# Конспект лекций по алгебре. Академический университет, 2015/16 уч. г.

А.В.Степанов

# Предисловие

Этот конспект по разным причинам не будет полностью совпадать с тем, что я говорил на лекциях. Однако я надеюсь, что слушателям будет нетрудно понять, что лекции и конспект эквивалентны, просто некоторые утверждения написаны другими словами, а некоторые вынесены под отдельный заголовок. В параграфе обозначения и терминология упомянуты те слова и символы, про смысл которых студенты задавали вопросы на лекции.

## Обозначения и терминология

$\coprod\limits_{k\in K} X_k$ – это объединение непересекающихся множеств $X_k$ (это называют дизъюнктным объединением).

*Собственное подмножество* – это подмножество, не совпадающее со всем множеством.

Глава 1

# Функции и операции, основные алгебраические структуры

## 1. Функции

Я далек от мысли, записать весь курс исходя только из аксиом теории множеств. Однако, на примере понятия функции мне хотелось бы показать, что можно определить любое математическое понятие не оперируя неопределенными ранее словами, что сплошь и рядом встречается в учебной литературе. Если определение начинается со слов "функция – это отображение...", то первый же вопрос, который возникает у внимательного читателя: "А что такое отображение?".

Определение 1.1. Кортеж длины $n$ (другие названия: последовательность длины $n$ или, короче, $n$-ка) определяется рекурсивно: кортеж длины 1 – это одноэлементное множество, кортеж длины $n$ – это множество, состоящее из кортежа длины $n-1$ и еще одного элемента. Кортеж длины $n$ обозначается $(a_1, \dots, a_n)$.

Упорядоченная пара $(x, y) = \big\{\{x\}, y\big\}$ – это кортеж длины 2.

Декартово произведение множеств $X$ и $Y$ – это множество

$$X \times Y = \{(x, y) \mid x \in X,\, y \in Y\}.$$

Определение 1.2. Функция – это тройка $(X, Y, \Gamma)$, где $X$ и $Y$ – множества, а $\Gamma$ – подмножество в $X \times Y$ такое, что для любого $x \in X$ существует единственный $y \in Y$, удовлетворяющий условию $(x, y) \in \Gamma$. При этом $X$ называется областью определения, $Y$ – множеством значений, а $\Gamma$ – графиком функции.

Пусть $f = (X, Y, \Gamma)$ – функция. Обычно говорят, что $f$ – это функция из $X$ в $Y$ и пишут $f : X \to Y$. Вместо $(x, y) \in \Gamma$ принято писать $f(x) = y$ и говорить, что $y$ – это образ элемента $x$ под действием функции $f$.

Определение 1.3. Образ функции $f : X \to Y$ – это множество $\operatorname{Im} f = \{f(x) \mid x \in X\}$. Если $X' \subseteq X$, то $f(X') = \{f(x) \mid x \in X'\}$ называется образом $X'$ под действием функции $f$.

Если $x \in X$, а $y = f(x)$, то $x$ называется прообразом элемента $y$. Полный прообраз $y$ – это множество всех его прообразов. Он обозначается через $f^{-1}(y)$. Полный прообраз подмножества $Y' \subseteq Y$ – это множество $f^{-1}(Y') = \{x \in X \mid f(x) \in Y'\}$. Ясно, что $f^{-1}(Y') = \coprod\limits_{y \in Y'} f^{-1}(y)$.

Пусть $X' \subseteq X$. Сужением функции $f : X \to Y$ называется функция $f|_{X'} : X' \to Y$, заданная формулой $f|_{X'}(x) = f(x)$. В обозначениях определения 1.2 $f|_{X'} = (X', Y, (X' \times Y) \cap \Gamma)$, где $\Gamma$ – график функции $f$.

Лемма 1.4. *Если $f : X \to Y$ – функция, то $X = \coprod\limits_{y \in Y} f^{-1}(y)$.*

Определение 1.5. Функция $f : X \to Y$ называется

- инъективной, если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$;
- сюръективной, если $\operatorname{Im} f = Y$;
- биективной, если она и инъективна, и сюръективна.

Определение 1.6. Пусть $f : X \to Y$ и $g : Y \to Z$ – функции. Композицией $g \circ f$ называется функция из $X$ в $Z$, заданная формулой $g \circ f(x) = g\big(f(x)\big)$ для любого $x \in X$. Композиция $g \circ f$ определена, только если множество значений функции $f$ совпадает с областью определения функции $g$.

Тождественной функцией $id_X : X \to X$ называется функция, заданная формулой $id_X(x) = x$. Часто индекс $X$ в обозначении тождественной функции опускают.

Функция $f^{-1} : Y \to X$ называется обратной к функции $f : X \to Y$, если $f^{-1} \circ f = id_X$, а $f \circ f^{-1} = id_Y$.

Лемма 1.7. *Пусть $f : X \to Y$ и $g : Y \to Z$ – функции.*

(1) *Если $g \circ f$ инъективна, то $f$ инъективна.*
(2) *Если $g \circ f$ сюръективна, то $g$ сюръективна.*
(3) *Для функции $f$ существует обратная тогда и только тогда, когда она биективна.*

Обратите внимание, что полный прообраз точки обозначается так же, как и значение обратной функции в этой точке. Это обычно не ведет к недоразумению, потому что если неизвестно, что $f$ биективна, то про обратную функцию говорить нельзя, и $f^{-1}(y)$ означает полный прообраз точки $y$; если же $f$ оказалась биекцией, то прообраз точки состоит из 1 элемента, и мы просто отождествляем одноэлементное множество с его элементом.

## 2. Отношения

Определение 2.1. Отношением на множестве $X$ называется подмножество в $X \times X$.

Если $R$ – отношение на $X$, то вместо $(x, y) \in R$ обычно пишут $xRy$. Это связано с тем, что конкретные отношения обычно обозначаются значками типа $\sim$ или $\geqslant$, а не буквами.

Определение 2.2. Отношение $\sim$ на множестве $X$ называется отношением эквивалентности, если для любых $x, y, z \in X$ выполнены следующие условия:

(1) $x \sim x$ (рефлексивность);
(2) $x \sim y \iff y \sim x$ (симметричность);
(3) $x \sim y \,\&\, y \sim z \implies x \sim z$ (транзитивность).

Определение 2.3. Пусть $\sim$ – отношение эквивалентности на $X$, а $x \in X$. Классом эквивалентности, содержащим $x$, называется множество всех элементов, эквивалентных $x$.

Лемма 2.4. *Два класса эквивалентности либо не пересекаются, либо совпадают. Множество $X$ распадается в дизъюнктное объединение классов эквивалентности.*

Определение 2.5. Фактормножеством $X$ по эквивалентности $\sim$ называется множество классов эквивалентности. Оно обозначается через $X/\sim$.

Определение 2.6. Отношение $\preccurlyeq$ называется отношением (частичного) порядка на множестве $X$, если для любых $x, y, z \in X$ выполнены следующие условия:

(1) $x \preccurlyeq x$ (рефлексивность);
(2) $x \preccurlyeq y \,\&\, y \preccurlyeq x \implies x = y$ (антисимметричность);
(3) $x \preccurlyeq y \,\&\, y \preccurlyeq z \implies x \preccurlyeq z$ (транзитивность).

Множество с заданным на нем отношением порядка называется частично упорядоченным множеством.

Отношение порядка называется линейным, если для любых $x, y \in X$ или $x \preccurlyeq y$ или $y \preccurlyeq x$.

Пусть $A$ – подмножество частично упорядоченного множества $X$.

В терминах отношения частичного порядка формулируется лемма Цорна, которая эквивалентна аксиоме выбора. Про все это вам подробно расскажут в курсе математической логики, желающие узнать об этом прямо сейчас могут прочитать формулировки, например, в Википедии или в любой книге по математической логике и теории множеств. Важным примером отношения частичного порядка является отношение включения на множество всех подмножеств данного множества. Для этого отношения лемма Цорна принимает следующий вид.

Лемма 2.7. *Пусть семейство множеств $\mathfrak{M}$ обладает тем свойством, что объединение любого линейно упорядоченного подмножества из $\mathfrak{M}$ есть снова множество из этого семейства. Тогда $\mathfrak{M}$ содержит максимальное множество.*

## 3. Алгебраические структуры

Определение 3.1. Операцией называется функция $X_1 \times \cdots \times X_n \to X$. 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 3.2. 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 3.3. *Нейтральный элемент единственен (это утверждение не зависит даже от ассоциативности).*

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

Лемма 3.4. *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 3.5. 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 3.6. *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 3.4, множество обратимых (по умножению) элементов кольца $R$ является группой. Эта группа называется мультипликативной подгруппой кольца и обозначается через $R^*$.

## 4. 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 4.1. Пусть $X$ – множество. Множество биекций $X \to X$ 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 $X \to X$ 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 $e$.

Циклическая запись перестановок. Транспозицией называется цикл длины 2.

Определение 4.2. Пусть $\sigma \in S_n$. Инверсией называется пара $(i, j)$, $1 \leqslant i < j \leqslant n$, такая, что $\sigma(i) > \sigma(j)$. Четность количества инверсий называется четностью перестановки $\sigma$.

Лемма 4.3. *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 $\sigma \circ (i\, i+1)$ инверсий на 1 меньше, чем в $\sigma$. Далее индукция по числу инверсий. □

Лемма 4.4. *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 $\sigma \circ (i\, i+1)$ инверсий на 1 меньше, чем в $\sigma$, в противном случае – на 1 больше. □

Теорема 4.5. *Отображение $\varepsilon : S_n \to \mathbb{Z}_2$, сопоставляющее перестановке ее четность, удовлетворяет соотношению $\varepsilon(\sigma\tau) = \varepsilon(\sigma) + \varepsilon(\tau) \mod 2$.*

## 5. 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 смысл считать, что группа – это множество с одной 0-арной, одной унарной и одной бинарной операциями; тогда свойства формулируются без квантора существования). Подробности я приведу только для интересующей нас ситуации групп и колец.

Определение 5.1. Непустое подмножество $H$ группы $G$ называется подгруппой, если $ab, a^{-1} \in H$ для любых $a, b \in H$.

Непустое подмножество $R$ кольца $A$ называется подкольцом, если $a+b, -a, ab \in R$ для любых $a, b \in R$.

Если $a \in H$, то $a^{-1} \in H$, а, следовательно, и их произведение равное нейтральному элементу лежит в подгруппе $H$. Аналогично любое подкольцо содержит 0. Ясно, что подгруппа (подкольцо) сама являются группой (соотв., кольцом) относительно тех же операций, которые заданы в объемлющей группе (соотв., кольце).

Если $H$ – подгруппа в $G$, то пишут $H \leqslant G$ (аналогичное обозначение для подкольца не используется).

В любой группе есть две тривиальные подгруппы: сама группа и множество состоящее из одного нейтрального элемента. Аналогично в кольце является подкольцом. По умолчанию мы всегда будем считать, что подкольцо содержит единицу самого кольца. При этой договоренности нулевое подмножество $\{0\}$ не является подкольцом.

Прямым произведением алгебраических структур одного типа называется декартово произведение 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. Дадим более подробные определения для групп и колец.

Определение 5.2. 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, $G = \bigoplus\limits_{k=1}^{n} G_n$.

Кольцо $R$ называется прямой суммой колец $R_1$ и $R_2$, если $R = R_1 \times R_2$, $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ и $(r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2)$, где $r_1, s_1 \in G_1$, а $r_2, s_2 \in G_2$. В этом случае пишут $R = R_1 \bigoplus R_2$.

Аналогично определяется прямая сумма любого конечного количества колец. Для бесконечного семейства колец подобная конструкция называется прямым произведением, а термин прямая сумма оставлен для множества последовательностей, у которых только конечное число элементов отлично от нуля (при этом прямая сумма бесконечного семейства ненулевых колец не имеет единицы, даже если все кольца семейства ее имеют!).

Лемма 5.3. *Мультипликативная группа прямой суммы конечного семейства колец равна прямому произведению мультипликативных групп этих колец, т. е.* $\left(\bigoplus\limits_{k=1}^{n} R_n\right)^* = \bigtimes\limits_{k=1}^{n} R_n^*$.

Глава 2

# Гомоморфизмы, факторгруппы и факторкольца

## 1. 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. Вместо этого я дам определение гомоморфизмов групп и колец отдельно.

Определение 1.1. Пусть $G$ с операцией $\star$ и $H$ с операцией $\#$ – группы. Функция $f : G \to H$ называется гомоморфизмом, если $f(a \star b) = f(a)\#f(b)$ для любых $a, b \in G$.

Пусть $R$ и $A$ – кольца. Функция $f : R \to A$ называется гомоморфизмом, если $f(a + b) = f(a) + f(b)$ и $f(ab) = f(a)f(b)$ для любых $a, b \in R$.

В нашем курсе по умолчанию все кольца являются кольцами с единицей, а все гомоморфизмы являются гомоморфизмами колец с единицей, т. е. $f(1) = 1$.

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

Ядро гомоморфизма $\operatorname{Ker} f = f^{-1}(e)$ (в случае гомоморфизма групп $e$ – нейтральный элемент множества значений, в случае колец $e = 0$).

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

Например, теорема 4.5 утверждает, что четность перестановки является гомоморфизмом $S_n \to \mathbb{Z}_2$. Ядро этого гомоморфизма, т. е. множество четных перестановок, называется знакопеременной группой (alternating group) и обозначается через $A_n$.

Лемма 1.2. *Если $f : G \to H$ – гомоморфизм групп, то $f(e_G) = e_H$, а $f(x^{-1}) = f(x)^{-1}$ для любого $x \in G$.*

*Если $f : R \to A$ – гомоморфизм колец, то $f(0) = 0$, а $f(-x) = -f(x)$ для любого $x \in R$. Кроме того, если $f$ – гомоморфизм колец с 1, то $f(x^{-1}) = f(x)^{-1}$ для любого обратимого $x \in R$.*

Лемма 1.3. *Пусть $f : G \to H$ – гомоморфизм групп, $g \in G$, а $h = f(g)$. Тогда $f^{-1}(h) = g \operatorname{Ker} f$.*

*Пусть $f : R \to A$ – гомоморфизм колец, $r \in R$, а $a = f(r)$. Тогда $f^{-1}(a) = r + \operatorname{Ker} f$.*

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

Определение 1.4. 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: $\forall g \in G : \ g^{-1}Hg \subseteq H$.

Аддитивная подгруппа $I$ кольца $R$ называется левым (правым) идеалом, если для любых $r \in R$ и $s \in I$ имеет место включение $rs \in I$ (соотв., $rs \in I$). В других обозначениях: $RI \subseteq I$ (соотв., $IR \subseteq I$). Если $I$ одновременно левый и правый идеал, то он называется двусторонним.

Заметим, что любая подгруппа абелевой группы является нормальной.

Лемма 1.5. *Подгруппа $H$ нормальна в группе $G$ тогда и только тогда, когда $\forall g \in G : \ gH = Hg$.*

Лемма 1.6. *Образ гомоморфизма групп является подгруппой, а ядро – нормальной подгруппой.*

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

## 2. Порождение

Определение 2.1. Пусть $X$ – подмножество группы или кольца $Y$. Подгруппой (соотв., подкольцом), порожденным множеством $X$, называется наименьшая подгруппа (соотв., подкольцо) в $Y$, содержащее $X$.

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

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

Подгруппа, порожденная одним элементом (точнее, одноэлементным множеством) называется циклической. Идеал, порожденный одним элементом, называется главным идеалом (этот термин не используется для двустороннего идеала некоммутативного кольца).

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

Лемма 2.2. *$\langle X\rangle$ состоит их всех элементов вида $x_1 \cdots x_k$, где $k$ – некоторое натуральное число, а $x_i \in X \cup X^{-1}$ (здесь, как обычно, $X^{-1} = \{x^{-1} \mid x \in X\}$).*

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

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

## 3. Смежные классы и теорема Лагранжа

Определение 3.1. Пусть $H$ – подгруппа в группе $G$. Левым смежным классом $G$ по $H$ называется множество $gH = \{gh \mid h \in H\}$ для некоторого элемента $g \in G$. Аналогично определяются правые смежные классы. Множество всех левых смежных классов обозначается $G/H$, а правых – $H\backslash G$. Элемент смежного класса часто называют его представителем.

Определим отношение "сравнимости по модулю $H$" на множестве $G$ по формуле:
$a \equiv b \mod H \iff a \in bH$.

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 1.5 $gH = Hg$, и сравнимость слева и справа совпадают.

Лемма 3.2. *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 $H$, таким образом второе утверждение леммы следует из леммы 2.4 главы 1. □

Лемма 3.3. *Любые два смежных класса равномощны, т. е. между ними существует биекция. В частности, если они конечны, то они содержат одинаковое количество элементов.*

Теорема 3.4 (теорема Лангранжа). *Если $H$ – подгруппа конечной группы $G$, то $|G| = |H| \cdot |G/H|$.*

Лемма 3.5. *Множества $G/H$ и $H\backslash G$ равномощны, т. е. между ними существует биекция.*

Доказательство. Биекция $G/H \to H\backslash G$ задается по правилу $aH \mapsto (aH)^{-1} = Ha^{-1}$ (здесь $(aH)^{-1} = \{(ah)^{-1} \mid h \in H\}$ ). □

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 $G = \mathbb{Z}$.

## 4. Факторгруппа и факторкольцо

Теорема 4.1. *Для любой нормальной подгруппы $H$ группы $G$ существует группа $F$ и эпиморфизм $f : G \to F$, ядро которого равно $H$.*

Доказательство. Положим $F = G/H$ и зададим отображение $f : G \to F$ по формуле $f(x) = xH$. 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 $f$ – гомоморфизм сразу следует из формулы умножения смежных классов. Очевидно, что $f$ – сюръективен. Уравнение $f(x) = e_{G/H} = H$ равносильно тому, что $x \in H$ (иначе смежные классы $f(x) = xH$ и $H$ не совпадают). Следовательно, $\operatorname{Ker} f = H$. □

Определение 4.2. Группа $G/H$, построенная в доказательстве, называется факторгруппой $G$ по $H$, а отображение $f$ – канонической проекцией или гомоморфизмом редукции по модулю $H$.

Теорема 4.3. *Для любого двустороннего идеала $I$ кольца $R$ существует кольцо $A$ и эпиморфизм $f : R \to A$, 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 $f$ задается также, как и в предыдущей теореме, где уже проверено, что оно сохраняет сложение, найдено ядро $f$ и отмечено, что это отображение сюръективно. Осталось проверить, что $f$ сохраняет умножение, но это сразу следует из определения произведения смежных классов. □

Определение 4.4. Кольцо $R/I$, построенное в доказательстве, называется факторкольцом $R$ по $I$, а отображение $f$ – канонической проекцией или гомоморфизмом редукции по модулю $I$.

Для двустороннего идеала $I$ кольца $R$ определено отношение "сравнение по модулю $I$", которое в соответствие с обсуждением в параграфе 3 является отношением эквивалентности. Доказательства утверждений настоящего параграфа показывают, что сравнения можно складывать и умножать, например, если $a \equiv b \mod I$, а $c \equiv d \mod I$, то $ac \equiv bd \mod I$. Таким образом, сравнения – это просто другая запись вычислений в факторгруппе или факторкольце.

## 5. Теорема о гомоморфизме

Теорема 5.1. *Пусть $G$, $G'$ и $G''$ – группы, $f : G \to G'$ – эпиморфизм, а $g : G \to G''$ – гомоморфизм. Если* $\operatorname{Ker} f = \operatorname{Ker} g$, *то существует единственный мономорфизм $h : G' \to G''$ такой, что $g = h \circ f$. Если $g$ – эпиморфизм, то $h$ – изоморфизм.*

Доказательство. Пусть $x' \in G'$. Так как гомоморфизм $f$ сюръективен, то существует $x \in G$ такой, что $f(x) = x'$. Определим $h(x') = g(x)$. Докажем, что наше определение корректно, т. е. не зависит от выбора прообраза элемента $x'$. Пусть $y \in G$ – другой элемент, образ которого под действием $f$ равен $x'$. Тогда $f(y) = f(x)$, откуда по лемме 1.3 $y = xt$ для некоторого $t \in \operatorname{Ker} f = \operatorname{Ker} g$. Получаем: $g(y) = g(x)g(t) = g(x)$. По определению $g\big(x\big) = h\big(f(x)\big)$, т. е. $g = h \circ f$, что доказывает существование отображения с требуемыми свойствами.

Проверим, что $h$ – гомоморфизм. Пусть $x', z' \in G'$. Так как $f$ сюръективна, то существуют $x, z \in G$ такие, что $x' = f(x)$, а $z' = f(z)$. Так как $f$ – гомоморфизм, то $f(xz) = x'z'$. Пользуясь тем, что $g$ является гомоморфизмом, получаем $h(x'z') = g(xz) = g(x)g(z) = h(x')h(z')$.

Пусть $h(x') = h(z')$ для некоторых $x', z' \in G'$. Так как $f$ сюръективна, то существуют $x, z \in G$ такие, что $x' = f(x)$, а $z' = f(z)$. Тогда $g(x) = g(z)$, откуда $x = zt$ для некоторого $t \in \operatorname{Ker} g = \operatorname{Ker} f$. Но тогда $x' = f(x) = f(z)f(t) = f(z) = z'$, что доказывает инъективность $h$. Если $g = h \circ f$ – сюръективно, то по лемме 1.7 главы 1 $h$ также сюръективно, и, следовательно, является изоморфизмом.

Если $\tilde{h}$ другой гомоморфизм, удовлетворяющий условию теоремы, то $\tilde{h}\big(f(x)\big) = h\big(f(x)\big)$, а так как $f$ сюръективна, то $\tilde{h}(x') = h(x')$ для любого $x' \in G'$, а это и означает, что $\tilde{h} = h$. □

Следствие 5.2 (Теорема о гомоморфизме групп). *Пусть $f : G \to G''$ – гомоморфизм групп. Тогда* $\operatorname{Im} f \cong X/Ker f$.

