(A, B)$  состоит из точек аффинного пространства  $b = (b_1, \dots, b_n) \in B^n$ , для которых  $f_1(b) = \dots = f_m(b) = 0$ . Действительно, каждому гомоморфизму  $A \rightarrow B$  соответствует композиция  $R[t_1, \dots, t_n] \rightarrow A \rightarrow B$  и так определенное отображение  $\mathrm{Mor}(A, B) \rightarrow \mathrm{Mor}(R[t_1, \dots, t_n], B) \cong B^n$  инъективно. По универсальному свойству факторкольца гомоморфизм  $\varepsilon_b : R[t_1, \dots, t_n] \rightarrow B$  пропускается через  $A$  тогда и только тогда, когда  $\varepsilon_b(I) = 0 \iff \varepsilon_b(f_i) = f_i(b) = 0 \forall i$ .

Такие схемы (если  $A$  – факторкольцо кольца многочленов от конечного числа переменных по конечнопорожденному идеалу) называются схемами конечного типа над  $R$ . Множество общих корней конечного набора многочленов называется алгебраическим множеством в аффинном пространстве. Таким образом, каждому алгебраическому множеству соответствует аффинная схема конечного типа, это соответствие сюръективно, но разным множествам могут соответствовать изоморфные схемы.



Общим элементом представимого функтора  $\mathcal{G} \cong \text{Mor}(A, -)$  называется элемент  $g \in \mathcal{G}(A)$ , соответствующий тождественному морфизму  $\text{id}_A$ . Он обладает замечательным свойством:

$$\forall B \forall x \in \mathcal{G}(B) \exists ! \varphi_x \in \text{Mor}(A, B) : \mathcal{G}(\varphi_x)(g) = x.$$

Например, аффинной схемой над  $\mathbb{Z}$  является полная линейная группа  $\text{GL}_n(B) \cong \text{Mor}(A, B)$ , где  $A = \mathbb{Z}[t, g_{ij} \mid 1 \leq i, j \leq n] / (t \det g = 1)$  (главная локализация кольца многочленов  $\mathbb{Z}[g_{ij}]$  в элементе  $\det g$ ), а  $g$  матрица с элементами  $g_{ij}$ . Матрица  $b \in \text{GL}_n(B)$  отождествляется с гомоморфизмом  $\varphi_b$ , который отображает  $g_{ij}$  в  $b_{ij}$ , а  $t$  в  $(\det b)^{-1}$ . Ясно, что общим элементом является матрица  $g \in \text{GL}_n(A)$ .

**ТЕОРЕМА 8.3** (лемма Йонеды). Пусть  $\mathcal{C}$  – малая категория, а  $\mathcal{F} : \mathcal{C} \rightarrow \mathbf{Set}$  – функтор. Тогда существует биекция

$$\text{Nat}(\text{Mor}(A, -), \mathcal{F}) \rightarrow \mathcal{F}(A), \quad \varphi \mapsto \varphi_A(\text{id}_A)$$

где  $\text{Nat}$  обозначает множество естественных преобразований. Более того, эта биекция естественна по  $A$  и  $\mathcal{F}$ .

**СЛЕДСТВИЕ 8.4.** Если  $A, B$  – объекты малой категории  $\mathcal{C}$ , то

$$\text{Nat}(\text{Mor}(A, -), \text{Mor}(B, -)) \cong \text{Mor}(B, A).$$

Следовательно, категория представимых функторов  $\mathcal{C} \rightarrow \mathbf{Set}$  (морфизмы – естественные преобразования) антиэквивалентна категории  $\mathcal{C}$ . Например, категория аффинных схем над кольцом  $R$  антиэквивалентна категории  $R\text{-Alg}$ .

### 8.3. Абелевы категории.

**ОПРЕДЕЛЕНИЕ 8.5.** Категория называется *предаддитивной*, если на каждом множестве  $\text{Mor}(A, B)$  задана структура аддитивной абелевой группы, и это сложение дистрибутивно относительно композиции морфизмов.

Функтор из одной предаддитивной категории в другую называется аддитивным, если он переводит сумму морфизмов в сумму.

Предаддитивная категория называется *аддитивной*, если в ней существуют все конечные произведения, в том числе произведение пустого множества объектов – нулевой объект.

Аддитивная категория называется *абелевой*, если в ней существуют все ядра и коядра, а все мономорфизмы и эпиморфизмы (ко)нормальны.

**ТЕОРЕМА 8.6** (теорема Митчела о вложении). Для любой малой абелевой категории существует полный, строгий и точный функтор из нее в категорию  $R$ -модулей для некоторого кольца  $R$ .

В абелевой категории определяются понятия комплексов и точных последовательностей и может быть развита теория (ко)гомологий. Из определения следует, что любой морфизм в абелевой категории раскладывается в композицию эпиморфизма и мономорфизма. Объект, стоящий в середине, называется образом морфизма. Он равен (канонически изоморфен) ядру коядра и коядру ядра.

$$\begin{array}{ccc} & \text{Im } \varphi & \\ \text{coker ker } \varphi \nearrow & & \searrow \text{ker coker } \varphi \\ X & \xrightarrow{\varphi} & Y \end{array}$$

Комплекс – это последовательность морфизмов

$$\dots \rightarrow A_{k-1} \xrightarrow{\delta_{k-1}} A_k \xrightarrow{\delta_k} A_{k+1} \rightarrow \dots$$

с нулевой композицией. Легко доказать, что композиция  $\text{Im } \delta_{k-1} \rightarrow A_k \rightarrow A_{k+1}$  нулевая, следовательно существует единственный морфизм  $\text{Im } \delta_{k-1} \rightarrow \text{Ker } \delta_k$ . Коядро этого морфизма

(фактор ядра следующего по образцу предыдущего) называется гомологиями комплекса в  $k$ -м члене. Комплекс с нулевыми гомологиями называется точной последовательностью. Аддитивный функтор называется точным, если он сохраняет точные последовательности. Точная последовательность

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

называется короткой точной последовательностью. В категории модулей это означает, что  $C \cong B/A$  (формально, фактормодуль не по самому  $A$ , а по его образу в  $B$ ).

**8.4. И еще, еще, еще...** Расширения Кана: “Все понятия являются расширениями Кана!” – название одного из параграфов книги Маклэйна, имеются ввиду, конечно, сопряженные функторы и пределы; расширения Кана содержательно используются для доказательства эквивалентности функториального и топологического подходов к определению схемы.

Теория пучков: основа алгебраической геометрии, существенная часть топологии и анализа на гладких многообразиях.

Монады: содержательно используются в функциональном программировании, для понимания надо знать, что такое сопряженные функторы, так что полдороги к применению теории категорий в функциональном программировании мы прошли.

Фактор-категории и локализации категорий: содержательно используются в теории гомотопий и в различных разделах алгебры,

Триангулированные категории: тесно связаны с категориями комплексов в аддитивных категориях, а также, с некоторыми категориями, имеющими большое значение для алгебраической топологии.

2-категории. Частью структуры являются стрелки между морфизмами и их “вертикальная” и “горизонтальная” композиции. Например **Cat** является 2-категорией, где морфизмы – это функторы, а стрелки между ними – естественные преобразования.

$n$ -категория (угадайте, что это такое). Пример  $\infty$ -категории: топологическое пространство, объекты – точки, морфизмы – пути, 2-морфизмы, т. е. стрелки между морфизмами – гомотопии путей,  $n$ -морфизмы – гомотопии между  $(n - 1)$ -морфизмами.

и еще, еще, еще.....

## Полилинейная алгебра

### 1. Простейшие свойства тензорного произведения

В этом параграфе мы работаем в категории  $R\text{-}\mathcal{M}\text{od}$ . Множество морфизмов из  $M$  в  $N$  обычно обозначают  $\text{Hom}_R(M, N)$  вместо категорного  $\text{Mor}_{R\text{-}\mathcal{M}\text{od}}(M, N)$ . В разделе 5.5 предыдущей главы мы определили тензорное произведение модулей. Сейчас докажем несколько простейших свойств.

**ПРЕДЛОЖЕНИЕ 1.1.** *Существуют следующие естественные изоморфизмы:*

- (1)  $X \otimes Y \cong Y \otimes X$ ;
- (2)  $(X \otimes Y) \otimes Z \cong X \otimes (Y \otimes Z)$ ;
- (3)  $(X \oplus Y) \otimes Z \cong (X \otimes Z) \oplus (Y \otimes Z)$ ;
- (4)  $R \otimes_R X \cong X$ .
- (5)  $R^n \otimes_R X \cong X^n$ .
- (6)  $R^m \otimes R^n \cong R^{mn}$

**ДОКАЗАТЕЛЬСТВО.** Все эти изоморфизмы легко строятся и проверяются непосредственно. Укажем для каждого пункта образы разложимых тензоров, оставив необходимые проверки читателю (везде в этом доказательстве  $x \in X$ ,  $y \in Y$ ,  $z \in Z$ , а  $r \in R$ ).

- (1)  $x \otimes y \mapsto y \otimes x$ ;
- (2)  $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$ ;
- (3)  $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$ ;
- (4)  $r \otimes x = 1 \otimes rx \mapsto rx$ ;
- (5) следует из 3 и 4, учитывая, что  $X^n = \underbrace{X \oplus \cdots \oplus X}_{n \text{ раз}}$ ;
- (6) является частным случаем предыдущего пункта.

□

Заметим, что первые 4 свойства говорят о том, что класс  $R$ -модулей является (большим) коммутативным полукольцом с 1 относительно операций прямой суммы и тензорного произведения. Коммутативное полукольцо с 1 – это множество с двумя операциями, относительно каждой из которых оно является коммутативным моноидом, и которые удовлетворяют дистрибутивности. Слово “большим” относится к тому, что вместо множеств рассматриваются классы. Тогда последние 2 свойства являются чисто формальными свойствами, выполненными в любом полукольце.

Из последнего пункта следует, что тензорное произведение свободных модулей свободно. Нетрудно видеть, что базисом будет набор из тензорных произведений базисных векторов.

Пусть  $\varphi : R \rightarrow A$  – гомоморфизм коммутативных колец. Он задает на  $A$  структуру  $R$ -алгебры, в частности,  $R$ -модуля. Пусть  $M$  –  $R$ -модуль. Тогда на  $A \otimes_R M$  легко задать структуру  $A$ -модуля:  $a \cdot (b \otimes m) := (ab) \otimes m \quad \forall a, b \in A, m \in M$ , и далее доопределяем по линейности. Это отображение легко превращается в функтор  $\varphi_{\#} : R\text{-}\mathcal{M}\text{od} \rightarrow A\text{-}\mathcal{M}\text{od}$ , который называется *расширением скаляров*. Терминология пришла из теории векторных пространств, где  $R$  и  $A$  поля, следовательно,  $\varphi$  инъективно. В частности, для перехода к векторному пространству над алгебраическим замыканием  $\bar{F}$  базового поля  $F$  (то, что мы делали, например, при доказательстве разложения Жордана) не обязательно выбирать базис, а потом

вкладывать пространство столбцов над  $F$  в пространство столбцов над  $\overline{F}$ . Вместо этого можно рассмотреть тензорное произведение пространства на  $\overline{F}$ .

Из конструкции тензорного произведения легко видеть, что функтор  $M \otimes \_$  сохраняет эпиморфизмы. С другой стороны, он не обязан сохранять мономорфизмы даже для  $\mathbb{Z}$ -модулей, т.е. абелевых групп:  $\mathbb{Z} \hookrightarrow \mathbb{Q}$ , но  $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z} \otimes \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Q} \otimes \mathbb{Z}/p\mathbb{Z} = 0$  совсем не инъективно. Если для модуля  $M$  функтор  $M \otimes \_$  сохраняет мономорфизмы (и, следовательно, является точным), то модуль  $M$  называется *плоским*. Из предыдущего предложения легко следует, что свободные модули являются плоскими.

**УПРАЖНЕНИЕ 1.2.** Пусть  $L, L'$  – линейные операторы на конечномерных векторных пространствах  $V$  и  $V'$  соответственно. По функториальности тензорного произведения они индуцируют оператор  $L \otimes L'$  на пространстве  $V \otimes V'$ . Найдите след и определитель оператора  $L \otimes L'$  (выразите их через следы и определители операторов  $L$  и  $L'$  и размерности пространств).

Следующие естественные отображения, связывающие между собой функторы  $\text{Hom}_R$  и тензорного произведения, менее очевидны, и не все из них являются изоморфизмами в общем случае. Однако для классического случая конечномерных векторных пространств они – изоморфизмы, что будет содержательно использоваться в дальнейшем.

**ЛЕММА 1.3.** В категории модулей над (коммутативным) кольцом  $R$  с 1 существуют следующие естественные преобразования функторов.

- (1)  $\text{Hom}(R, X) \cong X$ .
- (2)  $\text{Hom}(X, \text{Hom}(Y, Z)) \cong \text{Bil}(X \times Y, Z) \cong \text{Hom}(X \otimes Y, Z)$ .
- (3)  $M \rightarrow M^{**}$ .
- (4)  $\text{Hom}(X, Y \otimes Z) \rightarrow \text{Hom}(X \otimes Y^*, Z)$ .

**ДОКАЗАТЕЛЬСТВО.** Первая эквивалентность очевидна:  $f \mapsto f(1)$ , обратно  $x \mapsto f(r) = rx$ . Следующие две были построены в примере 9 параграфа 6 и примере 6 параграфа 3 предыдущей главы.

Пусть  $f : X \rightarrow Y \otimes Z$  – линейное отображение,  $x \in X$ ,  $\varphi \in Y^*$ , а  $g \in \text{Hom}(X \otimes Y^*, Z)$  – образ  $f$ , который мы хотим построить. Положим

$$g(x \otimes \varphi) = \sum_{i=1}^k \varphi(y_i) z_i, \text{ где } f(x) = \sum_{i=1}^k y_i \otimes z_i,$$

и продолжим по линейности.<sup>1</sup> Так как разложение  $f(x)$  в сумму разложимых тензоров неоднозначно, надо еще проверить, что  $g(x \otimes \varphi)$  не зависит от выбора этого разложения. Так как тензорное произведение – фактормодуль свободного по подмодулю, порожденному 4 типами элементов, то достаточно проверить, что  $g$  не изменится при добавлении элемента одного из этих четырех типов. Все эти проверки очевидны. Например, если к  $f(x)$  добавится  $(a + b) \otimes z - a \otimes z - b \otimes z$ , то к  $g(x \otimes \varphi)$  добавится  $\varphi(a + b)z - \varphi(a)z - \varphi(b)z = 0$ .

Естественность построенного отображения по каждому из аргументов  $X$ ,  $Y$  и  $Z$  проверяется непосредственно (надо только не забыть, что функтор  $\text{Hom}$  контравариантен по первому аргументу).  $\square$

**ТЕОРЕМА 1.4.** Все естественные преобразования из леммы 1.3 являются естественными изоморфизмами на категории конечномерных векторных пространств.

**ДОКАЗАТЕЛЬСТВО.** Учитывая, что  $\dim(U \otimes V) = (\dim U) \cdot (\dim V) = \dim \text{Hom}(U, V)$ , легко заметить, что размерности левой и правой части каждого естественного преобразования

<sup>1</sup>На самом деле, когда говорят, “зададим отображение  $g$  на разложимых тензорах, а потом продолжим по линейности”, имеют ввиду следующую формальную процедуру. Зададим отображение  $G : X \times Y^* \rightarrow Z$  формулой  $G(x, \varphi) = \sum_{i=1}^k \varphi(y_i) z_i$ , проверим, что оно билинейно, и определим  $g$  как единственное отображение  $X \otimes Y^* \rightarrow Z$ , соответствующее  $G$  по универсальному свойству тензорного произведения.

совпадают. Таким образом достаточно доказать, что указанные отображения инъективны. Инъективность отображения 3 очевидна, что уже отмечалось в предыдущей главе.

Осталось доказать инъективность отображения 4. Пусть  $(y_1, \dots, y_n)$  – базис пространства  $Y$ . Запишем  $f(x) = \sum_{i=1}^n y_i \otimes z_i$  для некоторых  $z_i \in Z$ . Так как  $f \neq 0$ , то найдется  $x \in X$  и индекс  $m$  такие, что  $z_m \neq 0$ . Зададим  $\varphi \in Y^*$  действием на базисных элементах:  $\varphi(y_i) = \delta_{im}$ . Тогда

$$g(x \otimes \varphi) = \sum_{i=1}^n \varphi(y_i) z_i = z_m \neq 0.$$

Таким образом, ненулевой гомоморфизм  $f$  не может отобразиться в 0, т.е. ядро нашего естественного отображения нулевое.  $\square$

Следующие естественные биекции являются ключевыми для понимания того, что два разных подхода к понятию тензора эквивалентны.

**СЛЕДСТВИЕ 1.5.** Пусть  $U_1, \dots, U_m, V_1, \dots, V_n$  – конечномерные векторные пространства над полем  $F$ . Множество полилинейных отображений

$$U_1 \times \dots \times U_m \rightarrow V_1 \otimes \dots \otimes V_n$$

естественно изоморфно множеству полилинейных отображений

$$U_1 \times \dots \times U_m \times V_1^* \times \dots \times V_n^* \rightarrow F,$$

а также пространству

$$U_1^* \otimes \dots \otimes U_m^* \otimes V_1 \otimes \dots \otimes V_n.$$

Следующая группа естественных преобразований менее важна, чем предыдущая, поэтому их доказательство оставляется читателю в качестве упражнения.

**УПРАЖНЕНИЕ 1.6.** Постройте следующие естественные отображения и докажите, что в категории конечномерных векторных пространств они являются изоморфизмами.

- (1)  $\text{Hom}(X, Y) \rightarrow \text{Hom}(Y^*, X^*)$ .
- (2)  $\text{Hom}(X, Y) \rightarrow (Y^* \otimes X)^*$ .
- (3)  $Y \otimes X^* \rightarrow \text{Hom}(X, Y)$ .
- (4)  $X^* \otimes Y^* \rightarrow (X \otimes Y)^*$ .

## 2. Тензоры

Пусть  $V$  – конечномерное векторное пространство над  $F$ .

**ОПРЕДЕЛЕНИЕ 2.1.** Тензором называется полилинейное отображение

$$T : \underbrace{V \times \dots \times V}_{p \text{ раз}} \times \underbrace{V^* \times \dots \times V^*}_{q \text{ раз}} \rightarrow F.$$

Другими словами, тензор – это линейное отображение

$$T : \underbrace{V \otimes \dots \otimes V}_{p \text{ раз}} \otimes \underbrace{V^* \otimes \dots \otimes V^*}_{q \text{ раз}} \rightarrow F.$$

Такой тензор называется  $p$  раз ковариантный и  $q$  раз контравариантный или, короче, тензором типа  $(p, q)$ .

Билинейная форма – тензор типа  $(2, 0)$ , линейный оператор отождествляется с тензором типа  $(1, 1)$ , так как  $\text{Hom}(V, V)$  естественно изоморфно  $\text{Hom}(V \otimes V^*, F)$ . Билинейная бинарная операция  $V \times V \rightarrow V$  задается тензором типа  $(2, 1)$ .

Тензорное произведение тензора  $T$  типа  $(p, q)$  и тензора  $T'$  типа  $(p', q')$  – это тензорное произведение отображений  $T \otimes T'$ , определенное в примере 5.5 предыдущей главы.  $T \otimes T'$  является тензором типа  $(p + p', q + q')$ .

Ясно, что полилинейное отображение однозначно определяется своими значениями на наборах базисных элементов. Эти числа будут называться координаты тензора. Но прежде чем их определить, нам надо выбрать базис в двойственном пространстве.

**ОПРЕДЕЛЕНИЕ 2.2.** Пусть  $X$  – векторное пространство с базисом  $(e_1, \dots, e_n)$ . Зададим функционалы  $e^k \in X^*$  равенствами  $e^k(e_i) = \delta_{ki}$  для всех  $k = 1, \dots, n$ . Тогда  $e^* = \{e^1, \dots, e^n\}$  называется двойственным (по отношению к  $e$ ) базисом пространства  $X^*$ .

**ЛЕММА 2.3.** Для  $x \in X$  число  $e^k(x)$  – это  $k$ -я координата вектора  $x$  в базисе  $e$ . Множество  $e^*$  действительно является базисом пространства  $X^*$ .

**ДОКАЗАТЕЛЬСТВО.** Первое утверждение сразу следует из линейности  $e_k^*$  и определения его значений на базисных векторах. Для любого функционала  $f \in X^*$  имеем

$$f(x) = f\left(\sum_{i=1}^n e_i e^i(x)\right) = \sum_{i=1}^n f(e_i) e^i(x),$$

т.е.  $f = \sum_{i=1}^n f(e_i) e^i$ , откуда  $e^*$  – система образующих. Пусть  $\sum_{i=1}^n \alpha_i e^i = 0$ . Подставляя в это равенство базисный элемент  $e_k$  имеем  $\alpha_k = 0$ , что доказывает линейную независимость.  $\square$

**ЗАМЕЧАНИЕ 2.4.** Если  $e$  бесконечный базис, то набор  $\{e^i\}$  не является системой образующих. Для конкретного  $x \in X$  вынесенная формула все еще верна, и в ней конечное число слагаемых, потому что только для конечного числа индексов  $e^i(x)$  отлично от нуля. Но убрать  $x$  из этой формулы уже не получится, потому что все коэффициенты  $f(e_i)$  могут быть не равны 0.

В дальнейшем мы будем использовать обозначения для координат векторов и ковекторов, принятые в полилинейной алгебре (напомним, что ковекторы – это элементы  $V^*$ , в анализе они называются линейными функционалами, еще их можно называть линейными формами). Координаты вектора  $x$  в базисе  $e$  обозначаются через  $x^1, \dots, x^n$ , а координаты ковектора  $f$  в базисе  $e^*$  – через  $f_1, \dots, f_n$ . Элементы набора векторов, также как и элементы базиса  $V$ , нумеруются нижними индексами, а ковекторов – верхними. Все эти соглашения нужны для того, чтобы суммирование всегда происходило по тем индексам, которые встречаются и сверху и снизу. Элементы матриц в этой системе обозначений надо было бы писать в виде  $a_j^i$ , где верхний индекс – номер строки, но мы не будем пользоваться этим обозначением.

**ОПРЕДЕЛЕНИЕ 2.5.** Координатами тензора в базисе  $e = (e_1, \dots, e_n)$  пространства  $V$  называется  $p + q$ -мерный массив, состоящий из элементов поля

$$T_{i_1 \dots i_p}^{j_1 \dots j_q} = T(e)_{i_1 \dots i_p}^{j_1 \dots j_q} = T(e_{i_1}, \dots, e_{i_p}, e^{j_1}, \dots, e^{j_q}), \quad i_1, \dots, i_p, j_1, \dots, j_q \in \{1, \dots, n\}$$

Ясно, что координаты тензора полностью определяют этот тензор:

$$T(v_1, \dots, v_p, f^1, \dots, f^q) = \sum T_{i_1 \dots i_p}^{j_1 \dots j_q} v_1^{i_1} \dots v_p^{i_p} f_{j_1}^1 \dots f_{j_q}^q,$$

где сумма берется по всем  $i_1, \dots, i_p, j_1, \dots, j_q$ , независимо друг от друга пробегающих множество  $\{1, \dots, n\}$ .

Для того, чтобы увидеть, как координаты тензора меняются при замене базиса, посмотрим, как связаны между собой матрицы перехода  $C_{e \rightarrow g}$  и  $C_{e^* \rightarrow g^*}$ . Для этого определим “умножение”  $V^* \times V \rightarrow F$ , по формуле  $f \cdot v = f(v)$ . Ясно, что это умножение билинейно, поэтому можно пользоваться формализмом, определенном в параграфе 2 главы 2. В этих обозначениях определение двойственного базиса можно записать в виде  $(e^*)^\top e = E$ .

**ЛЕММА 2.6.**  $C_{e^* \rightarrow g^*} = (C_{e \rightarrow g}^{-1})^\top$ .

**ДОКАЗАТЕЛЬСТВО.** По определению матрицы перехода  $g = e C_{e \rightarrow g}$  и  $g^* = e^* C_{e^* \rightarrow g^*}$ . По определению двойственного базиса

$$E = (g^*)^\top g = C_{e^* \rightarrow g^*}^\top (e^*)^\top e C_{e \rightarrow g} = C_{e^* \rightarrow g^*}^\top C_{e \rightarrow g},$$

откуда получается требуемое равенство.  $\square$

**ТЕОРЕМА 2.7.** Пусть  $e$  и  $g$  – базисы пространства  $V$ , а  $T$  – тензор на  $V$  типа  $(p, q)$ .

$$T(g)_{k_1 \dots k_p}^{m_1 \dots m_q} = \sum (c')_{j_1 \dots j_q}^{m_1 \dots m_q} T(e)_{i_1 \dots i_p}^{j_1 \dots j_q} c_{k_1 \dots k_p}^{i_1 \dots i_p}, \text{ где}$$

$$c_{k_1 \dots k_p}^{i_1 \dots i_p} = \prod_{l=1}^p (C_{e \rightarrow g})_{i_l k_l}, \quad (c')_{j_1 \dots j_q}^{m_1 \dots m_q} = \prod_{r=1}^q (C_{g \rightarrow e})_{m_r j_r}.$$

ДОКАЗАТЕЛЬСТВО.

$$T(g_{k_1}, \dots, g_{k_p}, g^{m_1}, \dots, g^{m_q}) =$$

$$T \left( \sum_{i_1=1}^n e_{i_1} (C_{e \rightarrow g})_{i_1 k_1}, \dots, \sum_{i_p=1}^n e_{i_p} (C_{e \rightarrow g})_{i_p k_p}, \sum_{j_1=1}^n e^{j_1} (C_{g \rightarrow e})_{m_1 j_1}, \dots, \sum_{j_p=1}^n e^{j_p} (C_{g \rightarrow e})_{m_p j_p} \right).$$

Пользуясь полилинейностью  $T$  получаем требуемое равенство.  $\square$

### 3. Тензорная алгебра и алгебра Грассмана

Пусть  $R$  – коммутативное кольцо с 1, а  $\mathcal{F} : R\text{-Alg} \rightarrow R\text{-Mod}$  – забывающий функтор. Сейчас мы построим функтор  $T$ , сопряженный к  $\mathcal{F}$ . Для  $R$ -модуля  $M$  алгебра  $T(M)$  называется тензорной алгеброй модуля  $M$ .

Напомним, что  $\bigoplus_{k=0}^{\infty} M_k$  – это прямая сумма или копроизведение  $R$ -модулей  $M_k$ , т.е. множество всех финитных последовательностей  $(m_1, m_2, \dots)$ , где  $m_k \in M_k$ .

Обозначим через  $M^{\otimes k}$  тензорное произведение  $k$  экземпляров модуля  $M$ , при этом положим  $M^{\otimes 0} = R$ , так как именно  $R$  является “нейтральным элементом” по отношению к тензорному произведению. Тогда формула  $T(M) = \bigoplus_{k=0}^{\infty} M^{\otimes k}$  задает структуру  $R$ -модуля на  $T(M)$ . Умножение достаточно задать на разложимых тензорах после чего распространить это определение по линейности. Итак

$$(x_1 \otimes \dots \otimes x_k) \cdot (y_1 \otimes \dots \otimes y_n) = x_1 \otimes \dots \otimes x_k \otimes y_1 \otimes \dots \otimes y_n$$

(таким образом, произведение любого элемента из  $M^{\otimes k}$  на элемент из  $M^{\otimes n}$  лежит в  $M^{\otimes(k+n)}$ ). Действие функтора  $T$  на морфизмах очевидна.

**ТЕОРЕМА 3.1.** Функтор  $T$ , построенный выше, является сопряженным к забывающему функтору  $\mathcal{F} : R\text{-Alg} \rightarrow R\text{-Mod}$ . Вложение  $f : M = M^{\otimes 1} \hookrightarrow T(M)$  является единицей сопряжения.

ДОКАЗАТЕЛЬСТВО. Достаточно доказать, что  $f$  – единица сопряжения, т.е. для любого  $R$ -линейного отображения  $g : M \rightarrow A$  модуля  $M$  в алгебру  $A$  существует единственный гомоморфизм  $R$ -алгебр  $g' : T(M) \rightarrow A$  такой, что  $g = g' \circ f$ . Ясно, что отображение

$$G_k : M^k \rightarrow A, \quad (m_1, \dots, m_k) \mapsto g(m_1) \cdot \dots \cdot g(m_k)$$

является полилинейным. По универсальному свойству тензорного произведения оно пропускается через  $M^{\otimes k}$  единственным образом. Далее, по универсальному свойству копроизведения модулей все отображения  $G_k$  единственным образом пропускаются через  $T(M) = \bigoplus_k M^{\otimes k}$ . Легко проверить, что полученное отображение  $T(M) \rightarrow A$  сохраняет операцию умножения, т.е. является гомоморфизмом алгебр.  $\square$

Для свободного модуля с базисом  $X$  тензорная алгебра – это свободная алгебра на множестве  $X$ . Действительно, забывающий функтор  $R\text{-Alg} \rightarrow \mathbf{Set}$  является композицией забывающих функторов  $R\text{-Alg} \rightarrow R\text{-Mod} \rightarrow \mathbf{Set}$ . Следовательно, и сопряженный к нему является композицией сопряженных, т.е.  $R\langle X \rangle = T(\langle X \rangle_R)$ .

Перейдем теперь к изучению полилинейных [анти]симметричных отображений. Напомним, что полилинейное отображение называется симметричным, если его значение не меняется

при перестановке аргументов, и антисимметричным, если его значение равно нулю, как только какие-либо 2 аргумента равны (если  $1/2 \in R$ , то это равносильно тому, что оно меняет знак при транспозиции аргументов). Сначала мы построим универсальное  $n$ -линейное [анти]симметричное отображение из фиксированного модуля  $M^n = M \times \cdots \times M$ .

Пусть  $M$  –  $R$ -модуль, а  $n \in \mathbb{N}$ . Рассмотрим категории  $\mathcal{S}_{M,n}^\pm$ :

- $\text{Obj } \mathcal{S}^\pm = \{(N, f) \mid N \in R\text{-}\mathcal{M}\text{od}, f - [\text{анти}] \text{симметричное полилинейное отображение } M^n \rightarrow N\}$ ; (симметричное для категории  $\mathcal{S}_{M,n}^+$  и антисимметричное – для  $\mathcal{S}_{M,n}^-$ ).
- $\text{Mor}_{\mathcal{S}_{M,n}^\pm}((N, f), (N', f')) = \{g \in \text{Mor}_{R\text{-}\mathcal{M}\text{od}}(N, N') \mid g \circ f = f'\}$ ;
- композиция – это композиция отображений:

$$\begin{array}{ccccc} & & M^n & & \\ & \swarrow & \downarrow & \searrow & \\ N & \longrightarrow & N' & \longrightarrow & N'' \end{array}$$

Инициальный объект в категории  $\mathcal{S}_{M,n}^\pm$  называется  $n$ -ой симметрической (соотв. внешней) степенью модуля  $M$  и обозначаются через  $S^n(M)$  и  $\Lambda^n(M)$  соответственно.

**ТЕОРЕМА 3.2.**  $S^n(M) = M^{\otimes n} / \langle x \otimes a \otimes b \otimes y - x \otimes b \otimes a \otimes y \rangle$ ;  
 $\Lambda^n(M) = M^{\otimes n} / \langle x \otimes a \otimes a \otimes y \rangle$ ;

где  $a \in M$ , а  $x, y$  – разложимые тензоры.

**ДОКАЗАТЕЛЬСТВО.** Любое полилинейное отображение из  $M^n \rightarrow N$  единственным образом пропускается через  $M^{\otimes n}$ . Так как отображение [анти]симметрично, то указанные в формулировке элементы лежат в его ядре. По универсальному свойству фактормодуля наше отображение единственным образом пропускается через фактормодуль  $S^n(M)$  или  $\Lambda^n(M)$ .

Обозначим канонический образ элемента  $m_1 \otimes \cdots \otimes m_n$  в  $S^n(M)$  через  $m_1 \dots m_n$ , а в  $\Lambda^n(M)$  – через  $m_1 \wedge \cdots \wedge m_n$  (символ “ $\wedge$ ” в этом контексте называется символом внешнего произведения).

Так как  $(a + b) \otimes (a + b) - a \otimes a - b \otimes b = a \otimes b + b \otimes a$ , то подмодуль в  $M^{\otimes n}$ , порожденный элементами  $\cdots \otimes a \otimes a \otimes \dots$  содержит все элементы вида  $\cdots \otimes a \otimes b \otimes \cdots + \cdots \otimes b \otimes a \otimes \dots$ , что позволяет в элементах  $\Lambda^n(M)$  переставлять сомножители со сменой знака. Следовательно, любой элемент вида  $\cdots \otimes a \otimes \cdots \otimes a \otimes \dots$  также равен нулю в  $\Lambda^n(M)$ . Таким образом, канонические отображения  $M^n \rightarrow S^n(M)$  и  $M^n \rightarrow \Lambda^n(M)$  являются [анти]симметричными.  $\square$

Алгебра, в которой умножение является симметричным билинейным отображением, называется коммутативной. Неудивительно, что конструкция, аналогичная тензорной алгебре, но с симметрической вместо тензорной степени модуля выдаст функтор, сопряженный к забывающему из коммутативных  $R$ -алгебр в  $R$ -модули. Алгебра

$$S(M) := \bigoplus_{n=0}^{\infty} S^n(M) \cong T(M) / (a \otimes b - b \otimes a)$$

называется *симметрической алгеброй* модуля  $M$ . Доказательство изоморфизма использует то, что группа перестановок порождена транспозициями соседних индексов. Ясно, что  $S$  является функтором из  $R\text{-}\mathcal{M}\text{od}$  в категорию коммутативных  $R$ -алгебр с очевидным действием на морфизмах.

**ТЕОРЕМА 3.3.** Построенный выше функтор является левым сопряженным к забывающему функтору из категории коммутативных  $R$ -алгебр в категорию  $R$ -модулей.

Если  $M$  – свободный модуль с базисом  $X$ , то  $S(M) = R[X]$  – кольцо многочленов от  $X$ .

Оба утверждения доказываются аналогично подобным утверждениям для тензорной алгебры. Ключевым соображением является то, что для симметричности полилинейного отображения достаточно, что значение не меняется при любой *транспозиции соседних аргументов*.



**ОПРЕДЕЛЕНИЕ 3.4.** Алгебра

$$\Lambda(M) := T(M)/I,$$

где  $I$  – идеал, порожденный всеми элементами вида  $t \otimes t$ ,  $t \in M$ , называется внешней алгеброй (алгеброй Грассмана) модуля  $M$ .

Заметим, что конструкция внешней алгебры, очевидно, функториальна, т.е. гомоморфизм модулей  $\varphi : M \rightarrow M'$  индуцирует гомоморфизм внешних алгебр  $\Lambda(\varphi) : \Lambda(M) \rightarrow \Lambda(M')$ . При этом следующая диаграмма коммутативна.

$$\begin{array}{ccc} M & \longrightarrow & \Lambda(M) \\ \varphi \downarrow & & \downarrow \Lambda(\varphi) \\ M' & \longrightarrow & \Lambda(M') \end{array}$$

В заключении этого параграфа мы докажем, что внешняя алгебра, также как и тензорная и симметрическая, является градуированной, а на основании этого утверждения найдем базис модуля  $\Lambda^n(R^k)$ .

**ЛЕММА 3.5.** В тензорной алгебре модуля  $M$ :

$$I = \bigoplus_{k=2}^{\infty} I \cap M^{\otimes k} \quad (\text{т.е. идеал } I \text{ является однородным})$$

$$\left( \bigoplus_{k \neq n} M^{\otimes k} + I \right) \cap M^{\otimes n} = I \cap M^{\otimes n} = \langle m_1 \otimes \cdots \otimes m_l \otimes t \otimes t \otimes m_{l+3} \otimes \cdots \otimes m_n \rangle.$$

**ДОКАЗАТЕЛЬСТВО.** По определению, любой элемент идеала  $I$  имеет вид  $u = \sum_i x_i \otimes m_i \otimes m_i \otimes y_i$ , где  $x_i, y_i \in T(M)$ ,  $m_i \in M$ . Так как разложимые тензоры порождают  $T(M)$ , то можно считать, что все  $x_i$  и  $y_i$  – разложимые. Пусть  $x_i \otimes m_i \otimes m_i \otimes y_i \in M^{\otimes k_i}$ . Положим  $u_h = \sum_{i: k_i=h} x_i \otimes m_i \otimes m_i \otimes y_i \in M^{\otimes h} \cap I$ . Тогда  $u = \sum_l u_l \in \bigoplus_{l=2}^{\infty} I \cap M^{\otimes l}$ .

Если  $v + u \in M^{\otimes n}$  для некоторого  $v \in \bigoplus_{k \neq n} M^{\otimes k}$ , то  $v + u - u_n = v + \sum_{i \neq n} u_i \in (\bigoplus_{k \neq n} M^{\otimes k}) \cap M^{\otimes n} = \{0\}$ . Таким образом,  $v + u = u_n \in I \cap M^{\otimes n}$ , причем по первой части доказательства этот элемент имеет требуемый вид.  $\square$

**ПРЕДЛОЖЕНИЕ 3.6.**  $\Lambda(M) = \bigoplus_{k=0}^{\infty} \Lambda^k(M)$  с умножением  $\wedge$ . Также как и в тензорной алгебре,  $\Lambda^k(M) \wedge \Lambda^n(M) \subseteq \Lambda^{k+n}(M)$ .

**ДОКАЗАТЕЛЬСТВО.** По предыдущей лемме  $(\bigoplus_{k \neq n} M^{\otimes k} + I) \cap M^{\otimes n} \subseteq I$  для любых  $k \neq n \in \mathbb{N}$ . Следовательно, сумма образов  $M^{\otimes k}$  по  $k \neq n$  в  $\Lambda(M)$  пересекается с образом  $M^{\otimes n}$  по нулю. С другой стороны, сумма образов равна  $\Lambda(M)$ . Поэтому  $\Lambda(M)$  является прямой суммой образов  $M^{\otimes k}$  по всем  $k \in \mathbb{N}_0$ . Снова по предыдущей лемме  $\Lambda^k(M) \cong M^{\otimes k} / (M^{\otimes k} \cap I)$ , а это означает, что образ  $M^{\otimes k}$  в  $\Lambda(M)$  изоморфен  $\Lambda^k(M)$ . Второе утверждение очевидно.  $\square$

Для доказательства следующего утверждения удобно будет ввести обозначения:

- $[n] = \{1, \dots, n\}$ ;
- для набора индексов  $I = \{i_1, \dots, i_k\} \subseteq [n]$ ,  $i_1 < \dots < i_k$ , и кортежа элементов  $(x_1, \dots, x_n)$  из  $M$  положим  $x_I = x_{i_1} \wedge \dots \wedge x_{i_k}$ .

**ПРЕДЛОЖЕНИЕ 3.7.** Если  $M \cong R^n$  – конечнопорожденный свободный модуль над  $R$  с базисом  $e = (e_1, \dots, e_n)$ , то базисом  $S^k(M)$  является набор  $\{e_{i_1} \cdots e_{i_k} \mid 1 \leq i_1 \leq \dots \leq i_k \leq n\}$ , а базисом  $\Lambda^k(M)$  – набор  $\{e_{i_1} \wedge \dots \wedge e_{i_k} \mid 1 \leq i_1 < \dots < i_k \leq n\}$ . В частности, ранг модуля  $\Lambda^k(M)$  равен  $\binom{n}{k}$ .

**ДОКАЗАТЕЛЬСТВО.** Ясно, что указанные наборы порождают модули  $S^k(M)$  и  $\Lambda^k(M)$ . Утверждение про симметрическую степень следует из определения многочлена от нескольких

переменных (линейная комбинация различных одночленов равна 0  $\iff$  все коэффициенты равны 0). Пусть

$$\sum_{I \subseteq [n], |I|=k} \alpha_I e_I = 0$$

Для каждого  $k$ -элементного подмножества  $J \subseteq [n]$  домножим это равенство на  $e_{[n] \setminus J}$  в алгебре  $\Lambda(M)$ . Ясно, что в сумме останется только одно слагаемое  $\pm \alpha_J e_{[n]}$ . Для того чтобы доказать, что  $e_{[n]} \neq 0$  в  $\Lambda^n(M)$  зададим антисимметричное полилинейное отображение  $\varphi : M^n \rightarrow R$  формулой  $\varphi(m_1, \dots, m_n) = \det((m_1)_e, \dots, (m_n)_e)$ . По определению  $\Lambda^k(M)$  оно единственным образом пропускается через линейное отображение  $\varphi' : \Lambda^n(M) \rightarrow R$ . При этом  $\varphi'(e_{[n]}) = \varphi(e_1, \dots, e_n) = \det E = 1$ . Следовательно,  $e_{[n]} \neq 0$ , откуда  $\alpha_J = 0$ . Таким образом, все коэффициенты вынесенной линейной комбинации равны 0, а это и означает, что наш набор элементов линейно независим.  $\square$

#### 4. Вычисления в алгебре Грассмана

В этом параграфе  $V$  – конечномерное векторное пространство над  $F$ , а все вычисления происходят в алгебре Грассмана  $\Lambda(V)$ .

Для  $k$ -элементного подмножества  $I = \{i_1, \dots, i_k\} \subseteq [n]$  и матрицы  $C \in M_{n,k}(F)$  обозначим через  $C^I$  подматрицу матрицы  $C$ , состоящую из строк с номерами  $i_1, \dots, i_k$ . Аналогично, для  $B \in M_{k,n}(F)$  через  $B_I$  обозначается матрица, составленная из столбцов с номерами  $i_1, \dots, i_k$ .

**ЛЕММА 4.1.** Пусть  $u = (u_1, \dots, u_n)$  и  $v = (v_1, \dots, v_k)$  два набора элементов пространства  $V$ , а  $C \in M_{n,k}(F)$ . Если  $v = uC$ , то

$$v_{[k]} = \sum_{I \subseteq [n], |I|=k} u_I \cdot \det C^I,$$

В частности, если  $k = n$ , то  $v_{[n]} = u_{[n]} \cdot \det C$ .

**ДОКАЗАТЕЛЬСТВО.** Докажем сначала частный случай  $k = n$  при условии, что  $u$  – базис  $V$ . Тогда любой элемент пространства  $\Lambda^n(V)$  однозначно записывается в виде  $u_{[n]} \alpha$  для некоторого  $\alpha \in F$ . Обозначим  $v_{[n]} = u_{[n]} \cdot \varphi(C)$ . Легко видеть, что  $\varphi : M_n(F) \rightarrow F$  – антисимметричная полилинейная форма столбцов матрицы  $C$ , а  $\varphi(E) = 1$ . Поэтому  $\varphi(C) = \det C$ .

Пусть теперь  $k \leq n$ , а  $u$  по-прежнему является базисом. По предложению 3.7 множество  $\{u_I \mid I \subseteq [n], |I| = k\}$  является базисом пространства  $\Lambda^k(V)$ . Поэтому

$$v_{[k]} = \sum_{I \subseteq [n], |I|=k} u_I \cdot \alpha_I,$$

для некоторых  $\alpha_I \in F$ . Зафиксируем  $k$ -элементное подмножество  $J \subseteq [n]$ . Пусть  $V_J$  факторпространство пространства  $V$  по подпространству, порожденному  $u_i$  по всем  $i \notin J$ . Обозначим через  $\bar{x}$  канонический образ элемента  $x \in V$  в  $V_J$ . Аналогичное обозначение будем использовать для набора элементов пространства  $V$ . Тогда

$$\bar{v} = (\bar{u}_{j_1}, \dots, \bar{u}_{j_k}) C^J,$$

где  $J = \{j_1, \dots, j_k\}$  и  $j_1 < \dots < j_k$ . По первой части доказательства  $\bar{v}_{[k]} = \bar{u}_J \cdot \det C^J$ . С другой стороны ясно, что  $\bar{u}_I = 0$  для любого  $I \neq J$ . Поэтому  $\bar{v}_{[k]} = \bar{u}_J \cdot \alpha_J$ . Так как  $(\bar{u}_{j_1}, \dots, \bar{u}_{j_k})$  является базисом пространства  $V_J$ , то  $\bar{u}_J \neq 0$ , следовательно  $\alpha_J = \det C^J$ .

Рассмотрим теперь общий случай. Пусть  $(e_1, \dots, e_n)$  – стандартный базис пространства  $F^n$ . По доказанному в предыдущем параграфе

$$c_{*1} \wedge \dots \wedge c_{*k} = \sum_{I \subseteq [n], |I|=k} e_I \cdot \det C^I,$$

Рассмотрим гомоморфизм  $\varphi : F^n \rightarrow V$ , заданный равенством  $\varphi(a) = ua$ . Тогда  $\varphi(e_i) = u_i$  и  $\varphi(c_{*i}) = v_i$ . Так как  $\Lambda$  является функтором, то  $\varphi$  индуцирует гомоморфизм

$\Lambda(\varphi) : \Lambda(F^n) \rightarrow \Lambda(V)$ . Применяя  $\Lambda(\varphi)$  к последней вынесенной формуле, получаем результат.  $\square$

**ТЕОРЕМА 4.2** (Бине–Коши). Пусть  $A = BC \in M_k(F)$ , где  $B \in M_{k,n}(F)$ , а  $C \in M_{n,k}(F)$ . Тогда

$$\det A = \sum_{I \subseteq [n], |I|=k} \det B_I \det C^I.$$

**ДОКАЗАТЕЛЬСТВО.** Пусть  $u_i = b_{*i}$ ,  $v_i = a_{*i}$ , а  $e$  – стандартный базис  $F^k$ . Тогда  $u = (u_1, \dots, u_n) = eB$ , а  $v = (v_1, \dots, v_k) = eA = uC$ . По лемме 4.1 имеем

$$e_{[k]} \det A = v_{[k]} = \sum_{I \subseteq [n], |I|=k} u_I \det C^I = e_{[k]} \sum_{I \subseteq [n], |I|=k} \det B_I \det C^I.$$

$\square$

Пусть  $I = \{i_1, \dots, i_k\} \subseteq [n]$ ,  $[n] \setminus I = \{j_1, \dots, j_{n-k}\}$ ,  $i_1 < \dots < i_k$  и  $j_1 < \dots < j_{n-k}$ . Для доказательства следующего утверждения нам необходимо вычислить четность перестановки

$$\sigma_I = \begin{pmatrix} 1 & \dots & k & k+1 & \dots & n \\ i_1 & \dots & i_k & j_1 & \dots & j_{n-k} \end{pmatrix}$$

**ЛЕММА 4.3.**  $\varepsilon(\sigma_I) = \left( \sum_{i \in I} i + \frac{k(k+1)}{2} \right) \mod 2$ .

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство индукцией по  $k$ . При  $k = 0$  утверждение очевидно. Рассмотрим перестановку  $\sigma_{I \setminus \{i_k\}}$

$$\sigma_{I \setminus \{i_k\}} = \begin{pmatrix} 1 & \dots & k-1 & k & \dots & i_k & \dots & n \\ i_1 & \dots & i_{k-1} & j_1 & \dots & i_k & & j_{n-k} \end{pmatrix}$$

По индукционному предположению ее четность равна  $\left( \sum_{i \in I} i - i_k + \frac{(k-1)k}{2} \right) \mod 2$ . Для того, чтобы получить  $\sigma_I$  из  $\sigma_{I \setminus \{i_k\}}$  надо переставить  $i_k$  на  $k$ -е место, не меняя порядок остальных индексов. Для этого надо выполнить  $i_k - k$  транспозиций. Таким образом,

$$\varepsilon(\sigma_I) = (\varepsilon(\sigma_{I \setminus \{i_k\}}) + i_k - k) \mod 2 = \left( \sum_{i \in I} i + \frac{(k-1)k}{2} + k \right) \mod 2 = \left( \sum_{i \in I} i + \frac{k(k+1)}{2} \right) \mod 2.$$

$\square$

Обозначим через  $\varepsilon_I$  четность перестановки  $\sigma_I$ .

**ЛЕММА 4.4.** Пусть  $V$  – векторное пространство с базисом  $e = (e_1, \dots, e_n)$ . Пространство  $\Lambda^{n-k}(V)$  отождествляется с пространством  $\Lambda^k(V)^*$  посредством отображения  $\varphi : \Lambda^{n-k}(V) \rightarrow \Lambda^k(V)^*$ , заданного формулой  $e_{[n]} \varphi(x)(y) = x \wedge y$ , где  $x \in \Lambda^{n-k}(V)$ , а  $y \in \Lambda^k(V)$  ( $x \wedge y$  всегда равно произведению некоторой константы на  $e_{[n]}$ ; эта константа и есть то число, в которое  $\varphi(x)$  отображает  $y$ ).

Положим  $e^I = e_{[n] \setminus I} \cdot (-1)^{\varepsilon_{[n] \setminus I}}$ . Тогда базисы  $\{e_I \mid |I| = k\}$  и  $\{e^I \mid |I| = k\}$  являются двойственными, другими словами,  $e^I \wedge e_I = e_{[n]}$  и  $e^I \wedge e_J = 0$  для любого  $J \neq I$ ,  $|J| = k$ .

**ТЕОРЕМА 4.5.** Пусть  $A = (BC)$  – матрица, разбитая на блоки  $B \in M_{n,k}(F)$  и  $C \in M_{n,n-k}(F)$ . Тогда

$$\det A = \sum_{I \subseteq [n], |I|=k} (-1)^{\varepsilon_I} \det B^I \cdot \det C^{[n] \setminus I}.$$

ДОКАЗАТЕЛЬСТВО. Пусть  $V = F^n$  – пространство со стандартным базисом  $e$ . По лемме 4.1 во внешней алгебре этого пространства имеет место равенство

$$e_{[n]} \cdot \det A = a_{*1} \wedge \cdots \wedge a_{*n} = (b_{*1} \wedge \cdots \wedge b_{*k}) \wedge (c_{*1} \wedge \cdots \wedge c_{*n-k}).$$

По лемме 4.1 сомножители правой части равны

$$\sum_{I \subseteq [n], |I|=k} e_I \cdot \det B^I \text{ и } \sum_{J \subseteq [n], |J|=n-k} e_J \cdot \det C^J, \text{ соответственно.}$$

По лемме 4.4 во внешнем произведении этих сумм остаются только слагаемые с  $J = [n] \setminus I$ . Таким образом

$$e_{[n]} \cdot \det A = \sum_{I \subseteq [n], |I|=k} e_I \cdot \det B^I \wedge e_{[n] \setminus I} \cdot \det C^{[n] \setminus I} = \sum_{I \subseteq [n], |I|=k} e_{[n]} (-1)^{\varepsilon_I} \det B^I \det C^{[n] \setminus I}.$$

□

В следующей теореме мы выразим миноры матрицы  $A^{-1}$  через миноры матрицы  $A$ . Для этого вначале создадим матрицу, состоящую из миноров матрицы  $A$ . Пусть  $I, J \subseteq [n]$ , а  $A \in M_n(F)$ . Обозначим через  $A_I^J$  подматрицу в  $A$ , стоящую на пересечении строк с номерами из  $J$  и столбцов с номерами из  $I$ .

Пусть  $L : V \rightarrow V$  – линейный оператор. Обозначим через  $\Lambda^k L : \Lambda^k(V) \rightarrow \Lambda^k(V)$  оператор, заданный на разложимых тензорах формулой  $\Lambda^k L(x_1 \wedge \cdots \wedge x_k) = L(x_1) \wedge \cdots \wedge L(x_k)$  и продолженный по линейности (таким образом,  $\Lambda^k$  превращается в функтор из категории векторных пространств в себя; аналогично можно сделать и для категории модулей над коммутативным кольцом). Если  $e$  – базис пространства  $V$ , то через  $\Lambda^k e$  обозначим базис пространства  $\Lambda^k(V)$  из предложения 3.7. Нам понадобится писать матрицу оператора в этом базисе, но упорядочивать его неудобно. Поэтому строки и столбцы матриц будут нумероваться  $k$ -элементными подмножествами в  $[n]$ , где  $n = \dim V$ , также как и базисные элементы  $e_I = e_{i_1} \wedge \cdots \wedge e_{i_k}$ .

**ЛЕММА 4.6.** Пусть  $V$  –  $n$ -мерное векторное пространство, а  $I, J \subseteq [n]$  – подмножества порядка  $n$ . Если  $L_e = A$ , то элемент матрицы оператора  $\Lambda^k L$  в базисе  $\Lambda^k e$  в позиции  $(J, I)$  равен  $\det A_I^J$ .

ДОКАЗАТЕЛЬСТВО. По определению матрицы линейного оператора  $L(e) = eA$ , откуда  $(L(e_{i_1}), \dots, L(e_{i_k})) = eA_I^{[n]}$ , где  $I = \{i_1, \dots, i_k\}$ ,  $i_1 < \cdots < i_k$ . По лемме 4.1

$$L(e_I) = L(e_{i_1}) \wedge \cdots \wedge L(e_{i_k}) = \sum_{|J|=k} e_J \det A_I^J,$$

что и требовалось. □

Так как  $\Lambda^k$  – функтор, то  $\Lambda^k L^{-1} = (\Lambda^k L)^{-1}$ . Мы хотим вычислить элементы матрицы этого оператора. Мы могли бы написать, что они равны алгебраическим дополнениям матрицы оператора  $\Lambda^k L$ , деленным на ее определитель. Однако эта формула слишком громоздка. Мы вычислим обратную к матрице оператора  $\Lambda^k L$ , пользуясь двойственным базисом к  $\Lambda^k e$ , указанном в лемме 4.4.

**ТЕОРЕМА 4.7.** Пусть  $A \in \text{GL}_n(F)$ . Тогда  $\det(A^{-1})_J^I = \frac{1}{\det A} (-1)^{s_{IJ}} \det A_{[n] \setminus I}^{[n] \setminus J}$ , где  $s_{IJ} = \sum_{l \in I \Delta J} l$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $L : F^n \rightarrow F^n$  – оператор умножения на матрицу  $A$ , так что  $L_e = A$ , где  $e$  – стандартный базис в  $F^n$ . Положим  $B = \Lambda^k L_{\Lambda^{n-k} e}$ . По предыдущей лемме

$$B^{-1} = (\det(A^{-1})_I^J)_{|I|=|J|=k} \text{ и } \Lambda^{n-k} L_{\Lambda^{n-k} e} = \left( \det A_{[n] \setminus I}^{[n] \setminus J} \right)_{|I|=|J|=k}.$$

Пусть  $f$  – двойственный к  $\Lambda^k e$  базис пространства  $\Lambda^{n-k}(V)$ , найденный в лемме 4.4. Так как знаки элементов базиса  $f$  отличаются от знаков элементов базиса  $\Lambda^{n-k}e$ , то предыдущая формула превращается в

$$D := \Lambda^{n-k} L_f = \left( (-1)^{\varepsilon_{[n] \setminus I} + \varepsilon_{[n] \setminus J}} \det A_{[n] \setminus I}^{[n] \setminus J} \right)_{|I|=|J|=k}.$$

Заметим, что

$$\begin{aligned} (\varepsilon_{[n] \setminus I} + \varepsilon_{[n] \setminus J}) \mod 2 &= \left( \sum_{l \notin I} l + \frac{(n-k)(n-k+1)}{2} + \sum_{l \notin J} l + \frac{(n-k)(n-k+1)}{2} \right) \mod 2 = \\ &= \left( \sum_{l=1}^n l - \sum_{l \in I} l + \sum_{l=1}^n l - \sum_{l \in J} l \right) \mod 2 = \left( \sum_{l \in I \Delta J} l \right) \mod 2 = s_{IJ}. \end{aligned}$$

По лемме 4.4  $(\Lambda^k e)^\tau f = e_{[n]} \cdot E$  (произведение матриц с элементами из алгебры  $\Lambda(F^n)$ ). Так как  $\Lambda$  – функтор, то  $L$  индуцирует эндоморфизм  $\Lambda(L)$  алгебры  $\Lambda(F^n)$ , а также эндоморфизмы  $M_{r,s}(\Lambda(L))$  модулей  $M_{r,s}(\Lambda(F^n))$ , сохраняющие произведения матриц. Допуская вольность речи, все эти отображения будут обозначаться через  $L$ .

Применяя  $L$  к последнему равенству, получаем

$$L(\Lambda^k e)^\tau L(f) = L(e_{[n]}) \cdot E \iff (\Lambda^k e B)^\tau f D = e_{[n]} \det A \cdot E \iff B^\tau D = \det A \cdot E \iff B^{-1} = \frac{1}{\det A} D^\tau.$$

Сравнивая 2 различных выражения для элементов матрицы  $B^{-1}$ , получаем требуемые формулы.  $\square$

## Теория представлений

И снова теория групп, но теперь немного в другом разрезе. Если в главе 8 мы изучали действия групп на множествах, что соответствует гомоморфизму группы в симметрическую группу, то теперь мы рассмотрим *линейное* действие групп на векторных пространствах, что будет соответствовать гомоморфизмам в полную линейную группу. Методы и результаты теории представлений используются не только в самой теории групп, но, например, и в теоретической физике.

Так как наш курс ознакомительный, то мы будем изучать только *конечномерные* представления *конечных* групп над *алгебраически замкнутым* полем *характеристики 0*. Однако, все определения и утверждения, которые не требуют этого предположения будут сформулированы в общем случае.

В отличие от предыдущих глав, в этой главе кольца не предполагаются по умолчанию коммутативными.

### 1. Основные определения

Пусть  $V$  – векторное пространство над полем  $F$ , а  $G$  – группа. Напомним, что  $\mathrm{GL}(V) = \mathrm{Aut}(V)$  – это группа всех обратимых линейных операторов на  $V$ .