Доказательство. Отображение $\bar{f} : G \to \operatorname{Im} f$ заданное формулой $\bar{f}(x) = f(x)$ является эпиморфизмом, причем его ядро равно $\operatorname{Ker} f$. Гомоморфизм редукции $G \to G/\operatorname{Ker} f$ обладает теми же свойствами. По предыдущей теореме существует изоморфизм $\operatorname{Im} f \to G/\operatorname{Ker} f$. □

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

Теорема 5.3. *Пусть $R$, $R'$ и $R''$ – кольца, $f : R \to R'$ – эпиморфизм, а $g : R \to R''$ – гомоморфизм. Если* $\operatorname{Ker} f = \operatorname{Ker} g$, *то существует единственный мономорфизм $h : R' \to R''$ такой, что $g = h \circ f$. Если $g$ – эпиморфизм, то $h$ – изоморфизм.*

Следствие 5.4 (Теорема о гомоморфизме колец). *Пусть $f : R \to R''$ – гомоморфизм колец. Тогда* $\operatorname{Im} f \cong R/Ker f$.

Глава 3

# Коммутативные кольца

## 1. Китайская теорема об остатках

Все кольца в этой главе являются коммутативными и содержат единицу.

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,

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

Определение 1.1. Идеалы $I$ и $J$ кольца $R$ называются взаимно простыми, если $I + J = R$.

Лемма 1.2. *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 $x = xa + xb \in (I \cap J)I + (I \cap J)J \subseteq IJ$. □

Теорема 1.3. $R/IJ \cong R/I \oplus R/J$.

Доказательство. Естественный гомоморфизм $R \to R/I \oplus R/J$ 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 $(x + I, y + J)$. □

Лемма 1.4. *Если идеал $J$ взаимно прост с каждым из идеалов $I_1, \ldots, I_n$, то он взаимно прост с их произведением.*

Доказательство. $R = J + I_1 = J + I_1 R = J + I_1(J + I_2) = (J + I_1 J) + I_1 I_2 \subseteq J + I_1 I_2$. Далее по индукции. □

Следствие 1.5 (китайская теорема об остатках). $R/(I_1 \cdots I_n) \cong R/I_1 \oplus \cdots \oplus R/I_n$.

Замечание 1.6. Если $R$ некоммутативно, то $IJ$ надо заменить на $IJ + JI$.

## 2. Простые и максимальные идеалы

Определение 2.1. 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 2.2. *Для любого собственного идеала существует максимальный идеал, содержащий его.*

Определение 2.3. 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 2.4. *Прообраз простого идеала – простой. Прообраз максимального идеала при эпиморфизме – максимальный.*

Следствие 2.5. *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.*

Определение 2.6. Кольцо $R$ называется кольцом главных идеалов, если любой идеал в $R$ является главным (напомним, что это означает, что он имеет вид $aR$ для некоторого $a \in R$).

Лемма 2.7. *В области главных идеалов любой ненулевой простой идеал является максимальным.*

Доказательство. Пусть $p \in R \setminus \{0\}$ таков, что $pR$ – простой идеал. Пусть $M$ – собственный идеал, содержащий $pR$. Так как любой идеал в $R$ является главным, то $M = qR$ для некоторого необратимого элемента $q$. Следовательно, $p = qr$ для некоторого $r \in R$. Если $r \in pR$, то $p = qps$ для некоторого $s \in R$, а так как $R$ – область целостности, то $qs = 1$, что противоречит условию $qR \neq R$.
Так как $pR$ – простой идеал, $qr \in pR$, а $r \notin pR$, то $q \in pR$, откуда $M = qR = pR$. □

## 3. Факториальность колец главных идеалов

Определение 3.1. 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 $a$.

Лемма 3.2. *Пусть $R$ область целостности. Элементы $a, b \in R$ ассоциированы тогда и только тогда, когда $a = b\varepsilon$ для некоторого $\varepsilon \in R^*$. Элемент $a \in R$ неприводим, если он не раскладывается в произведение необратимых элементов.*

Определение 3.3. 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 $i = 1, \ldots, n$.

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

Лемма 3.4. *Пусть $R$ – область главных идеалов, а $a, c \in R$, причем $c$ – неприводимый, а $a$ не делится на $c$. Тогда $aR + cR = R$.*

Доказательство. Так как любой идеал главный, то $aR + cR = bR$ для некоторого $b \in R$. Так как $c \in bR$ неприводим, то либо $cR = bR$, либо $bR = R$. Но из $cR = bR$ следует, что $a \in cR$, что противоречит условию. □

Лемма 3.5. *Пусть $R$ – область главных идеалов, $a, b, c \in R$, причем $c$ – неприводимый. Если $ab$ делится на $c$, то $a$ или $b$ делится на $c$. Другими словами, $c$ неприводим тогда и только тогда, когда идеал $cR$ – простой.*

Доказательство. Если ни $a$ ни $b$ не делится на $c$, то по лемме 3.4 $aR + cR = bR + cR = R$. Но тогда по лемме 1.4 $cR + abR = R$, откуда $ab \notin cR$. □

Лемма 3.6. *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

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

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 $p_n R$ простой. Поэтому найдется $l$ такое, что $q_l \in p_n R$. 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 $\varepsilon p_1 \cdots p_{n-1} = \theta\delta q_1 \cdots q_m / q_l$. По индукционному предположению $n - 1 = m - 1$ и существует биекция $\tau : \{1, \ldots, n-1\} \to \{1, \ldots, m\} \setminus \{l\}$ 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. □

Лемма 3.7. *Если $R$ – область главных идеалов, то каждый необратимый элемент раскладывается в произведение неприводимых.*

Доказательство. Пусть $r \in R$ – необратимый элемент. Идеал $rR$ содержится в каком-то максимальном идеале, а так как любой идеал главный, то $rR$ содержится в некотором максимальном идеале $p_1 R$. Так как максимальный идеал является простым, то $p_1$ неприводим. Таким образом, $r = r_1 p_1$ для некоторого $r_1 \in R$ и неприводимого $p_1 \in R$. Если $r_1$ обратим, то все доказано. Иначе $r_1 = r_2 p_2$ для некоторого $r_2 \in R$ и неприводимого $p_2 \in R$. Продолжим процесс. Если на каком-то шаге получим обратимый элемент $r_k$, то все доказано. Иначе получим строго возрастающую цепочку идеалов $rR \subset r_1 R \subset r_2 R \subset \cdots$.

Пусть $I = \bigcup\limits_{k=1}^{\infty} r_k R$. Ясно, что $I$ – идеал, поэтому $I = qR$ для некоторого $q \in R$. По определению объединения $q \in r_j R$ для некоторого $j$. Тогда $I = qR = r_j R$, откуда $r_{j+1} R = r_j R$, т.е. $p_{j+1}$ обратим, что противоречит его неприводимости. □

Из результатов настоящего параграфа непосредственно вытекает следующий факт.

Теорема 3.8. *Область главных идеалов является факториальным кольцом.*

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.

## 4. Евклидовы кольца

Определение 4.1. Пусть $R$ – область целостности. Предположим, что задана функция $f : R \to \mathbb{N} \cup \{-\infty\}$ 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”.

Теорема 4.2. *Евклидово кольцо является кольцом главных идеалов.*

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 $a \in I$. □

## 5. Наибольший общий делитель

Определение 5.1. 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 $b$ обозначется 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 5.2 (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 $d = \gcd(a, b)$. □

Следствие 5.3. *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 5.4. *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. □

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 $\gcd(a, b) = r_0 x_0 + r_1 y_0 = ax_0 + by_0$, что и требовалось.

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

Определение 5.5. 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 $\operatorname{lcm}(a, b)$.

Лемма 5.6. *Если $R$ – область главных идеалов, $a, b \in R \setminus \{0\}$, то* $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$.

Доказательство. Пусть $d = \gcd(a, b)$, $a = a'd$, 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 $a'b'd = \frac{ab}{\gcd(a,b)}$. □

## 6. Поле частных и разложение на простейшие дроби

Вначале мы хотим вложить произвольную область целостности $R$ в поле, состоящее из дробей $r/s$, $r, s \in R$, $s \neq 0$, как кольцо целых чисел вложено в поле рациональных чисел. Такое поле будет называться полем частных кольца $R$.

Лемма 6.1. *Пусть $R$ – область целостности. Тогда существует поле $F$ и мономорфизм $\lambda : R \rightarrowtail F$, обладающие следующим универсальным свойством: для любого поля $K$ и мономорфизма $\varphi : R \rightarrowtail K$ существует единственный мономорфизм $\psi : F \rightarrowtail K$ такой, что $\varphi = \psi \circ \lambda$.*

Доказательство. Зададим отношение "$\sim$" на множестве $R \times \big(R \smallsetminus \{0\}\big)$ по следущему правилу:

$$(r_1, s_1) \sim (r_2, s_2), \text{ если } r_1 s_2 = r_2 s_1.$$

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. $r_1 s_2 = r_2 s_1$ и $r_2 s_3 = r_3 s_2$. Если $r_2 = 0$, то учитывая, что $s_2 \neq 0$, получаем $r_1 = r_3 = 0$. В противном случае, перемножая равенства имеем $r_1 s_2 r_2 s_3 = r_2 s_1 r_3 s_2$, которое можно сократить на $s_2 r_2$, потому что $R$ – область целостности. В любом случае $r_1 s_3 = r_3 s_1$, что доказывает транзитивность.

Обозначим через $r/s$ или $\frac{r}{s}$ класс эквивалентности "$\sim$". Обозначим через $F$ множество классов эквивалентности и определим на $F$ операции сложения и умножения:

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}, \qquad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2},$$

Докажем, что наше определение не зависит от выбора представителя класса 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. $r_1 s_1' = r_1' s_1$ и $r_2 s_2' = r_2' s_2$. перемножая последние равенства получаем $r_1 s_1' r_2 s_2' = r_1' s_1 r_2' s_2$, откуда $\frac{r_1 r_2}{s_1 s_2} = \frac{r_1' r_2'}{s_1' s_2'}$. Далее,

$$(r_1 s_2 + r_2 s_1) s_1' s_2' = r_1 s_2 s_1' s_2' + r_2 s_1 s_1' s_2' = r_1' s_2 s_1 s_2' + r_2' s_1 s_1' s_2 = (r_1' s_2' + r_2' s_1') s_1 s_2,$$

что доказывает равенство $\frac{r_1 s_2 + r_2 s_1}{s_1 s_2} = \frac{r_1' s_2' + r_2' s_1'}{s_1' s_2'}$.

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

$$\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) + \frac{r_3}{s_3} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} + \frac{r_3}{s_3} = \frac{r_1 s_2 s_3 + r_2 s_1 s_3 + r_3 s_1 s_2}{s_1 s_2 s_3}$$
$$\frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right) = \frac{r_1}{s_1} + \frac{r_2 s_3 + r_3 s_2}{s_2 s_3} = \frac{r_1 s_2 s_3 + r_2 s_3 s_1 + r_3 s_2 s_1}{s_1 s_2 s_3}.$$

Нейтральным элементом по сложению является $\frac{0}{1} = \frac{0}{s}$, обратным к $\frac{r}{s}$ – $\frac{-r}{s}$. Мультипликативно нейтральным является $\frac{1}{1} = \frac{s}{s}$. Если $\frac{r}{s} \neq 0$, то $r \neq 0$ и и для этого элемента существует мультипликативно обратный $\frac{s}{r}$. Таким образом, $F$ – поле. Зададим отображение $\lambda : R \to F$ по формуле $\lambda(r) = \frac{r}{1}$. Сразу видно, что $\lambda$ – гомоморфизм, причем $\lambda(r) = 0 \iff r = 0$, откуда $\operatorname{Ker} \lambda = \{0\}$.

Пусть теперь $\varphi : R \rightarrowtail K$ – вложение $R$ в поле $K$. Определим отображение $\psi : F \to K$ равенством $\psi(r/s) = \varphi(r)\varphi(s)^{-1}$ (так как $s \neq 0$, а $\varphi$ – мономорфизм, то $\varphi(s) \neq 0$, а так как $K$ – поле, то существует $\varphi(s)^{-1}$). Если $\frac{r'}{s'} = \frac{r}{s}$, то $r's = rs'$, и $\varphi(r')\varphi(s) = \varphi(r)\varphi(s')$. Домножая на $\varphi(s)^{-1}\varphi(s')^{-1}$ 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 $\varphi = \psi \circ \lambda$. Легко проверить, что $\psi$ является гомоморфизмом. Наконец, любой гомоморфизм полей является мономорфизмом. □

Определение 6.2. Поле $F$, построенное в доказательстве теоремы, называется полем частных кольца $R$. Обычно мы отождествляем элементы $R$ с их образами в $F$ под действием $\lambda$ 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 6.3. 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 6.4. *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 $p_1, \ldots, p_m \in R$ – 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. □

## 7. Целые числа: теорема Эйлера

Разберем подробнее случай кольца целых чисел. Так как $\mathbb{Z}$ является евклидовым кольцом, то оно является областью главных идеалов. По лемме 2.7 любой ненулевой простой идеал является максимальным, откуда $\mathbb{Z}/p\mathbb{Z}$ является полем тогда и только тогда, когда $p$ – простое число.

Если числа $n_1, \ldots, n_l$ – 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 7.1. Порядок мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^*$ обозначается $\varphi(n)$. Функция $\varphi : \mathbb{N} \to \mathbb{N}$ называется функцией Эйлера.

Лемма 7.2. *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 5.3 означает, что $m$ взаимно просто с $n$.

Второе утверждение очевидно. □

Лемма 7.3. *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 7.4. *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* $n=\prod\limits_{i=1}^{l}p_i^{k_i}$. *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 7.5 (теорема Эйлера). *Если* $a$ *взаимно просто с* $n$, *то* $a^{\varphi(n)}\equiv 1 \mod n$.

На самом деле несложно получить более точный результат, а именно заменить произведение чисел $\varphi(p_i^{k_i})$ на их наименьшее общее кратное. Для этого нам понадобится следующее понятие из теории групп.

Определение 7.6. 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 7.7 (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 $d=p_1^{k_1}\cdots p_l^{k_l}$ – 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 $\operatorname{ord} g=mn$, то $\operatorname{ord} g^m=n$. Возводя элементы $g_1,\dots,g_l$ в подходящие степени, можно считать, что $\operatorname{ord} g_i=p_i^{k_i}$ 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 $\operatorname{ord}(ab)=\operatorname{ord} a\operatorname{ord} b$. 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 $\operatorname{ord} a$ и $\operatorname{ord} b$, 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 $\operatorname{ord} a$, а $t$ – на $\operatorname{ord} b$. Если $(ab)^n=e$, то $a^n=b^{-n}$, откуда $n$ делится на $\operatorname{ord} a$ и $\operatorname{ord} b$. Так как эти порядки взаимно просты, то $n$ делится на их произведение, а так как при $n=\operatorname{ord} a\operatorname{ord} b$ верно, то $\operatorname{ord}(ab)=\operatorname{ord} a\operatorname{ord} b$.

Теперь индукцией по $l$ легко доказать, что $\operatorname{ord}(g_1\cdots g_l)=\operatorname{ord} g_1\cdots\operatorname{ord} g_l=d$. □

Определим функцию $\varphi'\colon\mathbb{N}\to\mathbb{N}$ равенством

$$\varphi'\Big(\prod_{i=1}^{l}p_i^{k_i}\Big)=\operatorname{lcm}_{1\leqslant i\leqslant l}\big(p_i^{k_i}-p_i^{k_i-1}\big).$$

Теорема 7.8. *Если* $a$ *взаимно просто с* $n$, *то* $a^{\varphi'(n)}\equiv 1 \mod n$.

Доказательство. Пусть $n=\prod\limits_{i=1}^{l}p_i^{k_i}$. 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 предыдущей леммы 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. □

Оценка экспоненты группы $(\mathbb{Z}/n\mathbb{Z})^*$ из теоремы Кармайкла почти точна. Можно доказать, что группа $(\mathbb{Z}/p^k\mathbb{Z})^*$ циклическая для любого простого $p \neq 2$ и при $p = 2$, $k \leqslant 2$, а при $k \geqslant 3$ экспонента группы $(\mathbb{Z}/2^k\mathbb{Z})^*$ равна $2^{k-2}$ (т. е. в 2 раза меньше ее порядка). Определим функцию Кармайкла $\lambda : \mathbb{N} \to \mathbb{N}$ как точное значение экспоненты группы $(\mathbb{Z}/n\mathbb{Z})^*$. Тогда утверждения, приведенные в этом абзаце можно сформулировать следующим образом.

Теорема 7.9. *Если $n$ не делится на 8, то $\lambda(n) = \varphi'(n)$. Если $n = 2^k m$, где $m$ нечетно, а $k \geqslant 3$, то $\lambda(n) = \operatorname{lcm}(\varphi'(m), 2^{k-2})$.*

## 8. Многочлены

Определение многочлена (одной переменной) и его степени. Отличие многочлена от полиномиальной функции.

Теорема 8.1. *Кольцо многочленов $F[t]$ над полем $F$ является евклидовым кольцом с евклидовой нормой* deg.

Заметим, что в отличии от целых чисел с евклидовой нормой "модуль", деление с остатком в кольце многочленов с евклидовой нормой deg единственно.

Теорема 8.2 (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.*

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 8.3. *Пусть $t_0, y_0, \ldots, t_n, y_n \in F$, 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 $i = 0, \ldots, n$. Этот многочлен можно найти по формуле*

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

Доказательство. По теореме Безу условия $p(t_i) = y_i$ равносильны условиям $p \equiv y_i \mod (t - t_i)$. По китайской теореме об остатках существует единственный по модулю $w(t) = \prod\limits_{i=0}^{n}(t - t_j)$ 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. □

Другой, итерационный, способ решить задачу интерполяции называется интерполяцией по Ньютону. На $k$-ом шаге строится многочлен степени $\leqslant k - 1$, удовлетворяющий первым $k$ условиям. На первом шаге положим $p_0(t) = y_0$. Предположим, что построен многочлен $p_k$, удовлетворяющий условиям $\deg p_k \leqslant k - 1$ и $p_k(t_i) = y_i$ для любого $i = 0, \ldots, k - 1$. 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.

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 8.4. 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 8.5. *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

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

□

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

Лемма 8.7 (универсальное свойство кольца многочленов). *Пусть $R$ коммутативное кольцо с 1, $n \in \mathbb{N}$, а $c_1, \ldots, c_n \in R$. Существует единственный гомоморфизм $\varphi : \mathbb{Z}[z_1, \ldots, z_n] \to R$ такой, что $\varphi(z_k) = c_k$ при всех $k = 1, \ldots, n$.*

Доказательство. Для того чтобы выполнялись требуемые равенства мы должны положить $\varphi(z) = z(c_0, \ldots, c_n)$ для любого многочлена $z \in \mathbb{Z}[z_1, \ldots, z_n]$. 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 $\varphi : \mathbb{Z}[z_1, \ldots, z_n] \to R$ и он единственный. □

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

Доказательство леммы 8.5 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 $a_0, \ldots, a_n, b_0, \ldots, b_m$ (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 8.7 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 $\varphi : P \to R$ 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 $\psi : A \to B$ 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 8.6 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. □

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 8.8. 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 8.9. *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

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

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

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 8.10. *(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 $a_n$.*

## 9. Комплексные числа

Так как многочлен $t^2+1$ неприводим в кольце $\mathbb{R}[t]$, а $\mathbb{R}[t]$ – кольцо главных идеалов, то идеал $(t^2+1)\mathbb{R}[t]$ максимален. Следовательно, факторкольцо $\mathbb{R}[t]/(t^2+1)$ является полем.

Определение 9.1. Поле $\mathbb{C} = \mathbb{R}[t]/(t^2+1)$ называется полем комплексных чисел.

Композиция отображений $\mathbb{R} \hookrightarrow \mathbb{R}[t] \twoheadrightarrow \mathbb{C}$ 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 $\leqslant 1$ (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 $\overline{z} = x-iy$ называется комплексно сопряженным к $z$. Из определения сразу следует, что $z \in \mathbb{R} \iff z = \overline{z}$, $z+\overline{z}, z\overline{z} \in \mathbb{R}$. Мы знаем, что $\mathbb{C}$ является полем, значит любой ненулевой элемент имеет мультипликативный обратный. Для того чтобы его найти, 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 9.2. *Отображение $\mathbb{C} \to \mathbb{C}$, отображающее $z$ в $\overline{z}$ является автоморфизмом поля $\mathbb{C}$.*

Следствие 9.3. *Пусть $g \in \mathbb{C}[t]$, а $w \in \mathbb{C}$. Обозначим через $\overline{g}$ многочлен, коэффициенты которого сопряжены с коэффициентами многочлена $g$.*

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

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 $g(t) = \overline{g}(t) = (t-\overline{w})^k \overline{f}(t)$, причем $\overline{f}(\overline{w}) = \overline{f(w)} \neq 0$, что и означает, что кратность $\overline{w}$ в $g$ равна $k$. □

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

Определение 9.4. Поле $F$ называется алгебраически замкнутым, если любой многочлен из $F[t]$ степени $\geqslant 1$ имеет хотя бы один корень в $F$.

Теорема 9.5 (Основная теорема алгебры). *Поле комплексных чисел алгебраически замкнуто.*

Лемма 9.6. *Если поле $F$ алгебраически замкнуто, то любой многочлен из $F[t]$ раскладывается на множители степени 1.*

Следствие 9.7. *Любой многочлен степени $\geqslant 3$ из кольца $\mathbb{R}[x]$ приводим. Следовательно, любой многочлен над $\mathbb{R}$ раскладывается на множители степени $\leqslant 2$.*

Доказательство. Пусть $p \in \mathbb{R}[t] \subseteq \mathbb{C}[t]$, $\deg p \geqslant 3$. 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 9.2 $p(\overline{w}) = 0$. Так как в этом случае $t - w$ и $t - \overline{w}$ взаимно просты, а по теореме Безу $p$ делится на каждый из этих многочленов, то он делится и на их произведение $(t - w)(t - \overline{w}) = t^2 - (w + \overline{w})t + w\overline{w}$, 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. □

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,

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

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:

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

Другими словами, при перемножении комплексных чисел их модули перемножаются, а аргументы складываются. Геометрически это означается, 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:

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

Последняя формула называется формулой Муавра.

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

$$\mathbb{C}^* \cong \mathbb{R}^*_{>0} \times \mathbb{R}/2\pi\mathbb{Z}. \tag{1}$$

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

Предложение 9.8. $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z}$.

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

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:

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

При этом из теории функций комплексной переменной известно, что если две функции $\mathbb{C} \to \mathbb{C}$ 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 9.8 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 (1) 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 $k \in \mathbb{Z}/nZ$. 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 $\mathbb{C} \to \mathbb{C}$, 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 отличии 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 $k \in (\mathbb{Z}/n\mathbb{Z}))^*$.