**ОПРЕДЕЛЕНИЕ 1.1.** Линейным представлением  $G$  на  $V$  называется гомоморфизм  $\pi : G \rightarrow \mathrm{GL}(V)$ . Размерность пространства  $V$  называется степенью представления и обозначается  $\deg \pi$ .

Базис пространства  $V$  задает изоморфизм  $\mathrm{GL}(V) \cong \mathrm{GL}_n(F)$ , где  $n = \dim V$ : оператору сопоставляется его матрица в выбранном базисе. Гомоморфизм  $\pi : G \rightarrow \mathrm{GL}_n(F)$  называется матричным представлением группы  $G$ . Говоря про линейное или матричное представление  $\pi$  обычно пишут  $\pi_g$  вместо  $\pi(g)$ , потому что выражение  $\pi_g(v)$  выглядит приятнее для глаза, чем  $\pi(g)(v)$ . Матричное представление задает  $n^2$  функций  $\pi_{ij} : G \rightarrow F$  по правилу  $\pi_{ij}(g) = (\pi_g)_{ij}$ . Говорят что  $G$  действует линейно на  $V$ , если задано действие  $G \curvearrowright V$ ,  $(g, v) \mapsto gv$ , удовлетворяющее равенствам

$$g(u + v) = gu + gv \text{ и } g(\alpha v) = \alpha gv \quad \forall g \in G, v \in V, \alpha \in F.$$

Линейное представление определяет линейное действие  $G \curvearrowright V$  по правилу  $gv = \pi_g(v)$ . Линейное действие  $G$  на  $V$  очевидным образом продолжается до действия групповой алгебры  $FG$  на  $V$ :

$$\left(\sum_{g \in G} \alpha_g g\right)v := \sum_{g \in G} \alpha_g (gv), \text{ где } \alpha_g \in F, v \in V.$$

Таким образом,  $V$  превращается в левый  $FG$ -модуль. Аналогично, говоря про линейное или матричное представление  $\pi : G \rightarrow \mathrm{GL}(V)$ , мы продолжим его по линейности до гомоморфизма алгебр  $FG \rightarrow \mathrm{End}(V)$ , которое будем обозначать той же буквой  $\pi$ .

Мы связали с линейным представлением группы еще 3 объекта. Класс объектов каждого типа естественным образом превращается в категорию так, чтобы четыре получившиеся категории были эквивалентны. Определим морфизмы в каждой из категорий.

**ОПРЕДЕЛЕНИЕ 1.2.** Морфизмом представлений  $\pi : G \rightarrow \mathrm{GL}(U)$  в  $\rho : G \rightarrow \mathrm{GL}(V)$  называется линейное отображение  $\varphi : U \rightarrow V$  удовлетворяющее условию  $\varphi(\pi_g(u)) = \rho_g(\varphi(u))$

для любых  $g \in G$  и  $u \in U$ . Морфизм представлений называется еще гомоморфизмом представлений или сплетающим отображением.

**ОПРЕДЕЛЕНИЕ 1.3.** Морфизмом матричных представлений  $\pi : G \rightarrow \mathrm{GL}_n(F)$  в  $\rho : G \rightarrow \mathrm{GL}_m(F)$  называется матрица  $A \in M_{m,n}(F)$  такая, что  $A\pi_g = \rho_g A$  при всех  $g \in G$ .

**ОПРЕДЕЛЕНИЕ 1.4.** Морфизмом линейных действий  $G \curvearrowright U$  в  $G \curvearrowright V$  называется  $G$ -эквивариантное линейное отображение  $\varphi : U \rightarrow V$  (напомним, что эквивариантность означает:  $\varphi(gu) = g\varphi(u)$  для любых  $g \in G$  и  $u \in U$ ).

Таким образом, мы определили категории линейных представлений, матричных представлений и линейных действий данной группы  $G$ , а что такое категория левых  $FG$ -модулей мы уже знаем. Доказательство следующего утверждения является рутинным.

**ПРЕДЛОЖЕНИЕ 1.5.** Категории линейных представлений, матричных представлений и линейных действий данной группы  $G$ , а также категория левых  $FG$ -модулей эквивалентны между собой (для категории матричных представлений необходима аксиома выбора для классов).

Сформулируем теперь несколько определений на языке линейных представлений и модулей. Пусть  $\pi : G \rightarrow \mathrm{GL}(V)$  – линейное представление группы  $G$  на векторном пространстве  $V$  над полем  $F$ .

- Два представления называются эквивалентными, если они изоморфны в категории линейных представлений. Другими словами, представления  $\pi : G \rightarrow V$  и  $\pi' : G \rightarrow V'$  эквивалентны, если существует изоморфизм  $\varphi : V \rightarrow V'$  такой, что  $\varphi\pi_g = \pi'_g\varphi$  для любого  $g \in G$ . Последнее равенство можно переписать в виде  $\pi_g = \varphi^{-1}\pi'_g\varphi$ . Ясно, что из эквивалентности представлений следует  $\dim V = \dim V'$ . В случае матричных представлений  $V = V' = F^n$ . Матричные представления  $\pi : G \rightarrow \mathrm{GL}_n(F)$  и  $\pi' : G \rightarrow \mathrm{GL}_m(F)$  эквивалентны тогда и только тогда, когда  $m = n$  и существует  $C \in \mathrm{GL}_n(F)$  такая, что  $\pi_g = C^{-1}\pi'_g C$ . Таким образом, если  $C$  интерпретировать как матрицу замены базиса, то получится, что эквивалентные матричные представления отличаются друг от друга только выбором базиса в  $F^n$ . Модули эквивалентных представлений называются изоморфными.
- Подпространство  $U \leq V$  называется  $G$ -инвариантным, если оно инвариантно относительно всех операторов  $\pi_g$ ,  $g \in G$ . Ясно, что в этом случае  $U$  является подмодулем  $FG$ -модуля  $V$ .
- Если  $U$  –  $G$ -инвариантное подпространство в  $V$ , то индуцированные гомоморфизмы  $G \rightarrow \mathrm{GL}(U)$  и  $G \rightarrow \mathrm{GL}(V/U)$  называются подпредставлением и факторпредставлением соответственно. На языке модулей этому соответствует подмодуль  $U$  и фактормодуль  $V/U$   $FG$ -модуля  $V$ . На матричном языке  $G$ -инвариантному подпространству соответствует представление  $\pi'$ , эквивалентное  $\pi$ , у которого все матрицы  $\pi'_g$  имеют клеточно треугольный вид  $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$  с диагональными клетками размера  $\dim U$  и  $\dim V - \dim U$ . Тогда клетка в верхнем левом углу является подпредставлением, а в нижнем правом – факторпредставлением.
- Представление называется неразложимым, если  $V$  не раскладывается в прямую сумму ненулевых 2  $G$ -инвариантных подпространств. В этом случае  $FG$ -модуль  $V$  также называется неразложимым. На матричном языке это означает, что не существует представления,  $\pi'$  эквивалентного  $\pi$  такого, что все  $\pi'_g$  имеют клеточно диагональный вид  $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ .
- Представление называется неприводимым, если в  $V$  ровно 2  $G$ -инвариантных подпространства:  $\{0\} \neq V$ . В этом случае  $FG$ -модуль  $V$  называется простым.

- Представление называется вполне приводимым, если  $V$  раскладывается в прямую сумму конечного числа неприводимых  $G$ -инвариантных подпространств. В этом случае  $FG$ -модуль  $V$  называется полупростым.
- Представление  $\pi : G \rightarrow \mathrm{GL}(V)$  называется точным, если  $\pi$  инъективно. Из этого *не следует*, что  $FG$ -модуль  $V$  точен ( $R$ -модуль  $M$  называется точным, если  $rM \neq 0$  для любого  $r \in R \setminus \{0\}$ ).

## 2. Строение артиновых колец

**Артиновы кольца.** Сначала мы изучим представления на языке модулей. Для этого мы классифицируем все артиновы кольца, в частности, групповые кольца конечных групп.

**ОПРЕДЕЛЕНИЕ 2.1.** Кольцо  $R$  называется *артиновым слева*, если любое линейно упорядоченное (по включению) множество левых идеалов содержит наименьший элемент.

Это условие равносильно условию обрыва убывающих цепей левых идеалов или, коротко, DCC (descending chain condition). Это – упражнение на применение леммы Цорна. Так как идеал групповой алгебры в первую очередь является подпространством, то групповая алгебра конечной группы над полем всегда является артиновым (и слева, и справа) из соображений размерности.

Любое факторкольцо артинова кольца артиново, потому что прообраз под действием эпиморфизма цепочки строго вложенных идеалов является цепочкой строго вложенных идеалов. Однако, это не верно для подколец:  $\mathbb{Z}$  не артиново подкольцо артинова кольца  $\mathbb{Q}$ . Идеал  $I \triangleleft R$  называется нильпотентным, если существует натуральное  $n$  такое, что  $I^n = 0$ . По определению степени идеала это означает, что  $r_1 \cdot \dots \cdot r_n = 0$  для любых  $r_1 \dots r_n \in I$ . Этот параграф посвящен следующим 2 утверждениям.

**ПРЕДЛОЖЕНИЕ 2.2.** В артиновом (слева) кольце существует наибольший нильпотентный идеал, фактор по которому не содержит ненулевых нильпотентных идеалов. Этот идеал совпадает с радикалом Джекобсона.

Артиново (слева) кольцо с нулевым радикалом Джекобсона называется *классически полупростым*.

**ТЕОРЕМА 2.3** (Веддербарна–Артина). Классически полупростое кольцо изоморфно прямой сумме конечного числа полных матричных колец над телами.

Казалось бы, что артиновость в каком-то смысле двойственна к нетеровости, однако это совсем не так. Самые простые нетеровы кольца:  $\mathbb{Z}$ , кольцо многочленов над полем и т. п. не являются артиновыми, но:

**ТЕОРЕМА 2.4.** Любое артиново слева (справа) кольцо является нетеровым слева (соотв. справа).

Этот факт следует из двух только что сформулированных результатов. Как и теорему Веддербарна–Артина последняя теорема в нашем курсе идет без доказательства.

**Радикал Джекобсона.** Для того чтобы сформулировать определение радикала Джекобсона, докажем следующее утверждение. Кольцо  $R$ , как левый (правый) модуль над собой, называется *регулярным левым (правым)  $R$ -модулем*.

**ЛЕММА 2.5.** Пусть  $r$  – элемент произвольного (ассоциативного с 1) кольца  $R$ . Следующие условия эквивалентны.

- 1L.  $r$  содержится в любом максимальном левом идеале кольца  $R$ .
- 1R.  $r$  содержится в любом максимальном правом идеале кольца  $R$ .
- 2L.  $r$  можно исключить из любой системы образующих регулярного левого  $R$ -модуля.



2R.  $r$  можно исключить из любой системы образующих регулярного правого  $R$ -модуля.

3L. Для любого  $x \in R$  элемент  $1 + xr$  обратим.

3R. Для любого  $x \in R$  элемент  $1 + rx$  обратим.

ДОКАЗАТЕЛЬСТВО. (1L  $\implies$  3L). Если  $1 + xr$  не обратим, то  $R(1 + xr)$  лежит в каком-то максимальном левом идеале  $\mathfrak{m}$  (следует из теоремы о существовании максимального идеала).  $r, 1 + xr \in \mathfrak{m} \implies 1 \in \mathfrak{m}$  – противоречие.

(3L  $\implies$  2L). Если  $S \cup \{r\}$  порождает  $R$  как левый  $R$ -модуль, то  $1 = xr + \sum_{s \in S} x_s s$ , откуда  $1 - xr = \sum_{s \in S} x_s s$  и  $1 = \sum_{s \in S} (1 - xr)^{-1} x_s s$ . Следовательно, уже  $S$  порождает  $R$ .

(2L  $\implies$  1L). Если  $r$  не лежит в максимальном левом идеале  $\mathfrak{m}$ , то  $\mathfrak{m} + Rr = R$ , т.е.  $\mathfrak{m} \cup \{r\}$  порождает  $R$ . Но тогда  $\mathfrak{m}$  порождает  $R$  – противоречие.

(3L  $\implies$  3R).  $(1 + xr)x = x(1 + rx) \implies x = (1 + xr)^{-1}x(1 + rx) \implies 1 + rx = 1 + r(1 + xr)^{-1}x(1 + rx) \implies (1 - r(1 + xr)^{-1}x)(1 + rx) = 1$ , откуда  $1 + rx$  обратим слева. Нетрудно проверить, что  $(1 + rx)(1 - r(1 + xr)^{-1}x) = 1$ .

Импlicationи (3R  $\implies$  2R  $\implies$  1R  $\implies$  3R  $\implies$  3L) абсолютно аналогичны.  $\square$

**ОПРЕДЕЛЕНИЕ 2.6.** Множество элементов, удовлетворяющих условиям предыдущей леммы, называется радикалом Джекобсона кольца.

Радикал Джекобсона кольца  $R$  обозначается через  $\text{Rad } R$  или  $\text{JRad } R$ . Он равен пересечению максимальных левых (правых) идеалов, и, следовательно, является двусторонним идеалом. Если  $\text{Rad } R = \{0\}$ , то кольцо  $R$  называется полупростым.

**ПРЕДЛОЖЕНИЕ 2.7.**  $R/\text{Rad } R$  – полупростое кольцо.

ДОКАЗАТЕЛЬСТВО. Пусть  $r \in R$  такой, что его образ  $\bar{r}$  в кольце  $R/\text{Rad } R$  лежит в радикале. Тогда для любого  $\bar{x} \in R/\text{Rad } R$  существует  $\bar{y} \in R/\text{Rad } R$  такой, что  $(1 + \bar{x}\bar{r})\bar{y} = \bar{y}(1 + \bar{x}\bar{r}) = 1$ . Взяв прообраз этого равенства в  $R$  получаем, что  $(1 + xr)y = 1 + j_1$  и  $y(1 + xr) = 1 + j_2$  для некоторых  $j_1, j_2 \in \text{Rad } R$ . Так как  $1 + j_1$  и  $1 + j_2$  обратимы, то  $1 + xr$  обратим и справа, и слева, откуда  $r \in \text{Rad } R$ , а  $\bar{r} = 0$ .  $\square$

Из пункта (3L) леммы 2.5 вытекает следующее утверждение.

**ПРЕДЛОЖЕНИЕ 2.8.** Любой нильпотентный идеал содержится в радикале Джекобсона.

ДОКАЗАТЕЛЬСТВО. Для любого  $r$ , принадлежащего нильпотентному левому идеалу, и любого  $x \in R$  выполнено равенство  $(xr)^n = 0$  при каком-то  $n \in \mathbb{N}$ . Тогда  $(1 + xr)(1 - xr + (xr)^2 - \dots \pm (xr)^{n-1}) = 1 - (xr)^n = 1$ . Следовательно,  $1 + xr$  обратим для любого  $x \in R$ , откуда  $r \in \text{Rad } R$ .  $\square$

Для доказательства обратного утверждения для артиновых колец нам понадобится следующая лемма.

**ЛЕММА 2.9.** Если  $M$  – простой (левый)  $R$ -модуль, то  $\text{Rad } R \cdot M = 0$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $J = \text{Rad } R$ . Предположим, что  $JM \neq 0$ . Пусть  $t \in M \setminus \{0\}$ . Так как  $M$  простой, то  $Rt = JM = M$  и  $Jt = JRt = JM = M$ . Определим эпиморфизм левых  $R$ -модулей  $R \rightarrow M$ ,  $r \mapsto rt$ , и обозначим через  $I$  его ядро. Существует  $j \in J$  такой, что  $jt = t$ , следовательно,  $1 - j \in I$ . Тогда  $I \cup \{j\}$  порождают  $R$ , а по пункту (2L) леммы 2.5  $j$  можно исключить из множества образующих. Таким образом  $I = R$ , т.е.  $M = 0$ .  $\square$

**ОПРЕДЕЛЕНИЕ 2.10.** Аннулятором (левого)  $R$ -модуля  $M$  называется множество  $\{r \in R \mid rM = 0\}$ .

Легко видеть, что аннулятор любого модуля является двусторонним идеалом кольца  $R$ .

**СЛЕДСТВИЕ 2.11.** Радикал Джекобсона равен пересечению аннуляторов всех простых (левых) модулей.

**ДОКАЗАТЕЛЬСТВО.** Для максимального левого идеала  $\mathfrak{m}$  кольца  $R$  аннулятор простого модуля  $R/\mathfrak{m}$  содержится в  $\mathfrak{m}$  ( $x(1 + \mathfrak{m}) = 0 + \mathfrak{m} \iff x \in \mathfrak{m}$ ). Поэтому пересечение аннуляторов содержится в пересечении максимальных левых идеалов. Обратное включение – это предыдущая лемма.  $\square$

**ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 2.2.** Пусть  $J = \text{Rad } R$ . Так как  $R$  артиново слева, то цепочка  $J \supseteq J^2 \supseteq \dots$  обрывается. Пусть  $J^n = J^{n+1}$ . Обозначим  $I := \{r \in R \mid J^n r = 0\}$ . Ясно, что  $I$  – двусторонний идеал.

Пусть  $J^n \not\subseteq I$ . Обозначим чертой проекцию  $R \rightarrow \bar{R} := R/I$ . Тогда  $\bar{J}^n \neq 0$ . Так как полный прообраз максимального (левого) идеала при эпиморфизме является максимальным идеалом, то полный прообраз радикала содержит радикал. Поэтому  $\bar{J}^n \subseteq \text{Rad } \bar{R}$ . Пусть  $\bar{M}$  – минимальный ненулевой левый идеал кольца  $\bar{R}$ , содержащийся в  $\bar{J}^n$  (существует, потому что  $\bar{R}$  артиново слева). Ясно, что  $\bar{M}$  – простой модуль. По лемме 2.9  $\bar{J}^n \bar{M} = 0$ . Взяв прообраз последнего равенства в  $R$  получим

$$J^n M \subseteq I \implies J^n M = J^{2n} M \subseteq J^n I = 0 \implies M \subseteq I \implies \bar{M} = 0.$$

Противоречие показывает, что  $J^n \subseteq I$ , откуда  $J^n = J^{2n} \subseteq J^n I = 0$ .  $\square$

**Модули над классически полупростым кольцом.** Пусть  $R = R_1 \oplus \dots \oplus R_k$  – прямая сумма колец, а  $M$  –  $R$ -модуль. Легко видеть, что как абелева группа  $M$  равен прямой сумме подмодулей  $R_i M$ . Для  $n = 2$ :  $m = (1, 0)m + (0, 1)m$ , а если  $m = (r_1, 0)m' = (0, r_2)m''$ , то  $m = (1, 1)m = (1, 0)(0, r_2)m'' + (0, 1)(r_1, 0)m' = 0$ . Таким образом, неприводимый  $R$ -модуль – это неприводимый  $R_i$ -модуль, на котором остальные  $R_j$ ,  $j \neq i$ , действуют тривиально. Можно показать, что конечнопорожденный левый модуль над кольцом  $M_n(D)$  (где  $D$  – тело) равен прямой сумме нескольких модулей  $D^n$ .

**ТЕОРЕМА 2.12.** Пусть  $R$  – полупростое артиново кольцо. Тогда любой левый  $R$ -модуль полупрост, а простые левые модули изоморфны  $M_n(D)$ -модулям  $D^n$  для некоторого тела  $D$ .

Если  $R$  – конечномерная алгебра над замкнутым полем  $F$ , то все тела  $D$  изоморфны  $F$ .

**Пример неполупростой групповой алгебры.** Пусть  $C_p$  – циклическая группа порядка  $p$ , а  $F$  – поле характеристики  $p$ . Тогда  $FC_p \cong F[x]/(x^p - 1) \cong F[t]/(t^p)$  – кольцо усеченных многочленов. Действительно, зададим эпиморфизм  $F[x] \rightarrow FC_p$ , переводящий  $x$  в образующую группы  $C_p$ . По определению групповой алгебры образ ненулевого многочлена степени меньше, чем  $p$ , не равен нулю, а  $x^p - 1$  переходит в 0. Поэтому ядро порождено  $x^p - 1$ . В характеристике  $p$  имеем  $x^p - 1 = (x - 1)^p$ . Делая замену переменных  $t = x - 1$ , получаем второй изоморфизм. отождествим  $x$  с образующей  $C_p$ . Радикал  $FC_p$  – это главный идеал, порожденный  $x - 1$ . Действительно,  $x - 1$  нильпотентен, а  $FC_p/(x - 1) \cong F$  полупросто.

Представление  $\pi : C_p \rightarrow \text{GL}_n(F)$  однозначно определяется матрицей  $\pi_x$ .  $(\pi_x - E)^p = \pi_x^p - E = 0$ , откуда все собственные числа  $\pi_x$  равны 1. Если  $\pi \neq 1$ , то  $\pi$  – точное, потому что  $C_p$  простая группа. Следовательно  $\pi_x$  имеет порядок  $p$ . Если  $\pi$  неразложимое, то  $\pi_x$  – жорданова клетка порядка  $\leq p + 1$  по диагонали.

**Кольцо представлений.** Скелет категории конечномерных линейных представлений группы  $G$  над полем  $F$  (или эквивалентной ей категории  $FG$ -модулей) является малой категорией, потому что уже категория матричных представлений малая (объект – гомоморфизм  $G \rightarrow \text{GL}_n(F)$ ; имеем право образовать множество всех таких гомоморфизмов).

На объектах этого скелета мы хотим определить структуру полукольца. Проще сделать это, если стартовать с категории  $FG$ -модулей. Итак: элементы полукольца  $\text{Rep}_F(G)$  – классы изоморфизмов  $FG$ -модулей, конечномерных над  $F$ .

$$[M] + [N] := [M \oplus N]; \quad [M] \cdot [N] := [M \otimes N].$$

Ясно, что результат не зависит от представителя класса изоморфизма. Свойства полукольца проверены в предложении 1.1 главы 10. Из этого полукольца можно универсальным образом

сделать кольцо  $R_F(G)$ , подействовав на него левым сопряженным к функтору вложения категории колец в категорию полуколец (везде есть 1, которую сохраняют морфизмы). Конструктивно:  $R_F(G) := \{[M] - [N]\}$ , где  $M$  и  $N$  пробегает  $F$ -конечномерные  $FG$ -модули, с операциями, продолженными по линейности с полукольца  $\text{Per}_F(G)$ .

### 3. Лемма Шура

Пусть сначала  $R$  – произвольное кольцо.

**ЛЕММА 3.1** (Лемма Шура). *Пусть  $U$  и  $V$  простые  $R$ -модули. Тогда*

- (1) *Если  $U \not\cong V$ , то  $\text{Hom}(U, V) = 0$ .*
- (2)  *$\text{End}(U)$  – тело.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\varphi : U \rightarrow V$  – гомоморфизм  $R$ -модулей. Образ  $\varphi$  – подмодуль в  $V$ , а ядро – подмодуль в  $U$ . Так как  $U$  и  $V$  простые, есть два варианта:

- (1)  $\text{Ker } \varphi = U$  и  $\text{Im } \varphi = 0$ , т.е.  $\varphi = 0$ .
- (2)  $\text{Ker } \varphi = 0 \neq U$  и  $\text{Im } \varphi = V$ , т.е.  $\varphi$  – изоморфизм.

□

**СЛЕДСТВИЕ 3.2.** *Пусть  $F$  – алгебраически замкнутое поле,  $R$  является  $F$ -алгеброй, а  $U$  – простой  $R$ -модуль конечномерный над  $F$ . Тогда  $\text{End}_R(U) \cong F$ . Другими словами, любой эндоморфизм простого конечномерного  $R$ -модуля – это умножение на константу (гомотетия).*

**ДОКАЗАТЕЛЬСТВО.** Любой  $R$ -линейный эндоморфизм является  $F$ -линейным, поэтому  $\text{End}_R(U) \subseteq \text{End}_F(U) \cong M_n(F)$ , где  $n = \dim_F U$ . С другой стороны, если  $\varphi \in \text{End}_R(U)$ , то и  $\alpha\varphi \in \text{End}_R(U)$  для любого  $\alpha \in F$ . Поэтому  $\text{End}_R(U)$  является подпространством в  $n^2$ -мерном пространстве  $\text{End}_F(U)$ . Доказательство заканчивает следующая лемма. □

Тело  $D$ , являющееся  $F$ -алгеброй, называется алгеброй с делением над  $F$ .

**ЛЕММА 3.3.** *Любая конечномерная алгебра  $D$  с делением над алгебраически замкнутым полем  $F$  изоморфна  $F$ .*

**ДОКАЗАТЕЛЬСТВО.** Для  $\alpha \in D$  рассмотрим гомоморфизм  $F$ -алгебр  $F[t] \rightarrow D$ ,  $t \mapsto \alpha$ . Его образ  $F[\alpha]$  – подкольцо в  $D$ . Его ядро – главный идеал  $pF[t]$ , так что  $F[\alpha] \cong F[t]/(p)$ . Если  $\deg p > 1$ , то он раскладывается на нетривиальные множители, так как  $F$  замкнуто. Но тогда в  $F[\alpha]$  есть делители нуля, чего не может быть. Следовательно,  $\deg p = 1$ , т.е.  $p = t - \alpha$ , откуда  $\alpha \in F$ . □

### Неприводимые представления абелевой группы.

**СЛЕДСТВИЕ 3.4.** *Каждое неприводимое конечномерное представление абелевой группы над алгебраически замкнутым полем одномерно.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $V$  – простой конечномерный  $FG$ -модуль, а  $F$  алгебраически замкнуто. Для любых  $h, g \in G$  имеем  $hgv = ghv$ , так что умножение на  $h$  является автоморфизмом  $V$ . По следствию 3.2 любой автоморфизм  $V$  – это умножение на скаляр. Таким образом, любое  $F$ -линейное подпространство  $V$  является  $FG$ -подмодулем. Для того чтобы быть простым  $V$  должно не иметь нетривиальных подпространств, т.е. быть одномерным. □

Обратное утверждение: “Если все неприводимые представления группы  $G$  одномерны, то группа  $G$  абелева.” тоже верно. Оно будет доказано ниже.

Для поля, не являющегося алгебраически замкнутым, утверждение неверно. Циклическая группа  $C_4 = \langle g \rangle$  имеет над  $\mathbb{R}$  двумерное представление  $g \mapsto \pi_g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . Так как  $\chi_{\pi_g}(t) = t^2 + 1$  неприводим над  $\mathbb{R}$ , матрица  $\pi_g$  не приводится к (блочной) треугольному виду, следовательно представление неприводимо.

#### 4. Полная приводимость

**Однозначность разложения на неприводимые.** Доказательство следующего результата совпадает с доказательством следствия 9.3 главы 8.

**ТЕОРЕМА 4.1** (Жордана–Гёльдера). *Пусть  $R$  – ассоциативное кольцо с 1. Если  $R$ -модуль обладает композиционным рядом, то набор факторов этого ряда определен однозначно с точностью до изоморфизма.*

“Набор” в этом контексте означает мультимножество, т.е. множество с учетом кратности, с формальной точки зрения – множество вместе с функцией из него в натуральные числа.

**СЛЕДСТВИЕ 4.2** (теорема Ремака–Крулля–Шмидта). *Если линейное представление вполне приводимо, то набор неприводимых прямых слагаемых определен однозначно с точностью до изоморфизма.*

**Полная приводимость.** В отличие от примера в конце параграфа 2, если порядок группы не делится на характеристику поля, то любое конечномерное представление вполне приводимо.

**ТЕОРЕМА 4.3** (Машке). *Если характеристика поля  $F$  не делит порядок конечной группы  $G$ , то любое конечномерное линейное представление  $\pi : G \rightarrow \mathrm{GL}(V)$  над  $F$  вполне приводимо.*

Для доказательства теоремы Машке достаточно проверить, что любой подмодуль  $U \leq V$  выделяется прямым слагаемым. Это условие равносильно наличию ретракции  $V \twoheadrightarrow U$ . Доказательство следующего утверждения аналогично доказательству предложения 8.1 главы 8, но проще за счет коммутативности операции сложения.