## 10. 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`.

Следующая теорема будет полезна при тестировании натурального числа или многочлена над конечным полем на простоту (неприводимость).

Теорема 10.1. *Конечная подгруппа мультипликативной группы поля – циклическая.*

Доказательство. Пусть $G$ – подгруппа мультипликативной группы поля порядка $n$, а экспонента этой группы равна $d$. Тогда уравнение $t^d = 1$ имеет в поле $n$ решений, откуда следует, что $d = n$. Теперь по пункту (5) леммы 7.7 группа $G$ является циклической. □

Следствие 10.2. *Пусть $\mathbb{F}_q$ – конечное поле нечетного порядка $q$. Положим $(\mathbb{F}_q^*)^2 = \{x^2 \mid x \in \mathbb{F}_q^*\}$. Очевидно, что $(\mathbb{F}_q^*)^2$ является подгруппой в $\mathbb{F}_q^*$.*

(1) $|\mathbb{F}_q^* : (\mathbb{F}_q^*)^2| = 2$.

(2) *Для любого* $x \in \mathbb{F}_q^*$ *имеем* $x^{\frac{q-1}{2}} = \pm 1$.

(3) *Пусть* $x \in \mathbb{F}_q^*$. *Элемент* $x$ *принадлежит* $(\mathbb{F}_q^*)^2$ *тогда и только тогда, когда* $x^{\frac{q-1}{2}} = 1$.

Доказательство. По теореме $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$, а в этой группе все утверждения легко проверяются, учитывая, что $q-1$ четно (только возведение в квадрат надо заменить умножением на 2). □

Определение 10.3. Пусть $p$ – нечетное простое число, а $a \in \mathbb{N}$ не делится на $p$. Символом Лежандра $\left(\frac{a}{p}\right)$ называется число 1, если $a \in (\mathbb{F}_p^*)^2$ и $-1$ в противном случае. Другими словами, $\left(\frac{a}{p}\right) = \pm 1$ и $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

Пусть $n = p_1 \cdots p_m$, где $p_k$ – нечетные простые числа (не обязательно различные), а $a \in \mathbb{N}$ взаимно просто с $N$. Символом Якоби называется число $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_n}\right)$.

Следующие 2 утверждения дают возможность эффективно вычислять символ Якоби.

Предложение 10.4 (свойства символа Якоби). *Пусть* $n$ *– нечетное число. Тогда*

$$\left(\frac{1}{n}\right) = 1; \qquad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}; \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}.$$

Теорема 10.5 (квадратичный закон взаимности). *Если* $a$ *и* $n$ *– взаимно простые нечетные числа, то* $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}}$.

Теорема 10.6. *Пусть* $n$ *– нечетное число. Если* $n$ *не простое, то существует не более* $n/2$ *элементов* $a \in \mathbb{Z}_n^*$, *для которых* $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \mod n$.

Теорема 10.7. *Пусть* $R$ *– кольцо целых чисел или кольцо многочленов от одной переменной над полем. Тогда в нем существует бесконечно много простых элементов.*

Доказательство. Пусть $p_1, \ldots, p_m$ – все простые элементы кольца $R$. Тогда произведение $p_1 \cdots p_m + 1$ не делится ни на один простой и не является обратимым, что противоречит факториальности кольца. □

Теорема 10.8 (Теорема Дирихле о простых в арифметической прогрессии). *Если* $a$ *и* $b$ *взаимно простые целые числа, то множество* $a + b\mathbb{Z}$ *содержит бесконечно много простых чисел.*

Теорема 10.9 (распределение простых чисел). *Обозначим через* $\pi(n)$ *количество простых чисел от 2 до* $n$. *Тогда* $\frac{\pi(n)}{n/\ln n} \to 1$ *при* $n \to \infty$.

Практически важной задачей является нахождение больших простых чисел. В соответствии с предыдущей теоремой простых числе 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 $\frac{|T|}{\varphi(n)}$ 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 равен 1, то тест плохой и применять его в коммерческих целях нецелесообразно. Те числа $n$, для которых $\frac{|T|}{\varphi(n)} = 1$, 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 | $\sup \frac{\lvert T\rvert}{\varphi(n)}$ |
|---|---|---|---|
| Ферма | $\{a \mid a^{n-1} = 1\}$ | 561, 1105, 1729,... | $\leqslant 1/2$ |
| Эйлера | $\{a \mid a^{\frac{n-1}{2}} = \pm 1\}$ | 1729,2465,... | $\leqslant 1/2$ |
| Соловея–Штрассена | $\{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}$ | $\varnothing$ | $\leqslant 1/2$ |
| Миллера–Рабина | $\{a \mid a^k = 1$ или $\exists j < m : a^{2^j k} = -1\}$ где $n-1 = 2^m k$, а $k$ нечетно | $\varnothing$ | $\leqslant 1/4$ |

Глава 4

# Векторные пространства

## 1. Основные определения

Определение 1.1. Пусть $V$ – абелева группа в аддитивной записи, $F$ – поле, и задана операция (умножение) $F \times V \to V$. Предположим, что для любых $u, v \in V$ и $\alpha, \beta \in F$ выполнены следующие свойства:

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

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

Далее в настоящей главе используются следующие обозначения и соглашения:

- $F$ – поле;
- $V$ – векторное пространство над $F$;
- $F^n$ – множество столбцов высоты $n$ 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 1.2 (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 $u_1, \ldots, u_n \in V$, а $\alpha_1, \ldots, \alpha_n \in F$. Сумма

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

называется линейной комбинацией векторов $u_1, \ldots, u_n \in V$ с коэффициентами $\alpha_1, \ldots, \alpha_n \in F$. 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 1.3. $\langle S \rangle = \{ \sum\limits_{k=1}^{n} u_k \alpha_k \mid u_1, \ldots, u_n \in S,\ \alpha_1, \ldots, \alpha_n \in F \}$.

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 1.4. Базисом называется линейно независимая система образующих.

## 2. Другие определения базиса и его существование

Теорема 2.1 (эквивалентные определения базиса). *Следующие условия на подмножество $S$ векторного пространства $V$ эквивалентны.*

(1) *$S$ – базис.*
(2) *$S$ – максимальная линейно независимая система.*
(3) *$S$ – минимальная система образующих.*
(4) *Для любого элемента $v \in V$ существует единственный набор чисел $\alpha_s \in F$, почти все из которых равны нулю, такой, что $v = \sum_{s\in S} s\alpha_s$.*

Теорема 2.2 (о существовании базиса). *Пусть $X, Y \subseteq V$, причем $X$ – линейно независима, 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 максимальности $Z$ множество $Z \cup \{y\}$ линейно зависимо, т. е. существуют $\alpha_y, \alpha_z \in F$, где $z \in Z$, почти все, но не все равные нулю, такие что $y\alpha_y + \sum_{z\in Z} z\alpha_z = 0$. Коэффициент $\alpha_y$ не может быть равен нулю, это противоречило бы линейной независимости множества $Z$. Следовательно, $y$ принадлежит линейной оболочке множества $Z$. Поэтому и все множество $Y$ содержится в $\langle Z\rangle$, откуда $V = \langle Y\rangle = \langle Z\rangle$, т. е. $Z$ – система образующих, а значит и базис. □

## 3. Размерность пространства и координаты вектора

Лемма 3.1 (о замене). *Пусть $B$ – базис пространства $V$, $u \in B$, а вектор $v \in V$ не лежит в линейной оболочке множества $B \setminus \{u\}$. Тогда множество $B \setminus \{u\} \cup \{v\}$ также является базисом пространства $V$.*

Доказательство. Положим $B' = B \setminus \{u\}$. Так как $B$ – базис, существуют числа $\alpha_u, \alpha_b \in F$, $b \in B'$, почти все равные нулю, такие что $v = u\alpha_u + \sum_{b\in B'} b\alpha_b$. Заметим, что $\alpha_u \neq 0$, иначе $v$ принадлежал бы линейной оболочке множества $B'$, что не так по условию. Следовательно, $u = \frac{1}{\alpha_u}(v - \sum_{b\in B'} b\alpha_b) \in \langle B' \cup \{v\}\rangle$. Таким образом, $V = \langle B\rangle \subseteq \langle B' \cup \{v\}\rangle$, т. е. $B' \cup \{v\}$ – система образующих.

Предположим, что $v\beta_v + \sum_{b\in B'} b\beta_b = 0$ для некоторых $\beta_v, \beta_b \in F$, почти всех равных нулю. Подставляя вместо $v$ его выражение через линейную комбинацию векторов базиса $B$, получаем $u\alpha_u\beta_v + \sum_{b\in B'} b(\beta_b + \alpha_b\beta_v) = 0$. Так как $B$ базис, то все коэффициенты этой линейной комбинации равны нулю, в частности, $\alpha_u\beta_v = 0$. Так как $\alpha_u \neq 0$, то $\beta_v = 0$. Подставляя это в исходное равенство, получаем $\sum_{b\in B'} b\beta_b = 0$, откуда $\beta_b = 0$ при всех $b \in B'$. Таким образом, множество $B' \cup \{v\}$ линейно независимо, и, следовательно, является базисом. □

Заметим, что обычно леммой о замене называется следствие только что доказанного утверждения, утверждающее, что несколько элементов линейно независимого набора можно заменить тем же количеством элементов из данной системы образующих так, чтобы набор остался линейно независимым.

Теорема 3.2 (количество элементов в базисе). *Любые два базиса пространства $V$ равномощны.*

Доказательство. Приведем доказательство для случая, когда один из базисов конечен. Доказательство для бесконечномерного случая в каком-то смысле проще. 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 $B$ и $C = \{c_1, \ldots, c_n\}$ – базисы пространства $V$. Не умоляя общности можно считать, что мощность множества $B$ больше $n$. Тогда существует подмножество $\{b_1, \ldots, b_n\} \subseteq B$ Индукцией по $k = 0, \ldots, n$ докажем, что существует инъективная функция $\sigma_k : \{1, \ldots, k\} \to \{1, \ldots, n\}$ такая, что множество $B \setminus \{b_1, \ldots, b_k\} \cup \{c_{\sigma_k(1)}, \ldots, c_{\sigma_k(k)}\}$ является базисом. При $k = 0$ доказывать нечего. Пусть $0 < k \leqslant n$. По индукционному предположению существует инъективная функция $\sigma_{k-1} : \{1, \ldots, k-1\} \to \{1, \ldots, n\}$ такая, что множество $B_{k-1} = B \setminus \{b_1, \ldots, b_{k-1}\} \cup \{c_{\sigma_{k-1}(1)}, \ldots, c_{\sigma_{k-1}(k-1)}\}$ является базисом. Линейная оболочка множества $B' = B_{k-1} \setminus \{b_k\}$ не равна всему пространству, иначе $b_k$ выражалось бы через линейную комбинацию векторов из $B'$, что противоречит линейной независимости $B_{k-1}$. Множество $C$ не содержится в $\langle B' \rangle$, иначе $V = \langle C \rangle \subseteq \langle B' \rangle$, что не так. Следовательно, существует $m$ от 1 до $n$ такое, что $c_m \notin \langle B' \rangle$. Так как $\sigma_{k-1}(i) \subseteq B'$ при всех $1 \leqslant i \leqslant k-1$, то $m \notin \operatorname{Im} \sigma_{k-1}$. Поэтому функция $\sigma_k : \{1, \ldots, k\} \to \{1, \ldots, n\}$, заданная равенствами $\sigma_k(i) = \sigma_{k-1}(i)$ при $i < k$ и $\sigma_k(k) = m$, является инъективной. Наконец, по лемме о замене $B' \cup \{c_{\sigma_k(k)}\}$ является базисом, что доказывает наше утверждение.

При $k = n$ получим, что $B \setminus \{b_1, \ldots, b_n\} \cup C$ является базисом, содержащим базис $C$. Так как две максимальных линейно независимых системы не могут строго содержаться одна в другой, то $B \setminus \{b_1, \ldots, b_n\} \cup C = C$, откуда $B = \{b_1, \ldots, b_n\}$. □

Определение 3.3. Размерностью пространства называется количество элементов в (любом) базисе этого пространства.

Пространство называется конечномерным, если в нем существует конечный базис. Для того чтобы определить координаты вектора, удобно считать, что базис конечномерного пространства – это не множество, а кортеж векторов. Начиная с этого момента и далее по умолчанию мы будем считать, что базис конечномерного пространства – это кортеж векторов. При необходимости уточнить, какое из определений базиса имеется ввиду, мы будем говорить что кортеж векторов – это упорядоченный базис.

Пусть $f = (f_1, \ldots, f_n)$ – базис пространства $V$, а $x \in V$. По пункту (4) теоремы 2.1 $x$ раскладывается в линейную комбинацию $f_1\alpha_1 + \cdots + f_n\alpha_n$. Тогда *столбец* $(\alpha_1, \ldots, \alpha_n)^\intercal$ называется столбцом координат $x$ в базисе $e$ и обозначается через $x_e$.

## 4. Матрицы

В предыдущем параграфе каждому элементу конечномерного пространства мы сопоставили столбец (одномерный массив). Аналогично, в следующем параграфе линейному отображению (гомоморфизму векторных пространств) будет сопоставлена матрица (двумерный массив). Сейчас мы введем операции на множестве матриц и укажем их простейшие свойства.

Определение 4.1. Двумерный массив $m \times n$ элементов поля $F$ называется матрицей размера $m \times n$ над $F$. Множество всех таких матриц обозначается $\mathrm{M}_{m\times n}(F)$. Если $m = n$, то вместо $\mathrm{M}_{n\times n}(F)$ пишут $\mathrm{M}_n(F)$. Элемент матрицы $A$ в $i$-й строке и $j$-м столбце будут обычно обозначаться 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: $(\alpha A)_{ij} = \alpha a_{ij}$.

Произведением матрицы $A \in \mathrm{M}_{m\times n}(F)$ на матрицу $B \in \mathrm{M}_{n\times k}(F)$ называется матрица $C = AB \in \mathrm{M}_{m\times k}(F)$ 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 4.2. *Множество* $\mathrm{M}_{m\times n}(F)$ *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*

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

*Множество* $\mathrm{M}_n(F)$ *с операциями сложения и умножения является кольцом с единицей.*

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

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

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

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

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 $\mathrm{M}_n(F)$. Остальные утверждения теоремы проверяются непосредственно. □

Определение 4.3. Пусть $R$ – 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 $A \times F \to A$ является сужением операции умножения в кольце $A \times A \to A$).

Таким образом, множество $\mathrm{M}_n(F)$ квадратных матриц фиксированного размера является (некоммутативной) алгеброй с единицей над полем $F$. В данном случае элементы поля $F$ не принято отождествлять со скалярными матрицами $E\alpha$.

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 $i = 1, \ldots, m$, $j = 1, \ldots, n$, $h = 1, \ldots, k$, и функции "умножения" $X_{ij} \times Y_{jh} \to Z_{ih}$, $(x, y) \mapsto xy$. Обозначим через $X$, $Y$ и $Z$ наборы множеств $X_{ij}$, $Y_{jh}$ и $Z_{ih}$, соответственно, через $\mathrm{M}(X)$ – множество матриц $A$ с элементами $a_{ij} \in X_{ij}$, и аналогично введем обозначения $\mathrm{M}(Y)$ и $\mathrm{M}(Z)$. Тогда можно определить произведение матриц $A \in \mathrm{M}(X)$ и $B \in \mathrm{M}(Y)$ как матрицу $C = AB \in \mathrm{M}(Z)$ с элементами $c_{ih} = \sum\limits_{j=1}^{n} a_{ij} b_{jh}$. Также, как произведение обычных матриц, вновь введенная операция будет ассоциативна. Если все $X_{ij}$ и $Y_{jh}$ будут абелевыми группами, а функции "умножения" дистрибутивными, то умножение матриц также будет дистрибутивным.

Одно из приложений этой 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 $v = (v_1, \ldots, v_n)$ 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.

Пусть $f = (f_1, \ldots, f_n)$ – базис пространства $V$, а $x \in V$. В новых обозначениях формула для координат вектора выглядит следующим образом:

$$x = f x_f.$$

Если $V = F^n$, а $e$ – стандартны базис, т. е. базис, состоящий из столбцов единичной матрицы, то получаем $x = e x_e$. Легко видеть, что можно отождествить строку из столбцов с матрицей. Следовательно, $x = E x_e = x_e$ (столбец координат столбца в стандартном базисе совпадает с ним самим).

Другое приложение – блочное произведение матриц (это очень легко показать на доске, и очень долго писать, поэтому пока не пишу).

Есть еще одна полезная унарная операция с матрицами – транспонирование.

Определение 4.4. Пусть $A \in \mathrm{M}_{m \times n}(F)$. Матрица $A^\intercal \in \mathrm{M}_{n \times m}(F)$ с элементами $(A^\intercal)_{ij} = a_{ji}$ называется транспонированной к $A$.

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

Предложение 4.5. $(AB)^\intercal = B^\intercal A^\intercal$.

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, $(a_1, \ldots, a_n)^\intercal$.

## 5. Линейные отображения

Определение 5.1. Пусть $U$ и $V$ – векторные пространства, а $L$ – функция $U \to V$. 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.

Ясно, что линейные отображения характеризуются тем, что сохраняют линейные комбинации векторов. Для строки векторов $v = (v_1, \dots, v_n)$ и линейного отображения $L$ положим $L\big(v\big) = \big(L(v_1), \dots, L(v_n)\big)$. В этих обозначениях свойство линейности можно выразить следующей формулой:

$$L(va) = L(v)a, \text{ где } a \in F^n.$$

Лемма 5.2. *Пусть $U$ – векторное пространство над полем $F$, а $f = (f_1, \dots, f_n)$ – базис $U$. Отображение $\varphi_f : U \to F^n$, заданное равенством $\varphi_f(u) = u_f$, является изоморфизмом векторных пространств.*

Следствие 5.3 (классификация конечномерных пространств). *Любое конечномерное векторное пространство изоморфно пространству $F^n$ для некоторого $n$. Все линейные пространства одной и той же размерности изоморфны между собой.*

Предложение 5.4. *Пусть $L : U \to V$ – линейное отображение, $f = (f_1, \dots, f_n)$ – базис $U$, а $g = (g_1, \dots, g_m)$ – базис $V$. Существует матрица $A \in \mathrm{M}_{m\times n}(F)$ такая, что для любого $u \in U$ имеет место равенство $L(u)_g = Au_f$.*

Доказательство. По определению столбца координат $u = fu_f$. Применяя к этому равенству отображения $L$ и $\varphi_g$ из леммы 5.2 и пользуясь их линейностью, получаем $\varphi_g \circ L(u) = \varphi_g \circ L(f)u_f$. По определению $\varphi_g \circ L(f) = \big(L(f_1)_g, \dots, L(f_n)_g\big) \in \mathrm{M}_{m\times n}(F)$. Обозначая эту матрицу буквой $A$, получаем $L(u)_g = Au_f$. □

Матрица $A$ из последнего предложения называется матрицей отображения $L$ в базисах $f$ и $g$ и обозначается через $L_{f,g}$. В случае, когда $U = V$, а $f = g$, говорят о матрице оператора $L$ в базисе $f$ и обозначают ее через $L_f$. Таким образом имеют место равенства

$$L(u)_g = L_{f,g}u_f \text{ или } L(u)_f = L_f u_f \text{ в случае } U = V,\ f = g.$$

Следующее утверждение является мотивировкой для определения произведения матриц. С другой стороны, его доказательство непосредственно вытекает из ассоциативности произведения матриц.

Предложение 5.5. *Матрица композиции линейных операторов является произведением матриц этих операторов. Точнее, если $U$, $V$ и $W$ – конечномерные линейные пространства с базисами $f$, $g$ и $h$, соответственно, а $L : U \to V$ и $M : V \to W$ – линейные отображения, то $(M \circ L)_{f,h} = M_{g,h}L_{f,g}$. В частности, при $U = V = W$ и $f = g = h$ получаем $(M \circ L)_f = M_f L_f$.*

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

Следствие 5.6. *Пусть $f$ – базис $n$-мерного пространства $V$. Определим отображение $\psi_f : \mathrm{End}(V) \to \mathrm{M}_n(F)$ формулой $\psi_f(L) = L_f$. Тогда $\psi_f$ является изоморфизмом алгебр.*

## 6. Замена базиса

Предложение 6.1. *Пусть $f$ – базис $n$-мерного пространства $V$ над полем $F$. Набор $g = (g_1, \dots, g_n)$ является базисом тогда и только тогда, когда существует $A \in \mathrm{GL}_n(F)$ такая, что $g = fA$.*

Определение 6.2. Матрица $A$ из предыдущего предложения называется матрицей перехода от базиса $f$ к базису $g$ и обозначается через $C_{f\to g}$.

Следующее утверждение вытекает из доказательства предыдущего предложения.

Следствие 6.3.

(1) *Столбец матрицы $C_{f\to g}$ с номером $k$ равен столбцу координат вектора $g_k$ в базисе $f$. Одной формулой: $(C_{f\to g})_k = (g_k)_f$.*
(2) $C_{f\to g}^{-1} = C_{g\to f}$.
(3) *Если матрица двусторонне обратима, то она квадратная.*

Предложение 6.4 (Преобразование координат при замене базиса).

(1) *Пусть $f$ и $f'$ – базисы пространства $V$.*
(2) *Для $x \in V$ имеет место равенство $x_f = C_{f\to f'} x_g$.*
(3) *Пусть $g$ и $g'$ – базисы пространства $U$, а $L : V \to U$ – линейное отображение. Тогда $L_{f',g'} = C_{g'\to g} L_{f,g} C_{f\to f'}$.*

Предложение 6.5. *Пусть $f = (f_1, \dots, f_n)$ – базис пространства $V$, а $g = (g_1, \dots, g_n)$ – набор элементов пространства $U$. Тогда существует единственное линейное отображение $L : V \to U$ такое, что $L(f_i) = g_i$ для любого $i = 1, \dots, n$. При этом*

(1) *$L$ инъективен тогда и только тогда, когда $g$ линейно независим;*
(2) *$L$ сюръективен тогда и только тогда, когда $g$ – система образующих;*
(3) *$L$ биективен тогда и только тогда, когда $g$ базис;*
(4) *Если $U = V$, а $g$ – базис, то $L_f = C_{f\to g}$.*

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

Теорема 7.1. *Пусть $L : U \to V$ – линейное отображение. Тогда* $\dim \operatorname{Im} L + \dim \operatorname{Ker} L = \dim U$.

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

Следствие 7.2. *Если $\dim U = \dim V$, то инъективность $L$ равносильна сюръективности.*

Суммой $U + W$ подпространств $U$ и $W$ называется совокупность всевозможных векторов вида $v = u + w$, где $u \in U$, $w \in W$. Сумма подпространств есть подпространство. Пересечение подпространств является подпространством.

Определение 7.3. Пространство $V$ называется прямой суммой подпространств $U$ и $W$, если каждый элемент $v \in V$ может быть единственным способом представлен в виде суммы $v = u + w$, где $u \in U$, а $w \in W$.

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

Пространства $U$ и $W$ естественно вкладываются в их внешнюю прямую сумму: $U \ni u \mapsto (u, 0)$, а $W \ni w \mapsto (0, w)$. Если отождествить $U$ и $W$ с их образами, то внешняя прямая сумма превращается в прямую сумму подпространств, поэтому довольно часто их не различают.

Обозначение: $V = U \oplus W$. Эквивалентная формулировка: $V = U \oplus W$, если $V = U + W$ и $U \cap V = \varnothing$. Если $V = U \oplus W$, то объединение базисов подпространств $U$ и $W$ есть базис пространства $V$. Поэтому $\dim(U \oplus W) = \dim(U) + \dim(W)$.

Предложение 7.4. *Для любого подпространства $U \leqslant V$ существует подпространство $W \leqslant V$ такое, что $V = U \oplus W$ (здесь пространства не предполагаются конечномерными).*

Доказательство. Выберем базис $f$ подпространства $U$ и дополним его до базиса $f \cup g$ всего пространства. Если $W = \langle g \rangle$, то легко проверить, что $V = U \oplus W$. □

Теорема 7.5 (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 $\operatorname{Im} L = U + V$, а $\operatorname{Ker} L = \{(u, -u) \mid u \in U \cap V\} \cong U \cap V$. Теперь теорема следует из теоремы о размерности ядра и образа. □

## 8. Ранг, PDQ-разложение и разложение Гаусса

Определение 8.1. 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 8.2. *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 множестве 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. □

Лемма 8.3. *Пусть $A \in \mathrm{M}_{m,n}(F)$.*

(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 $m = n$. В этом случае матрица $A$ обратима.*
(4) *Если все строки $A$ линейно независимы, и все ее столбцы обладают тем же свойством, то $m = n$, а матрица $A$ обратима.*

Доказательство. Утверждения (1) и (2) очевидны. Из них следует, что столбцовый ранг равен $m = n$ 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 $n \leqslant m$. Аналогичное рассуждение для строк доказывает обратное неравенство, т. е. $m = n$. □

Теорема 8.4 (PDQ-разложение). *Любая матрица $A \in \mathrm{M}_{m,n}(F)$ представляется в виде $A = PDQ$, где $P \in \mathrm{GL}_m(F)$, $Q \in \mathrm{GL}_n(F)$, 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. Существование разложения, очевидно, равносильно следующему утверждению: умножая матрицу $A$ справа и слева на обратимые матрицы можно получить матрицу $D$. В частности, мы можем выполнять элементарные преобразования как со столбцами, так и со строками $A$, потому что элементарные преобразования соответствуют умножению на обратимые матрицы.

Пусть столбцовый ранг $A$ равен $k$, а строчный – $h$. Столбцы $A$ являются системой образующих в своей линейной оболочке, поэтому существует базис из $k$ столбцов матрицы $A$. Переставляя столбцы, поставим эти $k$ столбцов на первые $k$ мест. Так как остальные столбцы являются линейными комбинациями первых $k$, то при помощи первого элементарного преобразования со столбцами можно получить нули во всех столбцах, кроме первых $k$. Заметим, что строчный и столбцовый ранг $A$ не изменился при этих преобразованиях.

Проделав аналогичные элементарные преобразования со строками полученной матрицы, получим матрицу $\left(\begin{smallmatrix} X & 0 \\ 0 & 0 \end{smallmatrix}\right)$, где $X \in \mathrm{M}_{h,k}(F)$. При этом строки и столбцы матрицы $X$ линейно независимы. По пункту (4) леммы 8.3 $h = k$, а матрица $X$ обратима. Умножая (слева или справа) на обратимую матрицу $\left(\begin{smallmatrix} X^{-1} & 0 \\ 0 & E \end{smallmatrix}\right)$ получаем матрицу $D$ из условия, что завершает доказательство. □

Аналогичное утверждение верно с заменой поля на евклидово кольцо, а единичной матрицы на диагональную. Если в качестве евклидова кольца взять $\mathbb{Z}$, то это утверждение является ключевым шагом классификации конечнопорожденных абелевых групп.

Лемма 8.5. *Квадратная матрица обратима тогда только тогда, когда ее ранг равен ее размеру.*

Теорема 8.6 (Разложение Гаусса). *Любая матрица $A \in \mathrm{GL}_n(F)$ представляется в виде $A = PLU$, где $P$ – матрица-перестановка, $L$ нижнетреугольная, а $U$ – верхнетреугольная матрица.*

Для доказательства последней теоремы надо выбрать перестановку строк так, чтобы все квадратные подматрицы (любого размера), стоящие в левом верхнем углу, были бы обратимы. 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 матрицы.

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

## 9. Билинейные и квадратичные формы

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

Определение 9.1. Функция $B : V \times V \to F$ 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 $\mathrm{Bil}(V)$ – множество всех билинейных форм на $V$, а через $\mathrm{Bil}^{(s)}(V)$ и $\mathrm{Bil}^{(a)}(V)$ – множества симметричных и антисимметричных билинейных форм. Ясно, что все 3 множества являются подпространствами пространства всех функций $V \times V \to F$ (с поточечными операциями).

Лемма 9.2. *Если* $\operatorname{char} F \neq 2$, *то* $\operatorname{Bil}(V) = \operatorname{Bil}^{(s)}(V) \oplus \operatorname{Bil}^{(a)}(V)$.

Доказательство. Положим $B^{(s)}(x,y) = \frac{1}{2}\big(B(x,y) + B(y,x)\big)$ и $B^{(a)}(x,y) = \frac{1}{2}\big(B(x,y) - B(y,x)\big)$. Ясно, что $B^{(s)}$ является симметричной билинейной формой, $B^{(a)}$ антисимметричной, а $B = B^{(s)} + B^{(a)}$. Тот факт, что $\operatorname{Bil}^{(s)}(V) \cap \operatorname{Bil}^{(a)}(V) = \{0\}$ очевиден (и тоже использует условие, что $2 \neq 0$ в поле $F$). □

*До конца этого параграфа мы считаем, что характеристика поля* $F$ *не равна* 2.

Теорема 9.3 (поляризация квадратичной формы). *Пусть* $Q$ *– квадратичная форма на* $V$, *соответствующая билинейной форме* $B$. *Положим*

$$B^{(s)}(x,y) = \frac{1}{2}\big(Q(x+y) - Q(x) - Q(y)\big).$$

*Тогда* $B^{(s)}$ *является симметризацией формы* $B$, *и* $Q(x) = B^{(s)}(x,x)$.

Таким образом, мы имеем биекцию между множеством квадратичным и симметричных билинейных форм.

Предложение 9.4. *Пусть* $B$ *билинейная форма на* $V$, *а* $f = (f_1, \dots, f_n)$ *– базис* $V$. *Тогда существует матрица* $A \in \mathrm{M}_n(F)$ *такая, что* $B(x,y) = x_f^\tau A y_f$ *для любых* $x, y \in V$.

Определение 9.5. Матрица $A$, построенная в доказательстве леммы, называется матрицей билинейной формы $B$ в базисе $f$ и обозначается через $B_f$. Матрицей квадратичной формы называется матрица ассоциированной с ней *симметричной* билинейной формы.

Предложение 9.6. *Пусть* $B$ *билинейная форма на* $V$, *а* $f$ *и* $g$ *– базисы пространства* $V$. *Тогда* $B_g = C_{f\to g}^\tau B_f C_{f\to g}$.

Определение 9.7. Билинейная форма называется вырожденной, если существует $v \in V \smallsetminus \{0\}$ такой, что $B(v,x) = 0$ при всех $x \in V$.

Предложение 9.8. *Пусть* $B$ *симметричная билинейная форма на* $V$. *Положим* $V_0 = \{u \in V \mid B(u,v) = 0 \,\forall v \in V\}$. *Если* $V = V_0 \oplus U$, *то сужение формы* $B$ *на* $U \times U$ *невырождено.*

Доказательство. Заметим, что по предложению 7.4 всегда существует такое $U$, что $V = V_0 \oplus U$. Пусть $u \in U$ такой, что $B(u,w) = 0$ для любого $w \in U$. Любой вектор $v \in V$ представляется в виде суммы $v = w + x$ для некоторых $w \in U$ и $x \in V_0$. Тогда $B(u,v) = B(u,w) + B(u,x) = 0$. Таким образом, $u \in U \cap V_0 = \{0\}$, следовательно, сужение $B$ на $U \times U$ невырождено. □

Лемма 9.9. *Пусть* $Q$ *– невырожденная квадратичная форма на* $V$. *Тогда существует вектор* $v \in V$ *такой, что* $Q(v) \neq 0$.

Доказательство. Если $Q(v) = 0$ для любого $v \in V$, то по формуле поляризации (см. теорему 9.3) симметричная билинейная форма $B$, ассоциированная с $Q$, нулевая, что противоречит невырожденности. □

Теорема 9.10 (диагонализация матрицы квадратичной формы). *Для любой квадратичной формы существует базис, в котором ее матрица диагональна.*

Доказательство. Пусть $Q$ – квадратичная форма на $V$, а $B$ – симметричная билинейная форма, ассоциированная с $Q$. Мы должны доказать, что существует базис $f$ пространства $V$ ортогональный относительно формы $B$. По предложению 9.8 $V = V_0 \oplus U$, 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 $g_1 \in U$ такой, что $Q(g_1) \neq 0$. Дополним $g_1$ до базиса

$g = (g_1, \ldots, g_n)$ пространства $U$. Положим $h_k = g_k - \frac{B(g_k,g_1)}{Q(g_1)} g_1$ при $2 \leqslant k \leqslant n$. Тогда

$$B(h_k, g_1) = B(g_k - \frac{B(g_k, g_1)}{Q(g_1)} g_1, g_1) = B(g_k, g_1) - \frac{B(g_k, g_1)}{Q(g_1)} B(g_1, g_1) = 0.$$

Таким образом, $g_1$ $B$-ортогонален всем векторам $h_k$ при $2 \leqslant k \leqslant n$, а, следовательно, и всему подпространству $W = \langle h_2, \ldots, h_n \rangle$. По индукционному предположению существует $B$-ортогональный базис $(f_2, \ldots, f_n)$ подпространства $W$. Положив $f_1 = g_1$, получим ортогональный базис $(f_1, \ldots, f_n)$ пространства $U$. □

Определение 9.11. Если $Q$ – квадратичная форма на векторном пространстве $V$, то пара $(V, Q)$ называется квадратичным пространством. Квадратичное пространство называется невырожденным, если форма $Q$ невырождена.

Морфизмом квадратичных пространств $(V, Q) \to (V', Q')$ называется линейное отображение $L : V \to V'$, обладающее свойством $Q'\big(L(x)\big) = Q\big(x\big)$ для всех $x \in V$. Биективный морфизм называется изоморфизмом.

Задача теории квадратичных форм – классификация всех конечномерных квадратичных пространств над данным полем с точностью до изоморфизма. Ясно, что пространства разной размерности не могут быть изоморфны. Очевидно также, что изоморфизм сохраняет подпространство $V_0$ из предложения 9.8. Таким образом, достаточно классифицировать невырожденные квадратичные пространства любой фиксированной размерности.

Лемма 9.12. *Квадратичные пространства $(V, Q)$ и $(V', Q')$ изоморфны тогда и только тогда, когда существуют такие базисы $f$ и $f'$ пространств $V$ и $V'$ соответственно, что $Q_f = Q'_{f'}$.*

Доказательство. Пусть $L(V, Q) \to (V', Q')$ – изоморфизм квадратичных пространств, а $f = (f_1, \ldots, f_n)$ – базис $V$. Тогда $f' = \big(L(f_1), \ldots, g_n\big)$ является базисом $V'$. Так как $Q'\big(L(x)\big) = Q\big(x\big)$, то из теоремы 9.3 следует, что $B'\big(L(x), L(y)\big) = B\big(x, y\big)$ для любых $x, y \in V$, где $B$ и $B'$ – симметричные билинейные формы, ассоциированные с $Q$ и $Q'$ соответственно. Поэтому $Q_f = Q'_{f'}$.

Обратно, если $Q_f = Q'_{f'}$, то отображение $L(x) = f' x_f$ является изоморфизмом квадратичных пространств. Действительно, $L(x)_{f'} = x_f$, поэтому

$$Q'\big(L(x)\big) = L(x)^{\mathsf{T}}_{f'} Q'_{f'} L(x)_{f'} = x_f^{\mathsf{T}} Q_f x_f.$$

□

Если матрица $Q_f$ диагональна, а $g_k = f_k \lambda_k$, то матрица $Q_g$ также диагональна, причем ее диагональные элементы отличаются от диагональных элементов $Q_f$ умножением на $\lambda_k^2$. Таким образом, для невырожденных форм, играют роль только классы вычетов диагональных элементов $Q_f$ в $F^*/(F^*)^2$. В частности, если из любого элемента поля $F$ можно извлечь квадратный корень, то классификация совсем простая.

Определение 9.13. 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 9.14. *Любые два невырожденных квадратичных пространства одинаковой размерности над квадратично замкнутым полем изоморфны.*

В общем случае неверно, что любые две диагональные матрицы $Q_f$ и $Q_g$ квадратичной формы $Q$ отличаются только перестановкой диагональных элементов и умножением их на квадраты. Однако, как мы докажем в параграфе 4, для поля вещественных чисел это так, и роль играют только знаки диагональных элементов.

Глава 5

# Определители

## 1. Полилинейные и антисимметричные формы.

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

Определение 1.1. Отображение $f : \underbrace{V \times \cdots \times V}_{m \text{ раз}} \to F$ 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

$$f(\dots, a+b, \dots) = f(\dots, a, \dots) + f(\dots, b, \dots),$$
$$f(\dots, \lambda a, \dots) = \lambda f(\dots, a, \dots)$$

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*

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

*где $A = \big((x_1)_v, \dots, (x_n)_v\big)$.*

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. □

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

Определение 1.3. Пусть $X$ – множество. Функция $f : X \times X \to F$ 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* $\operatorname{char} F \neq 2$, *то* (1) $\implies$ (2). *Если же $X$ – векторное пространство, а форма $f$ билинейна, то* (2) $\implies$ (1).

Доказательство. Первое утверждение очевидно. Доказательство второго похоже на поляризацию билинейной формы:

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

□

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 4.2.

Лемма 1.5. *Пусть* $f : \underbrace{V \times \cdots \times V}_{n\ раз} \to F$ *– полилинейная антисимметричная форма,* $v = (v_1, \dots, v_n)$ *– базис пространства* $V$*,* $x_1, \dots, x_n \in V$*, а* $A = \big((x_1)_v, \dots, (x_n)_v\big)$*. 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 $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ – 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. □

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. Определитем матрицы $A \in \mathrm{M}_n(F)$ 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. $\det A = ba_{*k}$ для некоторой строки $b \in F^n$. 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

$$\det A = \sum_{\sigma \in A_n} \prod_{k=1}^{n} a_{\sigma(k)\,k} - \sum_{\rho \in A_n\tau} \prod_{k=1}^{n} a_{\rho(k)\,k}. \tag{2}$$

Заменяя $\rho = \sigma\tau$ получим

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

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 (2), получаем $\det A = 0$. □

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

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

*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 $f(u) = f(v)\det C_{v\to u}$.*
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. □

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

- *Фунция $f_L: V\times\cdots\times V\to F$, заданная формулой $f_L\big(x_1,\dots,x_n\big) = f\big(L(x_1),\dots,L(x_n)\big)$ 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

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

Если $g$ – другая форма объема, то

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

в соответствии со следствием 2.3. □

Определителем линейного оператора $L: V\to V$ 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. $\det A = \det A^\intercal$. *Поэтому все свойства, сформулированные для столбцов матрицы $A$ верны и для ее строк.*

Доказательство. По определению 2.1,

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

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

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

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

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

□

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

Таким образом, свойство доказано для нижних клеточно-треугольных матриц. Доказательство для верхних клеточно-треугольных матриц легко следует теперь из свойства 3.2. □

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

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

По свойству 3.4 первый определитель из суммы равен $b_{11} A_{11}(B)$. Для вычисления $i$-ого 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. □

## 4. Формула для элементов обратной матрицы и формулы Крамера

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 $k$-ый столбец матрицы $B$ на $j$-ый, 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 $k$-ого 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. □

Определение 4.2. Матрица называется *невырожденной*, если она квадратная, а ее определитель не равен нулю. Квадратная матрица с нулевым определителем называется *вырожденной*.

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 $\det A \neq 0$. □

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

Теорема 4.5. *Если $A \in \mathrm{M}_n(F)$, то*

$$AA^{adj} = A^{adj}A = E \det A.$$

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

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

Доказательство. Положим $B = A \cdot A^{adj}$. Элемент матрицы $A^{adj}$ 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, $A^{adj} A = E \det A$. Второе утверждение сразу вытекает из первого. □

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 $F^n \to F^n$ 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 $x = \frac{1}{\Delta} A^{adj} b$ или $x_i = \frac{1}{\Delta} \sum_{k=1}^{n} A_{ki} b_k$. Осталось заметить, что по теореме 3.6 $\sum_{k=1}^{n} A_{ki} b_k = \Delta_i$. □

## 5. Минорный ранг матрицы

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

Определение 5.1. Минорным рангом матрицы $A \in \mathrm{M}_{m,n}(F)$ называется наибольший размер квадратной подматрицы, определитель которой не равен нулю.

Теорема 5.2. *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, $k \leqslant r$.

Обратно, возьмем подматрицу $k \times n$, состоящую из линейно независимых строк матрицы $A$. По теореме 8.4 столбцовый ранг этой подматрицы также равен $k$, следовательно в ней найдется $k$ линейно независимых столбцов. Наконец, по лемме 2.4 квадратная матрица с линейно независимыми столбцами имеет ненулевой определитель, откуда $k \geqslant r$. □

Глава 6

# Собственные числа и жорданова форма

## 1. Собственные числа и вектора

В этой главе мы будем искать базис, в котором матрица оператора $L : V \to V$ 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 $u = (u_1, \ldots, u_n)$ 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 $L : V \to V$, 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 $A \in \mathrm{M}_n(F)$, 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 $A \in \mathrm{M}_n(F)$ 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 $\det(A - \lambda E) = 0$. □

Матрица $A - tE$, принадлежит матричному кольцу $M_n(F[t])$ над кольцом многочленов $F[t]$[1] 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 $(-1)^n t^n$).

[1]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.

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 $f$ и $g$ пространства $V$ характеристические многочлены матриц $L_f$ и $L_g$ равны.*

Доказательство. Пусть $C = C_{f\to g}$. Тогда $L_g = C^{-1}L_fC$ и

$$\chi_{L_g}(t) = \det\bigl(L_g - tE\bigr) = \det\bigl(C^{-1}L_fC - tE\bigr) = \det\bigl(C^{-1}(L_f - tE)C\bigr) = \det\bigl(L_f - tE\bigr) = \chi_{L_f}(t).$$

□

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 $x_1, \ldots, x_m$ – собственные вектора оператора $L$, соответствующие различным собственным числам $\lambda_1, \ldots, \lambda_m$, 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 $k = 1, \ldots, m-1$. Так как $\lambda_k \neq \lambda_m$ при $k \neq m$, то $\alpha_k = 0$ при всех $k = 1, \ldots, m-1$. Подставляя эти значения в исходную формулу, получаем $x_m\alpha_m = 0$, откуда $\alpha_m = 0$. □

Если у многочлена $n$-ой 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 $k = \dim \operatorname{Ker}(L - \lambda I)$ геометрическую кратность собственного числа $\lambda$. Выберем базис $(u_1, \dots, u_k)$ пространства $\operatorname{Ker}(L-\lambda I)$ 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 $k$. □

В следующей теореме собраны различные условия диагонализуемости оператора.

Теорема 1.10. *Пусть $L : V \to V$ – 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. □

## 2. Жорданова форма и ее следствия

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 $J_{n,0}$ 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 $J_{n,\lambda}=\lambda E+J_{n,0}$. 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 $L:V\to V$ – линейный оператор. Тогда существует базис и пространства $V$ такой, что матрица $L_u$ является жордановой. Она называется жордановой формой оператора $L$ и определена единственным образом с точностью до перестановки блоков.*

Доказательство этой теоремы будет дано при изучении модулей над евклидовыми кольцами, а сейчас мы выведем некоторые следствия этой теоремы. Для этого нам понадобится следующее несложное вычисление.

Лемма 2.3. *Матрица $J_{n,0}^m$ имеет 1 во всех позициях $(k,k+m)$, $1\leqslant k\leqslant n-m$. В частности, если $m\geqslant n$, то $J_{n,0}^m=0$.*

.....

Глава 7

# Евклидовы и эрмитовы пространства

.....

## 1. Определение, примеры, матрица Грама

.....

## 2. Неравенства КБШ и треугольника

Теорема 2.1. *Пусть $V$ – векторное пространство (не обязательно конечномерное) с евклидовым или эрмитовым скалярным произведением. Тогда для любых $x, y \in V$ имеют место неравенства:*

(1) $|(x,y)|^2 \leqslant \|x\|^2\|y\|^2$ *(неравенство Коши–Буняковского–Шварца — КБШ);*
(2) $\|x+y\| \leqslant \|x\| + \|y\|$ *(неравенство треугольника).*

Доказательство. (1). Если $y = 0$, то обе части равенства равны 0, поэтому можно считать, что $y \neq 0$. $0 \leqslant \|x + y\lambda\|^2 = \|x\|^2 + (x,y)\lambda + \bar{\lambda}(y,x) + \|y\|^2|\lambda|^2$. Положим $\lambda = -\frac{(y,x)}{(y,y)}$. Тогда последнее выражение равно $\|x\|^2 - \frac{(x,y)(y,x)+\overline{(y,x)}(y,x)}{(y,y)} + \frac{\|y\|^2|(y,x)|^2}{\|y\|^4} = \|x\|^2 - \frac{|(y,x)|^2}{\|y\|^2} \geqslant 0$. После домножения на знаменатель (который больше 0) получаем неравенство КБШ.