**ЛЕММА 4.4.** *Пусть  $R$  – ассоциативное кольцо с 1, а  $U \leq V$  –  $R$ -модули. Следующие условия эквивалентны.*

- (1) *Существует подмодуль  $W \leq V$  такой, что  $V = U \oplus W$ .*
- (2) *Существует ретракция  $V \twoheadrightarrow U$ .*

**ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ МАШКЕ.** Пусть  $U$  –  $FG$ -подмодуль  $V$ . Так как любой  $F$ -модуль имеет прямое дополнение, существует  $F$ -линейная ретракция  $\rho : V \twoheadrightarrow U$ . Определим  $F$ -линейное отображение  $\rho' : V \rightarrow U$  формулой

$$\rho'(v) = \frac{1}{|G|} \sum_{g \in G} g\rho(g^{-1}v) \in \frac{1}{|G|} \sum_{g \in G} g\rho(V) = \frac{1}{|G|} \sum_{g \in G} gU \subseteq U.$$

(по условию  $|G|$  обратимо в  $F$ ). Проверим, что это отображение  $FG$ -линейно. Для любого  $h \in G$  имеем

$$\rho'(hv) = \frac{1}{|G|} \sum_{g \in G} g\rho(g^{-1}hv) = h \left( \frac{1}{|G|} \sum_{g \in G} h^{-1}g\rho((h^{-1}g)^{-1}v) \right) = h\rho'(v)$$

Далее,  $u \in U \implies g^{-1}u \in U \implies g\rho(g^{-1}u) = u$ , откуда  $\rho'(u) = u$ . Таким образом,  $\rho'$  является ретракцией  $FG$ -модулей, что по предыдущей лемме влечет, что  $U$  выделяется прямым слагаемым. Доказательство заканчивается индукцией по размерности  $V$  над  $F$ .  $\square$

**Унитаризуемость.** Трюк усреднения отображения по группе, использованный для доказательства теоремы Машке, помогает доказать, что над  $\mathbb{C}$  любую группу можно вложить не в полную линейную, а в унитарную группу. Пусть  $B : V \times V \rightarrow \mathbb{C}$  – эрмитово скалярное произведение на комплексном векторном пространстве  $V$ . Напомним, что (классическая) унитарная группа  $U(B) = U(V, B)$  – это подгруппа в  $\mathrm{GL}(V)$ , состоящая из операторов  $\varphi$  удовлетворяющих равенству

$$B(\varphi(x), \varphi(y)) = B(x, y) \text{ для любых } x, y \in V.$$

**ТЕОРЕМА 4.5.** Пусть  $G$  – конечная группа, а  $V$  – конечномерное векторное пространство над  $\mathbb{C}$ . Для любого представления  $\pi : G \rightarrow \mathrm{GL}(V)$  существует эрмитово скалярное произведение  $B : V \times V \rightarrow \mathbb{C}$  такое, что  $\mathrm{Im} \pi \subseteq \mathrm{U}(B)$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $B'$  – произвольное скалярное произведение на  $V$ . Тогда

$$B(x, y) := \frac{1}{|G|} \sum_{g \in G} B'(\pi_g(x), \pi_g(y))$$

является  $G$ -инвариантным скалярным произведением.  $\square$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ МАШКЕ НАД  $\mathbb{C}$ . Если  $\mathrm{Im} \pi \subseteq \mathrm{U}(B)$ , а  $U$  –  $G$ -инвариантное подпространство, то  $U^{\perp_B}$  также  $G$ -инвариантно, а  $V = U \oplus U^{\perp_B}$ , см. предложение 4.6 и лемму 5.8 главы 7.  $\square$

Еще один бонус унитаризуемости состоит в том, что унитарная группа компактна в топологии, индуцированной (любой) нормой на  $\mathrm{End}(V)$ , в отличие от  $\mathrm{GL}(V)$ .

## 5. Характеры представления

До конца настоящей главы мы рассматриваем только конечномерные представления конечных групп. Пусть  $\rho : G \rightarrow \mathrm{GL}(V)$  – такое представление.

**ОПРЕДЕЛЕНИЕ 5.1.** Характером представления  $\rho$  называется функция  $\chi_\rho : G \rightarrow F$  сопоставляющая каждому элементу  $g \in G$  след оператора  $\rho_g$ :

$$\chi_\rho(g) = \mathrm{Tr} \rho_g.$$

Напомним свойства следа:

- (1)  $\mathrm{Tr}(A + B) = \mathrm{Tr}(\mathrm{diag}(A, B)) = \mathrm{Tr} A + \mathrm{Tr} B$ ;
- (2)  $\mathrm{Tr} AB = \mathrm{Tr} BA$  как только произведения существуют;
- (3)  $\mathrm{Tr} C^{-1}AC = \mathrm{Tr} A$ ;
- (4) След матрицы равен сумме ее собственных чисел (над замыканием поля) с учетом алгебраической кратности.

**Простейшие свойства характеров.** Первые 2 пункта следующего утверждения очевидны.

**ПРЕДЛОЖЕНИЕ 5.2** (простейшие свойства характеров). Пусть  $\pi$  и  $\rho$  – представления группы  $G$ , а  $\chi = \chi_\rho$ .

- (1)  $\chi(1) = n = \deg \rho$ .
- (2)  $\chi(hgh^{-1}) = \chi(g)$ . Последнее свойство обычно выражается так: характер представления является центральной функцией на группе или функцией классов (*class function*). Иными словами, значение характера на элементе  $g \in G$  зависит не от самого этого элемента, а только от его класса сопряженности.
- (3)  $\chi_{\pi \oplus \rho} = \chi_\pi + \chi_\rho$ .
- (4)  $\chi_{\pi \otimes \rho} = \chi_\pi \cdot \chi_\rho$ .
- (5) Если  $F \subseteq \mathbb{C}$ , то  $\chi(g^{-1}) = \overline{\chi(g)}$ .
- (6) Если  $F \subseteq \mathbb{C}$ , то  $|\chi(g)| \leq \deg \rho$ .

ДОКАЗАТЕЛЬСТВО. (3). Можно считать, что  $\pi$  и  $\rho$  – матричные представления. Тогда матрица  $(\pi \oplus \rho)_g$  равна  $\mathrm{diag}(\pi_g, \rho_g)$ , а ее след равен сумме следов.

(4). При доказательстве этого пункта удобно говорить о линейных представлениях  $\pi : G \rightarrow \mathrm{GL}(U)$  и  $\rho : G \rightarrow \mathrm{GL}(V)$ . Пусть  $u$  и  $v$  – базисы пространств  $U$  и  $V$  соответственно

Рассмотрим матрицу оператора  $\pi_g \otimes \rho_g$  в базисе  $w = \{u_i \otimes v_j\}$ .

$$\pi_g \otimes \rho_g(u_i \otimes v_j) = \pi_g(u_i) \otimes \rho_g(v_j) = \left( \sum_k (\pi_g)_{ki} u_k \right) \otimes \left( \sum_m (\rho_g)_{mj} v_m \right) = (\pi_g)_{ii} (\rho_g)_{jj} u_i \otimes v_j.$$

Таким образом, диагональные элементы матрицы  $(\pi_g \otimes \rho_g)_w$  равны  $(\pi_g)_{ii} (\rho_g)_{jj}$ , а их сумма:

$$\sum_{i,j} (\pi_g)_{ii} (\rho_g)_{jj} = \left( \sum_i (\pi_g)_{ii} \right) \left( \sum_j (\rho_g)_{jj} \right) = (\text{Tr } \pi_g) (\text{Tr } \rho_g).$$

(5). Каждый элемент группы имеет конечный порядок, поэтому его собственные числа  $\lambda_i$  – корни из 1. В частности,  $|\lambda_i| = 1$ , откуда  $\lambda_i^{-1} = \overline{\lambda_i}$ . Таким образом,

$$\chi(g^{-1}) = \text{Tr } \rho_{g^{-1}} = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda_i} = \overline{\chi(g)}.$$

(6).  $|\chi(g)| = |\sum \lambda_i| \leq \sum |\lambda_i| = 1 + \dots + 1 = \deg \rho$ . □

**Двойственное представление и его характер.** Как мы знаем, переход от пространства к сопряженному является контравариантным функтором. Поэтому для *левого* линейного представления  $\pi : G \rightarrow \text{GL}(V)$  имеем *правое* линейное представление (антигомоморфизм)  $\pi' : G \rightarrow \text{GL}(V^*)$ , заданное формулой  $\pi'_g(f)(x) := f(\pi_g(x))$ . Так как мы хотим, чтобы *двойственное представление*  $\pi^* : G \rightarrow \text{GL}(V^*)$  было бы левым, определим его формулой

$$\pi_g^*(f)(x) := f(\pi_g^{-1}(x)).$$

Нетрудно видеть, что матрицы операторов  $\pi_g$  и  $\pi'_g$  в двойственных базисах пространств  $V$  и  $V^*$  транспонированы друг к другу. Следовательно,  $(\pi_g^*)_{e^*} = (\pi_g)_e^{-\top}$ , где  $a^{-\top}$  – обратная транспонированная (т.е. контргradientная) к  $a$ .

**ПРЕДЛОЖЕНИЕ 5.3.** Пусть  $\pi : G \rightarrow \text{GL}(V)$  конечномерное комплексное представление группы  $G$ . Тогда  $\chi_{\pi^*} = \overline{\chi_{\pi}}$ .

## 6. Соотношения ортогональности

Пусть  $G$  – конечная группа, а  $F$  – поле, характеристика которого не делит порядок  $G$ . На пространстве функций  $F^G$  определим симметричную билинейную форму

$$B(\eta, \theta) := \frac{1}{|G|} \sum_{g \in G} \eta(g) \theta(g^{-1}).$$

Ортогональность таких функций по умолчанию будет означать ортогональность относительно формы  $B$ . Рассмотрим два линейных представления  $\pi : G \rightarrow \text{GL}(U)$  и  $\rho : G \rightarrow \text{GL}(V)$  и произвольное линейное отображение  $\varphi : U \rightarrow V$ . Назовем усреднением этого отображения относительно группы  $G$  отображение

$$\varphi_0 = \frac{1}{|G|} \sum_{g \in G} \rho_g \circ \varphi \circ \pi_g^{-1}.$$

В доказательстве теоремы Машке мы проверили, что это отображение  $G$ -эквивариантно, т.е. является морфизмом представлений. По лемме Шура, если представления  $\pi$  и  $\rho$  неприводимы и неэквивалентны, то  $\varphi_0 = 0$ .

**ЛЕММА 6.1** (матричная форма леммы Шура). Пусть  $\pi : G \rightarrow \text{GL}_n(F)$  и  $\rho : G \rightarrow \text{GL}_m(F)$  – неприводимые матричные представления группы  $G$ , а  $A \in M_{m,n}(F)$ . Положим  $A_0 = \frac{1}{|G|} \sum_{g \in G} \rho_g A \pi_g^{-1}$ .

(1) Если  $\pi$  и  $\rho$  не эквивалентны, то  $A_0 = 0$ .

- (2) Если  $\pi = \rho$ , а поле  $F$  алгебраически замкнуто, то  $A_0 = \frac{\text{Tr } A}{\deg \pi} E$ . В частности,  $\deg \pi \neq 0$  в  $F$ .

**ДОКАЗАТЕЛЬСТВО.** Заметим, что оператор умножения на матрицу  $A_0$  является  $G$ -эквивариантным, т.е.  $A_0$  является морфизмом матричных представлений. Если  $\pi$  и  $\rho$  не эквивалентны, то по лемме Шура  $A_0 = 0$ .

В случае (2) по лемме Шура  $A_0 = \lambda E$  для некоторого  $\lambda \in F$ .

$$\lambda n = \text{Tr } A_0 = \frac{1}{|G|} \sum_{g \in G} \text{Tr}(\rho_g A \pi_g^{-1}) = \frac{1}{|G|} \sum_{g \in G} \text{Tr } A = \text{Tr } A.$$

□

**ТЕОРЕМА 6.2** (соотношения ортогональности Шура). Пусть  $\pi, \rho$  – неприводимые матричные представления группы  $G$  над полем  $F$ , характеристика которого не делит  $|G|$ .

- (1) Если  $\pi$  и  $\rho$  не эквивалентны, то для любых  $i, j \in [\deg \pi]$  и  $k, h \in [\deg \rho]$  функции  $\pi_{ij}$  и  $\rho_{kh}$  ортогональны.  
 (2) Если поле  $F$  алгебраически замкнуто, то

$$B(\pi_{ij}, \pi_{kh}) = \frac{1}{\deg \pi} \delta_{jk} \delta_{ih}.$$

**ДОКАЗАТЕЛЬСТВО.** Сразу следует из предыдущей леммы с  $A = E_{jk}$ . В случае (2) с  $j = k$  равенство  $A_0 = \frac{1}{\deg \pi} E$  влечет

$$\frac{1}{|G|} \sum_{g \in G} \pi_{ij}(g) \pi_{jh}(g^{-1}) = \frac{1}{\deg \pi} \delta_{ih}.$$

□

Если  $F = \mathbb{C}$ , то мы можем изучать только унитарные представления. Для унитарных представлений  $\pi_{ij}(g^{-1}) = (\pi_g^{-1})_{ij} = \overline{\pi_{ji}(g)}$ . Определим эрмитово скалярное произведение  $C$  на множестве функций  $\mathbb{C}^G$  по формуле

$$C(\eta, \theta) := \frac{1}{|G|} \sum_{g \in G} \eta(g) \overline{\theta(g)}$$

Тогда из соотношений ортогональности вытекает следующее утверждение.

**СЛЕДСТВИЕ 6.3.** Пусть  $\pi^{(i)}$  – все (с точностью до эквивалентности) неприводимые унитарные матричные представления группы  $G$  над  $\mathbb{C}$ , Тогда набор функций  $\sqrt{\deg \pi^{(i)}} \pi_{jk}^{(i)}$  ортонормирован относительно формы  $C$ .

Возвращаемся к общей ситуации алгебраически замкнутого поля  $F$ , характеристика которого не делит порядок группы  $G$ .

**СЛЕДСТВИЕ 6.4.** Пусть  $\pi^{(i)}$  – все (с точностью до эквивалентности) неприводимые представления группы  $G$  над  $F$ , а  $\chi_i = \chi_{\pi^{(i)}}$ . Тогда набор  $\chi_i$  является ортонормированным набором функций классов.

**ДОКАЗАТЕЛЬСТВО.**

$$B(\chi_i, \chi_k) = B\left(\sum_j \pi_{jj}^{(i)}, \sum_h \pi_{hh}^{(k)}\right) = \sum_{jh} B(\pi_{jj}^{(i)}, \pi_{hh}^{(k)}) = \delta_{ik} \sum_j B(\pi_{jj}^{(i)}, \pi_{jj}^{(i)}).$$

Таким образом, характеры разных представлений ортогональны, а  $B(\chi_i, \chi_i)$  является суммой  $n_i$  слагаемых, равных  $1/n_i$ , где  $n_i = \deg \pi^{(i)}$ . □

По умолчанию, везде далее  $F$  – алгебраически замкнутое поле характеристики 0.

Заметим, что для характеров комплексных представлений  $\chi$  и  $\theta$  имеем  $B(\chi, \theta) = C(\chi, \theta)$ . Из полной приводимости и первого соотношения ортогональности сразу следует, что на множестве характеров обе формы принимают целые неотрицательные значения.

Пусть  $\pi$  – неприводимое, а  $\rho$  – любое представление группы  $G$ . По теореме Машке  $\rho$  раскладывается в прямую сумму неприводимых.

**СЛЕДСТВИЕ 6.5.** *Количество раз, которое  $\pi$  встречается в разложении  $\rho$  на неприводимые, равно  $B(\chi_\pi, \chi_\rho)$ .*

Для доказательства достаточно вспомнить, что характер прямой суммы равен сумме характеров прямых слагаемых.

Заметим, что из этого следует теорема Ремака–Крулля–Шмидта для частного случая замкнутых полей характеристики 0.

**СЛЕДСТВИЕ 6.6.**  $\pi \sim \rho \iff \chi_\pi = \chi_\rho$ .

Это утверждение совершенно неверно при  $\text{char } F = p \neq 0$ . В качестве контрпримера достаточно взять прямую сумму любого представления в количестве  $p + 1$  штук, его характер такой же, как у самого представления.

**СЛЕДСТВИЕ 6.7.**  $B(\chi_\pi, \chi_\pi) = 1 \iff \pi$  неприводимо.

Неприводимый характер – это характер неприводимого представления.

**СЛЕДСТВИЕ 6.8** (ортогональность характеру тривиального представления). *Для любого неприводимого характера  $\chi \neq 1$*

$$\sum_{g \in G} \chi(g) = 0.$$

## 7. Разложение регулярного представления

Пусть  $G$  действует на множестве  $X$ . Это действие индуцирует линейное действие  $G$  на свободном модуле  $\langle X \rangle_F$ . Обозначим через  $\chi$  характер этого действия.

**ЛЕММА 7.1.**  $\chi(g) = |\text{Fix}_X(g)|$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\chi$  – характер представления  $\pi$ . Ясно, что для любого  $g \in G$  каждый столбец матрицы  $\pi_g$  в базисе  $X$  имеет ровно одну единицу и остальные нули. Столбцы, в которых эти единицы стоят на диагонали соответствуют  $x \in X$ , для которых  $gx = x$ .  $\square$

Обозначим через  $\text{reg}$  – регулярное представление.

**СЛЕДСТВИЕ 7.2.**  $\chi_{\text{reg}}(g) = \begin{cases} |G|, & \text{если } g = 1, \\ 0, & \text{иначе.} \end{cases}$

Пусть  $\chi_1, \dots, \chi_s$  – характеры всех неприводимых представлений, а  $n_i = \chi_i(1)$  – их степени.

**ТЕОРЕМА 7.3** (Веддербарна). *Каждое неприводимое представление входит в регулярное с кратностью, равной степени.*

**ДОКАЗАТЕЛЬСТВО.** Вычислим  $B(\chi_{\text{reg}}, \chi_i)$ :

$$B(\chi_{\text{reg}}, \chi_i) = \frac{1}{|G|} \sum_{g \in G} \chi_{\text{reg}}(g) \chi_i(g^{-1})$$

так как все слагаемые, кроме слагаемых с  $g = 1$ , равны 0, а  $\chi_{\text{reg}}(1) = |G|$ , то эта сумма равна

$$\frac{1}{|G|} |G| \chi_i(1) = \chi_i(1) = n_i.$$

$\square$



**СЛЕДСТВИЕ 7.4.**  $n_1^2 + \dots + n_s^2 = |G|$

**ТЕОРЕМА 7.5** (Петера–Вейля). Матричные элементы  $\pi_{ij}$ ,  $1 \leq i, j \leq \dim(\pi)$ , всех неэквивалентных неприводимых представлений  $\pi$ , образуют базис пространства  $FG = F^G$  всех функций на  $G$ .

В случае  $F = \mathbb{C}$ , а все  $\pi$  унитарны, этот базис является ортогональным относительно формы  $C$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\pi^{(1)}, \dots, \pi^{(s)}$  – набор всех неэквивалентных между собой неприводимых представлений группы  $G$ . По предыдущему следствию количество функций  $\pi_{ij}^{(k)}$  равно  $|G| = \dim FG$ . Пусть  $\sum_{k,i,j} \alpha_{kij} \pi_{ij}^{(k)} = 0$ . Тогда по теореме 6.2

$$\alpha_{hqp} = \dim \pi^h \sum_{k,i,j} \alpha_{kij} B(\pi_{ij}^{(k)}, \pi_{pq}^{(h)}) = \dim \pi^h B(\sum_{k,i,j} \alpha_{kij} \pi_{ij}^{(k)}, \pi_{pq}^{(h)}) = 0.$$

Поэтому функции  $\pi_{ij}$  линейно независимы. Второе утверждение вытекает из следствия 6.3.  $\square$

## 8. Количество неприводимых представлений

Пусть  $f : G \rightarrow F$  – функция классов, а  $\rho : G \rightarrow \text{GL}(V)$  – линейное представление. Следующая формула определяет усреднение с весом  $f$ :

$$\rho_f := \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) \rho_g \in \text{End}(V).$$

Заметим, что  $\text{Tr}(\rho_f) = B(f, \chi_\rho)$ .

**ЛЕММА 8.1.** Для любого поля  $F$  оператор  $\rho_f$  является морфизмом представлений.

Если  $\rho$  неприводимо степени  $n$ , а  $F$  – алгебраически замкнуто, то  $\rho_f$  гомотетия с константой  $B(f, \chi_\rho)/n$ .

**ДОКАЗАТЕЛЬСТВО.** Для любого  $h \in G$  имеем

$$\rho_h \rho_f = \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) \rho_h \rho_g \rho_{h^{-1}} \rho_h = \frac{1}{|G|} \sum_{g \in G} f(({}^h g)^{-1}) \rho_{hg} \rho_h = \rho_f \rho_h.$$

Тот факт, что  $\rho_f$  – умножение на константу  $\lambda \in F$ , следует из первого утверждения и леммы Шура над замкнутым полем. Тогда  $\lambda n = \text{Tr} \rho_f = B(f, \chi_\rho)$ , что и требовалось.  $\square$

**ТЕОРЕМА 8.2.** Пусть  $F$  – алгебраически замкнутое поле характеристики 0. Неприводимые характеры  $\chi_1, \dots, \chi_s$  образуют ортонормированный базис пространства функций классов на группе  $G$ .

**ДОКАЗАТЕЛЬСТВО.** Мы уже знаем, что  $\chi_1, \dots, \chi_s$  ортонормированная система относительно формы  $B$ . Обозначим через  $Y$  пространство функций классов, а через  $X$  – подпространство, порожденное неприводимыми характерами. Так как  $B$  невырождена на  $X$ , то по лемме 4.6 главы 7  $Y = X \oplus X^{\perp_B}$ . Поэтому достаточно показать, что любая функция  $f$ , ортогональная ко всем  $\chi_1, \dots, \chi_s$  равна 0. По предыдущей лемме  $\rho_f$  равно 0 для всех неприводимых представлений  $\rho$ .

По теореме Машке любое представление  $\pi$  вполне приводимо. На матричном языке это означает, что  $\pi_g = \text{diag}(\rho_g^{(1)}, \dots, \rho_g^{(k)})$  для некоторых неприводимых  $\rho^{(1)}, \dots, \rho^{(k)}$ . Из того, что  $\rho_f^{(i)} = 0$  для всех прямых слагаемых сразу следует, что  $\pi_f = 0$ . В частности, для регулярного представления  $\text{reg}_f = 0$ . Применим это равенство к  $1_G \in FG$ :

$$0 = \text{reg}_f(1_G) = \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) \text{reg}_g(1_G) = \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) g.$$

Так как  $G$  – базис групповой алгебры, то  $f(g^{-1}) = 0$  для всех  $g \in G$ , а это и значит, что  $f = 0$ .  $\square$

**СЛЕДСТВИЕ 8.3.** *Количество неприводимых представлений равно количеству классов сопряженных элементов.*

ДОКАЗАТЕЛЬСТВО. И то, и другое равно размерности пространства функций классов.  $\square$

**ПРЕДЛОЖЕНИЕ 8.4.** *Для любого поля  $F$  центр групповой алгебры  $FG = F^G$  состоит из функций классов.*

ДОКАЗАТЕЛЬСТВО. Пусть  $f = \sum_{g \in G} \alpha_g g \in FG$ . Элемент  $f$  лежит в центре  $\iff f = h^{-1}fh \forall h \in G$ . Последнее условие равносильно тому, что

$$\sum_{g \in G} \alpha_g g = h^{-1} \left( \sum_{g \in G} \alpha_g g \right) h = \sum_{g \in G} \alpha_g g^h \iff \alpha_g = \alpha_{g^h} \forall g, h \in G$$

Таким образом,  $f$  лежит в центре тогда и только тогда, когда коэффициенты при сопряженных элементах равны, что и означает, что  $f$  соответствует функции классов.  $\square$

**ТЕОРЕМА 8.5** (Второе соотношение ортогональности). *Пусть  $\chi_1 = 1, \chi_2, \dots, \chi_s$  – все различные неприводимые характеры. Если  $h, g \in G$ , то*

$$\sum_{i=1}^s \chi_i(h) \chi_i(g^{-1}) = \begin{cases} |C_G(h)|, & h \text{ сопряжен с } g, \\ 0, & \text{иначе.} \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Пусть  $g_1 = 1, g_2, \dots, g_s$  – представители различных классов сопряженности группы  $G$  (по следствию 8.3 их количество равно  $s$ ). Положив  $m_i = |g_i^G|$ , первое соотношение ортогональности можно переписать в виде

$$\frac{1}{|G|} \sum_{k=1}^s m_k \chi_i(g_k) \chi_j(g_k^{-1}) = \delta_{ij}.$$

Рассмотрим матрицы  $A, D \in M_s(F)$  с элементами  $a_{ik} = \chi_i(g_k)$  и  $d_{pq} = m_p \chi_q(g_p^{-1})$ . Тогда  $\frac{1}{|G|} AD = E$ .

Так как  $A$  и  $D$  квадратные, то и  $\frac{1}{|G|} DA = E$ . Записав последнее равенство поэлементно, получим

$$\frac{1}{|G|} \sum_{k=1}^s m_i \chi_k(g_i^{-1}) \chi_k(g_j) = \delta_{ij}$$

Заметим, что  $m_i = |G : C_G(g_i)|$ , откуда  $|C_G(g_i)| = |G|/m_i$ . Таким образом,

$$\sum_{k=1}^s \chi_k(g_j) \chi_k(g_i^{-1}) = \delta_{ij} |C_G(g_i)|.$$

Так как характеры являются функциями классов, а порядок централизатора одинаков для всех элементов данного класса сопряженных, то можно заменить  $g_j$  на  $g$ ,  $g_i$  на  $h$ , а  $\delta_{ij}$  на  $\delta_{g^G, h^G}$ .  $\square$

## 9. Таблицы характеров

В строках таблицы – все неприводимые характеры ( $\chi_i := \chi_{\pi_i}$ ), в столбцах – классы сопряженных элементов, а в клетках – значение характера на представителе  $g_i$  класса. Из следствия 8.3 вытекает, что эта таблица – квадратная ( $s \times s$ ). В первой строке стоят единицы – характер единичного представления. В первом столбце –  $\chi_i(1) = \deg \pi_i$ . По следствию 7.4  $\sum_{i=1}^s \chi_i(1)^2 = |G|$ . Из соотношения ортогональности характеров следует, что строки ортонормированы относительно формы  $B$ :

$$B(\chi, \theta) = \frac{1}{|G|} \sum_{g \in G} \chi(g) \theta(g^{-1}) = \frac{1}{|G|} \sum_{i=1}^s |g_i^G| \chi(g_i) \theta(g_i^{-1}).$$

Над  $\mathbb{C}$  для любого характера  $\theta(g^{-1}) = \overline{\theta(g)}$ , так что строки ортонормированы относительно эрмитова скалярного произведения с матрицей  $\frac{1}{|G|} \text{diag}(|g_1^G|, \dots, |g_s^G|)$ . По второму соотношению ортогональности столбцы также ортогональны, а их скалярные квадраты равны  $|C_G(g_i)| = |G|/|g_i^G|$ .

Если  $G$  – абелева, то все неприводимые представления одномерны, т. е. это гомоморфизмы в  $F^*$ . Характеры совпадают с представлениями.

$G = \mathbb{Z}/2$			$G = \mathbb{Z}/3$				$G = \mathbb{Z}/2 \times \mathbb{Z}/2$				
	0	1		0	1	2		(0,0)	(0,1)	(1,0)	(1,1)
$\chi_1$	1	1	$\eta_1$	1	1	1	$\theta_1$	1	1	1	1
$\chi_2$	1	-1	$\eta_2$	1	$\omega$	$\omega^2$	$\theta_2$	1	-1	1	-1
			$\eta_3$	1	$\omega^2$	$\omega$	$\theta_3$	1	1	-1	-1
							$\theta_4$	1	-1	-1	1

Неприводимые характеры прямого произведения равны произведению неприводимых характеров сомножителей, как, например,  $\theta_k(x, y) = \chi_i(x)\chi_j(y)$ .

Одномерные представления неабелевой группы  $G$  соответствуют представлениям  $G^{\text{ab}} = G/[G, G]$ .

Нарисуем таблицу характеров для  $S_3$ .

$g_i^G$	$e$	(1 2)	(1 2 3)
$ g_i^G $	1	3	2
$\chi_1$	1	1	1
$\chi_2$	1	-1	1
$\chi_3$	2	0	-1

Приведем регулярное представление  $S_3$  к блочно диагональному виду. Достаточно привести в такому виду образующие. В качестве образующих возьмем (1 2) и (1 2 3).

$$\text{reg}(12) = \begin{pmatrix} & & 0 & 0 & 1 \\ & & 0 & 1 & 0 \\ & & 1 & 0 & 0 \\ 0 & 0 & 1 & & \\ 0 & 1 & 0 & & \\ 1 & 0 & 0 & & \end{pmatrix} \quad \text{reg}(123) = \begin{pmatrix} 0 & 0 & 1 & & \\ 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ & & & 0 & 0 & 1 \\ & & & 1 & 0 & 0 \\ & & & 0 & 1 & 0 \end{pmatrix}$$

Базис  $u$ :

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ 1 \\ \omega \\ \omega^2 \end{pmatrix} \begin{pmatrix} \omega^2 \\ \omega \\ 1 \\ \omega^2 \\ \omega \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix}$$

$$\text{reg}(1\ 2)_u = \begin{pmatrix} 1 & & & & \\ & -1 & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix} \quad \text{reg}(1\ 2\ 3)_u = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & \omega^2 & 0 & \\ & & 0 & \omega & \\ & & & & 0 & -1 \\ & & & & 1 & -1 \end{pmatrix}$$

Нарисуем таблицу характеров для неабелевой группы порядка 8.

Центр  $p$ -группы нетривиален, а факторгруппа по центру не может быть циклической.

Следовательно, центр неабелевой группы порядка 8 имеет порядок 2.

Фактор по центру изоморфен  $\mathbb{Z}/2 \times \mathbb{Z}/2$ .

Так как фактор по центру абелев, то центр содержит коммутант, а так как группа неабелева, то коммутант не равен 1.

Следовательно коммутант равен центру.

$g_i^G$	$e$	$c$	$g_3$	$g_4$	$g_5$
$ g_i^G $	1	1	2	2	2
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	1	-1	-1
$\chi_3$	1	1	-1	1	-1
$\chi_4$	1	1	-1	-1	1
$\chi_5$	2	-2	0	0	0

## 10. Представления прямого произведения

Следующее утверждение не понадобится для нашей основной цели, но дает представление о том, что происходит с декартовым произведением групп. Доказательство оставляется в качестве упражнения.

**ПРЕДЛОЖЕНИЕ 10.1.**  $F(H \times G) = FH \otimes_F FG$ .

Пусть  $\pi : H \rightarrow \text{GL}(U)$  и  $\rho : G \rightarrow \text{GL}(V)$  – линейные представления. Их тензорным произведением называется представление  $\pi \otimes \rho : H \times G \rightarrow \text{GL}(U \otimes V)$ , заданное формулой

$$(\pi \otimes \rho)_{(h,g)}(u \otimes v) = \pi_h(u) \otimes \rho_g(v).$$

В частности,  $\chi_{\pi \otimes \rho}(h, g) = \chi_\pi(h) \chi_\rho(g)$ , см. доказательство свойства 4 предложения 5.2. Обозначим через  $\text{Irr}(G)$  множество всех неэквивалентных между собой неприводимых представлений группы  $G$ . Напомним, что по следствию 8.3  $|\text{Irr}(G)|$  равно количеству смежных классов в  $G$ . Теперь у нас все готово, чтобы доказать основной результат настоящего параграфа.

**ТЕОРЕМА 10.2.** • Если  $\pi, \rho$  – неприводимые представления групп  $H$  и  $G$ . Тогда представление  $\pi \otimes \rho$  группы  $H \times G$  неприводимо.

• Каждое неприводимое представление группы  $H \times G$  имеет такой вид.

ДОКАЗАТЕЛЬСТВО. Пусть  $\pi, \pi'$  – представления группы  $H$ , а  $\rho, \rho'$  – представления группы  $G$ . Тогда

$$\begin{aligned} B(\chi_{\pi \otimes \rho}, \chi_{\pi' \otimes \rho'}) &= \frac{1}{|H \times G|} \sum_{(h,g) \in H \times G} \chi_{\pi \otimes \rho}(h, g) \chi_{\pi' \otimes \rho'}(h^{-1}, g^{-1}) = \\ &= \frac{1}{|H| \cdot |G|} \sum_{h \in H} \sum_{g \in G} \chi_{\pi}(h) \chi_{\rho}(g) \chi_{\pi'}(h^{-1}) \chi_{\rho'}(g^{-1}) = \\ &= \frac{1}{|H|} \sum_{h \in H} \chi_{\pi}(h) \chi_{\pi'}(h^{-1}) \cdot \frac{1}{|G|} \sum_{g \in G} \chi_{\rho}(g) \chi_{\rho'}(g^{-1}) = B(\chi_{\pi}, \chi_{\pi'}) B(\chi_{\rho}, \chi_{\rho'}). \end{aligned}$$

Если  $\pi$  и  $\rho$  неприводимы то по следствию 6.7 скалярные квадраты их характеров равны 1. Следовательно, скалярный квадрат характера  $\chi_{\pi \otimes \rho}$  также равен 1, откуда по тому же следствию  $\pi \otimes \rho$  неприводимо.

Если  $\pi \not\sim \pi'$  или  $\rho \not\sim \rho'$  и все четыре представления неприводимы, то по следствию 6.4  $B(\chi_{\pi}, \chi_{\pi'}) = 0$  или  $B(\chi_{\rho}, \chi_{\rho'}) = 0$ . Следовательно,  $B(\chi_{\pi \otimes \rho}, \chi_{\pi' \otimes \rho'}) = 0$ , откуда вытекает, что  $\pi \otimes \rho$  не эквивалентно  $\pi' \otimes \rho'$ . Таким образом, мы построили  $|\text{Irr}(H)| \cdot |\text{Irr}(G)|$  неприводимых представлений группы  $H \times G$ .

Заметим, что класс сопряженных элементов  $(h, g)^{H \times G}$  равен  $(h^H, g^G)$ . Поэтому количество классов сопряженных в  $H \times G$  равно количеству классов сопряженных в  $H$  умножить на количество классов сопряженных в  $G$ . Учитывая, что последнее равно  $|\text{Irr}(H)| \cdot |\text{Irr}(G)|$ , заключаем, что мы построили все неприводимые представления группы  $H \times G$ .  $\square$

## 11. Целые алгебраические числа

Задача следующего параграфа – доказать, что степень неприводимого представления  $\pi$  делит порядок группы. Для этого мы докажем, что рациональное число  $|G|/\deg \pi$  является корнем унитарного многочлена с целыми коэффициентами и, следовательно, является целым числом.

Напомним, что  $F$  – алгебраически замкнутое поле характеристики 0. Целым алгебраическим числом называется элемент  $F$ , являющийся корнем унитарного многочлена с целыми коэффициентами. Множество целых алгебраических чисел обозначается через  $\mathbb{A}$ . Так как характеристика  $F$  равна нулю, то любая подгруппа аддитивной группы  $F$  не имеет кручения. По теореме 9.1 и следствию 8.3 главы 6 любая конечнопорожденная абелева группа без кручения изоморфна  $\mathbb{Z}^n$ , а любая ее подгруппа конечно порождена.

**ЛЕММА 11.1.** *Элемент  $\alpha \in F$  принадлежит  $\mathbb{A}$  тогда и только тогда, когда  $\mathbb{Z}[\alpha]$  является конечнопорожденной абелевой группой.*

ДОКАЗАТЕЛЬСТВО. Если  $\alpha \in \mathbb{A}$ , то  $\alpha^n = \sum_{k=0}^{n-1} m_k \alpha^k$  для некоторых целых  $n, m_1, \dots, m_{n-1}$ . Поэтому любую степень  $\alpha$ , большую чем  $n-1$ , можно выразить через линейную комбинацию меньших с целыми коэффициентами. По индукции получаем, что  $\mathbb{Z}[\alpha]$  порождено элементами  $1, \alpha, \dots, \alpha^{n-1}$ .

Обратно, пусть  $\mathbb{Z}[\alpha]$  порождено многочленами  $p_1(\alpha), \dots, p_k(\alpha)$ . Выберем  $n$  больше максимума из степеней  $p_i$  и выразим  $\alpha^n$  через образующие:  $\alpha^n = \sum_{i=1}^k m_i p_i(\alpha)$ ,  $m_i \in \mathbb{Z}$ . Тогда  $\alpha$  является корнем унитарного многочлена  $t^n - \sum_{i=1}^k m_i p_i \in \mathbb{Z}[t]$ .  $\square$

**ТЕОРЕМА 11.2.** *Множество целых алгебраических чисел является подкольцом в  $F$ .*

ДОКАЗАТЕЛЬСТВО. Пусть  $\alpha, \beta \in \mathbb{A}$ , где  $\alpha$  и  $\beta$  являются корнями унитарных многочленов степеней  $a$  и  $b$  соответственно. Тогда  $\alpha^h \beta^k = (\sum_{i=0}^{a-1} m_i \alpha^i)(\sum_{j=0}^{b-1} n_j \beta^j)$ ,  $m_i, n_j \in \mathbb{Z}$ . Таким образом, любой многочлен от  $\alpha, \beta$  выражается через линейную комбинацию  $\alpha^i \beta^j$ ,  $0 \leq i < a$ ,  $0 \leq j < b$ , с целыми коэффициентами, т. е. лежит в конечнопорожденном  $\mathbb{Z}$ -модуле. Таким образом,  $\mathbb{Z}[\alpha + \beta]$  и  $\mathbb{Z}[\alpha\beta]$  содержатся в конечнопорожденном  $\mathbb{Z}$ -модуле и, следовательно, конечно порождены.

По предыдущей лемме получаем, что  $\alpha + \beta, \alpha\beta \in \mathbb{A}$ . Так как  $\pm 1$  также лежат в  $A$ , то  $\mathbb{A} -$  подкольцо.  $\square$

**ТЕОРЕМА 11.3** (лемма Гаусса).  $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\alpha = h/k$ ,  $h, k \in \mathbb{Z}$  – несократимая дробь, удовлетворяющая уравнению  $\alpha^n = \sum_{i=0}^{n-1} m_i \alpha^i$ . Домножая обе части на  $k^n$  имеем:  $h^n = k \sum_{i=0}^{n-1} m_i k^{n-1-i} h^i$ . Все числа под знаком суммы целые, т.е.  $h^n$  делится на  $k$ . Но если  $k$  не обратим в  $\mathbb{Z}$ , то это противоречит несократимости дроби. Значит  $\alpha \in \mathbb{Z}$ , что и требовалось.  $\square$

Заметим, что из свойств целых чисел в доказательстве использовалось только факториальность, так что лемма Гаусса верна над любым факториальным кольцом. Этот факт будет использован в следующей главе.

## 12. Степени неприводимых представлений

**ЛЕММА 12.1.** Пусть  $\text{Irr}(G) = \{\pi_1, \dots, \pi_s\}$ ,  $\chi_i = \chi_{\pi_i}$ , а  $C_1 = \{1\}, C_2, \dots, C_s$  – классы сопряженных в  $G$ . Тогда для любых  $1 \leq p, q \leq s$

$$|C_p| \chi_q(g_p) = \lambda_{pq} \deg \pi_q$$

при некоторых  $\lambda_{pq} \in \mathbb{A}$  и любого  $g_p \in C_p$ .

**ДОКАЗАТЕЛЬСТВО.** Из предложения 8.4 следует, что элементы  $c_i = \sum_{g \in C_i} g$  образуют базис центра групповой алгебры  $FG$ . Так как  $c_i c_j$  также лежит в центре  $FG$ , то

$$c_i c_j = \sum_{k=1}^s \alpha_{ijk} c_k$$

для некоторых  $\alpha_{ijk} \in \mathbb{N}_0$  (число  $\alpha_{ijk}$  равно количеству решений уравнения  $xy = z$ , где  $x \in C_i$ ,  $y \in C_j$ , а  $z$  – фиксированный элемент из  $C_k$ ). Так как  $c_i$  центральны, то  $\pi_j(c_i)$  коммутирует с  $\pi_j(g)$  для всех  $g \in G$ . Следовательно,  $\pi_j(c_i)$  является эндоморфизмом неприводимого представления  $\pi_j$ . По лемме Шура над замкнутым полем любой такой эндоморфизм является гомотетией, т.е.  $\pi_j(c_i) = \lambda_{ji} E$ .

Вычисляя следы получаем

$$\text{Tr}(\pi_j(c_i)) = \text{Tr}\left(\sum_{g \in C_i} \pi_j(g)\right) = \sum_{g \in C_i} \chi_j(g) = |C_i| \chi_j(g_i) = \lambda_{ji} \deg \pi_j, \text{ где } g_i \in C_i.$$

Применяя  $\pi_r$  к вынесенной формуле, получаем  $\pi_r(c_i) \pi_r(c_j) = \sum_{k=1}^s \alpha_{ijk} \pi_r(c_k)$ , откуда  $\lambda_{ri} \lambda_{rj} = \sum_{k=1}^s \alpha_{ijk} \lambda_{rk}$ . Последнее равенство переписывается в виде  $\sum_{k=1}^s (\alpha_{ijk} - \delta_{ik} \lambda_{rj}) \lambda_{rk} = 0$ . Зафиксируем  $r$  и  $j$ . При  $i = 1, \dots, s$  получим однородную систему линейных уравнений с матрицей  $A - \lambda_{rj} E$ , где  $a_{ik} = \alpha_{ijk}$ . Так как  $\chi_r(1) \neq 0$ , то  $\lambda_{r1} \neq 0$ , поэтому система имеет ненулевое решение. Следовательно,  $\det(A - \lambda_{rj} E) = 0$ . Таким образом,  $\lambda_{rj}$  являются корнями характеристического многочлена целочисленной матрицы, в частности, целыми алгебраическими числами.  $\square$

**ТЕОРЕМА 12.2.** Степень неприводимого представления делит порядок группы.

**ДОКАЗАТЕЛЬСТВО.** Так как любой элемент конечной группы имеет конечный порядок, то все собственные числа матрицы  $\pi(g)$  являются корнями из 1 для любого представления  $\pi$  и любого  $g \in G$ . Поэтому  $\chi(g)$  является суммой корней из 1 для любого характера  $\chi$ . По теореме 11.2  $\chi(g) \in \mathbb{A}$ . Первое соотношение ортогональности 6.4 показывает, что в обозначениях предыдущей леммы

$$\sum_{p=1}^s |C_p| \chi_q(g_p) \chi_q(g_p^{-1}) = |G|.$$

Подставляя сюда равенство из предыдущей леммы имеем

$$\sum_{p=1}^s \deg \pi_q \lambda_{pq} \chi_q(g_p^{-1}) = |G| \iff \frac{|G|}{\deg \pi_q} = \sum_{p=1}^s \lambda_{pq} \chi_q(g_p^{-1}).$$

По теореме 11.2  $|G|/\deg \pi_q \in \mathbb{A}$ . А так как эта дробь очевидно рациональна, то по лемме Гаусса она целая.  $\square$

Этот результат можно уточнять и далее.

**ТЕОРЕМА 12.3.** Пусть  $\pi$  – неприводимое представление  $n$  группы  $G$ , а  $A$  – абелева нормальная подгруппа. Тогда  $\deg \pi$  делит  $|G : A|$ .

Если  $A \leq G$  абелева подгруппа, то, вообще говоря, неверно, что  $\deg \pi$  делит  $|G : A|$ . Однако в любом случае можно утверждать, что  $\deg \pi \leq |G : A|$ .

Доказательство этих результатов требует более продвинутой техники, поэтому мы его опускаем.

### 13. Индуцированные представления

Пусть  $\varphi : A \rightarrow B$  – гомоморфизм колец (некоммутативных с 1). Если  $M$  – левый  $B$ -модуль, то его можно рассматривать как левый  $A$ -модуль, задав умножение по правилу  $a \cdot m := \varphi(a)m$ . Нетрудно видеть, что это сопоставление определяет функтор  $\varphi^\# : B\text{-Mod} \rightarrow A\text{-Mod}$ . Этот функтор называется ограничением (в случае, когда  $\varphi$  инъективно, это действительно ограничивает множество “скаляров”). Если задан гомоморфизм групп  $G \rightarrow H$ , то представление группы  $H$  индуцирует представление группы  $G$ . Мы использовали это в случае  $H = G/[G, G]$  при построении таблиц характеров.

Левым сопряженным к функтору ограничения будет функтор тензорного домножения на  $B$ . Действительно,  $\varphi$  задает на  $B$  структуру правого  $A$ -модуля, поэтому левый  $A$ -модуль  $M$  можно тензорно домножить на  $B$  над  $A$ . Структура левого  $B$ -модуля задается на разложимых тензорах посредством  $b' \cdot (b \otimes m) := (b'b) \otimes m$ . Этот функтор называется индуцированием и обозначается  $\varphi_\# : A\text{-Mod} \rightarrow B\text{-Mod}$ .

До сих пор мы изучали только тензорные произведения над коммутативными кольцами, поэтому сформулируем хотя бы определения для некоммутативного случая. Пусть  $A$  – кольцо,  $M$  – левый, а  $N$  – правый  $A$ -модуль. Так как  $M$  и  $N$  – абелевы группы, то можно образовать абелеву группу  $N \otimes_{\mathbb{Z}} M$ . Тогда  $N \otimes_A M := N \otimes_{\mathbb{Z}} M / K$ , где  $K$  – подгруппа, порожденная всеми элементами  $na \otimes m - n \otimes am$ ,  $a \in A$ ,  $m \in M$ ,  $n \in N$ .

Если  $N$  – левый  $B$ -модуль, правый  $A$ -модуль, и имеет место внешняя ассоциативность:  $(bn)a = b(na)$  для любых  $b \in B$ ,  $n \in N$  и  $a \in A$ , то  $N$  называется  $B$ - $A$ -бимодулем. Если  $N$  является  $B$ - $A$ -бимодулем, то на  $N \otimes_A M$  естественно определена структура левого  $B$ -модуля:  $b \cdot (n \otimes m) := (bn) \otimes m$ . Проверка корректности последнего определения использует, в частности, внешнюю ассоциативность.

Вернемся к ситуации, когда задан гомоморфизм колец  $\varphi : A \rightarrow B$ . Тот факт, что функторы  $\varphi_\#$  и  $\varphi^\#$  сопряжены, выражается следующим универсальным свойством (см. теорему 6.2 главы 9):

$$\begin{array}{ccc} M & \xrightarrow{m \mapsto 1 \otimes m} & B \otimes_A M \\ & \searrow & \downarrow \\ & & N \end{array}$$

Для любого  $A$ -линейного отображения  $A$ -модуля  $M$  в  $B$ -модуль  $N$  существует единственное  $B$ -линейное отображение  $B \otimes_A M \rightarrow N$ , для которого эта диаграмма коммутативна.

Пусть  $H \leq G$ , а  $V$  – (левый)  $FH$ -модуль. Функторы ограничения и индуцирования, соответствующие вложению  $H$  в  $G$  обозначаются  $\text{res}_H^G$  и  $\text{ind}_H^G$ . Таким образом, индуцированный

модуль определяется как  $\text{ind}_H^G(V) = V^G = FG \otimes_{FH} V$ . Построим этот модуль явно. Пусть  $G = g_1H \sqcup \dots \sqcup g_nH$  – разбиение  $G$  на левые смежные классы по  $H$  ( $g_1 = 1$ ). Каждый элемент групповой алгебры  $FG$  однозначно представляется в виде  $g_1x_1 + \dots + g_nx_n$ , где  $x_i \in FH$ . Иными словами,  $FG$  является свободным правым  $FH$ -модулем с базисом  $g_1, \dots, g_n$ . Таким образом,  $V^G = g_1 \otimes V \oplus \dots \oplus g_n \otimes V \cong V^n$ , как  $F$ -модуль. Поэтому  $\dim_F V^G = |G : H| \cdot \dim_F V$ . Каждый элемент  $V^G$  однозначно записывается в виде суммы  $g_1 \otimes v_1 + \dots + g_n \otimes v_n$ . Если  $u_1, \dots, u_m$  базис  $V$  над  $F$ , то  $g_i \otimes u_j$  представляет собой  $F$ -базис  $V^G$ . Посмотрим на индуцированное представление на матричном языке. Пусть  $\pi : H \rightarrow \text{GL}(V)$  – матричное представление, соответствующее  $FH$ -модулю  $V = F^m$ . Возьмем следующий (упорядоченный)  $F$ -базис модуля  $V^G$ :  $g_1 \otimes e_1, \dots, g_1 \otimes e_m, \dots, g_n \otimes e_1, \dots, g_n \otimes e_m$ . Пусть  $g \in G$ . Запишем в этом базисе матрицу  $\pi_g^G$  умножения на элемент  $g$ . Пусть  $gg_i = g_k h$  для некоторого  $k = k(i) \in [n]$  и  $h \in H$ . Тогда  $h = g_k^{-1} g g_i$ . Получим  $g \cdot (g_i \otimes e_j) = g_k h \otimes e_j = g_k \otimes h e_j = g_k \otimes (\pi_h)_{*j}$ .

Доопределим  $\pi$  до функции  $G \rightarrow M_m(F)$ , положив  $\pi_g = 0$  при всех  $g \in G \setminus H$ . Тогда в выбранном базисе матрица индуцированного представления  $\pi^G = \text{ind}_H^G(\pi) : G \rightarrow \text{GL}(V^G)$  имеет блочный вид:

$$\pi_g^G = \begin{pmatrix} \pi_{g_1^{-1}gg_1} & \dots & \pi_{g_1^{-1}gg_n} \\ \vdots & \dots & \vdots \\ \pi_{g_n^{-1}gg_1} & \dots & \pi_{g_n^{-1}gg_n} \end{pmatrix}$$

(в каждом столбце ровно 1 ненулевой блок, а так как матрица обратима, то и в каждой строке тоже). Заметим, что на категории матричных представлений  $\text{ind}_H^G$  становится функтором только после выбора трансверсали.

Пусть  $H \leq G$ ,  $\pi : H \rightarrow \text{GL}(V)$  – линейное представление,  $g \in G$ , а  $g_1, \dots, g_n$  – представители левых смежных классов  $G$  по  $H$ .

**УПРАЖНЕНИЕ 13.1.** Представление  $(1_H)^G$  является перестановочным. Оно соответствует действию  $G$  на множестве смежных классов  $G/H$ . В частности,  $(1_1)^G$  – левое регулярное представление группы  $G$ .

УКАЗАНИЕ. Рассмотрите действие  $g$  на базисе  $g_i \otimes 1$ . □

**УПРАЖНЕНИЕ 13.2.** Пусть  $H \leq K \leq G$ . Тогда  $\text{ind}_K^G(\text{ind}_H^K(V)) = \text{ind}_H^G(V)$ .

РЕШЕНИЕ.  $FG \otimes_{FK} (FK \otimes_{FH} V) \cong (FG \otimes_{FK} FK) \otimes_{FH} V \cong FG \otimes_{FH} V$ . □

**УПРАЖНЕНИЕ 13.3.** Если представление  $\pi$  точное, то  $\pi^G$  тоже точное.

РЕШЕНИЕ. Предположим, что  $g$  действует тривиально на базисе  $g_i \otimes u_j$ . Если  $gg_i \notin g_iH$ , то  $g \cdot (g_i \otimes u_j) \notin g_i \otimes V$ . Значит  $gg_i = g_i h$  для некоторого  $h \in H$ .  $g \cdot (g_i \otimes u_j) = g_i \otimes h u_j = g_i \otimes u_j$  при всех  $j$ . Так как  $H$  действует точно, то из этого следует  $h = 1$ , откуда  $g = 1$ . □

**УПРАЖНЕНИЕ 13.4.** Пусть  $U$  – левый  $FG$ -модуль,  $U = U_1 \oplus \dots \oplus U_n$  как векторные пространства над  $F$ , причем  $G$  переставляет  $U_i$  транзитивно. Обозначим через  $H$  стабилизатор подпространства  $U_1$ . Тогда  $U_1$  является  $FH$ -модулем и  $U \cong \text{ind}_H^G(U_1)$ .

РЕШЕНИЕ. Зададим гомоморфизм  $FG \otimes_{FH} U_1 \rightarrow U$  на разложимых тензорах по правилу  $g_i \otimes u \mapsto g_i u$  и продолжим по линейности. Ясно, что это – гомоморфизм  $FG$ -модулей. Транзитивность действия  $G$  на наборе  $U_i$  обеспечивает сюръективность отображения. Заметим, что  $g_i u = g_j u' \implies g_j^{-1} g_i u = u' \in U_1 \implies g_j^{-1} g_i \in H$ , что невозможно при  $i \neq j$ . Поэтому  $\sum_{i=1}^n g_i u^{(i)} = 0 \iff g_i u^{(i)} = 0$  при всех  $i$ , откуда все  $u^{(i)} = 0$ . Из этого следует инъективность. □

Индуцированный характер – это характер индуцированного представления. Пусть  $H \leq G$ ,  $\pi$  – представление  $H$  с характером  $\chi$ , а  $\pi^G$  – индуцированное представление  $G$  с характером  $\chi^G$ .



Пусть, по-прежнему,  $g_1, \dots, g_n$  – представители левых смежных классов  $G$  по  $H$ . Из построения матрицы  $\pi_g^G$  видно, что ее след  $\chi_g^G$  равен сумме следов ненулевых диагональных клеток. Клетка стоит на диагонали, если  $g_i^{-1}gg_i \in H$ . Положим  $I(g) := \{i \in [n] \mid g_i^{-1}gg_i \in H\}$ . Тогда

$$\chi^G(g) = \sum_{i \in I(g)} \chi(g_i^{-1}gg_i).$$

Пусть  $s = g_i h \in g_i H$ . Заметим, что  $s^{-1}gs \in H \iff i \in I(g)$ , причем в этом случае  $s^{-1}gs = (g_i^{-1}gg_i)^h$  для  $h \in H$ , так что  $\chi(g_i^{-1}gg_i) = \chi(s^{-1}gs)$ . Поэтому

$$\chi^G(g) = \frac{1}{|H|} \sum_{s: s^{-1}gs \in H} \chi(s^{-1}gs).$$

Пусть  $H \leq G$ .

**ТЕОРЕМА 13.5** (Закон взаимности Фробениуса). *Для любых характеров  $\chi$  на  $H$  и  $\theta$  на  $G$  имеет место равенство*

$$B(\chi, \text{res}_H^G(\theta))_H = B(\text{ind}_H^G(\chi), \theta)_G.$$

ДОКАЗАТЕЛЬСТВО.

$$B(\text{ind}_H^G(\chi), \theta)_G = \frac{1}{|G|} \sum_{g \in G} \text{ind}_H^G(\chi)(g) \theta(g^{-1}) = \frac{1}{|H| \cdot |G|} \sum_{\substack{s, g \in G \\ s^{-1}gs \in H}} \chi(s^{-1}gs) \theta(g^{-1}).$$

Положив теперь  $s^{-1}gs = h \in H$  мы можем переписать эту сумму в виде

$$\frac{1}{|H| \cdot |G|} \sum_{h \in H, s \in G} \chi(h) \theta(sh^{-1}s^{-1}).$$

Так как  $\theta$  – функция классов на  $G$ , то  $\theta(sh^{-1}s^{-1}) = \theta(h^{-1})$  не зависит от  $s$ , и, значит, эта сумма равна

$$\frac{1}{|H|} \sum_{h \in H} \chi(h) \theta(h^{-1}) = B(\chi, \text{res}_H^G(\theta))_H.$$

□

**СЛЕДСТВИЕ 13.6.** *Предположим, что представления  $\pi$  группы  $H$  и  $\rho$  группы  $G$  неприводимы. Тогда кратность вхождения  $\pi$  в  $\text{res}_H^G(\rho)$  равна кратности вхождения  $\rho$  в  $\text{ind}_H^G(\pi)$ .*

## Многочлены

Все кольца в этой главе предполагаются коммутативными с 1

Кольца многочленов над коммутативным кольцом  $R$  являются свободными объектами в категории коммутативных  $R$ -алгебр с 1, т.е. образами левого сопряженного к забывающему функтору в множества. Соответственно, любое кольцо является факторкольцом какого-то кольца многочленов. Довольно часто вопросы о произвольных коммутативных кольцах можно свести к конечнопорожденным кольцам. Поэтому важно изучать кольца многочленов над  $R$  от конечного числа переменных.

В настоящей главе мы докажем, что такие кольца являются нетеровыми и факториальными, как только  $R$  обладает этими свойствами. Кроме того, мы докажем теорему Гильберта о нулях, которая является началом классической алгебраической геометрии, изучим симметрические многочлены, играющие важнейшую роль в теории Галуа, а также узнаем, что такое базисы Грёбнера – инструмент позволяющий алгоритмически определять, является ли полиномиальное тождество следствием нескольких данных или нет. Стоит отметить, что базисы Грёбнера (единственная система образующих идеала кольца многочленов, удовлетворяющая определенным свойствам) являются важнейшей частью современных систем компьютерной алгебры.

### 1. Определения кольца многочленов

Мы уже знаем несколько определений кольца многочленов. Давайте их перечислим. Пусть  $R$  – коммутативное кольцо с 1 (различные обобщения на некоммутативные кольца коэффициентов оставляются читателю в качестве упражнения). Введем обозначения:  $T = \{t_1, \dots, t_n\}$ ,  $R[T] = R[t_1, \dots, t_n]$  – кольцо многочленов над  $R$  от переменных  $t_1, \dots, t_n$  – то, что мы сейчас определим. Если  $k = (k_1, \dots, k_n) \in \mathbb{N}_0^n$  – мультииндекс, то положим  $T^k := t_1^{k_1} \cdot \dots \cdot t_n^{k_n}$ . Сложение мультииндексов производится покомпонентно.

Мы пишем все определения для конечного множества  $T$ , однако конечность существенна только для рекурсивного определения.