(2). Возводя неравенство треугольника в квадрат, получаем $(x+y, x+y) \leqslant \|x\|^2 + \|y\|^2 + 2\|x\|\|y\|$. Раскрывая скобки в левой части и сокращая $\|x\|^2 + \|y\|^2$ имеем $2\,\mathrm{Re}(x,y) = (x,y) + (y,x) \leqslant 2\|x\|\|y\|$. Последнее неравенство следует из того, что $\mathrm{Re}(x,y) \leqslant |(x,y)|$ и неравенства КБШ. □

## 3. Ортогонализация и ее следствия

Лемма 3.1. *Набор ненулевых попарно ортогональных векторов линейно независим.*

Теорема 3.2. *Пусть $V$ – евклидово или эрмитово пространство, $f_1, \ldots, f_n \in V$. Положим*

$$g_1 = f_1$$
$$g_2 = f_2 - g_1\frac{(g_1, f_2)}{(g_1, g_1)}$$
$$\ldots\ldots\ldots\ldots$$
$$g_n = f_n - \sum_{i=1}^{n-1} g_i\frac{(g_i, f_n)}{(g_i, g_i)}$$

*Тогда для любых $i, j, k \in \{1, \ldots, n\}$, $i \neq j$ выполнены следующие утверждения.*

(1) $(g_i, g_j) = 0$.
(2) $\langle f_1, \ldots, f_k\rangle = \langle g_1, \ldots, g_k\rangle$.
(3) *Если $f_1, \ldots, f_k$ линейно независимы, то и $g_1, \ldots, g_k$ линейно независимы, в частности, $g_m \neq 0$ при всех $m = 1, \ldots, k$.*
(4) *Если $f_k \in \langle f_1, \ldots, f_{k-1}\rangle$, то $g_k = 0$.*
(5) *Если $(f_1, \ldots, f_n)$ – система образующих $V$, то ненулевые из векторов $g_1, \ldots, g_n$ образуют базис.*
(6) *Если $(f_1, \ldots, f_n)$ – базис $V$, то $(g_1, \ldots, g_n)$ – ортогональный базис $V$.*

## 4. Вещественные квадратичные формы

В этом параграфе $V$ обозначает вещественное векторное пространство размерности $m$.

Определение 4.1. 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 4.2. *Пусть $B$ – симметричная билинейная форма на $V$, а $f_1, \dots, f_k \in V$. Если $B(f_i, f_i) > 0$ при всех $i$, а $B(f_i, f_j) = 0$ при всех $j \neq i$, то форма $B$ положительно определена на подпространстве $\langle f_1, \dots, f_k \rangle$.*

Теорема 4.3 (закон инерции квадратичных форм). *Пусть $Q$ – квадратичная форма на вещественном векторном пространстве $V$, а $f, g$ – базисы $V$ такие, что матрицы $Q_f$ и $Q_g$ диагональны. Тогда сигнатуры матриц $Q_f$ и $Q_g$ равны.*

Доказательство. По предложению 9.8 можно считать, что форма $B$ невырождена. Пусть $(p_f, n_f)$ – сигнатура матрицы $Q_f$, а $(p_g, n_g)$ – сигнатура матрицы $Q_g$. Перенумеровав при необходимости базисные элементы, можно считать, что положительные диагональные элементы матриц $Q_f$ и $Q_g$ стоят выше (и левее) отрицательных.

Предположим, что $p_f > p_g$. По предыдущей лемме форма $Q$ положительно определена на подпространстве $U = \langle f_1, \dots, f_{p_f} \rangle$. Аналогично, $Q$ отрицательно определена на $W = \langle g_{p_g+1}, \dots, g_m \rangle$. Но по теореме о размерности ядра и образа

$$\dim U \cap W = p_f + (m - p_g) - \dim(U + W) \leqslant p_f + (m - p_g) - m = p_f - p_g > 0.$$

Следовательно, $U \cap W \neq \{0\}$, но форма $Q$ одновременно положительно и отрицательно определена на этом подпространстве. Противоречие показывает, что неравенство $p_f > p_g$ невозможно. По аналогичным причинам невозможно и обратное неравенство, следовательно, $p_f = p_g$. □

В соответствии с законом инерции можно дать следующее определение. Сигнатурой квадратичной формы называется сигнатура ее матрицы в таком базисе, в котором эта матрица диагональна.

Определение 4.4. Векторное пространство над полем $F$ (характеристики $\neq 2$) вместе с квадратичной формой на нем называется квадратичным пространством.

Два квадратичных пространства $(V, Q)$ и $(V', Q')$ называются изоморфными, если существует изоморфизм $L : V \to V'$ векторных пространств такой, что $Q'\big(L(x)\big) = Q\big(x\big)$ для любого $x \in V$.

Следствие 4.5 (классификация вещественных квадратичных форм). *Два вещественых квадратичных пространства $(V, Q)$ и $(V', Q')$ являются изоморфными тогда и только тогда, когда $\dim V = \dim V'$, а $\operatorname{Sign} Q = \operatorname{Sign} Q'$.*

Пусть $A$ – квадратная матрица. Минор $\begin{vmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{vmatrix}$ называется главным минором $k$-ого порядка матрицы $A$. Обозначим его для краткости $\Delta_k$. По определению положим $\Delta_0 = 1$. Матрица называется унитреугольной, если она треугольна с 1 на главной диагонали.

Лемма 4.6. *Умножение на нижнюю унитреугольную матрицу слева и на верхнюю унитреугольную справа не меняет главных миноров матрицы.*

Доказательство. Так как определитель произведения равен произведению определителей, а определитель унитреугольной матрицы равен 1, то умножение на унитреугольную матрицу не

меняет определителя. С помощью блочного умножения матриц не трудно убедиться, что при указанных в условии действиях $k \times k$-подматрица, стоящая в левом верхнем углу также умножается на унитреугольные матрицы. Следовательно, ее определитель не меняется. □

Теорема 4.7 (критерий Сильвестра). *Если главные миноры матрицы квадратичной формы не равны 0, то сигнатура этой формы 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. Пусть $Q$ – квадратичная форма на $V$, а $f = (f_1, \dots, f_m)$ – базис $V$. Обозначим через $B$ симметричную билинейную форму, ассоциированную с $Q$. Проведем доказательство индукцией по $m$. При $m = 1$ утверждение очевидно.

Пусть $m > 1$, $A = Q_f$. По условию первый главный минор $a_{11} \neq 0$. Пусть $g$ – такой базис пространства $V$, что

$$C := C_{f\to g} = \begin{pmatrix} 1 & -\frac{a_{12}}{a_{11}} & \cdots & -\frac{a_{1m}}{a_{11}} \\ 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

(это соответствует формулам $g_k = f_k - \frac{B(f_k,f_1)}{B(f_1,f_1)} f_1$, аналогичным процессу ортогонализации). Вычисление показывает, что $Q_g = C^{\mathsf{T}} Q_f C = \begin{pmatrix} a_{11} & 0 \\ 0 & D \end{pmatrix}$, где $D$ – матрица сужения формы $Q$ на подпространство $U = \langle g_2, \dots, g_m \rangle$ в базисе $(g_2, \dots, g_m)$ (обозначим это сужение через $Q'$).

По предыдущей лемме главные миноры матриц $Q_f$ и $Q_g$ совпадают. Обозначим через $\gamma_1 = d_{11}, \gamma_2, \dots, \gamma_{m-1}$ главные миноры матрицы $D$. Тогда $\Delta_k = a_{11}\gamma_{k-1}$ для всех $k = 1, \dots, m$. По индукционному предположению сигнатура формы $Q'$ равна сигнатуре последовательности

$$y = (\frac{\gamma_1}{\gamma_0}, \dots, \frac{\gamma_{m-1}}{\gamma_{m-2}}) = (\frac{\Delta_2}{\Delta_1}, \dots, \frac{\Delta_m}{\Delta_{m-1}}).$$

По теореме 9.10 существует такой базис $h_2, \dots, h_m$ подпространства $U$, что матрица $Q'_h$ диагональна. По определению сигнатуры квадратичной формы сигнатура матрицы $Q'_h$ равна сигнатуре последовательности $y$. Заметим, что в базисе $(f_1, h_2, \dots, h_m)$ форма $Q$ имеет диагональную матрицу $\begin{pmatrix} a_{11} & 0 \\ 0 & Q'_h \end{pmatrix}$, сигнатура которой равна сигнатуре строки $(a_{11}, y) = (\frac{\Delta_1}{\Delta_0}, \frac{\Delta_2}{\Delta_1}, \dots, \frac{\Delta_m}{\Delta_{m-1}})$, что и требовалось доказать.

Если все главные миноры положительны, то в любой диагонализации формы $Q$ все диагональные элементы положительны. По лемме 4.2 из этого следует, что форма положительно определена. Обратно, если $Q$ положительно определена, то все диагональные элементы матрицы этой формы в любом базисе положительны. □

Глава 8

# Основы теории категорий

## 1. Категория, универсальные объекты, типы морфизмов

Определение 1.1. *Категорией* $\mathcal{C}$ называется набор следующих данных:

- класс *объектов* $\mathcal{O}bj\,\mathcal{C}$;
- для каждых двух объектов $X, Y \in \mathcal{O}bj\,\mathcal{C}$ множество $\mathrm{Mor}(X, Y)$, называемое множеством *морфизмов* из $X$ в $Y$;
- для каждых трех объектов $X, Y, Z \in \mathcal{O}bj\,\mathcal{C}$ функция $\mathrm{Mor}(Y, Z) \times \mathrm{Mor}(X, Y) \to \mathrm{Mor}(X, Z)$, $(\varphi, \psi) \mapsto \varphi \circ \psi$, называемую *законом композиции* морфизмов;

удовлетворяющих следующим условиям:

(1) Если $X \neq U$ или $Y \neq V$, то $\mathrm{Mor}(X, Y) \cap \mathrm{Mor}(U, V) = \varnothing$.
(2) закон композиции морфизмов ассоциативен;
(3) для каждого объекта $X \in \mathcal{O}bj\,\mathcal{C}$ существует *тождественный морфизм* $id_X \in \mathrm{Mor}(X, X)$ такой, что для любых морфизмов $\alpha \in \mathrm{Mor}(X, Y)$ и $\beta \in \mathrm{Mor}(Y, X)$ выполнены равенства $id_X \circ \beta = \beta$ и $\alpha \circ id_X = \alpha$.

Категория называется *малой*, если класс объектов является множеством.

Определение 1.2. Категория $\mathcal{B}$ называется подкатегорией категории $\mathcal{C}$, если $\mathcal{O}bj\,\mathcal{B} \subseteq \mathcal{O}bj\,\mathcal{C}$ и $\mathrm{Mor}_{\mathcal{B}}(X, Y) \subseteq \mathrm{Mor}_{\mathcal{C}}(X, Y)$ для любых $X, Y \in \mathcal{O}bj\,\mathcal{B}$. 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 $\mathcal{C}^{op}$:

- $\mathcal{O}bj\,\mathcal{C}^{op} = \mathcal{O}bj\,\mathcal{C}$;
- $\mathrm{Mor}_{\mathcal{C}^{op}}(X, Y) = \mathrm{Mor}_{\mathcal{C}}(Y, X)$ для каждых двух объектов $X, Y \in \mathcal{O}bj\,\mathcal{C}$;
- закон композиции в $\mathcal{C}^{op}$ отличается от закона композиции в $\mathcal{C}$ порядком, т. е. $\alpha \underset{\mathcal{C}^{op}}{\circ} \beta = \beta \underset{\mathcal{C}}{\circ} \alpha$.

Определение 1.4. Декартовым произведением $\mathcal{C} \times \mathcal{B}$ категорий $\mathcal{C}$ и $\mathcal{B}$ называется следующая категория:

- $\mathcal{O}bj\,(\mathcal{C} \times \mathcal{B}) = \mathcal{O}bj\,\mathcal{C} \times \mathcal{O}bj\,\mathcal{B}$;
- $\mathrm{Mor}((X, Y), (Z, W)) = \mathrm{Mor}(X, Z) \times \mathrm{Mor}(Y, W)$;
- $(\alpha, \beta) \circ (\gamma, \delta) = (\alpha \circ \gamma, \beta \circ \delta)$.

Определение 1.5. Морфизм $\varphi$ называется *мономорфизмом*, если равенство $\varphi \circ \alpha = \varphi \circ \beta$ влечет равенство $\alpha = \beta$, и эпиморфизмом, если $\alpha \circ \varphi = \beta \circ \phi \implies \alpha = \beta$. Морфизм, являющийся одновременно мономорфизмом и эпиморфизмом называется биморфизмом. Морфизм $\varphi \in \mathrm{Mor}(X, Y)$ называется *изоморфизмом*, если существует $\varphi^{-1} \in \mathrm{Mor}(Y, X)$ такой, что $\varphi \circ \varphi^{-1} = id_Y$ и $\varphi^{-1} \circ \varphi = id_X$.

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 $\mathrm{Mor}(*, X)$ состоит ровно из одного элемента. Объект $*$ называется *финальным*, если для любого объекта $X$ множество $\mathrm{Mor}(X, *)$ состоит ровно из одного элемента.

**Примеры**.

(1) Категория множеств, пунктированных множеств.
(2) Категория групп, абелевых групп, векторных пространств.
(3) Категория колец, коммутативных колец, колец с 1.
(4) Частично упорядоченное множество.
(5) Ориентированный граф (категория путей, категория достижимости).
(6) Моноид – категория с одним объектом.
(7) Категория морфизмов (коммутативных треугольников, квадратов, в т.ч. с фиксированными вершинами).

## 2. Функторы

Определение 2.1. Функтором $\mathcal{F}$ из категории $\mathcal{B}$ в категорию $\mathcal{C}$ называется набор следующих отображений:

- $\mathcal{F} : \mathcal{O}bj\,\mathcal{B} \to \mathcal{O}bj\,\mathcal{C}$;
- $\mathcal{F}_{X,Y} : \mathrm{Mor}(X,Y) \to \mathrm{Mor}(\mathcal{F}(X),\mathcal{F}(Y))$ для каждой пары объектов $X, Y \in \mathcal{O}bj\,\mathcal{C}$, удовлетворяющие свойствам $\mathcal{F}_{X,Z}(\alpha \circ \beta) = \mathcal{F}_{Y,Z}(\alpha) \circ \mathcal{F}_{X,Y}(\beta)$ и $\mathcal{F}_{X,X}(id_X) = id_{\mathcal{F}(X)}$.

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 $\mathcal{F} : \mathcal{B} \to \mathcal{C}$ означает, что $\mathcal{F}$ является функтором из категории $\mathcal{B}$ в категорию $\mathcal{C}$.

Функтор $\mathcal{C}^{op} \to \mathcal{B}$ называется контравариантным функтором из $\mathcal{C}$ в $\mathcal{B}$ (обычный функтор, если хочется подчеркнуть, что он не меняет направление стрелок, называется ковариантным).

**Примеры**.

(1) Забывающие функторы.
(2) $\mathrm{M}_n$, $\mathrm{GL}_n$, обратимые элементы моноида.
(3) 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.
(4) Коммутантом $[G,G]$ группы $G$ называется наименьшая нормальная подгруппа в $G$, факторгруппа по которой абелева. Несложно показать, что $[G,G] = \langle [g,h] \mid g,h \in G \rangle$, где $[g,h] = g^{-1}h^{-1}gh$ – коммутатор элементов $g$ и $h$.

    Отображение, сопоставляющее группе ее коммутант, естественым образом определяет функтор, так как образ коммутанта очевидно содержится в коммутанте. Дейстие этого функтора на морфизмах – это просто сужение гомоморфизма групп на коммутанты (уменьшается как область определения, так и множество значений).
(5) 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 $\mathcal{B}$.
(6) $\mathcal{M}or : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{S}ets$. Если $\mathcal{C}$ – категория векторных пространств, то вместо категории множеств можно написать категорию векторных пространств. Можно зафиксировать первый или второй аргумент.

    В частности, если $F$ – поле, то $\mathcal{M}or(\_, F) : (\mathcal{V}ect/F)^{op} \to \mathcal{V}ect/F$ – контравариантный функтор на категории векторных пространств. Обычно его действие на объектах обозначается звездочкой. Пространство $V^* = \mathrm{Mor}(V,F)$ называется двойственным (или сопряженным) к $V$, а его элементы часто называются ковекторами.

## 3. Естественные преобразования

Определение 3.1. Пусть $\mathcal{F}, \mathcal{G} : \mathcal{B} \to \mathcal{C}$ – функторы. Естественным преобразованием функторов $\eta : \mathcal{F} \to \mathcal{G}$ называется набор отображений $\eta_X \in \mathrm{Mor}(\mathcal{F}(X), \mathcal{G}(X))$ по всем объектам $X$

категории $\mathcal{B}$, удовлетворяющих условию

$$\eta_Y \circ \mathcal{F}(\alpha) = \mathcal{G}(\alpha) \circ \eta_X$$

для любых объектов $X, Y \in \mathcal{O}bj\,\mathcal{B}$ и любого морфизма $\alpha \in \mathrm{Mor}(X, Y)$.

Последнее условие в определении означает коммутативность следующей диаграммы:

$$\begin{array}{ccc} \mathcal{F}(X) & \xrightarrow{\mathcal{F}(\alpha)} & \mathcal{F}(Y) \\ {\scriptstyle \eta_X}\big\downarrow & & {\scriptstyle \eta_Y}\big\downarrow \\ \mathcal{G}(X) & \xrightarrow{\mathcal{G}(\alpha)} & \mathcal{G}(Y). \end{array}$$

Функторы $\mathcal{F}, \mathcal{G} : \mathcal{B} \to \mathcal{C}$ называются естественно изоморфными, если существует естественное преобразования $\eta : \mathcal{F} \to \mathcal{G}$ такое, что $\eta_X$ является изоморфизмом для любого $X \in \mathcal{O}bj\,\mathcal{B}$. Очевидно, что в этом случае существует и обратное естественное преобразование $\eta^{-1} : \mathcal{G} \to \mathcal{F}$.

Категории $\mathcal{B}$ и $\mathcal{C}$ называются эквивалентными, если существуют функторы $\mathcal{F} : \mathcal{B} \to \mathcal{C}$ и $\mathcal{F}' : \mathcal{C} \to \mathcal{B}$ такие, что композиция $\mathcal{F} \circ \mathcal{F}'$ естественно изоморфна $id_{\mathcal{C}}$, а $\mathcal{F}' \circ \mathcal{F}$ естественно изоморфна $id_{\mathcal{B}}$. Другими словами, существуют естественные изморфизмы $X \cong \mathcal{F}\big(\mathcal{F}'(X)\big)$ и $Y \cong \mathcal{F}'\big(\mathcal{F}(Y)\big)$, где $X \in \mathcal{O}bj\,\mathcal{C}$, а $Y \in \mathcal{O}bj\,\mathcal{B}$. При этом функторы $F$ и $F'$ 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) $\det_n : \mathrm{GL}_n \to \mathrm{GL}_1, \;\; A \mapsto \det A$.

(4) $\mathrm{Mor}(X, \mathrm{Mor}(Y, Z)) \cong \mathrm{Mor}(X \times Y, Z)$ в категории множеств. Аналог этого естественного изоморфизма выполнен в разных других категориях $\mathcal{C}$, если множество $\mathrm{Mor}(Y, Z)$ 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 $\mathrm{Mor}(Y, Z)$ имеет естественную структуру векторного пространства. Поэтому можно считать, что $\mathrm{Mor}_{\mathcal{V}ect/F}(\_\,,\_)$ является функтором $(Vect/F)^{op} \times \mathcal{V}ect/F \to \mathcal{V}ect/F$. Тогда $\mathrm{Mor}\big(X, \mathrm{Mor}(Y, Z)\big)$ естественно изоморфно пространству $\mathrm{Bil}(X \times Y, Z)$ билинейных отображений из $X \times Y$ в $Z$. В следующем параграфе мы определим тензорное произведение $X \otimes Y$ так, чтобы $\mathrm{Bil(X \times Y, Z)}$ было бы естественно изоморфно $\mathrm{Mor}(X \otimes Y, Z)$.

(6) Рассмотрим контравариантный функтор $V \mapsto V^*$ на категории векторных пространств из примера 6. 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 $\eta_V : V \to V^{**}$. 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 $\mathcal{V} = \mathcal{V}ect_{fd}/F$ обозначает категорию конечномерных векторных пространств и их линейных отображений. Рассмотрим сужения функторов $* : \mathcal{V} \to \mathcal{V}^{op}$ и $** : \mathcal{V} \to \mathcal{V}$. Так как размерности пространств $V$, $V^*$ и $V^{**}$ совпадают, то построенные выше отображения $\eta_V$ являются изоморфизмами векторных пространств. Это доказывает, что функтор $** : \mathcal{V} \to \mathcal{V}$ 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 $\mathcal{F} \to \mathcal{G}$, где $\mathcal{F}, \mathcal{G} : \mathcal{C}_\Gamma \to \mathcal{B}$, – это просто морфизм соответствующих диаграмм (см. пример функторов номер 5).

(8) Пусть $\mathcal{F} : \mathcal{B} \to \mathcal{C}$ – функтор. Он определяет естественное преобразование функторов $\eta^{\mathcal{F}} : \mathrm{Mor}\big(\_,\_\big) \to \mathrm{Mor}\big(\mathcal{F}(\_),\mathcal{F}(\_)\big)$ по правилу: $\eta^{\mathcal{F}}_{(X,Y)}(\alpha) = \mathcal{F}(\alpha)$, где $\alpha \in \mathrm{Mor}(X,Y)$.

## 4. Универсальные квадраты

Особое значение имеют универсальные объекты в категории квадратов с тремя фиксированными вершинами. Пусть $\mathcal{C}$ – категория, $A, B, C \in \mathcal{O}bj\,\mathcal{C}$, $\alpha \in \mathrm{Mor}(A,C)$, $\beta \in \mathrm{Mor}(B,C)$. Обозначим через $\mathcal{S}$ категорию коммутативных квадратов вида

$$\begin{array}{ccc} \bullet & \longrightarrow & B \\ \downarrow & & \downarrow{\scriptstyle \beta} \\ A & \xrightarrow{\alpha} & C \end{array}$$

Формально:

$$\mathcal{O}bj\,\mathcal{S} = \{(X,\varphi,\psi) \mid X \in \mathcal{O}bj\,\mathcal{C},\ \varphi \in \mathrm{Mor}(X,B),\ \psi \in \mathrm{Mor}(X,A),\ \beta\circ\varphi = \alpha\circ\psi\},$$
$$\mathrm{Mor}\big((X,\varphi,\psi),(X',\varphi',\psi')\big) = \{\lambda \in \mathrm{Mor}(X,X') \mid \varphi'\circ\lambda = \varphi,\ \psi'\circ\lambda = \psi\}.$$

При этом композиция морфизмов задана очевидным образом. 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 $\mathcal{C}^{op}$.