- (1) Школьное определение.  $R[T] = \{ \sum_{k \in \mathbb{N}_0^n} \alpha(k) T^k \mid \alpha : \mathbb{N}_0^n \rightarrow R \text{ – финитная функция} \}$ . Вместо

$\alpha(k)$  пишут  $\alpha_k$ . Операции определены следующим образом:

$$\begin{aligned} \sum_{k \in \mathbb{N}_0^n} \alpha_k T^k + \sum_{k \in \mathbb{N}_0^n} \beta_k T^k &= \sum_{k \in \mathbb{N}_0^n} (\alpha_k + \beta_k) T^k, \\ \left( \sum_{k \in \mathbb{N}_0^n} \alpha_k T^k \right) \cdot \left( \sum_{k \in \mathbb{N}_0^n} \beta_k T^k \right) &= \sum_{k \in \mathbb{N}_0^n} \left( \sum_{i, j \in \mathbb{N}_0^n, i+j=k} (\alpha_i \beta_j) \right) T^k. \end{aligned}$$

- (2) То же самое с использованием понятия свободного модуля.  $R[T]$  – это  $R$ -алгебра, которая является свободным  $R$ -модулем с множеством образующих  $\{T^k \mid k \in \mathbb{N}_0^n\}$ , а умножение на базисных элементах задается формулой  $T^i T^j = T^{i+j}$ . Так как умножение в  $R$ -алгебре  $R$ -билинейно, то на базисе оно может быть задано произвольно, а затем продолжено единственным образом. Для линейного отображения это просто определение свободного модуля, для билинейного – применение определения 2 раза.
- (3) Рекурсивное определение:  $R[t_1, \dots, t_n] = R[t_1, \dots, t_{n-1}][t_n]$ . При этом кольцо многочленов от одной переменной определяем одним из вышеуказанных способов. Это

определение полезно для доказательств по индукции. Доказательство того, что оно эквивалентно предыдущим – рутинно.

- (4) Если  $\mathcal{P}$  – левый сопряженный к забывающему функтору из категории коммутативных  $R$ -алгебр в категорию множеств, то  $R[T] = \mathcal{P}(T)$ . Другими словами,  $R[T]$  – это  $R$ -алгебра, содержащая множество  $T$ , такая что любая функция из  $T$  в  $R$ -алгебру  $A$  однозначно продолжается до гомоморфизма  $R$ -алгебр  $R[T] \rightarrow A$ . Это универсальное свойство уже отмечалось в примерах 5.1 и 6.1 главы 9. Доказательство аналогично доказательству предложения 14.2 главы 4.
- (5) Кольцо многочленов  $R[T]$  – это симметрическая алгебра свободного  $R$ -модуля с базисом  $T$ . Эквивалентность этого определения предыдущему обсуждалась в теореме 3.3 главы 10.

## 2. Нетеровость кольца многочленов

Настоящий параграф посвящен доказательству следующего результата.

**ТЕОРЕМА 2.1** (теорема Гильберта о базисе). *Кольцо многочленов от конечного числа переменных над нетеровым кольцом нетерово.*

Пусть  $R$  – кольцо, а  $R[t]$  – кольцо многочленов над  $R$ . Обозначим через  $R[t]_m$  подмодуль в  $R[t]$ , состоящий из многочленов, степени не выше  $m$ . Ясно, что это модуль (свободно) порожден элементами  $t^k$ ,  $k = 0, \dots, m$ . В доказательстве теоремы мы сведем вопрос о конечнопорожденности идеала к конечнопорожденности подмодуля в  $R[t]_m$ .

**ЛЕММА 2.2.** *Кольцо  $R$  нетерово тогда и только тогда, когда любой подмодуль любого конечнопорожденного  $R$ -модуля конечно порожден.*

**ДОКАЗАТЕЛЬСТВО.** Если любой подмодуль регулярного  $R$ -модуля (т.е. любой идеал кольца  $R$ ) конечнопорожден, то по предложению 9.2 главы 4  $R$  нетерово.

Обратно, пусть  $M = \langle x_1, \dots, x_m \rangle_R$  – конечнопорожденный  $R$ -модуль, а  $N \leq M$ . Зададим эпиморфизм свободного  $R$ -модуля  $R^m$  на  $M$  по формуле  $a \mapsto \sum_{i=1}^m x_i a_i$ . Пусть  $N'$  – полный прообраз  $N$  под действием этого гомоморфизма. Ясно, что из конечнопорожденности  $N'$  следует конечнопорожденность  $N$ . Индукцией по  $m$  докажем, что  $N'$  конечнопорожден. Пусть  $\pi : R^m \rightarrow R$  – проекция на последнюю компоненту, т.е.  $\pi(a) = a_m$ . Образ подмодуля – подмодуль, поэтому  $\pi(N')$  идеал в  $R$ . Так как  $R$  нетерово, то этот идеал конечнопорожден, скажем множеством  $\{\alpha_1, \dots, \alpha_n\}$ . Выберем прообразы  $y_i \in \pi^{-1}(\alpha_i)$ . Тогда  $N' = \langle y_1, \dots, y_n \rangle + N' \cap \text{Ker } \pi$  (см. доказательство теоремы 8.2 главы 6). По индукционному предположению  $N' \cap \text{Ker } \pi$ , являющийся подмодулем в свободном модуле  $\text{Ker } \pi \cong R^{m-1}$ , конечнопорожден. Следовательно, и  $N'$  конечнопорожден.  $\square$

**ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ.** Применяя индукцию по количеству переменных и рекурсивное определение кольца многочленов, легко свести задачу к случаю одной переменной.

Для подмножества  $X \subseteq R[t]$  обозначим через  $L(X)$  множество старших коэффициентов многочленов из  $X$ . Легко видеть, что если  $X$  – идеал в  $R[t]$ , то  $L(X)$  – идеал в  $R$ . Действительно, если  $\alpha, \beta \in L(X)$ , то существуют многочлены  $p = \alpha t^m + \dots$  и  $q = \beta t^k + \dots$  из  $X$ . Тогда  $\gamma p = \gamma \alpha t^m + \dots \in X$ , откуда  $\gamma \alpha \in L(X)$  для любого  $\gamma \in R$ . Считая для определенности, что  $m \geq k$  имеем  $t^{m-k}q + p = (\alpha + \beta)t^m + \dots \in X$ , откуда  $\alpha + \beta \in L(X)$ .

Пусть  $I$  – идеал в  $R[t]$ . Так как  $R$  нетерово, то идеал  $L(I) \leq R$  конечно порожден, скажем, элементами  $\alpha_1, \dots, \alpha_n$ . Это значит, что существуют многочлены  $p_i = \alpha_i t^{m_i} + \dots \in I$ . Пусть  $q = \alpha t^k + \dots \in I$ , где  $k \geq m := \max m_i$ . Так как  $\alpha \in L(I)$ , то существуют  $\beta_i \in R$  такие, что  $\alpha = \sum \alpha_i \beta_i$ . Тогда  $\deg(q - \sum \beta_i t^{k-m_i} p_i) < k$ . Таким образом, вычитая линейную комбинацию многочленов  $p_1, \dots, p_n$  мы можем уменьшить степень любого многочлена из  $I$  до  $m-1$  (процесс аналогичен делению многочленов “в столбик”). Следовательно,  $I = \langle p_1, \dots, p_n \rangle_{R[t]} + I \cap R[t]_{m-1}$ .

По предыдущей лемме второе слагаемое правой части конечно порождено над  $R$ , следовательно,  $I$  конечно порожденный идеал, что завершает доказательство.  $\square$

### 3. Факториальность кольца многочленов

В этом параграфе мы покажем, что кольцо многочленов над факториальной областью целостности факториально. Также как и в предыдущем доказательстве, достаточно рассмотреть случай одной переменной. Для этого мы докажем полную версию леммы Гаусса и воспользуемся факториальностью кольца многочленов над полем частных кольца коэффициентов. Напомним, что по лемме 10.2 главы 4 факториальность нетерова кольца эквивалентна следующему условию: любой неприводимый элемент порождает простой идеал. Это равносильно также тому, что факторкольцо по главному идеалу, порожденному неприводимым элементом является областью целостности.

Пусть  $R$  – кольцо,  $I$  – идеал в  $R$ , а  $I[t]$  – идеал кольца  $R[t]$ , состоящий из многочленов с коэффициентами из  $I$ .

**ЛЕММА 3.1.**  $R[t]/I[t] \cong (R/I)[t]$ .

**ДОКАЗАТЕЛЬСТВО.** Определим очевидный эпиморфизм  $R[t] \rightarrow (R/I)[t]$  и посчитаем его ядро.  $\square$

**ЛЕММА 3.2** (лемма Гаусса). Пусть  $R$  – факториальная область целостности,  $\beta \in R$  – неприводимый элемент, а  $u, v \in R[t]$ . Если  $uv$  делится на  $\beta$  в кольце  $R[t]$ , то либо  $u$  либо  $v$  делится на  $\beta$  в  $R[t]$ .

**ДОКАЗАТЕЛЬСТВО.** Так как  $\beta$  неприводим, то идеал  $I = \beta R$  прост. По предыдущей лемме  $R[t]/I[t] \cong (R/I)[t]$  и, поэтому, является областью целостности. Образ  $uv$  в этом факторкольце равен нулю, следовательно, образ одного из многочленов равен нулю. Но это означает, что этот многочлен лежит в  $I[t] = \beta R[t]$ , т.е. делится на  $\beta$ .  $\square$

**ТЕОРЕМА 3.3** (лемма Гаусса). Пусть  $R$  – факториальная область целостности, а  $F$  – ее поле частных. Предположим, что коэффициенты многочлена  $p \in R[t]$  не имеют общих необратимых делителей. Тогда  $p$  неприводим в  $R[t]$  тогда и только тогда, когда он неприводим в  $F[t]$ .

**ДОКАЗАТЕЛЬСТВО.** Предположим, что  $p$  приводим в  $R[t]$ , т.е.  $p = uv$  для некоторых необратимых элементов  $u, v \in R[t]$ . Так как коэффициенты многочлена  $p$  не имеют общих необратимых делителей, то  $u, v \notin R$ . Но тогда  $p = uv$  – разложение на небратимые в  $F[t]$ , т.е.  $p$  приводим в  $F[t]$ .

Обратно, пусть  $p$  приводим в  $F[t]$ , т.е.  $p = uv$  для некоторых многочленов  $u, v \in F[t]$  ненулевой степени. Приводя коэффициенты многочленов  $u, v$  к общему знаменателю получим  $uv = \tilde{u}\tilde{v}/\alpha$  для некоторых  $\tilde{u}, \tilde{v} \in R[t]$  и  $\alpha \in R$ . Домножая на  $\alpha$  получаем  $\alpha p = \tilde{u}\tilde{v}$ . Для любого неприводимого делителя  $\beta$  элемента  $\alpha$  по предыдущей лемме либо  $\tilde{u}/\beta$ , либо  $\tilde{v}/\beta$  лежит в  $R[t]$ . Таким образом мы можем сократить все неприводимые делители элемента  $\alpha$  и получить разложение  $p$  на множители ненулевой степени в  $R[t]$ .  $\square$

**ТЕОРЕМА 3.4.** Кольцо многочленов от конечного числа переменных над факториальным кольцом факториально.

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство только для случая кольца многочленов над нетеровой факториальной областью целостности  $R$ . Тогда  $R[t]$  также нетерова область целостности, поэтому достаточно доказать, что каждый неприводимый элемент в  $R[t]$  прост, после чего воспользоваться индукцией по количеству переменных.

Пусть  $p$  – неприводимый элемент кольца  $R[t]$ . Если  $\deg p = 0$ , т.е.  $p \in R$ , то  $R[t]/(p) \cong (R/(p))[t]$  – область целостности за счет факториальности  $R$ . Иначе, коэффициенты  $p$  не имеют необратимых общих делителей. По предыдущей теореме  $p$  неприводим в  $F[t]$ , где

$F$  – поле частных  $R$ . Кольцо  $F[t]$  евклидово, следовательно факториальное, поэтому  $F[t]/pF[t]$  – область целостности. Ядро очевидного гомоморфизма  $R[t] \rightarrow F[t]/pF[t]$  равно  $R[t] \cap pF[t]$ , поэтому  $R[t]/(R[t] \cap pF[t])$  вкладывается в  $F[t]/pF[t]$  и, следовательно, является областью целостности. Если  $q = pu$  для  $q \in R[t]$  и  $u \in F[t]$ , то доказательство теоремы 3.3 показывает, что  $p$  делится в  $R[t]$  на любой неприводимый делитель общего знаменателя коэффициентов  $u$ . Так как это невозможно, то  $u \in R[t]$ . Таким образом,  $R[t] \cap pF[t] = pR[t]$ , следовательно,  $R[t]/pR[t]$  – область целостности, что и требовалось.  $\square$

#### 4. Теорема Гильберта о нулях и основы алгебраической геометрии

В этом параграфе мы построим взаимно однозначное соответствие между радикальными идеалами кольца многочленов и алгебраическими множествами в аффинном пространстве, что является основой классической алгебраической геометрии. Для этого нам потребуется несколько сведений о целых расширениях колец и полей.

Пусть  $A \subseteq B$  – пара колец. Элемент  $\beta \in B$  называется целым над  $A$ , если он является корнем унитарного многочлена с коэффициентами из  $A$  (таким образом, целые алгебраические числа – это комплексные числа целые над  $\mathbb{Z}$ ). Кольцо  $B$  называется целым над  $A$  (или целым расширением  $A$ ), если все элементы являются целыми над  $A$ . Целое расширение поля называется алгебраическим расширением. Если  $B$  – конечнопорожденный  $A$ -модуль, то  $B$  называется конечным расширением  $A$ . Легко видеть, что элемент  $\beta \in B$  является целым над  $A$  тогда и только тогда, когда  $A[\beta]$  является конечным расширением  $A$ . Это соображение уже использовалось в параграфе 11 главы 11. Для нетеровых колец любое конечное расширение является целым.

**ЛЕММА 4.0.** *Пусть  $A$  – нетерово кольцо. Конечное расширение  $B$  кольца  $A$  является целым.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\beta \in B$ . Если  $B$  является конечнопорожденным  $A$ -модулем, то по лемме 2.2  $A[\beta]$  также является конечно порожденным  $A$ -модулем. Если он порожден элементами  $p_1(\beta), \dots, p_m(\beta)$  для некоторых  $p_1, \dots, p_m \in A[t]$ , а  $d > \max(\deg p_i)$ , то существуют элементы  $a_1, \dots, a_m \in A$  такие, что  $\beta^d = \sum_i a_i p_i$ , что и означает, что  $\beta$  является корнем унитарного многочлена.  $\square$

**ЛЕММА 4.1.** *Последовательность конечных расширений является конечным расширением.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $A \subseteq B \subseteq C$  – кольца, причем  $\beta_1, \dots, \beta_n$  порождают  $B$ , как  $A$ -модуль, а  $\gamma_1, \dots, \gamma_m$  порождают  $C$ , как  $B$ -модуль. Тогда любой элемент  $\gamma \in C$  представляется в виде  $\gamma = \sum_i \gamma_i \delta_i = \sum_{i,j} \gamma_i \beta_j \varepsilon_{ij}$ , где  $\delta_i \in B$ , а  $\varepsilon_{ij} \in A$ . Таким образом,  $C$  порождено элементами  $\gamma_i \beta_j$ ,  $i = 1, \dots, n$ ,  $j = 1, \dots, m$  как  $A$ -модуль. Для более длинных последовательностей конечных расширений работает индукция по длине последовательности.  $\square$

**ЛЕММА 4.2.** *Пусть  $B$  является целым над  $A$ . Если  $B$  – поле, то и  $A$  – поле.*

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\alpha \in A \setminus \{0\}$ . Так как  $B$  – поле, то  $1/\alpha \in B$  является целым над  $A$ . Следовательно,  $\frac{1}{\alpha^n} + \frac{\gamma_{n-1}}{\alpha^{n-1}} + \dots + \gamma_0 = 0$  для некоторых  $\gamma_i \in A$ . Умножая на  $\alpha^n$ , получаем  $1 + \gamma_{n-1}\alpha + \dots + \gamma_0\alpha^n = 0$ , откуда  $1/\alpha = -\gamma_{n-1} - \dots - \gamma_0\alpha^{n-1} \in A$ .  $\square$

При доказательстве основной теоремы мы получим, что поле является целым расширением главной локализации кольца многочленов. Предыдущая и следующая леммы показывают, что это невозможно.

**ЛЕММА 4.3.** *Пусть  $p \in F[t]$ . Тогда главная локализация  $F[t]_p = F[t, p^{-1}]$  не является полем.*

**ДОКАЗАТЕЛЬСТВО.** По теореме 18.1 главы 4 в кольце  $F[t]$  существует бесконечно много неприводимых многочленов. Пусть  $q$  – неприводимый многочлен, не делящий  $p$ . Если  $F[t]_p$  –

поле, то  $\frac{1}{q} = \frac{c}{p^m}$  для некоторых  $c \in F[t]$  и  $m \in \mathbb{N}$ , откуда  $cq = p^m$ . Так как  $p^m$  делится на  $q$  в  $F[t]$ , а  $q$  неприводим, то  $p$  делится на  $q$  – противоречие.  $\square$

**ЛЕММА 4.4.** Пусть  $F$  – поле, а  $I$  – максимальный идеал в кольце многочленов  $F[t_1, \dots, t_n]$ . Поле  $K = F[t_1, \dots, t_n]/I$  является конечным расширением  $F$  тогда и только тогда, когда  $I \cap F[t_k] \neq 0$  для любого  $k = 1, \dots, n$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $\tau_1, \dots, \tau_n$  – образы  $t_1, \dots, t_n$  в  $K$ . Если  $K$  – конечномерно над  $F$ , то  $\tau_k$  является целым над  $F$ , т.е.  $p(\tau_k) = 0$  для некоторого ненулевого многочлена  $p \in F[t_k]$ , а это означает, что  $p \in I$ .

Обратно, так как  $I \cap F[t_k] \neq 0$ , то  $\tau_k$  является корнем ненулевого многочлена с коэффициентами из  $F$ . Поэтому  $F \subseteq F[\tau_1] \subseteq \dots \subseteq F[\tau_1, \dots, \tau_n] = K$  – последовательность конечных расширений, которая по лемме 4.1 является конечным расширением.  $\square$

**ТЕОРЕМА 4.5.** Пусть  $F$  – поле, а  $I$  – максимальный идеал в кольце многочленов  $F[t_1, \dots, t_n]$ . Тогда  $K = F[t_1, \dots, t_n]/I$  – конечное расширение поля  $F$ .

**ДОКАЗАТЕЛЬСТВО.** Проведем доказательство индукцией по  $n$ . Случай  $n = 1$  очевиден. Предположим, что  $I \cap F[t_k] = 0$  для некоторого  $k$ . Для определенности будем считать, что  $I \cap F[t_1] = 0$ . Так как  $K$  – поле, то канонический гомоморфизм  $F[t_1, \dots, t_n] \rightarrow K$  пропускается через локализацию кольца  $F[t_1, \dots, t_n]$  в мультипликативном подмножестве  $F[t_1] \setminus \{0\}$  равную  $R = F(t_1)[t_2, \dots, t_n]$ . Очевидно, что индуцированный гомоморфизм  $R \rightarrow K$  сюръективен, поэтому его ядро – максимальный идеал. По индукционному предположению  $K$  является конечным расширением поля  $F(t_1)$ .

Пусть  $\tau_2, \dots, \tau_n$  – образы  $t_2, \dots, t_n$  в  $K$ . Так как расширение  $F(t_1) \subseteq K$  конечно, то  $\tau_k$  является корнем некоторого унитарного многочлена  $f_k \in F(t_1)[t_k]$ . Пусть  $p \in F[t_1]$  – общий знаменатель всех коэффициентов многочленов  $f_k$ . Тогда элементы  $\tau_k$  являются целыми над подкольцом  $F[t_1]_p = F[t_1, p^{-1}]$ . По леммам 4.1 и 4.0  $K$  – целое расширение  $F[t_1]_p$ , следовательно, по лемме 4.2  $F[t_1]_p$  является полем. Но это противоречит лемме 4.3.

Противоречие показывает, что равенство  $F[t_k] \cap I = \{0\}$  невозможно, а по лемме 4.4 из этого следует, что  $K$  – конечное расширение  $F$ .  $\square$

Единичным идеалом кольца  $R$  называется идеал, содержащий 1, т.е. само кольцо, как идеал над собой. Смысл введения этого термина: выражение “порождает единичный идеал” уже уточняет, что кольцо порождается как идеал, а не как алгебра.

**ТЕОРЕМА 4.6** (Слабая теорема Гильберта о нулях). Пусть  $F$  – алгебраически замкнутое поле. Набор многочленов  $P \subseteq F[t_1, \dots, t_n]$  не имеет общих корней тогда и только тогда, когда  $P$  порождает единичный идеал кольца  $F[t_1, \dots, t_n]$ .

**ДОКАЗАТЕЛЬСТВО.** Если  $P$  имеет общий корень  $\tau \in F^n$ , то  $\sum_{p \in P} f_p(\tau)p(\tau) = 0$  для любых  $f_p \in F[t_1, \dots, t_n]$ . Поэтому равенство  $\sum_{p \in P} f_p p = 1$  невозможно.

Обратно, если  $P$  не порождает единичный идеал, то оно содержится в некотором максимальном идеале  $I \leq F[t_1, \dots, t_n]$ . По предыдущей теореме  $K = F[t_1, \dots, t_n]/I$  является конечным расширением  $F$ , следовательно, все элементы  $K$  алгебраические над  $F$ . Так как  $F$  замкнуто, то любой алгебраический над  $F$  элемент лежит в  $F$ . Таким образом,  $K = F$ . Пусть  $\tau_1, \dots, \tau_n$  – образы  $t_1, \dots, t_n$  в  $F$ . Тогда многочлены  $t_k - \tau_k$  лежат в идеале  $I$  (то же самое можно было бы доказать, исходя из того, что  $F[t_k] \cap I$  – ненулевой простой идеал в  $F[t_k]$ ). Легко видеть, что факторкольцо по идеалу, порожденному всеми  $t_k - \tau_k$  – поле, поэтому этот идеал максимален. Таким образом,  $I = \sum_k (t_k - \tau_k)F[t_1, \dots, t_n]$ , и точка  $(\tau_1, \dots, \tau_n)$  является общим корнем всех многочленов из  $I$ .  $\square$

**СЛЕДСТВИЕ 4.7.** Любой максимальный идеал кольца многочленов  $F[t_1, \dots, t_n]$  над замкнутым полем  $F$  порожден элементами  $t_1 - \tau_1, \dots, t_n - \tau_n$  для некоторых  $\tau_k \in F$ .

Обозначим через  $\text{Спекс } R$  – множество максимальных идеалов кольца  $R$ . Последнее следствие устанавливает биективное соответствие между  $\text{Спекс } F[t_1, \dots, t_n]$  аффинным пространством  $F^n$ . По теореме 4.5  $F[t_1, \dots, t_n]/I$  – конечное расширение  $F$ . Если  $F$  замкнуто, то оно равно  $F$ . Таким образом, мы установили биективное соответствие между множеством гомоморфизмов  $F$ -алгебр  $F[t_1, \dots, t_n] \rightarrow F$  и  $\text{Спекс } F[t_1, \dots, t_n] \cong F^n$ .

Для подмножества  $P \subseteq F[t_1, \dots, t_n]$  обозначим через  $V(P)$  множество общих корней всех многочленов из  $P$ . Такое множество называется алгебраическим множеством или аффинным алгебраическим многообразием. Заметим, что  $V(P) = V(\langle P \rangle)$ , где  $\langle P \rangle$  обозначает идеал, порожденный  $P$ . Если  $I$  – произвольный идеал кольца  $F[t_1, \dots, t_n]$ , то множество максимальных идеалов, содержащих  $I$ , взаимно однозначно соответствует множеству максимальных идеалов факторкольца  $F[t_1, \dots, t_n]/I$ . Легко видеть, что максимальный идеал, порожденный элементами  $t_1 - \tau_1, \dots, t_n - \tau_n$ , содержит  $I$  тогда и только тогда, когда  $(\tau_1, \dots, \tau_n) \in V(I)$ . Таким образом, существует естественная биекция  $V(I) \cong \text{Спекс } F[t_1, \dots, t_n]/I \cong \text{Мор}_{F\text{-}\mathfrak{Alg}}(F[t_1, \dots, t_n]/I, F)$ . Если  $I$  – идеал всех многочленов, аннулирующих алгебраическое подмножество  $X \subseteq F^n$ , то кольцо  $F[t_1, \dots, t_n]/I$  называется аффинной алгеброй многообразия  $X = V(I)$ .

При помощи следующей теоремы устанавливается антиэквивалентность категорий аффинных алгебраических многообразий и конечнопорожденных редуцированных  $F$ -алгебр (коммутативное кольцо называется редуцированным, если оно не содержит нильпотентов).

**ТЕОРЕМА 4.8** (Теорема Гильберта о нулях). *Пусть  $F$  – алгебраически замкнутое поле,  $P \subseteq F[t_1, \dots, t_n]$ , а  $f \in F[t_1, \dots, t_n]$ . Для того чтобы  $f(V(P)) = 0$  необходимо и достаточно, чтобы многочлен  $f^d$  принадлежал идеалу, порожденному  $P$ , для некоторого натурального  $d$ .*

Если  $f^d$  принадлежит идеалу, порожденному  $P$ , то  $f^d(V(P)) = 0$ , откуда  $f(V(P)) = 0$ . Обратную импликацию выведем из слабой теоремы о нулях при помощи трюка Рабиновича.

**ДОКАЗАТЕЛЬСТВО.** В кольце многочленов  $F[t_0, \dots, t_n]$  рассмотрим подмножество  $P \cup \{1 + t_0 f\}$ . Для  $a \in F^n$ , если  $P(a) = 0$ , то  $1 + t_0 f(a) = 1$ , поэтому  $V(P \cup \{1 + t_0 f\}) = \emptyset$ . По слабой теореме о нулях множество  $P \cup \{1 + t_0 f\}$  порождает единичный идеал, т.е. существуют  $g, g_1, \dots, g_m \in F[t_0, \dots, t_n]$  и  $p_1, \dots, p_m \in P$  такие, что

$$(1 + t_0 f)g + \sum_{k=1}^m g_k p_k = 1.$$

Существует единственный гомоморфизм  $F[t_0, \dots, t_n]$ -алгебр  $F[t_0, \dots, t_n] \rightarrow F[t_1, \dots, t_n]_f$ , посылающий  $t_0$  в  $-1/f$ . Применяя его к выделенной формуле, получаем  $\sum h_k p_k = 1$ , где  $h_k = g_k(-1/f, t_1, \dots, t_n)$  – образ  $g_k$  при указанном гомоморфизме. Любой элемент локализации  $F[t_1, \dots, t_n]_f$  записывается в виде  $q/f^d$  для  $q \in F[t_1, \dots, t_n]$  и  $d \in \mathbb{N}_0$ . Записав все  $h_k$  в виде  $h_k = q_k/f^d$  для  $q_k \in F[t_1, \dots, t_n]$  и достаточно большого  $d$  и домножив на знаменатель, получим  $f^d = \sum q_k p_k$ , что и требовалось.  $\square$

Для подмножества  $X \subseteq F^n$  обозначим через  $I(X)$  множество многочленов, аннулирующих  $X$ . Легко проверить, что  $I(X)$  – идеал в  $F[t_1, \dots, t_n]$ , причем  $f^d \in I(X) \implies f \in I(X)$ . Идеалы, обладающие этим свойством, называются радикальными идеалами. Радикалом идеала  $J$  кольца  $R$  называется множество  $\sqrt{J} := \{r \in R \mid \exists d \in \mathbb{N} : r^d \in J\}$ . Так что идеал  $J$  радикальный  $\iff \sqrt{J} = J$ . Можно показать, что  $\sqrt{J}$  равен пересечению всех простых идеалов, содержащих  $J$ . Еще одна характеристика:  $\sqrt{J} = \rho_J^{-1}(\text{NRad } R/J)$  – полный прообраз нильпотентного радикала кольца  $R/J$  под действием канонического гомоморфизма  $R \rightarrow R/J$  (напомним, что  $\text{NRad } A$  – это множество всех нильпотентных элементов кольца  $A$ , которое называется нильпотентным радикалом  $A$ ). Таким образом, идеал  $J$  является радикальным тогда и только тогда, когда  $R/J$  не имеет нильпотентов.

Набор замкнутых подмножеств  $V(P) \subseteq F^n$ , где  $P \subseteq F[t_1, \dots, t_n]$ , задает топологию на  $F^n$ , которая называется топологией Зариского. Легко видеть, что  $V(I(X))$  является замыканием множества  $X$  в топологии Зариского. В то же время, теорема Гильберта о нулях утверждает, что  $I(V(P))$  является радикалом идеала, порожденного  $P$ . Таким образом, функции  $I$  и  $V$  являются взаимно обратными биекциями между замкнутыми по Зарискому подмножествами аффинного пространства и радикальными идеалами кольца многочленов.