**Примеры**.

## 5. Сопряженные функторы

Определение 5.1. Пусть $\mathcal{F} : \mathcal{B} \to \mathcal{C}$ и $\mathcal{G} : \mathcal{C} \to \mathcal{B}$ – функторы. $\mathcal{G}$ называется левым сопряженным к $\mathcal{F}$, если существует естественный изоморфизм между функторами $\mathrm{Mor}_{\mathcal{C}}\big(\_,\mathcal{F}(\_)\big)$ и $\mathrm{Mor}_{\mathcal{B}}\big(\mathcal{G}(\_),\_\big)$ (как нетрудно заметить, эти функторы действуют из $\mathcal{C}^{op}\times\mathcal{B}$ в $\mathcal{S}ets$). При этом $\mathcal{F}$ называется правым сопряженным к $\mathcal{G}$.

Теорема 5.2. *Для функтора $\mathcal{F} : \mathcal{B} \to \mathcal{C}$ существует левый сопряженный тогда и только тогда, когда для любого $X \in \mathcal{O}bj\,\mathcal{C}$ существует инициальный объект в категории $\mathcal{M}_X$, определенной следующим образом:*

- $\mathcal{O}bj\,\mathcal{M}_X = \big\{(Y,f) \mid Y \in \mathcal{O}bj\,\mathcal{B},\ f \in \mathrm{Mor}_{\mathcal{C}}\big(X,\mathcal{F}(Y)\big)\big\}$;
- $\mathrm{Mor}\big((Y,f),(Z,g)\big) = \big\{h \in \mathrm{Mor}_{\mathcal{B}}(Y,Z) \mid \mathcal{F}(h)\circ f = g\big\}$;
- *композиция морфизмов – это их композиция в $\mathcal{B}$.*

Доказательство. Пусть $\mathcal{G}$ – левый сопряженный к $\mathcal{F}$, а

$$\eta : \mathrm{Mor}_{\mathcal{C}}\big(\_,\mathcal{F}(\_)\big) \to \mathrm{Mor}_{\mathcal{B}}\big(\mathcal{G}(\_),\_\big)$$

– естественный изоморфизм. Рассмотрим биекцию

$$\eta_{X,\mathcal{G}(X)} : \mathrm{Mor}_{\mathcal{C}}\big(X,\mathcal{F}(\mathcal{G}(X))\big) \to \mathrm{Mor}_{\mathcal{B}}\big(\mathcal{G}(X),\mathcal{G}(X)\big).$$

Положим $f_X = \eta^{-1}_{X,\mathcal{G}(X)}(id_{\mathcal{G}(X)})$. Мы докажем, что пара $(\mathcal{G}(X), f_X)$ является инициальным объектом в категории $\mathcal{M}_X$. Действительно, пусть $(Y,f) \in \mathcal{O}bj\,\mathcal{M}_X$. Положим $g = \eta_{X,Y}(f)$. Рассмотрим коммутативную диаграмму, связанную с естественным преобразованием $\eta^{-1}$ и морфизмом

$(id_X, g) : (X, \mathcal{G}(X)) \to (X, Y)$:

$$\begin{array}{ccc} \mathrm{Mor}_{\mathcal{C}}(X, \mathcal{F}(\mathcal{G}(X))) & \xrightarrow{\varphi \mapsto \mathcal{F}(g)\circ\varphi} & \mathrm{Mor}_{\mathcal{C}}(X, \mathcal{F}(Y)) \\ \eta^{-1}_{X,\mathcal{G}(X)} \uparrow & & \eta^{-1}_{X,Y} \uparrow \\ \mathrm{Mor}_{\mathcal{B}}(\mathcal{G}(X), \mathcal{G}(X)) & \xrightarrow{\psi \mapsto g\circ\psi} & \mathrm{Mor}_{\mathcal{B}}(\mathcal{G}(X), Y) \end{array}$$

Запишем условие коммутативности, примененное к тождественному морфизму $\psi = id_{\mathcal{G}(X)}$:

$$\eta^{-1}_{X,Y}(g) = \mathcal{F}(g) \circ \eta^{-1}_{X,\mathcal{G}(X)}(id_{\mathcal{G}(X)}).$$

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 $(\mathcal{G}(X), f_X) \to (Y, f)$ в категории $\mathcal{M}_X$.

Пусть $g'$ другой морфизм $(\mathcal{G}(X), f_X) \to (Y, f)$ в категории $\mathcal{M}_X$. Это означает, что $f = \mathcal{F}(g') \circ f_X$. Заменив на коммутатвном квадрате $g$ на $g'$, получим

$$\eta^{-1}_{X,Y}(g') = \mathcal{F}(g') \circ \eta^{-1}_{X,\mathcal{G}(X)}(id_{\mathcal{G}(X)}) = \mathcal{F}(g') \circ f_X = f,$$

то есть $g' = \eta_{X,Y}(f) = g$.

Обратно, пусть $(\mathcal{G}(X), f_X)$ – инициальный объект в категории $\mathcal{M}_X$. Если $\varphi \in \mathrm{Mor}(X, X')$, то $f_{X'} \circ \varphi \in \mathrm{Mor}(X, \mathcal{F}(\mathcal{G}(X')))$. По универсальному свойству существует единственный морфизм $\psi : \mathcal{G}(X) \to \mathcal{G}(X')$ 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 $G(id) = id$. Таким образом $\mathcal{G}$ является функтором $\mathcal{C} \to \mathcal{B}$.

Определим функцию

$$\eta_{X,Y} : \mathrm{Mor}_{\mathcal{C}}\big(X, \mathcal{F}(Y)\big) \to \mathrm{Mor}_{\mathcal{B}}\big(\mathcal{G}(X), Y\big)$$

по правилу: для $f : X \to \mathcal{F}(Y)$ морфизм $\eta_{X,Y}(f)$ – это тот единственный морфизм, для которого $f = \mathcal{F}\big(\eta_{X,Y}(f)\big) \circ f_X$. Проверка того, что определенный класс функций задает естественный изоморфизм $\eta$ является рутинной. $\square$

Глава 9

# Полилинейная алгебра

## 1. Модули над кольцами

Определение 1.1. Пусть $R$ – коммутативное кольцо с 1. Аддитивная абелева группа $M$ называется $R$-модулем, если задано умножение $M \times R \to M$ и для любых $m, m' \in M$ и $r, r' \in R$ имеют место равенства:

(1) $(mr)r' = m(rr')$;
(2) $(m + m')r = mr + m'r$;
(3) $m(r + r') = mr + mr'$;

Модуль называется унитальным, если $m \cdot 1 = m$ для любого $m \in M$. В нашем курсе все модули по умолчанию считаются унитальными.

Гомоморфизмом (или $R$-линейным отображением) $R$-модулей называется отображение $L : M \to M'$, удовлетворяющее условиям $L(m + m') = L(m) + L(m')$ и $L(mr) = L(m)r$.

**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 $\varphi : R \to A$ – гомоморфизм колец, то $A$ является $R$-модулем относительно действия: $r * a = \varphi(r)a$.
(5) Если $\varphi : R \to A$ – гомоморфизм колец, а $M$ – $A$-модуль, то $M$ является $R$-модулем относительно действия: $r * m = \varphi(r)m$.
(6) Модуль $R^n$.

Категория, объектами которой являются модули над кольцом $R$, а морфизмами – гомоморфизмы модулей, называется категорией $R$-модулей и обозначается через $R$-$\mathcal{M}od$.

Подмодуль, фактормодуль (по подмодулю), прямая сумма модулей, ядро и образ гомоморфизма, линейная комбинация, линейная оболочка, линейная независимость, система образующих определяется также, как для векторных пространств. Имеет место теорема о гомоморфизме. Базис – это линейно независимая система образующих. Далеко не любой модуль имеет базис.

Пусть $X$ – множество. Рассмотрим категорию $\mathcal{C}_X$.

- Объекты $\mathcal{C}_X$ – это пары $(M, f)$, где $M$ – $R$-модуль, а $f$ – функция из $X$ в $M$.
- Морфизм из $(M, f)$ в $(M', f')$ – это гомоморфизм модулей $L : M \to M'$ такой, что $L \circ f = f'$.
- Композиция морфизмов – это композиция гомоморфизмов.

Определение 1.2. Инициальный объект категории $\mathcal{C}_X$ называется свободным модулем с базисом $X$.

Теорема 1.3. *Пусть $Free_R(X)$ – множество финитных функций $X \to R$, т. е. множество тех функций, значения которых равны нулю везде, кроме конечного множества. Они образуют*

*модуль над $R$ относительно поточечных операций. Зададим функцию $i : X \to Free_R(X)$ 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 $Free_R(X)$ вместе с отображением $i$ – свободный модуль с базисом $X$.*

Доказательство. Пусть $(M, f) \in \mathcal{O}bj\,\mathcal{C}_X$. Зададим функцию $L : Free_R(X) \to M$ формулой $L(\varphi) = \sum\limits_{x \in X} \varphi(x) f(x)$. Так как функция $\varphi$ финитна, то в этой сумме только конечное число слагаемых отлично от нуля. Ясно, что эта функция является линейным отображением. Кроме того, $L\big(i(y)\big) = \sum\limits_{x \in X} \mathbb{1}_y(x) f(x) = f(x)$, что доказывает существование морфизма $L : (Free_R(X), i) \to (M, f)$.

Пусть $L' : (Free_R(X), i) \to (M, f)$ – морфизм в категории $\mathcal{C}_X$. Заметим, что любая финитная функция $\varphi : X \to R$ является линейной комбинацией $\varphi = \sum\limits_{x \in X} \varphi(x)\mathbb{1}_x$. Из линейности $L'$ следует, что $L'(\varphi) = \sum\limits_{x \in X} \varphi(x) L'(\mathbb{1}_x)$, а из условия $L' \circ i = f$ вытекает, что $L'(\mathbb{1}_x) = f(x)$. Таким образом, $L' = L$. □

Теорема 1.4. *Если $X$ конечно, то $Free_R(X) \cong R^{|X|} \cong \underbrace{R \oplus \cdots \oplus R}_{|X| \text{ раз}}$.*

Доказательство. Фактически множество столбцов высоты $n = |X|$ – это и есть множество функций $X \to R$, или множество кортежей длины $n$, которое совпадает с прямой суммой. Легко проверить, что после отождествления окажется, что операции определены одинаково. □

Замечание 1.5. Для бесконечного множества $X$ утверждение тоже верно, если правильно определить прямую сумму бесконечного набора модулей.

Следующее утверждение сразу следует из определения свободного модуля.

Следствие 1.6. *Пусть $\mathcal{F} : R\text{-}\mathcal{M}od \to \mathcal{S}ets$ – забывающий функтор. Тогда множество $\mathrm{Mor}_{\mathcal{S}ets}(X, \mathcal{F}(M))$ естественно изоморфно множеству $\mathrm{Mor}_{R\text{-}\mathcal{M}od}(Free_R(X), M)$, где $X \in \mathcal{O}bj\,\mathcal{S}ets$, а $M \in \mathcal{O}bj\,R\text{-}\mathcal{M}od$.*

## 2. Тензорное произведение

В этом параграфе мы работаем в категории $R\text{-}\mathcal{M}od$.

Определение 2.1. Тензорное произведение $X \otimes_R Y$ модулей $X$ и $Y$ над кольцом $R$ – это инициальный объект в следующей категории $\mathcal{M}$ (зависящей от $X$ и $Y$):

- $\mathcal{O}bj\,\mathcal{C} = \{(Z, B) \mid Z \in R\text{-}\mathcal{M}od,\ B : X \times Y \to Z \text{ билинейное}\}$;
- $\mathrm{Mor}\big((Z, B), (Z', B')\big) = \{L \in \mathrm{Mor}(Z, Z') \mid B' = L \circ B\}$;
- композиция морфизмов – это композиция линейных отображений.

Сейчас мы построим модуль $X \otimes Y$ и докажем, что он удовлетворяет универсальному свойству. Рассмотрим свободный модуль $N = Free_R(X \times Y)$. Пусть $M$ – подмодуль в $N$, порожденный множеством

$$\{\mathbb{1}_{(x+x',y)} - \mathbb{1}_{(x,y)} - 1_{(x',y)},\ \mathbb{1}_{(xr,y)} - \mathbb{1}_{(x,y)} r,\ \mathbb{1}_{(x,y+y')} - \mathbb{1}_{(x,y)} - 1_{(x,y')},\ \mathbb{1}_{(x,yr)} - \mathbb{1}_{(x,y)} r \mid x, x' \in X,\ y, y' \in Y,\ r \in R\}.$$

Обозначим через $\rho : N \to N/M$ канонический гомоморфизм, а через $j : X \times Y \to N/M$ – композицию $\rho \circ i$. Для $x \in X$ и $y \in Y$ положим $x \otimes y = j(x, y) = \mathbb{1}_{(x,y)} + M$.

Теорема 2.2. *Фактормодуль $N/M$ вместе с отображением $j$, построенные выше, является тензорным произведением модулей $X$ и $Y$ над $R$.*

Доказательство. Тот факт, что отображение $j$ билинейно, сразу следует из определения подмодуля $M$.

Пусть $B : X \times Y \to Z$ – билинейное отображение. По универсальному свойству свободного модуля существует единственное линейное отображение $\tilde{L} : N \to Z$ такое, что $\tilde{L} \circ i = B$. Вычисление показывает, что все образующие модуля $M$ лежат в ядре отображения $\tilde{L}$, следовательно $M \leqslant \operatorname{Ker} \tilde{L}$. По универсальному свойству фактормодуля (факторгруппы) существует единственное линейное отображение $L : N/M \to Z$ такое, что $\tilde{L} = L \circ \rho$.

Единственность отображения $L$ следует из универсального свойства свободного модуля и единственности выбора $\tilde{L}$ и $L$ или может быть доказана непосредственно. □

Пусть $\alpha : X \to Y$ и $\beta : X' \to Y'$ – гомоморфизмы $R$-модулей. Пусть $j : X \times Y \to X \otimes Y$ и $j' : X' \times Y' \to X' \otimes Y'$ – канонические билинейные отображения. Определим отображение $\big(\alpha, \beta\big) : X \times Y \to X' \times Y'$ по формуле $\big(\alpha, \beta\big)(x, y) = \big(\alpha(x), \beta(y)\big)$. Легко проверить, что $j' \circ (\alpha, \beta)$ является билинейным отображением. По универсальному свойству тензорного произведения существует гомоморфизм $\alpha \otimes \beta$, делающий следующую диаграмму коммутативной:

$$\begin{array}{ccc} X \times Y & \xrightarrow{\ j\ } & X \otimes Y \\ {\scriptstyle (\alpha,\beta)}\big\downarrow & & \big\downarrow{\scriptstyle \alpha\otimes\beta} \\ X' \times Y' & \xrightarrow{\ j'\ } & X' \otimes Y' \end{array}$$

Этот гомоморфизм называется тензорным произведением гомоморфизмов $\alpha$ и $\beta$.

Предложение 2.3. *Отображения $(X, Y) \mapsto X \otimes Y$ и $(\alpha, \beta) \mapsto \alpha \otimes \beta$ задают функтор $\_ \otimes \_ : R\text{-}\mathcal{M}od \times R\text{-}\mathcal{M}od \to R\text{-}\mathcal{M}od$.*

Предложение 2.4. *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) $R \otimes_R M \cong M$.

Базис тензорного произведения свободных модулей.

Расширение скаляров.

Неприятности в случае колец (неточность функтора $\_ \otimes M$).

## 3. Естественные изоморфизмы

Лемма 3.1. *В категории модулей над (коммутативным) кольцом $R$ с 1 существуют следующие естественные преобразования функторов.*

(1) $\operatorname{Mor}(R, X) \cong X$.
(2) $R \otimes X \cong X$.
(3) $\operatorname{Mor}\big(X, \operatorname{Mor}(Y, Z)\big) \cong \operatorname{Bil}\big(X \times Y, Z\big) \cong \operatorname{Mor}\big(X \otimes Y, Z\big)$.
(4) $M \to M^{**}$.
(5) $\operatorname{Mor}(X, Y) \to \operatorname{Mor}(Y^*, X^*)$.
(6) $\operatorname{Mor}(X, Y) \to (Y^* \otimes X)^*$.
(7) $Y \otimes X^* \to \operatorname{Mor}(X, Y)$.
(8) $X^* \otimes Y^* \to (X \otimes Y)^*$.

Доказательство. Первые 3 эквивалентности были построены в предыдущем параграфе. Естественное преобразование 4 было построено в примере 6 параграфа 3. Естественное преобразование 5 – это частный случай примера 8 параграфа 3 для функтора $\mathcal{F}(V) = V^*$ с очевидными изменениями из за контравариантности функтора $\mathcal{F}$.

Естественное преобразование 6 является композицией предыдущих:

$$\mathrm{Mor}(X,Y) \to \mathrm{Mor}(Y^*,X^*) = \mathrm{Mor}\big(Y^*,\mathrm{Mor}(X,F)\big) \cong \mathrm{Mor}(Y^*\otimes X,F) = (Y^*\otimes X)^*.$$

Зададим отображение $\theta : Y\times X^* \to \mathrm{Mor}(X,Y)$ формулой $\theta(y,f)(x) = yf(x)$. Ясно, что это отображение билинейно. По универсальному свойству тензорного произведения существует единственное отображение $\eta_{X,Y} : Y\otimes X^* \to \mathrm{Mor}(X,Y)$, такое, что $\eta_{X,Y}\circ j = \theta$ (здесь $j : Y\times X^* \to Y\otimes X^*$ – каноническое отображение). Проверка того, что класс морфизмов $\eta_{X,Y}$ задает требуемое в пункте 7 естественное преобразование, оставляется читателю в качестве упражнения.

Естественное преобразование 8 является композицией предыдущих:

$$X^*\otimes Y^* \cong Y^*\otimes X^* \mapsto \mathrm{Mor}(X,Y^*) = \mathrm{Mor}(X,\mathrm{Mor}(Y,F)) \cong \mathrm{Mor}(X\otimes Y,F) = (X\otimes Y)^*.$$

□

Теорема 3.2. *Все естественные преобразования из леммы 3.1 являются естественными эквивалентностями на категории конечномерных векторных пространств.*

Доказательство. Учитывая, что $\dim(U\otimes V) = (\dim U)\cdot(\dim V) = \dim \mathrm{Mor}(U,V)$, легко заметить, что размерности левой и правой части каждого естественного преобразования совпадают. Таким образом достаточно доказать, что указанные отображения инъективны. Инъективность отображения 4 уже доказана. Отображения 6 и 8 являются композицией остальных, поэтому осталось доказать, что инъективны являются отображения 5 и 8. Мы докажем это даже для бесконечномерных пространств.

Докажем тривиальность ядра отображения 5. Обозначим это отображение через $\eta_{X,Y}$. Пусть $f \in \mathrm{Mor}(X,Y)$ – такое отображение, что $\eta_{X,Y}(f) = 0$. Это означает, что для любого $g\in Y^*$ композиция $g\circ f$ равно нулю. Если $f(x)\neq 0$ для некоторого $x\in X$, то существует базис $B$ пространства $Y$, содержащий $f(x)$. Тогда существует линейное отображение $g : Y\to F$, такое, что $g\big(f(x)\big) = 1$ (на остальных базисных векторах можно задать его как угодно). Получили $g\circ f \neq 0$. Противоречие показывает, что $f = 0$, откуда следует тривиальность ядра.

Как мы видели в параграфе 2, если $B$ – базис пространства $Y$, а $C$ – базис пространства $X^*$, то $B\otimes C = \{b\otimes c \mid b\in B,\, c\in C\}$ является базисом $Y\otimes X^*$. Поэтому произвольный элемент пространства $Y\otimes X^*$ может быть записан в виде $\sum\limits_{b\in B,\,c\in C} b\otimes c\alpha_{bc}$, где почти все коэффициенты $\alpha_{bc}$ равны нулю. Образ этого элемента в $\mathrm{Mor}(X,Y)$ – это функция $f$, заданная формулой

$$f(x) = \sum_{b\in B,\,c\in C} bc(x)\alpha_{bc} = \sum_{b\in B} b\Big(\sum_{c\in C} c(x)\alpha_{bc}\Big).$$

Предположим, что эта функция нулевая. Так как набор $B$ линейно независим, то при каждом $b\in B$ имеем $\sum\limits_{c\in C} c(x)\alpha_{bc} = 0$ для любого $x\in X$, т. е. $\sum\limits_{c\in C} c\alpha_{bc} = 0$. Но так как набор функционалов $C$ также линейно независим, то все коэффициенты $\alpha_{bc} = 0$. □

## 4. Тензоры

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

Определение 4.1. Тензором называется полилинейное отображение

$$T : \underbrace{V\times\cdots\times V}_{p\text{ раз}} \times \underbrace{V^*\times\cdots\times V^*}_{q\text{ раз}} \to F.$$

Другими словами, тензор – это линейное отображение

$$T : \underbrace{V\otimes\cdots\otimes V}_{p\text{ раз}} \otimes \underbrace{V^*\otimes\cdots\otimes V^*}_{q\text{ раз}} \to F.$$

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 $\mathrm{Mor}(V,V)$ естественно изоморфно $\mathrm{Mor}(V\otimes V^*,F)$. Билинейная бинарная операция $V\times V\to V$ 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 параграфе 2. $T\otimes T'$ 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 4.2. 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 4.3. *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 $b^*$ и определения его значений на базисных векторах. Для любого функционала $f\in X^*$ имеем

$$f\big(x\big)=f\big(\sum_{i=1}^n e_ie^i(x)\big)=\sum_{i=1}^n f(e_i)e^i(x),$$

т. е. $f=\sum_{i=1}^n f(e_i)e^i$, откуда $e^*$ – система образующих. Пусть $\sum_{i=1}^n\alpha_ie^i=0$. Подставляя в это равенство базисный элемент $e_k$ имеем $\alpha_k=0$, что доказывает линейную независимость. □

Замечание 4.4. Если $e$ бесконечный базис, то набор $\{e^i\}$ не является системой образуюших. 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 $a^i_j$, где верхний индекс – номер строки, но мы не будем пользоваться этим обозначением.

Определение 4.5. Координатами тензора в базисе $e=(e_1,\dots,e_n)$ пространства $V$ называется $p+q$-мерный массив, состоящий из элементов поля

$$T^{j_1\dots j_q}_{i_1\dots i_p}=T(e)^{j_1\dots j_q}_{i_1\dots i_p}=T(e_{i_1},\dots,e_{i_p},e^{j_1},\dots,e^{j_q}),\quad i_1,\dots,i_p,j_1,\dots,j_q\in\{1,\dots,n\}$$

Ясно, что координаты тензора полностью определяют этот тензор:

$$T(v_1,\dots,v_p,f^1,\dots,f^q)=\sum T^{j_1\dots j_q}_{i_1\dots i_p}v^{i_1}_1\dots v^{i_p}_pf^1_{j_1}\dots f^q_{j_q},$$

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 $C_{e\to g}$ и $C_{e^*\to g^*}$. Для этого определим "умножение" $V^*\times V\to F$, по формуле $f\cdot v=f(v)$. Ясно, что это умножение билинейно, поэтому можно пользоваться формализмом, определенном в параграфе 4. В этих обозначениях определение двойственного базиса можно записать в виде $(e^*)^\intercal e=E$.

Лемма 4.6. $C_{e^*\to g^*} = (C_{e\to g}^{-1})^\intercal$.

Доказательство. По определению матрицы перехода $g = eC_{e\to g}$ и $g^* = e^*C_{e^*\to g^*}$. По определению двойственного базиса

$$E = (g^*)^\intercal g = C_{e^*\to g^*}^\intercal (e^*)^\intercal e C_{e\to g} = C_{e^*\to g^*}^\intercal C_{e\to g},$$

откуда получается требуемое равенство. □

Теорема 4.7. *Пусть $e$ и $g$ – базисы пространства $V$, а $T$ – тензор на $V$ типа $(p,q)$.*

$$T(g)_{k_1\dots k_p}^{m_1\dots m_q} = \sum (c')_{j_1\dots j_q}^{m_1\dots m_q} T(e)_{i_1\dots i_p}^{j_1\dots j_q} c_{k_1\dots k_p}^{i_1\dots i_p}, \text{ где}$$

$$c_{k_1\dots k_p}^{i_1\dots i_p} = \prod_{l=1}^{p} (C_{e\to g})_{i_l k_l}, \qquad (c')_{j_1\dots j_q}^{m_1\dots m_q} = \prod_{r=1}^{q} (C_{g\to e})_{m_r j_r}.$$

Доказательство.

$$T(g_{k_1},\dots,g_{k_p},g^{m_1},\dots,g^{m_q}) =$$
$$T\left(\sum_{i_1=1}^{n} e_{i_1}(C_{e\to g})_{i_1k_1},\dots,\sum_{i_p=1}^{n} e_{i_p}(C_{e\to g})_{i_pk_p},\sum_{j_1=1}^{n} e^{j_1}(C_{g\to e})_{m_1j_1},\dots,\sum_{j_p=1}^{n} e^{j_p}(C_{g\to e})_{m_pj_p}\right).$$

Пользуясь полилинейностью $T$ получаем требуемое равенство. □

## 5. Тензорная алгебра и алгебра Грассмана

Пусть $R$ – коммутативное кольцо с 1. Напомним, что $R$-алгеброй называется $R$-модуль $A$ вместе в билинейным отображением $A\times A\to A$, называемым умножением и обозначаемым как умножение. При этом в общем случае не предполагается, что умножение ассоциативно. Однако в настоящем курсе все алгебры по умолчанию будут ассоциативными алгебрами 1, т.,е. заданное в них умножение будет ассоциативным и обладать нейтральным элементом. Гомоморфизмом $R$-алгебр называется линейное отображение, сохраняющее умножение. Категория $R$-алгебр и их гомоморфизмов обозначается через $R$-$\mathcal{A}lg$.

Упражнение 5.1. Докажите, что $R$-$\mathcal{A}lg$ эквивалентна категории гомоморфизмов колец $R\to A$, при которых $R$ переходит в центр $A$, т. е. образы элементов из $R$ перестановочны со всеми элементами $A$.

Пусть $M$ – $R$-модуль. Рассмотрим следующую универсальную задачу: найти инициальный объект в категории $\mathcal{A}_M$:

- $\mathcal{O}bj\,\mathcal{A}_M = \{(A,f) \mid A\in \mathcal{O}bj\, R\text{-}\mathcal{A}lg,\ f\in \mathrm{Mor}_{R\text{-}\mathcal{M}od}(M,A)\}$;
- $\mathrm{Mor}_{\mathcal{A}_M}\big((A,f),(A',f')\big) = \{g\in \mathrm{Mor}_{R\text{-}\mathcal{A}lg}(A,A') \mid g\circ f = f'\}$;
- композиция – это композиция отображений.

Ответом на эту задачу будет так называемая тензорная алгебра $T(M)$ модуля $M$. Прежде, чем построить ее, сформулируем, что такое $\bigoplus_{k=0}^{\infty} M_k$, где $M_k$ – $R$-модули. По определению, это множество всех бесконечных последовательностей $(m_1,m_2,\dots)$, где $m_k\in M_k$, у которых только конечное число компонент не равно нулю. Более строго, $\bigoplus_{k=0}^{\infty} M_k$ – это множество финитных функций $\mathbb{N}\to\bigcup_{k=0}^{\infty} M_k$ таких, что $f(k)\in M_k$ для любого натурального $k$. При этом операции задаются покомпонентно (поточечно), т. е. $(f+g)(k) = f(k)+g(k)$ и $(fr)(k) = f(k)r$.

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 $M^{\otimes(k+n)}$).

Теорема 5.2. *Алгебра $T(M)$ вместе с вложением $f : M = M^{\otimes 1} \hookrightarrow T(M)$ является инициальным объектом категории $\mathcal{A}_M$.*

Доказательство. Пусть $A$ – $R$-алгебра, а $g : M \to A$ – $R$-линейное отображение. Ясно, что отображение $G_k(x_1, \dots, x_k) = g(x_1) \cdot \dots \cdot g(x_k)$ является полилинейным и по универсальному свойству тензорного произведения пропускается через $M^{\otimes k}$ единственным образом. Таким образом, искомое отображение $h : T(M) \to A$ на разложимых тензорах задано формулой $h(x_1 \otimes \dots \otimes x_k) = g(x_1) \cdot \dots \cdot g(x_k)$, а дальше распространено по линейности. Детали оставляются читателю для самостоятельной проработки. □

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).

Пусть $M$ – $R$-модуль. Рассмотрим категории $\mathcal{S}^{\pm}_{M,n}$:

- $\mathcal{O}bj\, \mathcal{S}^{\pm} =$
  $\{(N, f) \mid N \in \mathcal{O}bj\, R\text{-}\mathcal{M}od,\ f$ – [анти]симметричное полилинейное отображение $M^n \to N\}$;
  (симметричное для категории $\mathcal{S}^{+}_{M,n}$ и антисимметричное – для $\mathcal{S}^{-}_{M,n}$).
- $\mathrm{Mor}_{\mathcal{S}^{\pm}_{M,n}}\big((N, f), (N', f')\big) = \{g \in \mathrm{Mor}_{R\text{-}\mathcal{M}od}(N, N') \mid g \circ f = f'\}$;
- композиция – это композиция отображений.

Инициальный объект в категории $\mathcal{S}^{\pm}_{M,n}$ называется $n$-ой симметрической (соотв. внешней) степенью модуля $M$ и обозначаются через $S^n(M)$ и $\Lambda^n(M)$ соответственно.

Теорема 5.3. $S^n(M) = M^{\otimes n}/\langle \dots \otimes a \otimes b \otimes \dots - \dots \otimes b \otimes a \otimes \dots \rangle$.
$\Lambda^n(M) = M^{\otimes n}/\langle \dots \otimes a \otimes a \otimes \dots \rangle$.

Канонический образ элемента $m_1 \otimes \dots \otimes m_n$ в $S^n(M)$ обозначается через $m_1 \dots m_n$, а в $\Lambda^n(M)$ – через $m_1 \wedge \dots \wedge m_n$ (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 $\dots \otimes a \otimes a \otimes \dots$ содержит все элементы вида $\dots \otimes a \otimes b \otimes \dots + \dots \otimes b \otimes a \otimes \dots$, что позволяет в элементах $\Lambda^n(M)$ переставлять сомножители со сменой знака. Следовательно, любой элемент вида $\dots \otimes a \otimes \dots \otimes a \otimes \dots$ также равен нулю в $\Lambda^n(M)$.

Лемма 5.4. *Если $e_1, \dots, e_n$ – базис, то $e_1 \wedge \dots \wedge e_n \neq 0$.*

Доказательство. □

Предложение 5.5. *Если $M \cong R^k$ – конечнопорожденный свободный модуль над $R$ с базисом $e = (e^1, \dots, e^k)$, то базисом $S^n(M)$ является набор $\{e^{i_1} \cdots e^{i_n} \mid 1 \leqslant i_1 \leqslant \dots \leqslant i_n \leqslant k\}$, а базисом $\Lambda^n(M)$ – набор $\{e^{i_1} \wedge \dots \wedge e^{i_n} \mid 1 \leqslant i_1 < \dots < i_n \leqslant k\}$. В частности, ранг модуля $\Lambda^n(M)$ равен $\binom{k}{n}$.*

Определение 5.6. Алгебра $\Lambda(M) = T(M)/I$, где $I$ – идеал, порожденный множеством $\{a \otimes a \mid a \in M\}$, называется внешней алгеброй (алгеброй Грассмана) модуля $M$.

Заметим, что конструкция внешней алгебры, очевидно, функториальна, т. е. гомоморфизм модулей $\varphi : M \to M'$ индуцирует гомоморфизм внешних алгебр $\Lambda(\varphi) : \Lambda(M) \to \Lambda(M')$. При этом следующая диаграмма коммутативна.

$$\begin{array}{ccc} M & \longrightarrow & \Lambda(M) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\Lambda(\varphi)} \\ M' & \longrightarrow & \Lambda(M') \end{array}$$

Лемма 5.7. *Пусть $k \neq n$. В тензорной алгебре модуля $M$:*

$$I = \bigoplus_{k=2}^{\infty} I \cap M^{\otimes k}$$

$$(M^{\otimes k} + I) \cap M^{\otimes n} = I \cap M^{\otimes n} = \langle m_1 \otimes \cdots \otimes m_k \otimes m \otimes m \otimes m_{k+3} \otimes \cdots \otimes m_n \rangle.$$

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 $u_h = \sum_{i:\, k_i = h} x_i \otimes m_i \otimes m_i \otimes y_i \in M^{\otimes k_i} \cap I$. 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 $v \in M^{\otimes k}$, то $v + \sum_{i \neq n} u_i \in (\bigoplus_{l \neq n} M^{\otimes l}) \cap M^{\otimes n} = \{0\}$. Таким образом, $v + u = u_n \in I \cap M^{\otimes n}$, причем по первой части доказательства этот элемент имеет требуемый вид. □

Предложение 5.8. *$\Lambda M = \bigoplus_{k=0}^{\infty} \Lambda^k(M)$ 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 $(M^{\otimes k} + I) \cap M^{\otimes n} \subseteq I$ для любых $k \neq n \in \mathbb{N}$. Следовательно, образы $M^{\otimes k}$ и $M^{\otimes n}$ в $\Lambda(M)$ имеют тривиальное пересечение. 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. □

## 6. Вычисления в алгебре Грассмана

В этом параграфе $V$ – конечномерное векторное пространство над $F$, а все вычисления происходят в алгебре Грассмана $\Lambda(V)$.

Введем обозначение $[n] = \{1, \ldots, n\}$. Пусть $I = \{i_1, \ldots, i_k\} \subseteq [n]$, $i_1 < \cdots < i_k$, а $(x_1, \ldots, x_n)$ кортеж элементов из $V$. Положим $x_I = x_{i_1} \wedge \cdots \wedge x_{i_k}$. Для матрицы $C \in \mathrm{M}\, n, k(F)$ обозначим через $C^I$ подматрицу матрицы $C$, состоящую из строк с номерами $i_1, \ldots, i_k$. Аналогично, для $B \in \mathrm{M}_{k,n}(F)$ через $B_I$ обозначается матрица, составленная из столбцов с номерами $i_1, \ldots, i_k$.

Лемма 6.1. *Пусть $u = (u_1, \ldots, u_n)$ и $v = (v_1, \ldots, v_k)$ два набора элементов пространства $V$, причем $u$ линейно независим, а $C \in \mathrm{M}_{n,k}(F)$. 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 $\varphi : \mathrm{M}_n(F) \to F$ – антисимметричная полилинейная форма столбцов матрицы $C$, а $\varphi(E) = 1$. Поэтому $\varphi(C) = \det C$.

Пусть теперь $k \leqslant n$, а $u$ по-прежнему является базисом. По предложению 5.5 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 $V_I$. Аналогичное обозначение будем использовать для набора элементов пространства $V$. Тогда

$$\bar{v} = (\bar{u}_{j_1}, \ldots, \bar{u}_{j_k}) C^J,$$

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 $\alpha_I = \det C^I$.

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 $\varphi : F^n \to V$, 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 $\Lambda(\varphi) : \Lambda^k(F^n) \to \Lambda(V)$. Применяя $\Lambda(\varphi)$ к последней вынесенной формуле, получаем результат. □

Теорема 6.2 (Бине–Коши). *Пусть $A = BC \in \mathrm{M}_k(F)$, где $B \in \mathrm{M}_{k,n}(F)$, а $C \in \mathrm{M}_{n,k}(F)$. 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 $F^n$. По лемме 6.1 имеем

$$e_{[k]} \det A = a_{[k]} = \sum_{I \subseteq [n],\ |I|=k} v_I \det C^I = e_{[k]} \sum_{I \subseteq [n],\ |I|=k} \det B_I \det C^I.$$

□

Пусть $I = \{i_1, \dots, i_k\} \subseteq [n]$, $[n] \smallsetminus I = \{j_1, \dots, j_{n-k}\}$, $i_1 < \dots < i_k$ и $j_1 < \dots < j_k$. 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 6.3. $\varepsilon(\sigma_I) = \left(\sum\limits_{i \in I} i + \frac{k(k+1)}{2}\right) \mod 2$.

Доказательство. Заметим, что если $j_l > i_k$, то $j_l = l$ (действительно, $\sigma_I$ переставляет только индексы $i_i, \dots, i_k$ в начало, не трогая индексы, большие $i_k$).

Проведем доказательство индукцией по $k$. При $k = 0$ утверждение очевидно. Рассмотрим перестановку $\sigma_{I \smallsetminus \{i_k\}}$

$$\sigma_{I \smallsetminus \{i_k\}} = \begin{pmatrix} 1 & \dots & k-1 & k & \dots & i_k & \dots & n \\ i_1 & \dots & i_{k-1} & j_1 & \dots & i_k & & j_{n-k} \end{pmatrix}$$

По индукционному предположению ее четность равна $\left(\sum\limits_{i \in I} i - i_k + \frac{(k-1)k}{2}\right) \mod 2$. Для того, чтобы получить $\sigma_I$ из $\sigma_{I \smallsetminus \{i_k\}}$ надо переставить $i_k$ на $k$-е место, не меняя порядок остальных индексов. Для этого надо выполнить $i_k - k$ транспозиций. Таким образом,

$$\varepsilon(\sigma_I) = \left(\varepsilon(\sigma_{I \smallsetminus \{i_k\}}) + i_k - k\right) \mod 2 = \left(\sum_{i \in I} i + \frac{(k-1)k}{2} + k\right) \mod 2 = \left(\sum_{i \in I} i + \frac{k(k+1)}{2}\right) \mod 2.$$

□

Обозначим через $\varepsilon_I$ четность перестановки $\sigma_I$.

Лемма 6.4. *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 $\varphi : \Lambda^{n-k}(V) \to \Lambda^k(V)^*$, 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* $e^I = e_{[n]\smallsetminus I}\cdot(-1)^{\varepsilon_{[n]\smallsetminus I}}$. *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 6.5. *Пусть* $A=(B\,C)$ *– матрица, разбитая на блоки* $B\in \mathrm{M}_{n,k}(F)$ *и* $C\in \mathrm{M}_{n,n-k}(F)$. *Тогда*

$$\det A = \sum_{I\subseteq[n],\ |I|=k} (-1)^{\varepsilon_I}\det B^I\cdot\det C^{[n]\smallsetminus I}.$$

Доказательство. Пусть $V=F^n$ – пространство со стандартным базисом $e$. По лемме 6.1 в тензорной 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 6.1 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 6.4 во внешнем произведении этих сумм остаются только слагаемые с $J=[n]\smallsetminus I$. Таким образом

$$e_{[n]}\cdot\det A = \sum_{I\subseteq[n],\ |I|=k} e_I\cdot\det B^I\cdot e_{[n]\smallsetminus I}\cdot\det C^I = e_{[n]}(-1)^{\varepsilon_I}\det B^I\det C^I.$$

□

Пусть $I,J\subseteq[n]$, $|I|=|J|$, а $A\in \mathrm{M}_n(F)$. Обозначим через $A^I_J$ подматрицу в $A$, стоящую на пересечении строк с номерами из $I$ и столбцов с номерами из $J$.

Теорема 6.6. *Пусть* $A\in \mathrm{GL}_n(F)$. *Тогда* $\det(A^{-1})^I_J = \frac{1}{\det A}(-1)^{s_{IJ}}\det A^{[n]\smallsetminus J}_{[n]\smallsetminus I}$, *где* $s_{IJ}=\sum\limits_{l\in I\triangle J} l$.

Доказательство. Пусть $L: F^n\to F^n$ – оператор умножения на матрицу $A$, так что $L_e=A$, где $e$ – стандартный базис в $F^n$. Так как $\Lambda$ – функтор, то $L$ индуцирует эндоморфизм $\Lambda(L)$ алгебры $\Lambda(F^n)$, а также эндоморфизмы $\mathrm{M}_{n,k}\big(\Lambda(L)\big)$ модулей $\mathrm{M}_{n,k}\big(\Lambda(F^n)\big)$, сохраняющие произведения матриц. Допуская вольность записи, все отображения, индуцированные $L$, будут обозначаться тем же символом $L$. Это не может привести к путанице, если следить за типом аргумента отображения $L$.

Пусть $f=\{e_I \mid |I|=k\}$ – базис пространства $\Lambda^k(F^n)$, а $f^*=\{e^I \mid |I|=k\}$ – двойственный базис пространства $\Lambda^{n-k}(F^n)$. В этом доказательстве будем нумеровать столбцы и строки матриц не числами, а $k$-элементными подмножествами множества $[n]$. По лемме 6.1

$$L(e_I) = L(e_{i_1})\wedge\cdots\wedge L(e_{i_k}) = a_{*i_1}\wedge\cdots\wedge a_{*i_k} = \sum_{|J|=k} e_J\det A^J_I.$$

В матричном виде эти равенства можно записать так:

$$L(f) = f\cdot B,\ \text{где } B=\big(\det A^J_I\big)_{|I|=|J|=k}.$$

Аналогично (надо только аккуратно проследить за знаками),

$$L(f^*) = f^*\cdot D,\ \text{где } D=\Big((-1)^{\varepsilon_{[n]\smallsetminus I}+\varepsilon_{[n]\smallsetminus J}}\det A^{[n]\smallsetminus J}_{[n]\smallsetminus I}\Big)_{|I|=|J|=k}.$$

Заметим, что

$$(\varepsilon_{[n]\smallsetminus I}+\varepsilon_{[n]\smallsetminus J}) \mod 2 = \Big(\sum_{l\notin I} l + \frac{(n-k)(n-k+1)}{2} + \sum_{l\notin J} l + \frac{(n-k)(n-k+1)}{2}\Big) \mod 2 =$$

$$\Big(\sum_{l=1}^{n} l - \sum_{l\in I} l + \sum_{l=1}^{n} l - \sum_{l\in J} l\Big) \mod 2 = \Big(\sum_{l\in I\triangle J} l\Big) \mod 2 = s_{IJ}.$$

По лемме 6.4 $f^\intercal f^* = e_{[n]} \cdot E$ (произведение матриц с элементами из алгебры $\Lambda(F^n)$ ). Применяя к этому равенству оператор $L$, получаем

$$L(f)^\intercal L(f^*) = L(e_{[n]}) \cdot E \iff (fB)^\intercal f^* D = e_{[n]} \det A \cdot E \iff B^\intercal D = \det A \iff B^{-1} = \frac{1}{\det A} D^\intercal.$$

Заменяя в формуле для $L(f)$ оператор $L$ на $L^{-1}$, получаем

$$L^{-1}(f) = f \cdot B', \text{ где } B' = \left(\det(A^{-1})_I^J\right)_{|I|=|J|=k}.$$

С другой стороны, $f = L^{-1} \circ L(f) = fBB'$, откуда $B' = B^{-1} = \frac{1}{\det A} D^\intercal$. Сравнивая две формулы для элементов матрицы $B'$, получаем результат. $\square$

Глава 10

# Теория групп

Мы возвращаемся к изучению теории групп и рассмотрим в этой главе несколько базовых конструкций.

## 1. Действие группы на множестве и лемма Бернсайда

Определение 1.1. Пусть $G$ – группа, а $X$ – множество. Будем говорить, что $G$ действует на $X$ и писать $G \curvearrowright X$, если задана операция $G \times X \to X$ (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 $X \to X$ с операцией композиции называется *симметрической группой* на множестве $X$ и обозначается через $S_X$. Заметим, что любой гомоморфизм $\varphi : G \to S_X$ задает действие группы $G$ на множестве $X$ по правилу $gx = \varphi(g)(x)$ (проверьте, что эта операция действительно удовлетворяет условиям определения 1.1). Обратно, если задано действие $G$ на $X$, то можно задать гомоморфизм $\varphi : G \to S_X$ формулой $\varphi(g)(x) = gx$ (проверьте, что $\varphi(g)$ биекция и что $\varphi$ – гомоморфизм). Таким образом, можно считать, что действие группы на множестве – это гомоморфизм $G \to S_X$, 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 1.2. Будем говорить, что $G$ действует справа на $X$ и писать $X \curvearrowleft G$, если задана операция $X \times G \to X$ (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 $\eta_X : G \to S_X$. Из правового действия довольно просто сделать левое действие, взяв композицию

$$G \overset{inv}{\to} G \overset{\eta_X}{\to} S_X, \text{ где } inv(g) = g^{-1}.$$

**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 1.3. *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 1.4. *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 1.5. Неподвижными точками элемента $g \in G$ называются те $x \in X$, для которых $gx = x$. *Множество неподвижных точек* элемента $g$ мы будем обозначать через $\mathrm{Fix}_X(g)$.