Морфизмом аффинных многообразий  $X \subseteq F^n$  в  $Y \subseteq F^m$  называется полиномиальное отображение  $X \rightarrow Y$  (отображение  $X \rightarrow Y$  называется полиномиальным, если оно является сужением отображения  $F^n \rightarrow F^m$ , все координатные функции которого являются полиномиальными). Обратите внимание, что полиномиальные функции  $F^n \rightarrow F^m$ , переводящие  $X$  в  $Y$  и совпадающие на  $X$ , считаются равными морфизмами. Класс (множество) аффинных многообразий с таким набором морфизмов является категорией, которую мы будем обозначать через  $\mathcal{A}\mathfrak{f}\mathfrak{f} = \mathcal{A}\mathfrak{f}\mathfrak{f}/F$ . Многочлены  $f, g \in F[t_1, \dots, t_n]$  задают морфизмы  $\hat{f}, \hat{g} : X \rightarrow F$ . Эти морфизмы равны тогда и только тогда, когда  $f - g$  аннулирует  $X$ , т.е.  $f - g \in I(X)$ . Таким образом, аффинная алгебра  $F[X] := F[t_1, \dots, t_n]/I(X)$  многообразия  $X$  отождествляется с кольцом  $\text{Mor}(X, F)$  регулярных функций на  $X$  (на множестве  $\text{Mor}(X, F)$  структура кольца задается поточечными операциями сложения и умножения).

Как обычно,  $\text{Mor}_{\mathcal{A}\mathfrak{f}\mathfrak{f}/F}(-, F)$  задает контравариантный функтор  $\mathcal{A}\mathfrak{f}\mathfrak{f}/F \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}$ . После того как мы задали на  $\text{Mor}(X, F)$  структуру  $F$ -алгебры, можно считать, что этот функтор действует в категорию конечнопорожденных редуцированных  $F$ -алгебр, которую мы обозначим через  $\mathcal{A}$ . При этом каждому многообразию он сопоставляет его аффинную алгебру.

Для того чтобы определить функтор в обратную сторону, для каждой конечнопорожденной  $F$ -алгебры  $A$  выберем эпиморфизм  $\pi_A : F[t_1, \dots, t_n] \rightarrow A$  (это равносильно выбору конечного набора образующих в  $A$ ). Снова  $\mathcal{X} := \text{Mor}_{\mathcal{A}}(-, F)$  является контравариантным функтором  $\mathcal{A} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}$ . Множество  $\mathcal{X}(F[t_1, \dots, t_n])$  естественно отождествляется с  $F^n$  по формуле  $\varphi \mapsto (\varphi(t_1), \dots, \varphi(t_n))$ . Таким образом, множество  $\mathcal{X}(A)$  вкладывается в  $F^n = \mathcal{X}(F[t_1, \dots, t_n])$  посредством  $\psi \mapsto \psi \circ \pi_A$ . При этом множество  $\mathcal{X}(A) = V(\text{Ker } \pi_A)$  является алгебраическим многообразием с аффинной алгеброй  $A$ . Таким образом, функторы  $\text{Mor}_{\mathcal{A}\mathfrak{f}\mathfrak{f}/F}(-, F)$  и  $\mathcal{X}$  являются квази-обратными и задают антиэквивалентность категорий  $\mathcal{A}\mathfrak{f}\mathfrak{f}/F$  и  $\mathcal{A}$ .

## 5. Симметрические многочлены

Пусть  $R$  – область целостности. Многочлен  $f \in A := R[x_1, \dots, x_n]$  называется симметрическим, если он не меняется при перестановке аргументов. Более строго: определим правое действие симметрической группы  $S_n$  на  $A$  по правилу

$$f^\sigma(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Таким образом,  $\sigma \in S_n$  задает автоморфизм  $R$ -алгебры  $A$ . Множество неподвижных точек под действием автоморфизма является подалгеброй. Неподвижный элемент под действием всей группы  $S_n$  называется симметрическим многочленом. Множество всех симметрических многочленов является подалгеброй в  $A$ .

Рассмотрим многочлен

$$f(t) = (t - x_1) \dots (t - x_n) = t^n - s_1^{(n)} t^{n-1} + \dots + (-1)^n s_n^{(n)}$$

из кольца  $A[t]$ . Так как  $f$  не меняется при перестановке переменных  $x_1, \dots, x_n$ , его коэффициенты (с точностью до знака)  $s_1^{(n)}, \dots, s_n^{(n)}$  являются симметрическими многочленами из  $A$ . Они называются *элементарными симметрическими многочленами*. Верхний индекс  $(n)$  обычно опускается. Легко видеть, что  $s_1$  – сумма переменных,  $s_2$  – сумма всех попарных произведений переменных и т.д. Очевидно также, что  $\deg s_k = k$ , а  $s_k^{(n)}(x_1, \dots, x_{n-1}, 0) = s_k^{(n-1)}(x_1, \dots, x_{n-1})$ . Основная цель этого параграфа – доказать что любой симметрический многочлен единственным образом выражается, как многочлен от



элементарных симметрических многочленов. Другие свойства симметрических многочленов не так важны и будут разобраны в виде задач на практических занятиях.

**ТЕОРЕМА 5.1.** *Алгебра симметрических многочленов порождена элементарными симметрическими многочленами, которые являются алгебраически независимыми.*

*Другими словами, гомоморфизм  $R$ -алгебр  $\varphi : R[z_1, \dots, z_n] \rightarrow A$ , посылающий  $z_k$  в  $s_k$ , является инъективным, а его образ равен алгебре симметрических многочленов.*

Для доказательства нам понадобится линейно упорядочить (унитальные) одночлены в  $A$ . Введем следующие обозначения (часть из них использовалась в начале текущей главы).

- $X = (x_1, \dots, x_n)$ ;  $R[X] = R[x_1, \dots, x_n]$ .
- Если  $k = (k_1, \dots, k_n) \in \mathbb{N}_0^n$  – мультииндекс, то положим  $X^k := x_1^{k_1} \cdot \dots \cdot x_n^{k_n}$ .
- Сложение мультииндексов производится покомпонентно.
- Введем алфавитный порядок на множестве мультииндексов:  $k > \ell$ , если первый ненулевой член последовательности  $(k_1 - \ell_1, \dots, k_n - \ell_n)$  положителен.
- Будем называть мультииндекс  $k$  мультистепенью одночлена  $\alpha X^k$ , где  $\alpha \in R$ .
- Одночлен наибольшей мультистепени, входящий в многочлен  $f$  будет называться старшим членом  $f$  и обозначаться через  $LM(f)$  (leading monomial=leading term).

Перед доказательством теоремы сформулируем 2 несложные леммы.

**ЛЕММА 5.2.**  $LM(fg) = LM(f) \cdot LM(g)$ .

Моном  $\alpha X^k$  называется монотонным, если его мультистепень является монотонно убывающей последовательностью:  $k_1 \geq k_2 \geq \dots \geq k_n$ .

**ЛЕММА 5.3.** *Старший член симметричного многочлена является убывающим мономом.*

**ДОКАЗАТЕЛЬСТВО.** Если моном  $\alpha X^k$  входит в симметричный многочлен  $f$ , то и  $\alpha x_1^{k_1} \dots x_i^{k_{i+1}} x_{i+1}^{k_i} \dots x_n^{k_n}$  также входит в  $f$ . Поэтому, если  $\alpha X^k$  – старший моном, то  $k_i \geq k_{i+1}$  для любого  $i$ .  $\square$

**ВЫЧИСЛЕНИЕ ОБРАЗА  $\varphi$ .** Пусть  $f$  – симметричный многочлен, а  $\alpha X^k$  – его старший моном. Проведем доказательство индукцией по мультииндексу  $k$ . По лемме 5.2

$$LM(S^\ell) = LM(s_1^{\ell_1} s_2^{\ell_2} \dots s_n^{\ell_n}) = x_1^{\ell_1} (x_1 x_2)^{\ell_2} \dots (x_1 \dots x_n)^{\ell_n} = \prod_{i=1}^n x_i^{\sum_{j=i}^n \ell_j}.$$

Положив  $\ell_i = k_i - k_{i+1}$ , где  $k_{n+1} := 0$ , получим  $LM(\alpha S^\ell) = \alpha X^k$  (по лемме 5.3 все  $\ell_i$  неотрицательны). Следовательно, старшая мультистепень многочлена  $f - \alpha S^\ell$  меньше, чем у  $f$ . По индукционному предположению  $f - \alpha S^\ell \in R[S]$ , следовательно, и  $f \in R[S] = \text{Im } \varphi$ .  $\square$

На самом деле, в процессе доказательства мы получили соотношение между степенями исходного симметрического многочлена и того многочлена, через который он выражается.

**СЛЕДСТВИЕ 5.4.** *Пусть  $f \in R[X]$  – симметрический многочлен, а  $g \in R[z_1, \dots, z_n]$  таков, что  $f(X) = g(s_1(X), \dots, s_n(X))$ . Тогда  $\deg g = \deg_{x_1} f$  (здесь  $\deg_{x_1} f$  обозначает степень  $f$  по переменной  $x_1$ ).*

**ДОКАЗАТЕЛЬСТВО.** В обозначениях предыдущего доказательства степень  $g$  равна максимально возможной сумме  $\ell_1 + \dots + \ell_n = k_1$ . А максимальное  $k_1$  как раз и есть степень  $f$ , как многочлена от  $x_1$ . Осталось заметить, что разным мультииндексам  $k$  соответствуют разные мультииндексы  $\ell$ , поэтому одночлен старшей степени не может сократиться.  $\square$

**ВЫЧИСЛЕНИЕ ЯДРА  $\varphi$ .** Если  $g(s_1, \dots, s_n) = 0$ , то по предыдущему следствию  $\deg g = -\infty$ , т.е.  $g = 0$ . Это наблюдение завершает доказательство теоремы 5.1.  $\square$

## 6. Результат

Рассмотрим многочлены  $f(t) = \sum_{i=0}^n \alpha_i t^i$  и  $g(t) = \sum_{j=0}^m \beta_j t^j$ , где  $\alpha_i, \beta_j$  лежат в некоторой области целостности  $R$  с полем частных  $F$ , а  $\alpha_n, \beta_m \neq 0$ . В терминах коэффициентов  $\alpha_i, \beta_j$  мы хотим сформулировать утверждение о том, что многочлены  $f$  и  $g$  взаимно просты.

**ЛЕММА 6.1.** *Многочлены  $f, g \in F[t]$  не являются взаимно простыми тогда и только тогда, когда существуют ненулевые многочлены  $u, v \in F[t]$  такие, что  $uf = vg$ ,  $\deg u < m$ , а  $\deg v < n$ .*

**ДОКАЗАТЕЛЬСТВО.** Если  $d(t) := \gcd(f, g) \in F[t]$  имеет ненулевую степень, то можно взять  $u = g/d, v = f/d \in F[t]$ .

Обратно, пусть  $f$  и  $g$  взаимно просты, а  $uf = vg$  для некоторых ненулевых  $u, v \in F[t]$ . Существуют  $p, q \in F[t]$  такие, что  $fp + gq = 1$ . Тогда  $u = ufp + uqg = g(vp + uq)$ , откуда  $\deg u \geq m$ .  $\square$

Равенство  $uf = vg$  можно записать в виде системы линейных уравнений относительно коэффициентов многочленов  $u = u_{m-1}t^{m-1} + \dots + u_0$  и  $v = v_{n-1}t^{n-1} + \dots + v_0$ :

$$\begin{aligned} \alpha_n u_{m-1} &= \beta_m v_{n-1} \\ \alpha_{n-1} u_{m-1} + \alpha_n u_{m-2} &= \beta_{m-1} v_{n-1} + \beta_m v_{n-2} \\ &\dots\dots\dots \\ \alpha_0 u_0 &= \beta_0 v_0 \end{aligned}$$

Многочлены  $f$  и  $g$  имеют необратимый общий делитель тогда и только тогда, когда эта система имеет ненулевое решение, т. е. когда определитель матрицы этой системы равен нулю:

$$\begin{vmatrix} \alpha_n & 0 & \dots & 0 & -\beta_m & 0 & \dots & 0 \\ \alpha_{n-1} & \alpha_n & \dots & 0 & -\beta_{m-1} & -\beta_m & \dots & 0 \\ \alpha_{n-2} & \alpha_{n-1} & \ddots & 0 & -\beta_{m-2} & -\beta_{m-1} & \ddots & 0 \\ \vdots & \vdots & \ddots & \alpha_n & \vdots & \vdots & \ddots & -\beta_m \\ \alpha_0 & \alpha_1 & \dots & \vdots & -\beta_0 & -\beta_1 & \dots & \vdots \\ 0 & \alpha_0 & \ddots & \dots & 0 & -\beta_0 & \dots & \vdots \\ \vdots & \vdots & \ddots & \alpha_1 & \vdots & \dots & \ddots & -\beta_1 \\ 0 & \dots & 0 & \alpha_0 & 0 & \dots & \dots & -\beta_0 \end{vmatrix} = 0$$

Убирая минусы перед всеми  $\beta_j$  и транспонируя, получаем определитель матрицы

$$S(f, g) := \begin{pmatrix} \alpha_n & \dots & \dots & \dots & \alpha_0 & 0 & \dots & 0 \\ 0 & \alpha_n & \dots & \dots & \dots & \alpha_0 & 0 & \dots \\ \dots & \ddots & \ddots & \dots & \dots & \dots & \ddots & \ddots \\ 0 & \dots & 0 & \alpha_n & \dots & \dots & \dots & \alpha_0 \\ \beta_m & \dots & \dots & \dots & \beta_0 & 0 & \dots & 0 \\ 0 & \beta_m & \dots & \dots & \dots & \beta_0 & \dots & 0 \\ \dots & \ddots & \ddots & \dots & \dots & \dots & \ddots & \dots \\ 0 & \dots & 0 & \beta_m & \dots & \dots & \dots & \beta_0 \end{pmatrix}$$

который совпадает с предыдущим определителем с точностью до знака.

Матрицу  $S(f, g)$  называют матрицей Сильвестра многочленов  $f$  и  $g$ . Определитель матрицы  $S(f, g)$  называют *результантом* многочленов  $f$  и  $g$ . Мы будем обозначать его через  $r(f, g)$ . Если  $f$  и  $g$  – многочлены от нескольких переменных  $t, t_1, \dots, t_n$ , а мы хотим вычислить их результат как многочленов от  $t$  над кольцом многочленов от остальных переменных, то такой результат будет обозначаться через  $r_t(f, g)$ . Ясно, что  $r(f, g)$  – однородный многочлен степени  $m$  по переменным  $\alpha_i$ , и степени  $n$  по переменным  $\beta_j$ .

**ПРЕДЛОЖЕНИЕ 6.2.** *Многочлены  $f$  и  $g$  имеют необратимый общий делитель тогда и только тогда, когда  $r(f, g) = 0$ .*

Результант имеет много разных приложений. Например, можно исключать переменные из системы полиномиальных уравнений.

**ПРЕДЛОЖЕНИЕ 6.3.** *Пусть  $f, g \in F[x, y_1, \dots, y_n]$ . Рассмотрим  $f$  и  $g$ , как многочлены от  $x$  и вычислим их результат  $r = r_x(f, g) \in F[y_1, \dots, y_n]$ . Если  $f(\lambda, \mu_1, \dots, \mu_n) = g(\lambda, \mu_1, \dots, \mu_n) = 0$  для некоторых  $\lambda, \mu_1, \dots, \mu_n \in F$ , то  $r(\mu_1, \dots, \mu_n) = 0$ .*

ДОКАЗАТЕЛЬСТВО. Многочлены  $f(x, \mu_1, \dots, \mu_n)$  и  $g(x, \mu_1, \dots, \mu_n) \in F[x]$  имеют общий корень  $x = \lambda$ . Поэтому  $r(\mu_1, \dots, \mu_n) = 0$ .  $\square$

Сейчас мы хотим представить результат  $r(f, g)$  в виде линейной комбинации  $r(f, g) = pf + qg$ . При такой постановке задачи это очевидно: если  $f, g$  взаимно просты, то можно представить любой многочлен, а если нет, то  $r(f, g) = 0$  и подойдут  $p = q = 0$ . Но мы хотим написать “естественное” представление, то есть представление, для которого коэффициенты многочленов  $p$  и  $q$  полиномиально зависят от коэффициентов  $f$  и  $g$ . Вот строгая постановка задачи.

**ТЕОРЕМА 6.4.** *Пусть  $R = \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m]$ , а  $f = \sum_{i=0}^n a_i t^i$  и  $g = \sum_{j=0}^m b_j t^j$  – многочлены над  $R$ . Тогда существуют  $p, q \in R[t]$  такие, что  $r(f, g) = pf + qg$ .*

Нет проблем написать такое представление над полем частных кольца  $R$ , потому что  $f$  и  $g$  очевидно взаимно просты (если бы они имели общий делитель, то специализируя  $a_i, b_j$  можно было получить утверждение, что почти любые 2 многочлена имеют общий делитель).

ДОКАЗАТЕЛЬСТВО. Положим  $z = (t^{m+n-1}, t^{m+n-2}, \dots, 1)^T$  и  $w = (t^{m-1}f(t), t^{m-2}f(t), \dots, f(t), t^{n-1}g(t), t^{n-2}g(t), \dots, g(t))^T$ . Вычисление показывает, что  $S(f, g)z = w$ . Рассматривая последнее равенство как систему линейных уравнений напомним формулу Крамера для последнего элемента столбца  $z$ :

$$r(f, g) = 1 \cdot \det S(f, g) = \det(s_1, \dots, s_{m+n-1}, w),$$

где  $s_i$  – столбцы матрицы  $S(f, g)$ . Раскладывая определитель в правой части по последнему столбцу получим требуемое равенство.  $\square$

**СЛЕДСТВИЕ 6.5.** *Для произвольного кольца  $R$  и многочленов  $f, g \in R[t]$  существуют  $p, q \in R[t]$  такие, что  $r(f, g) = pf + qg$ .*

Для того чтобы вывести следующие свойства результата, нам понадобится простое следствие теоремы Безу и леммы Гаусса.

**ЛЕММА 6.6.** *Пусть  $A$  – факториальное кольцо,  $h \in A[t]$ , а  $t_1 \in A$ . Если  $h(t_1) = 0$ , то  $h$  делится на  $t - t_1$ .*

ДОКАЗАТЕЛЬСТВО. Пусть  $K$  – поле частных кольца  $A$ . По теореме Безу  $h = (t - t_1)q$  для некоторого  $q \in K[t]$ . Если  $\alpha \in A$  – общий знаменатель коэффициентов многочлена  $q$ , то  $\alpha q \in A[t]$ . По лемме Гаусса 3.2 либо  $t - t_1$  либо  $\alpha q$  делится на  $\alpha$  в  $A[t]$ . Так как  $t - t_1$  неприводим, то  $q = \alpha q / \alpha \in A[t]$ .  $\square$

**ТЕОРЕМА 6.7.** Пусть  $R$  – кольцо. Предположим, что многочлены  $f, g \in R[t]$  раскладываются на линейные множители:

$$f(t) = \alpha_n \prod_{i=1}^n (t - \xi_i) \text{ и } g(t) = \beta_m \prod_{j=1}^m (t - \omega_j),$$

где  $\alpha_n, \beta_m, \xi_i, \omega_j \in R$ . Тогда

$$r := r(f, g) = \alpha_n^m \beta_m^n \prod_{i,j} (\xi_i - \omega_j) = \alpha_n^m \prod_{i=1}^n g(\xi_i) = (-1)^{mn} \beta_m^n \prod_{j=1}^m f(\omega_j).$$

**ДОКАЗАТЕЛЬСТВО.** Заметим, что второе и третье равенства выполнены по определению многочленов  $f$  и  $g$ . Требуемое равенство полиномиально относительно  $\alpha_n, \beta_m, \xi_1, \dots, \xi_n, \omega_1, \dots, \omega_m$ , поэтому его можно будет спроектировать из “generic case” в любое кольцо. В “generic case” давайте считать, что  $x_i$  и  $y_j$  – независимые переменные. Положим

$$f(t) = \sum_{i=0}^n a_i t^i = a_n \prod_{i=1}^n (t - x_i) \text{ и } g(t) = \sum_{j=0}^m b_j t^j = b_m \prod_{j=1}^m (t - y_j).$$

Таким образом, в первой части доказательства:

- $K = \mathbb{Z}[a_n, b_m, x_1, \dots, x_n, y_1, \dots, y_m]$  – кольцо многочленов,
- $f, g \in K[t]$ ,
- $a_0, \dots, a_n, b_0, \dots, b_m \in K$ ,

и мы хотим доказать равенство из условия теоремы с заменой соответствующих греческих букв на латинские, а  $K$  на  $R$ .

Если в многочлен  $f$  вместо одного из  $x_i$  подставить  $y_j$ , полученный многочлен будет иметь общий корень с  $g$ . По предложению 6.2  $r|_{x_i=y_j} = 0$ . По предыдущей лемме  $r$  делится на  $x_i - y_j$ . Так как  $b_j$  делится на  $b_m$  в  $K$ , а  $r$  является однородным многочленом степени  $n$  от  $b_0, \dots, b_m$ , то  $r$  делится на  $b_m^n$ . Аналогично,  $r$  делится на  $a_n^m$ . Так как кольцо  $K$  факториально, а элементы  $x_i - y_j$ ,  $a_n$  и  $b_m$  неприводимы, то  $r$  делится на

$$p := a_n^m b_m^n \prod_{i,j} (x_i - y_j) = a_n^m \prod_{i=1}^n (b_m x_i^m + \dots + b_0).$$

По теореме 5.1 элементы  $b_0, \dots, b_m$  являются алгебраически независимыми, т.е. подкольцо  $\mathbb{Z}[a_n, x_1, \dots, x_n][b_0, \dots, b_m] \subseteq K$  является кольцом многочленов от  $b_0, \dots, b_m$  над  $\mathbb{Z}[a_n, x_1, \dots, x_n]$ . Тогда  $p$  является однородным многочленом степени  $n$  по переменным  $b_0, \dots, b_m$ , также как и  $r$ . Коэффициент при  $b_0^n$  многочлена  $p$  очевидно равен  $a_n^m$ . Для того чтобы посчитать коэффициент многочлена  $r$  при  $b_0^n$ , достаточно вычислить  $r$  при  $b_1 = \dots = b_m = 0$ . Легко видеть, что он также равен  $a_n^m$ , следовательно,  $r = p$ .

По универсальному свойству кольца многочленов существует (единственный) гомоморфизм  $\varphi : K \rightarrow R$  такой, что  $\varphi(x_i) = \xi_i$ ,  $\varphi(y_i) = \omega_i$ ,  $\varphi(a_n) = \alpha_n$ ,  $\varphi(b_m) = \beta_m$ .

Так как  $\varphi$  сохраняет операции сложения и умножения, то доказанное равенство переходит под действием  $\varphi$  в равенство из условия теоремы.  $\square$

Далее  $R$  – область целостности, а коэффициенты всех многочленов лежат в  $R$ . Обозначим через  $\bar{F}$  алгебраическое замыкание поля частных кольца  $R$ .

**СЛЕДСТВИЕ 6.8.** Если  $f = gh + q$ , то  $r(f, g) = b_m^{n-\deg q} r(q, g)$ , где  $b_m$  – старший коэффициент многочлена  $g$ .

**ДОКАЗАТЕЛЬСТВО.** Пусть  $y_i$  – корни многочлена  $g$  в  $\bar{F}$ . Тогда  $q(y_i) = f(y_i)$ . Остается воспользоваться формулой из теоремы 6.7.  $\square$

**СЛЕДСТВИЕ 6.9.**  $r(f, gh) = r(f, g)r(f, h)$ .

ДОКАЗАТЕЛЬСТВО. Пусть  $\xi_i$  корни многочлена  $f$  в  $\overline{F}$ , а  $\alpha_n$  – его старший коэффициент. Тогда

$$r(f, gh) = \alpha_n^{\deg g + \deg h} \prod_{i=1}^n g(\xi_i) h(\xi_i) = \alpha_n^{\deg g} \prod_{i=1}^n g(\xi_i) \cdot \alpha_n^{\deg h} \prod_{i=1}^n h(\xi_i) = r(f, g) r(f, h).$$

□

## 7. Доказательство слабой теоремы о нулях с помощью результата

**ЛЕММА 7.1.** Пусть  $F$  – бесконечное поле, а  $f \in F[t_1, \dots, t_n]$  – многочлен степени  $d$ . Тогда существуют  $\lambda_1, \dots, \lambda_{n-1}$  такие, что коэффициент при  $t_n^d$  в многочлене  $f(t_1 + \lambda_1 t_n, \dots, t_{n-1} + \lambda_{n-1} t_n, t_n)$  не равен нулю.

ДОКАЗАТЕЛЬСТВО. Пусть  $g$  – однородная компонента  $f$  старшей степени. Тогда коэффициент при  $t_n^d$  в многочлене  $f(t_1 + \lambda_1 t_n, \dots, t_{n-1} + \lambda_{n-1} t_n, t_n)$  равен коэффициенту при  $t_n^d$  в многочлене  $g(t_1 + \lambda_1 t_n, \dots, t_{n-1} + \lambda_{n-1} t_n, t_n)$ , который равен значению последнего многочлена в точке  $(0, \dots, 0, 1)$ , т.е.  $g(\lambda_1, \dots, \lambda_{n-1}, 1)$ .

Последнее выражение является ненулевым многочленом от  $\lambda_1, \dots, \lambda_{n-1}$ , поэтому над бесконечным полем имеет ненулевое значение. Последнее утверждение очевидно для  $n = 2$ , общий случай доказывается индукцией по количеству переменных. Рассмотрев  $g(\lambda_1, \dots, \lambda_{n-1}, 1)$  как многочлен от  $\lambda_{n-1}$ , обозначим через  $h(\lambda_1, \dots, \lambda_{n-2})$  какой-нибудь из его ненулевых коэффициентов. По индукционному предположению существуют значения переменных, при которых  $h \neq 0$ . Подставив эти значения в  $g(\lambda_1, \dots, \lambda_{n-1}, 1)$ , получим ненулевой многочлен от  $\lambda_{n-1}$ , который имеет конечное число корней. □

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ГИЛЬБЕРТА О НУЛЯХ.  $F$  – алгебраически замкнутое поле,  $I$  – собственный идеал кольца многочленов  $R = F[t_1, \dots, t_n]$ . Надо доказать, что все многочлены из  $I$  имеют общий корень. Будем доказывать от противного индукцией по  $n$ . База ( $n = 1$ ) следует из того, что  $R$  – кольцо главных идеалов, а поле  $F$  алгебраически замкнуто.

Отображение  $R \rightarrow R$ ,  $t_i \mapsto t_i + \lambda_i t_n$  при  $i = 1, \dots, n-1$  является автоморфизмом кольца  $R$ . Применение автоморфизма не меняет ни наличия корней, ни свойства быть собственным идеалом. Поэтому, по предыдущей лемме можно считать, что в  $I$  существует многочлен

$$g = t_n^d + g_{d-1} t_n^{d-1} + \dots + g_0, \text{ где } g_i \in R' := F[t_1, \dots, t_{n-1}].$$

Пусть  $I' = I \cap R'$ . По предположению  $1 \notin I'$ , поэтому  $I'$  – собственный идеал в  $R'$ . По индукционному предположению существует общий корень  $(\alpha_1, \dots, \alpha_{n-1})$  всех многочленов из  $I'$ .

Пусть  $J = \{f(\alpha_1, \dots, \alpha_{n-1}, t_n) \mid f \in I\}$ . Ясно, что  $J$  – идеал в  $F[t_n]$ . По предположению элементы из  $J$  не имеют общих корней, следовательно,  $1 \in J$ . Другими словами, существует многочлен  $h \in I$  такой, что  $h(\alpha_1, \dots, \alpha_{n-1}, t_n) = 1$ . Запишем

$$h = h_m t_n^m + h_{m-1} t_n^{m-1} + \dots + h_0, \text{ где } h_i \in R'.$$

Положим  $r = r_{t_n}(g, h) \in R'$ . По следствию 6.5 существуют  $p, q \in R$  такие, что  $r = gp + hq$ . Поэтому,  $r \in I'$ , следовательно,  $r(\alpha_1, \dots, \alpha_{n-1}) = 0$ .

Так как  $h(\alpha_1, \dots, \alpha_{n-1}, t_n) = 1$ , то  $h_0(\alpha_1, \dots, \alpha_{n-1}) = 1$ , а  $h_i(\alpha_1, \dots, \alpha_{n-1}) = 0$  при всех  $i > 0$ . При подстановке этих значений в матрицу Сильвестра  $S(g, h)$  она становится треугольной, следовательно ее определитель  $r(\alpha_1, \dots, \alpha_{n-1})$  равен 1. Противоречие показывает, что все многочлены из  $I$  имеют общий корень. □

## 8. Дискриминант

Пусть  $x_1, \dots, x_n$  – корни многочлена  $f(t) = a_n t^n + \dots + a_0$ , причем  $a_n \neq 0$ .<sup>1</sup> Величину

$$d(f) = a_n^{2n-2} \prod_{i < j} (x_i - x_j)^2$$

называют *дискриминантом* многочлена  $f$ . Смысл дискриминанта над произвольным полем состоит в том, что он равен нулю тогда и только тогда, когда многочлен имеет кратные корни. Над  $\mathbb{R}$  с помощью знака дискриминанта можно сформулировать необходимое условие отсутствия вещественных корней. Очевидно, что произведение в определении дискриминанта является симметрическим многочленом от корней многочлена  $f$ , поэтому оно является многочленом (назовем его  $g$ ) от  $a_i/a_n$ . Степень  $g$  равна степени произведения по  $x_1$ , см. следствие 5.4, которая равна  $2(n-1)$ . Таким образом,

$$d(f) = a_n^{2n-2} \prod_{i < j} (x_i - x_j)^2 = a_n^{2n-2} g(a_0/a_n, \dots, a_{n-1}/a_n),$$

является многочленом от  $a_0, \dots, a_n$ .

**ТЕОРЕМА 8.1.**  $r(f, f') = (-1)^{n(n-1)/2} a_n d(f)$ , где  $a_n$  – старший коэффициент многочлена  $f$ .

**ДОКАЗАТЕЛЬСТВО.** По теореме 6.7  $r(f, f') = a_n^{n-1} \prod_i f'(x_i)$ , где  $x_1, \dots, x_n$  – корни многочлена  $f$ . Легко проверить, что  $f'(x_i) = a_n \prod_{j \neq i} (x_i - x_j)$ . Поэтому

$$r(f, f') = a_n^{2n-1} \prod_{i \neq j} (x_i - x_j) = a_n^{2n-1} (-1)^{n(n-1)/2} \prod_{i < j} (x_i - x_j)^2 = (-1)^{n(n-1)/2} a_n d(f).$$

□

Из теоремы снова следует что дискриминант является многочленом с целыми коэффициентами от коэффициентов многочлена  $f$  ( $a_n$  является общим множителем первого столбца матрицы Сильвестра).

**ТЕОРЕМА 8.2.** Пусть  $f, g, h$  – многочлены со старшим коэффициентом 1. Тогда

$$\begin{aligned} d(fg) &= d(f)d(g)r(f, g)^2, \\ d(fgh) &= d(f)d(g)d(h)r(f, g)^2r(g, h)^2r(h, f)^2. \end{aligned}$$

**ДОКАЗАТЕЛЬСТВО.** Пусть  $x_1, \dots, x_n$  – корни многочлена  $f$ , а  $y_1, \dots, y_m$  – корни многочлена  $g$ . Тогда

$$d(fg) = \prod_{i < j} (x_i - x_j)^2 \cdot \prod_{i < j} (y_i - y_j)^2 \cdot \prod_{i, j} (x_i - y_j)^2 = d(f)d(g)r(f, g)^2.$$

Вторая формула доказывается аналогично. □

**ТЕОРЕМА 8.3.** Пусть  $f$  – вещественный многочлен степени  $n$ , не имеющий кратных корней. Если  $f$  не имеет вещественных корней (заметьте, что в этом случае  $n$  четное), то  $\text{sign } d(f) = (-1)^{n/2}$ .

**ДОКАЗАТЕЛЬСТВО.** Так как старший коэффициент входит в выражение для дискриминанта в четной степени, можно считать, что он равен 1. Пусть  $a$  и  $\bar{a}$  – пара сопряженных корней многочлена  $f$ , т. е.  $f(t) = (t - a)(t - \bar{a})g(t)$ . Тогда по предыдущей теореме

$$\begin{aligned} d(f) &= d(g)r(t - a, t - \bar{a})^2 r(t - \bar{a}, g)^2 r(g, t - a)^2 = \\ &= d(g)(\bar{a} - a)^2 g(a)^2 g(\bar{a})^2 = -d(g)(\text{Im } a)^2 |g(a)|^4. \end{aligned}$$

Следовательно,  $\text{sign } d(f) = -\text{sign } d(g)$  и доказательство заканчивается индукцией по  $n$ . □

<sup>1</sup>Мы используем латинские буквы для обозначения коэффициентов и корней, а также не уточняем кольцо коэффициентов, потому что на самом деле все происходит над универсальным кольцом  $\mathbb{Z}[a_n, x_1, \dots, x_n]$ , из которого результаты могут быть спроектированы в кольцо многочленов с любым кольцом коэффициентов.

**УПРАЖНЕНИЕ 8.4.** Если многочлен, не имеющий кратных корней, имеет ровно  $m$  пар комплексно сопряженных корней, то  $\text{sign } d(f) = (-1)^m$ .

## 9. Базисы Гребнера

Задача: по данным многочленам  $f, f_1, \dots, f_m \in F[t_1, \dots, t_n]$  определить, лежит ли  $f$  в идеале, порожденном  $f_i$ -ми.

Решение: научиться делить с остатком  $f$  на  $f_1, \dots, f_m$ .

Для этого надо определить, что такое остаток, а для этого – определить линейный порядок на множестве мономов.

Мы продолжаем использовать обозначения из начала главы, см. также обозначения после формулировки теоремы 5.1.

Пусть  $\preccurlyeq$  линейный порядок на множестве мультииндексов  $\mathbb{N}_0^n$ . Он индуцирует линейный порядок на множестве  $M(T)$  унитарных мономов:  $T^k \preccurlyeq T^\ell \iff k \preccurlyeq \ell$ .

В случае  $T^k \preccurlyeq T^\ell$  говорят, что одночлен  $\alpha T^k$  *младше* одночлена  $\beta T^\ell$  или что  $\alpha T^k$  *старше*  $\beta T^\ell$ .

**ОПРЕДЕЛЕНИЕ 9.1.** Линейное упорядочение множества  $\mathbb{N}_0^n$  называется *допустимым*, если оно удовлетворяет свойствам

- (1)  $(0, \dots, 0) \prec k$  для любого  $k \in \mathbb{N}_0^n \setminus \{(0, \dots, 0)\}$ , и
- (2)  $k \preccurlyeq \ell \implies k + h \preccurlyeq \ell + h$  для любых  $h, k, \ell \in \mathbb{N}_0^n$ .

**ЛЕММА 9.2.** Пусть  $\preccurlyeq$  – допустимый линейный порядок на множестве одночленов. Тогда если  $T^k \preccurlyeq T^\ell$  и  $T^h \preccurlyeq T^j$ , то  $T^k T^h = T^{k+h} \preccurlyeq T^\ell T^j = T^{\ell+j}$ .

**УПРАЖНЕНИЕ 9.3.** Докажите, что допустимый порядок удовлетворяет DCC (descending chain condition = условие обрыва убывающих цепей).

Тремя основными примерами допустимых упорядочений являются:

**Lex:** – лексикографический порядок;

**InvLex:** – обратный лексикографический порядок (т.е. сначала учитывается степень старшей буквы); и

**DegLex:** – сначала сравниваются полные степени, а многочлены одинаковой степени упорядочиваются лексикографически.

Разумеется, каждый из этих порядков зависит от выбора линейного порядка на множестве переменных. Обычно подразумевается, что  $t_1 \prec t_2 \prec \dots \prec t_n$ .

Для обратного лексикографического порядка одночлены располагаются точно так же, как слова в словаре. Под чисто лексикографическим порядком в большинстве работ по компьютерной алгебре подразумевается именно **InvLex**.

Однако чисто лексикографический порядок не всегда удобен. Дело в том, что сложность проводимых с помощью **Lex** вычислений часто драматическим образом зависит от порядка переменных. Для вычислений обычно значительно удобнее пользоваться **DegLex**.

Введем какой-нибудь допустимый порядок на множестве унитарных мономов  $M(T)$ . Мы умеем делить с остатком многочлены от одной переменной. Принципиальное отличие деления в общем случае состоит в следующем. Для одной переменной всегда можно убрать именно *старший* член делимого. Обозначим через  $LT(f)$  – старший моном многочлена  $f$  без коэффициента, т.е.  $LT(f)$  – это унитарный моном пропорциональный старшему моному  $LM(f)$  многочлена  $f$ . В общем случае может оказаться, что старший моном  $LT(f)$  многочлена  $f$  не делится ни на один из старших членов  $LT(f_1), \dots, LT(f_m)$  но, тем не менее, какие-то другие члены  $f$  на них делятся. Это заставляет нас модифицировать процедуру деления с остатком следующим образом.

Рассмотрим старший среди тех членов многочлена  $f$ , которые делятся на старший член какого-то из многочленов  $f_1, \dots, f_m$ . Пусть, например,  $\alpha T^k$  – член  $f$ , делящийся на

$LM(f_i) = \beta T^\ell$ . Тогда в многочлене  $f - \frac{\alpha}{\beta} T^{k-\ell} f_i$  коэффициент при  $T^k$  равен нулю. А так как  $LT(\frac{\alpha}{\beta} T^{k-\ell} f_i) = T^{k-\ell} LT(f_i) = T^k$ , то никаких членов старше, чем  $T^k$  при этом не появляется.

Таким образом, при каждой такой операции старший из тех членов многочлена  $f$ , которые делятся на какой-то из  $LT(f_i)$ , *строго убывает*. Это значит, что продолжая действовать таким образом, мы проведя *конечное число* элементарных редукций придем к многочлену  $r$ , ни один из членов которого не делится на какой-либо из  $LT(f_i)$ . В этом случае говорят, что  $f$  *редуцируется* к  $r$  посредством  $f_1, \dots, f_m$ .

Таким образом мы доказали следующую теорему.

**ТЕОРЕМА 9.4.** *Для любых  $f, f_1, \dots, f_m \in F[T]$  таких, что не все  $f_i$  равны 0, найдутся многочлены  $q_1, \dots, q_m, r \in F[T]$  со следующими свойствами.*

- (1)  $f = q_1 f_1 + \dots + q_m f_m + r$ .
- (2) Ни один из членов  $r$  не делится ни на один из одночленов  $LT(f_1), \dots, LT(f_m)$ .
- (3) Все члены каждого из слагаемых  $q_i f_i$  не превосходят старший член  $f$ .

Любой многочлен  $r$ , удовлетворяющий условиям теоремы, будет называться **остатком** от деления  $f$  на  $f_1, \dots, f_m$ . Проблема, однако, состоит в том, что остаток от деления  $f$  на  $f_1, \dots, f_m$  определен неоднозначно. Неоднозначность может возникнуть из-за того, что  $\alpha T^k$  может делиться на старшие члены *нескольких* многочленов  $f_1, \dots, f_m$ .

Пусть  $f(x, y) = x^2 y$ ,  $f_1(x, y) = x^2$ ,  $f_2(x, y) = xy - 1$ . Тогда  $f = f_1 y + 0 = f_2 x + x$ , и оба равенства удовлетворяют определению деления с остатком  $f$  на  $f_1, f_2$ . Заметим, что в этом случае многочлен  $x$  принадлежит идеалу, порожденному  $f_1, f_2$ , но не делится на них без остатка, потому что неравенства  $LT(f_i q_i) \preccurlyeq LT(x)$  могут выполняться только при  $q_1 = q_2 = 0$ .

Оказывается, что для любого набора многочленов  $f_1, \dots, f_m \in F[T]$  найдутся  $g_1, \dots, g_s \in F[T]$ , порождающие тот же самый идеал  $I$ , для которых деление с остатком дает *единственный* остаток.

**ОПРЕДЕЛЕНИЕ 9.5.** Пусть  $f_1, \dots, f_m \in F[T]$  порождают идеал  $I$ . Говорят, что  $f_1, \dots, f_m$  образуют *базис Гребнера* идеала  $I$ , если старший член любого многочлена  $f \in I \setminus \{0\}$ , делится на старший член какого-то из многочленов  $f_1, \dots, f_m$ .

Обычно мы нормируем базис Гребнера таким образом, чтобы в каждом  $f_i$  коэффициент при старшем члене равнялся 1.

Далее мы дадим несколько эквивалентных формулировок базисов Гребнера, докажем, что в каждом идеале  $I$  кольца многочленов  $F[T]$  существует базис Гребнера и что базисы Гребнера действительно обладают сформулированным выше свойством единственности остатка.

После этого мы изложим алгоритм, который позволяет фактически построить базис Гребнера идеала за конечное число шагов и покажем, что при выполнении некоторые естественных дополнительных условий базис Гребнера является по существу единственным.

**ТЕОРЕМА 9.6.** *Следующие условия эквивалентны*

- (1)  $f_1, \dots, f_m$  — базис Гребнера идеала  $I$ .
- (2) Для любого  $f \in I$  остаток от деления  $f$  на  $f_1, \dots, f_m$  *единственен и равен 0*.
- (3) Идеал  $L(I)$ , порожденный  $LT(f)$ ,  $f \in I$ , порождается  $LT(f_1), \dots, LT(f_m)$ .

**ДОКАЗАТЕЛЬСТВО.** (1)  $\implies$  (2). Произвольным образом поделим  $f$  с остатком на  $f_1, \dots, f_m$ . Тогда  $r = f - q_1 f_1 - \dots - q_m f_m \in I$ . Если  $r \neq 0$ , то по определению базиса Гребнера его старший член делится на старший член какого-то из  $f_1, \dots, f_m$ . Однако по определению остатка, ни один из его членов не делится на старшие члены  $f_1, \dots, f_m$ .

(2)  $\implies$  (3). По предположению для  $f \in I$  остаток от деления  $f$  на  $f_1, \dots, f_m$  равен 0 и, таким образом,  $f = q_1 f_1 + \dots + q_m f_m$ . По определению деления с остатком  $LT(q_i f_i) \preccurlyeq LT(f)$ . Поэтому найдется  $i = 1, \dots, m$  такой, что  $LT(f)$  ассоциировано с  $LT(q_i f_i) = LT(q_i) LT(f_i)$ .

(3)  $\implies$  (1). Последнее условие означает, что для любого  $f \in I$  существуют  $q_1, \dots, q_m \in F[T]$  такие, что  $LT(f) = LT(f_1) q_1 + \dots + LT(f_m) q_m$ . Ясно, что все мономы  $p$  многочленов  $q_1, \dots, q_m$ ,



для которых мультистепени  $LT(f_i)p$  и  $LT(f)$  не совпадают, можно выкинуть. Какой-то из  $q_i$  останется после выкидывания ненулевым одночленом. Тогда  $LT(f)$  делится на  $LT(f_i)$ .  $\square$

В частности, теорема означает, что базис Гребнера – это в точности такой базис, для которого каждый элемент  $f \in I$  представляется в виде

$$f = q_1 f_1 + \dots + q_m f_m, \text{ где } LT(q_i f_i) \preceq LT(f).$$

Теперь мы готовы доказать, что в любом идеале существует базис Гребнера. Фактически, это сразу вытекает из теоремы Гильберта о базисе.

**ТЕОРЕМА 9.7** (Хиронака). *В любом идеале  $I$  кольца многочленов  $F[T]$  существует базис Гребнера.*

**ДОКАЗАТЕЛЬСТВО.** Рассмотрим идеал  $L(I) = \sum_{f \in I} LT(f)F[T]$ . По теореме Гильберта о базисе этот идеал порождается конечным числом мономов  $T^{k(1)}, \dots, T^{k(m)}$ . Тогда многочлены  $f_1, \dots, f_m \in I$  со старшими членами  $T^{k(1)}, \dots, T^{k(m)}$  образуют базис Гребнера  $I$ .  $\square$

**ТЕОРЕМА 9.8.** *Ненулевые многочлены  $f_1, \dots, f_m$  в том и только том случае образуют базис Гребнера порожденного ими идеала  $I$ , когда остаток от деления любого многочлена  $f \in R = K[x_1, \dots, x_n]$  на  $f_1, \dots, f_m$  определен однозначно.*

**ДОКАЗАТЕЛЬСТВО.** Предположим, что  $f_1, \dots, f_m$  – базис Гребнера идеала  $I$ , а  $f = q_1 f_1 + \dots + q_m f_m + r_1 = p_1 f_1 + \dots + p_m f_m + r_2$ , где  $r_1$  и  $r_2$  – два остатка при делении  $f$  на  $f_1, \dots, f_m$ . Тогда  $r_1 - r_2 = (p_1 - q_1)f_1 + \dots + (p_m - q_m)f_m \in I$  и по определению базиса Гребнера  $LT(r_1 - r_2)$  делится на старший член какого-то из многочленов  $f_1, \dots, f_m$ . Однако по определению остатка ни у  $r_1$  ни у  $r_2$  нет вообще *никаких* членов делящихся на старшие члены  $f_1, \dots, f_m$ .

Обратно, пусть  $f = q_1 f_1 + \dots + q_m f_m \in I$  – выражение  $f$  через образующие идеала  $I$  с минимально возможным  $\max(LT(q_i f_i))$ . Предположим для определенности, что этот максимум достигается при  $i = 1$ . Если  $LT(f_1 q_1) \preceq LT(f)$ , то остаток от деления  $f$  на  $f_1, \dots, f_m$  равен нулю.

В противном случае,  $LT(f - f_1 q_1) = LT(-f_1 q_1) \succ LT(f_1 q_1)$ . Следовательно, равенство  $f - q_1 f_1 = q_2 f_2 + \dots + q_m f_m + 0$  является делением с остатком. Пусть теперь  $f = p_1 f_1 + \dots + p_m f_m + r$  – деление с остатком  $f$  на  $f_1, \dots, f_m$ , т.е.  $LT(p_i f_i) \preceq LT(f)$ . Тогда равенство  $f - q_1 f_1 = (p_1 - q_1)f_1 + p_2 f_2 + \dots + p_m f_m + r$  также будет делением с остатком. Действительно, старшие члены всех слагаемых правой части, кроме первого, не старше  $LT(f) \prec LT(f - f_1 q_1)$ . Для первого же слагаемого

$$LT((p_1 - q_1)f_1) \preceq \max(LT(p_1 f_1), LT(q_1 f_1)) = LT(q_1 f_1) = LT(f - f_1 q_1).$$

По единственности остатка в любом случае  $r = 0$ . По теореме 9.6 из этого следует, что  $f_1, \dots, f_m$  – базис Гребнера.  $\square$

Предшествующие теоремы не являются конструктивными. При помощи следующего алгоритма Бухбергера можно узнать за конечное число шагов, будет ли набор многочленов  $f_1, \dots, f_m$  базисом Гребнера порожденного ими идеала  $I$ .

Пусть  $\alpha T^k = LM(f)$ ,  $\beta T^\ell = LM(g)$ , а  $T^h = \gcd(T^k, T^\ell)$ . Определим  $S$ -многочлен многочленов  $f$  и  $g$  посредством

$$S(f, g) = \frac{T^\ell}{\alpha T^h} f - \frac{T^k}{\beta T^h} g.$$

Он строится так, чтобы старшие члены  $f$  и  $g$  сокращались. Оказывается, равенство 0 остатка достаточно проверять только для конечного числа  $S$ -многочленов.

**ТЕОРЕМА 9.9** (Критерий Бухбергера). *Многочлены  $f_1, \dots, f_m$  в том и только том случае образуют базис Гребнера порожденного ими идеала  $I$ , когда все  $S$ -многочлены  $S(f_i, f_j)$ ,  $i \neq j$ , дают при делении на  $f_1, \dots, f_m$  остаток 0.*

В одну сторону утверждение следует из теоремы 9.6. Для доказательства обратной импликации нам потребуется следующая лемма.

**ЛЕММА 9.10.** Пусть  $f_1, \dots, f_m$  — многочлены со старшими мономы  $\alpha_i T^k$ ,  $i = 1, \dots, m$ . Если старший член их линейной комбинации  $f = \sum \lambda_i f_i$ ,  $\lambda_i \in F$ , строго меньше  $T^k$ , то  $f$  является линейной комбинацией многочленов  $S(f_i, f_j)$  с коэффициентами из  $F$ .

ДОКАЗАТЕЛЬСТВО. Так как по условию  $f_i = \alpha_i T^k + \dots$ , то  $S(f_i, f_j) = \frac{f_i}{\alpha_i} - \frac{f_j}{\alpha_j}$ . С другой стороны, так как коэффициент  $f$  при  $T^k$  равен 0, то  $\lambda_1 \alpha_1 + \dots + \lambda_m \alpha_m = 0$ . Таким образом, мы можем применить трюк накопления:

$$\begin{aligned} f &= \lambda_1 f_1 + \dots + \lambda_m f_m = \\ &\lambda_1 \alpha_1 S(f_1, f_2) + (\lambda_1 \alpha_1 + \lambda_2 \alpha_2) S(f_2, f_3) + \dots + \\ &(\lambda_1 \alpha_1 + \dots + \lambda_{m-1} \alpha_{m-1}) S(f_{m-1}, f_m) + \\ &(\lambda_1 \alpha_1 + \dots + \lambda_m \alpha_m) \frac{f_m}{\alpha_m}, \end{aligned}$$

причем, как мы только что заметили, последнее слагаемое равно 0.  $\square$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ. Пусть  $f = f_1 g_1 + \dots + f_m g_m$ , где  $g_1, \dots, g_m \in F[T]$  — произвольный элемент из  $I$ . Предположим, что  $T^k = \max(LT(f_1 g_1), \dots, LT(f_m g_m))$  — наименьший возможный для всех таких представлений  $f$ . Мы хотим доказать, что  $f$  делится на  $f_1, \dots, f_m$  без остатка, т.е.  $T^k \preccurlyeq LT(f)$ . Не умаляя общности, можно считать, что для некоторого  $u$   $LT(h_p f_p) = T^k \succcurlyeq LT(f_q h_q)$  при всех  $p \leq u < q$ . Если  $T^k \succcurlyeq LT(f)$ , то сумма старших членов равна нулю. Тогда, по предыдущей лемме сумма  $f_1 g_1 + \dots + f_u g_u$  представляется в виде линейной комбинации  $S$ -многочленов  $S(f_i g_i, f_j g_j)$  с коэффициентами из поля. По условию любой такой  $S$ -многочлен делится на  $f_1, \dots, f_m$  без остатка. Следовательно,

$$f_1 g_1 + \dots + f_u g_u = \sum_{i < j} \mu_{ij} S(f_i g_i, f_j g_j) = f_1 \tilde{g}_1 + \dots + f_m \tilde{g}_m,$$

где  $LT(f_i \tilde{g}_i) \preccurlyeq LT(\sum_{i < j} \mu_{ij} S(f_i g_i, f_j g_j)) \prec T^k$ . Но это означает, что в исходном представлении  $f$  мультистепень слагаемых можно уменьшить, что противоречит предположению.  $\square$

Эта теорема показывает, как *построить* базис Гребнера идеала. Пусть  $f_1, \dots, f_m$  — какая-то система образующих идеала  $I$ . Образует  $S$ -многочлены  $S(f_i, f_j)$  для всех  $i < j$  и вычислим их остатки при делении на  $f_1, \dots, f_m$ . Добавляя к набору  $f_1, \dots, f_m$  все получившиеся ненулевые остатки, составим набор  $f_1, \dots, f_{m_1}$ , где  $m_1 \geq m_0 := m$ . Продолжая действовать таким образом, на  $i$ -ом шаге получим набор  $f_1, \dots, f_{m_i}$ . Равенство  $m_i = m_{i-1}$  означает, что все  $S$ -многочлены делятся на  $f_1, \dots, f_{m_{i-1}}$  без остатка. В этом случае по критерию Бухбергера  $f_1, \dots, f_{m_{i-1}}$  уже базис Гребнера. В противном случае добавились многочлены, старшие члены которых, не выражаются через  $LT(f_1), \dots, LT(f_{m_{i-1}})$  (это верно для любого ненулевого остатка от деления на  $f_1, \dots, f_m$ ). Получим строго возрастающую цепочку идеалов, порожденных  $LT(f_1), \dots, LT(f_{m_i})$ , которая должна оборваться по теореме Гильберта о базисе.

Изложенная выше процедура является простейшим вариантом *алгоритма Бухбергера*. Разумеется, фактически настоящий алгоритм Бухбергера устроен чуть сложнее и работает гораздо быстрее, так как в нем на каждом шаге производится исключение лишних образующих и редукция каждой образующей по модулю остальных. Как это делается, мы сейчас увидим.

Базис Гребнера  $f_1, \dots, f_m$  называется *минимальным*, если старшие мономы двух любых многочленов  $f_i$  и  $f_j$ ,  $i \neq j$ , не делятся друг на друга, а все старшие коэффициенты равны 1.

**ТЕОРЕМА 9.11.** В каждом идеале кольца многочленов существует минимальный базис Гребнера.

Теорема сразу вытекает из следующего утверждения.

**ЛЕММА 9.12.** Если  $f_1, \dots, f_m$  – базис Гребнера, а  $LT(f_m)$  делится на  $LT(f_i)$  для некоторого  $i < m$ , то  $f_1, \dots, f_{m-1}$  – базис Гребнера того же идеала.

**ДОКАЗАТЕЛЬСТВО.** Пусть  $I$  – идеал, порожденный  $f_1, \dots, f_m$ , а  $r = f_m - \sum_{i=1}^{m-1} f_i g_i$  – остаток от деления  $f_m$  на  $f_1, \dots, f_{m-1}$ . Так как  $r \in I$ , то по определению базиса Гребнера его старший член старший член какого-то  $f_p$ . По условию  $LT(r) \prec LT(f_m)$ , поэтому  $p \neq m$ . Но это невозможно, если остаток ненулевой. Таким образом,  $f_m \in (f_1, \dots, f_{m-1})$  и  $LT(f_m) \in (LT(f_1), \dots, LT(f_{m-1}))$ .  $\square$

Оказывается, старшие мономы многочленов, входящих в минимальный базис Гребнера, определены однозначно, с точностью до перестановки.

**ПРЕДЛОЖЕНИЕ 9.13.** Пусть  $f_1, \dots, f_m$  и  $g_1, \dots, g_p$  – два минимальных базиса Гребнера идеала  $I$ . Тогда  $p = m$  и после перестановки  $LT(f_i) = LT(g_i)$ .

**ДОКАЗАТЕЛЬСТВО.** Так как  $g_1, \dots, g_l$  базис Гребнера, а  $f_1 \in I$ , то старший член  $f_1$  делится на старший член какого-то  $g_i$ . Перенумеровывая, если нужно,  $g_i$ , можно считать, что  $LT(f_1)$  делится на  $LT(g_1)$ . Поменяв в предыдущем рассуждении  $f$  и  $g$ , мы видим, что в свою очередь  $LT(g_1)$  делится на старший член какого-то  $f_i$ . Если при этом  $i \neq 1$ , то  $LT(f_1)$  делится на  $LT(f_i)$ ,  $i \neq 1$ , что противоречит минимальности. Таким образом,  $LT(f_1) = LT(g_1)$ .

Продолжая действовать таким образом, мы видим, что существует перестановка, для которой  $LT(f_i) = LT(g_i)$  при всех  $i \leq \min(m, p)$ . Если  $m > p$ , то, так как  $g_1, \dots, g_p$  – базис Гребнера, то  $LT(f_{p+1})$  делится на  $LT(g_j) = LT(f_j)$  для некоторого  $j$ , что снова противоречит минимальности. Аналогично,  $p > m$  невозможно, откуда  $p = m$ .  $\square$

Базис Гребнера  $f_1, \dots, f_m$  называется *редуцированным*, если ни один из членов любого многочлена  $f_i$  не делится на старшие члены многочленов  $f_j$ ,  $j \neq i$ . Другими словами, каждый элемент этого базиса редуцирован по модулю остальных. Иначе говоря, остаток при делении  $f_i$  на  $\{f_j \mid j \neq i\}$ , совпадает с  $f_i$ .

**ТЕОРЕМА 9.14.** В каждом идеале кольца многочленов существует единственный с точностью до перестановки редуцированный базис Гребнера.

**ДОКАЗАТЕЛЬСТВО.** Стартуем с минимального базиса Гребнера  $f_1, \dots, f_m$ . Пусть  $g_1$  – остаток от деления  $f_1$  на  $f_2, \dots, f_m$ . В силу минимальности базиса Гребнера  $LT(g_1) = LT(f_1)$ . Поэтому  $g_1, f_2, \dots, f_m$  – снова является базисом Гребнера того же идеала, причем ни один из мономов  $g_1$  не делится на старшие мономы остальных многочленов. Продолжая процесс, получим редуцированный базис  $g_1, \dots, g_m$ .

Пусть теперь  $f_1, \dots, f_m$  и  $g_1, \dots, g_p$  – два редуцированных базиса Гребнера идеала  $I$ . Так как эти базисы минимальны, то из предыдущей теоремы вытекает, что  $p = m$  и, после перестановки,  $LT(f_i) = LT(g_i)$ . Предположим, что  $f_i \neq g_i$  для какого-то  $i$ . По определению базиса Гребнера  $LT(f_i - g_i)$  делится на один из  $LT(f_j) = LT(g_j)$ . Но  $LT(f_i - g_i) \prec LT(f_i)$ , поэтому  $j \neq i$ . Но  $LT(f_i - g_i)$  пропорционален одному из мономов многочлена  $f_i$  или  $g_i$ , которые не делятся на  $LT(f_j) = LT(g_j)$  по определению редуцированного базиса. Таким образом,  $f_i = g_i$  для всех  $i$ .  $\square$

Глава 13

**Теория Галуа**