Определение 1.6. Множество элементов группы $G$, оставляющих на месте данный элемент $x \in X$ называется *стабилизатором* элемента $x$ и обозначается через $G_x$. Другими словами, $G_x = \{g \in G \,|\, gx = x\}$. Очевидно, что стабилизатор является подгруппой в $G$.

Замечание 1.7. 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:

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |\,\mathrm{Fix}_X(g)|.$$

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 1.8. *Отображение $f : G/G_x \to Gx$ заданное формулой $f\big(gG_x\big) = gx$ 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 $f\big(gG_x\big) = f\big(hG_x\big)$, т. е. $gx = hx$. Но тогда $h^{-1}gx = x$, откуда $h^{-1}g \in G_x$, а из этого сразу следует, что $gG_x = hG_x$. □

Определение 1.9. Пусть $G \curvearrowright X$.

- Действие называется точным, если $\mathrm{Ker}(\theta_X) = \{1\}$, другими словами, если из того что $\forall x \in X : gx = x$ следует, что $g = 1$.
- Действие называется свободным, если $gx = x \implies g = e$, другими словами, если $\forall x \in X$: $G_x = \{e\}$.
- 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 значение, равносильно можно написать $\exists x \in X : Gx = X$).

**Примеры**.

- $S_n \curvearrowright \{1, \ldots, n\}$.
- $\mathrm{GL}_n(R) \curvearrowright R^n$.
- $G \curvearrowright G$, $gx$ – умножение в группе (регулярное действие или действие левыми трансляциями) Оно является свободным и транзитивным.
- $G \curvearrowright G$, ${}^g x := gxg^{-1}$ – действие левым сопряжением.
  $\mathrm{Ker}(G \to S_G) = C(G)$ – центр группы $G$. Орбита называется классом сопряженных элементов.
- $G \curvearrowright G$, $x^g := g^{-1}xg$ – действие правым сопряжением. Это правое действие.
- $G \times G \curvearrowright G$: $(g, h)x := gxh^{-1}$.
- $G \curvearrowright X$, $H \leqslant G \implies H \curvearrowright X$.
  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 1.10 (лемма Бернсайда). *Количество орбит действия группы $G$ на множестве $X$ равно*

$$\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}_X(g)|.$$

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 1.8 получим $N=\sum_{x\in X}\frac{|G_x|}{|G|}=\frac{1}{|G|}\sum_{x\in X}|G_x|$. Используя формулу из замечания 1.7 получим $N=\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}_X(g)|$, что и требовалось доказать. □

## 2. 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 2.1. Пусть $X,Y$ – $G$-множества. Функция $f:X\to Y$ называется $G$-эквивариантной (морфизмом $G$-множеств), если $f(gx)=g\,f(x)$ для любых $x\in X$ и $g\in G$.

Таким образом, для фиксированной группы $G$ мы определили категорию $G$-множеств. Изоморфизмами в этой категории очевидно являются $G$-эквивариантные биекции. В этом параграфе мы дадим классификацию $G$-множеств с точностью до изоморфизма.

ЛЕММА 2.2. *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. □

ОПРЕДЕЛЕНИЕ 2.3. 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 2.4. *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 $\varphi:G/G_x\to Gx=X$, $\varphi(gG_x)=gx$, заданную в лемме 1.8, 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, $g^{-1}Hg\subseteq F$. Обратное включение доказывается аналогично. □

Следствие 2.5 (классификация $G$-множеств). *Любое $G$-множество изоморфно $\bigsqcup\limits_{i\in\mathcal{I}} G/H_i$, 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 $\sigma:\mathcal{I}\to\mathcal{J}$ и элементы $g_i\in G$ такие, что $g_iH_ig_i^{-1}=F_{\sigma(i)}$.*

Замечание 2.6. Если $H_i=H_j$ при некоторых $i\neq j\in\mathcal{I}$, то в формуле содержится дизъюнктное объединение множества $X=G/H_i$ с самим собой, что не является строгой записью. Формально, вместо $\bigsqcup\limits_{i\in\mathcal{I}} G/H_i$ должно быть $\bigsqcup\limits_{i\in\mathcal{I}}(G/H_i)\times\{i\}$ внутри декартова произведения $(\bigcup\limits_{i\in\mathcal{I}} G/H_i)\times\mathcal{I}$. При этом $G$ действует только на первую компоненту декартова произведения.

## 3. Теоремы Силова

Теорема 3.1 (2-я теорема об изоморфизме (ее надо в другой параграф!!!)). *Пусть $A,B$ – подгруппы группы $G$, причем $A$ нормализует $B$, т. е. $aBa^{-1}=B$ для любого $a\in A$. Тогда $AB=\{ab\mid a\in A,\,b\in B\}$ является подгруппой в $G$, $B$ нормальна в $AB$, и*

$$\frac{AB}{B}\cong\frac{A}{A\cap B}.$$

Доказательство. Первые 2 утверждения очевидны. Для доказательства последнего рассмотрим гомоморфизм $A\to(AB)/B$, являющийся композицией вложения и канонической проекции $A\hookrightarrow AB\twoheadrightarrow(AB)/B$, и докажем, что он сюръективен, а его ядро равно $A\cap B$. □

Далее в этом параграфе $G$ – конечная группа, а $p$ – простое число.

Группа порядка $p^k$ называется $p$-группой.

Следствие 3.2. *Если $A,B$ – $p$-подгруппы в $G$, причем $A$ нормализует $B$, то $AB$ также является $p$-подгруппой.*

Лемма 3.3. *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 $p$.*

Определение 3.4. $p$-Подгруппа $S\leqslant G$ называется силовской $p$-подгруппой, если если ее индекс взаимно прост с $p$.

Теорема 3.5 (теоремы Силова).

**$\mathbf{E}_p$**: *В $G$ существует силовская $p$-подгруппа.*
**$\mathbf{C}_p$**: *Все силовские $p$-подгруппы в $G$ сопряжены.*
**$\mathbf{D}_p$**: *Любая $p$-подгруппа содержится в силовской $p$-подгруппе.*
**$\mathbf{F}_p$**: *Количество силовских $p$-подгрупп сравнимо с 1 по модулю $p$.*

Доказательство. **$\mathbf{E}_p$**. Индукция по $|G|$. База тривиальна. Если $|G|$ не делится на $p$, то доказывать нечего. Поэтому считаем, что $|G|\vdots p$.

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 количество неподвижных точек относительно $G$ делится на $p$, т. е. порядок центра группы $G$ делится на $p$. По теореме о строении конечнопорожденных абелевых групп в центре существует подгруппа $C$ порядка $p$. По индукционному предположению в группе $G/C$ существует силовская $p$-подгруппа. Легко видеть, что ее полный прообраз является силосвкой $p$-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 $p$-подруппы $S$ на множестве $X$ всех силовских $p$-подгрупп сопряжением. Если $\{P\}$ – неподвижный элемент этого действия, то $S$ нормализует $P$ (т. е. $sPs^{-1} = P$ для любого $s \in S$). Тогда по следствию $PS$ является $p$-подгруппой и, следовательно, совпадает с $S$. Таким образом у этого действия ровно одна неподвижная точка. Теперь по лемме $1 \equiv |X| \bmod p$, что и требовалось доказать. □

## 4. Полупрямое произведение

В категории $\mathcal{C}$ рассмотрим морфизмы $A \xrightarrow{\varphi} B \xrightarrow{\psi} A$, композиция которых равна $id_A$. 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 $\mathrm{GL}_n(R[t]) \twoheadrightarrow \mathrm{GL}_n(R)$. В настоящем параграфе мы выясним, как устроена любая ретракция групп.

Предложение 4.1. *Пусть $H, K$ – подгруппы в $G$, причем $K$ – нормальна. Следующие условия эквивалентны.*

(1) *Существет ретракция $\psi : G \to H$ группы $G$ на подгруппу $H$ (сечение – это вложение $H$ в $G$), а $K = \operatorname{Ker}\psi$.*
(2) *$G = KH$ и $H \cap K = \{1\}$ (заметим, что $HK$ – подгруппа по теореме 3.1).*
(3) *Любой элемент группы $G$ единственным образом представляется в виде произведения $kh$, $h \in H$, $k \in K$.*

Доказательство. (1) $\Longrightarrow$ (2). По условию композиция вложения $H \hookrightarrow G$ и $\psi$ – тождественное отображение. Другими словами, $\psi(h) = h$ для любого $h \in H$, в частности, $\psi\big(\psi(g)\big) = \psi(g)$. Для любого $g \in G$ имеем: $g = g\psi(g)^{-1} \cdot \psi(g)$, причем $\psi\big(g\psi(g)^{-1}\big) = \psi(g)\psi(g)^{-1} = 1$, 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) $\Longrightarrow$ (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) $\Longrightarrow$ (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 $\operatorname{Ker}\psi = K$. С другой стороны, $\psi(h) = h$ для любого $h \in H$, т. е. композиция вложения $H \hookrightarrow G$ и $\psi$ тождественна. □

Определение 4.2. Если выполнены условия предложения 4.1, то $G$ называется (внутренним) полупрямым произведением подгрупп $H$ и $K$; это обозначается через $G = K \rtimes H$.

Пусть $G = K \rtimes H$, а $\theta : H \to S_K$ – 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 $\mathrm{Aut}(K)$ 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 $\theta : B \to \mathrm{Aut}(A)$.

Определение 4.3. 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 4.4. *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 $\theta : H \to \mathrm{Aut}(K)$ – действие $H$ на $K$ левыми сопряжениями, то $G \cong K \rtimes_\theta H$.*

## 5. Свободные группы, задание группы образующими и соотношениями

Универсальное свойство свободной группы аналогично определению свободного модуля. Пусть $X$ – множество. Рассмотрим категорию $\mathcal{C}$, объектами которой являются пары $(G, f)$, где $G$ – группа, а $f : X \to G$ – функция. Морфизм из $(G, f)$ в $(G', f')$ – это гомоморфизм $\varphi : G \to G'$ такой, что $\varphi \circ f = f'$. Свободная группа, с множеством образующих $X$, – это инициальный объект в категории $\mathcal{C}$. Как обычно, это определение ничего не говорит о существовании этого инициального объекта и про обозначения (если инициальный объект существует, то он единственный с точностью до единственного изоморфизма, но даже среди канонически изоморфных объектов удобно выбрать какой-то конкретный).

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 $W$, 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. Она называется свободной группой порожденной $X$ (или свободной группой множества $X$).

ТЕОРЕМА 5.1. *Группа $F(X)$ вместе с отображением $X \to F(X)$, $x \mapsto [x]$ является инициальным объектом в категории $\mathcal{C}$, определенной в начале параграфа.*

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 $f : X \to G$ – функция из $X$ в группу $G$. Зададим отображение $\psi : W \to G$ формулой

$$\psi(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} \cdot \ldots \cdot f(x_n)^{\varepsilon_n}, \text{ где } x_1, \dots, x_n \in X,\ \varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}.$$

Так как $\psi(w_1 x \bar{x} w_2) = \psi(w_1 w_2)$, то отношение $u \sim_\psi v \iff \psi(u) = \psi(v)$ на $W$ содержит $Q$. А так как оно является отношением эквивалентности, то оно содержит и отношение $\sim$ на $W$, определенное выше. Другими словами, $\psi(u) = \psi(v)$ при любых $u \sim v$. Поэтому функция

$$\varphi : F(X) \to G, \qquad \varphi([w]) = \psi(w)$$

задана корректно. Теперь очевидно, что $\varphi$ является гомоморфизмом, причем $\varphi([x]) = f(x)$ для любого $x \in X$, что равносильно коммутативности диаграммы. Так как любой гомоморфизм $F(X) \to G$, 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 $\varphi$. □

ТЕОРЕМА 5.2 (теорема Нильсена–Шрайера). *Любая подгруппа свободной группы свободна.*

ЗАМЕЧАНИЕ 5.3. При этом количество образующих подгруппы неабалевой свободной группы может быть любым от 1 до (счетной) бесконечности.

Далее: соотношения, универсальная группа, с данными образующими и соотношениями. *To be written.*

## 6. Конечнопорожденные модули над евклидовыми кольцами

Этот параграф лежит на стыке теории коммутативных колец и линейной алгебры. Поводом отнести его к теории групп является то, что мы в частности докажем теорему о строении конечнопорожденных абелевых групп (которая уже использовалась при доказательстве теорем Силова).

Пусть $R$ – коммутативное кольцо, а $M$ – конечнопорожденный $R$-модуль, т. е. существует конечный набор $X = \{x_1, \dots, x_k\}$ такой, что любой элемент модуля $M$ является линейной комбинацией этих элементов. Так как $X$ конечен, то свободный модуль $Free(X)$ можно отождествить с модулем $R^k$ столбцов высоты $k$. Положим $x = (x_1, \dots, x_k)$. Отображение $\varphi : R^k \to M$ заданное формулой $\varphi(a) = xa$ очевидно является эпиморфизмом, поэтому $M \cong R^k/N$, где $N = \operatorname{Ker}\varphi$. Таким образом, для описания произвольного конечнопорожденного $R$-модуля достаточно описать подмодули в $R^k$.

Прежде, чем перейти к классификации подмодулей, определим аналог размерности векторных пространств для конечнопорожденных свободных модулей. Если $f$ и $g$ – конечные базисы свободного модуля, то, также как и для векторных пространств, существуют взаимно обратные матрицы перехода $C_{f\to g}$ и $C_{g\to f}$. 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.

Теорема 6.1. *Пусть $R$ – евклидово кольцо. Существует базис $f = (f_1, \dots, f_k)$ модуля $R^k$ и элементы $\alpha_1, \dots, \alpha_k \in R$ такие, что*

(1) *элементы $f_1\alpha_1, \dots, f_k\alpha_k$ 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).*

Прежде, чем перейти к доказательству, напомним обозначения для элементарных матриц, т. е. матриц, умножение на которые реализуют элементарные преобразования Гаусса.[1]

- $T_{ij}(\lambda)$ (где $i \neq j$, а $\lambda \in R$) – элементарная трансвекция, т. е. матрица, отличающаяся от единичной только в позиции $(i, j)$, в которой стоит $\lambda$.
- $D_i(\varepsilon)$ (где $\varepsilon$ – обратимый элемент) – диагональная матрица с $\varepsilon$ на $i$-м диагональном месте и 1 на остальных.
- $P_\sigma$ (где $\sigma \in S_n$, а $n$ определено из контекста) – матрица перестановка, т. е. матрица, полученная из единичной перестановкой строк ($i$-я строка $E$ стоит на месте $\sigma(i)$ ).

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 евклидова кольца – главный. Таким образом, достаточно взять $f_1 = 1$, а $\alpha_1$ – образующая этого идеала.[2]

Пусть $k > 1$. Обозначим через $\varphi$ евклидову норму на $R$. Пусть $S = \{(Un)_1 \mid U \in \mathrm{GL}_k(R),\ n \in N\}$ (здесь индекс 1 означает, что берется первый элемент столбца). Пусть $\alpha_1 = (As)_1 \in S \setminus \{0\}$ – элемент с наименьшей евклидовой нормой, где $A \in \mathrm{GL}_k(R)$, а $s \in N$. Поделим $(As)_i$ на $\alpha_1$ с остатком: $(As)_i = \alpha_1\beta + \rho$. Тогда $i$-й элемент столбца $T_{i1}(-\beta)As$ равен $\rho$. Поэтому $\rho =$

[1] Эти обозначения должны быть в линейной алгебре! В современном научном языке только первая из этих матриц называется элементарной, потому что элементарная матрица должна иметь определитель 1, но для наших целей удобнее пользоваться старой терминологией.

[2] На самом деле можно было бы начинать индукцию с $k = 0$, при котором утверждение пусто, так как нулевой модуль порожден пустым множеством.

$\big(P_{(1\,i)}T_{i1}(-\beta)As\big)_1 \in S$. Так как $\varphi(\rho) < \varphi(\alpha_1)$, то $\rho = 0$ (иначе это противоречит минимальности $\varphi(\alpha_1)$ ). Следовательно, все элементы столбца $As$ делятся на первый, поэтому существует обратимая матрица $B$ такая, что $BAs = (\alpha_1, 0, \dots, 0)^\intercal$ (здесь $B$ – матрица, реализующая соответствующие элементарные преобразования).

Для элемента $n \in N$ разделим $(BAn)_1$ на $\alpha_1$ с остатком: $(BAn)_1 = \alpha_1\beta' + \rho'$. Тогда $\rho' = (BAn)_1 - (BAs)_1\beta' = \big(BA(n - s\beta')\big)_1 \in S$. Так как $\varphi(\rho') < \varphi(\alpha_1)$, то $\rho' = 0$. Таким образом, любой элемент подмодуля $BAN = \{BAn \mid n \in N\}$ лежит в линейной оболочке столбцов $BAs = e_1\alpha_1, e_2, \dots, e_k$, где $e_i$ – $i$-й столбец единичной матрицы. Положим $f_1 = (BA)^{-1}e_1$ и $f_i' = (BA)^{-1}e_i$ при $i = 2, \dots, k$. Заметим, что $s = f_1\alpha_1 \in N$.

Имеем $N \leqslant \langle s, f_2', \dots, f_k'\rangle$. Так как $s \in N$, а столбцы $f_1, f_2', \dots, f_k'$ линейно независимы, то $N = \langle s\rangle \oplus N'$, где $N' = N \cap \langle f_2', \dots, f_k'\rangle$. Модуль $N'$ содержится в свободном модуле $\langle f_2', \dots, f_k'\rangle$ ранга $k-1$, поэтому к нему можно применить индукционное предположение. Другими словами, существует базис $f_2, \dots, f_k$ модуля $\langle f_2', \dots, f_k'\rangle$ и элементы $\alpha_2, \dots, \alpha_k \in R$ такие, что $N'$ порожден элементами $f_2\alpha_2, \dots, f_k\alpha_k$ и $\alpha_{i+1}$ делится на $\alpha_i$ при всех $i = 2, \dots, k-1$. Легко проверить, что $f_1, \dots, f_k$ – базис модуля $R^k$, а $f_1\alpha_1, \dots, f_k\alpha_k$ порождает $N$. Осталось доказать, что $\alpha_2$ делится на $\alpha_1$.

Пусть $\alpha_2 = \alpha_1\beta'' + \rho''$. Обозначим через $C = C_{e\to f}$ матрицу, составленную из столбцов $f_1, \dots, f_n$. Тогда $C^{-1}(f_1\alpha_1\beta'' + f_2\alpha_2) = (\alpha_1\beta'', \alpha_2, 0, \dots, 0)^\intercal$, откуда

$$(\rho'', \alpha_2, 0, \dots, 0) = D_1(-1)T_{12}(-1)C^{-1}(f_1\alpha_1\beta'' + f_2\alpha_2) \in D_1(-1)T_{12}(-1)C^{-1}N.$$

следовательно, $\rho'' \in S$. Так как $\varphi(\rho'') < \varphi(\alpha_1)$, то минимальность $\varphi(\alpha_1)$ влечет равенство $\rho'' = 0$, что завершает доказательство. □

Следствие 6.2. *Любой подмодуль конечнопорожденного свободного модуля над евклидовым кольцом является свободным, причем ранг подмодуля не превосходит ранга модуля.*

Следствие 6.3 (Нормальная форма Смита). *Для любой матрицы $A \in \mathrm{M}_{k,l}(R)$ над евклидовым кольцом $R$ существуют матрицы $B \in \mathrm{GL}_k(R)$ и $C \in \mathrm{GL}_l(R)$ такие, что все недиагональные элементы матрицы $BAC$ равны нулю, а каждый диагональный элемент делится на предыдущий.*

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 $\pi : R \to M$, заданное формулой $\pi(r) = mr$ является эпиморфизмом модулей, следовательно $M \cong R/\operatorname{Ker}\pi$.

Циклический модуль $R/I$ называется примарным, если $I$ – степень простого идеала (для того, чтобы не делать лишних оговорок, модуль $R = R/\{0\}$ также называется примарным в случае, когда $R$ область целостности).

Теорема 6.4 (Классификация конечнопорожденных модулей). *Любой конечнопорожденный модуль над евклидовым кольцом изоморфен прямой сумме примарных модулей.*

Доказательство. Пусть $M$ – конечнопорожденный модуль над евклидовым кольцом $R$. Как уже говорилось, существует эпиморфизм $R^k \to M$. Обозначим его ядро через $N$ По теореме 6.1 существует базис $f_1, \dots, f_k$ модуля $R^k$ и элементы $\alpha_1, \dots, \alpha_k \in R$ такие, что $N = \langle f_1\alpha_1, \dots, f_n\alpha_n\rangle$. Зададим гомоморфизм $\rho : R^k \to \bigoplus_{i=1}^{k} R/\alpha_i R$ формулой

$$\rho(f_1\beta_1 + \dots + f_k\beta_k) = (\beta_1 \mod \alpha_1, \dots, \beta_k \mod \alpha_k)$$

(так как $f$ – 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. □

Замечание 6.5. Последняя теорема верна для любого кольца главных идеалов, но доказательство длиннее. Мы ограничиваемся случаем евклидовых колец, потому что для приложений нам необходимы только $\mathbb{Z}$ и кольца многочленов над полем.

Следствие 6.6 (Классификация конечнопорожденных абелевых групп). *Любая конечнопорожденная абелева группа изоморфна прямой сумме циклических групп бесконечного порядка и порядка $p^n$, где $p$ – простое число.*

В частности, если порядок абелевой группы делит простое число $p$, то среди прямых слагаемых обязательно должна быть циклическая группа порядка $p^n$, следовательно, в ней есть элемент порядка $p$ – утверждение, использованное при доказательстве первой теоремы Силова.

Из теоремы о строении конечнопорожденных модулей, примененной к кольцу многочленов над замкнутым полем, получаем доказательство существования из теоремы 2.2.

Доказательство существования жордановой формы. Пусть $F$ – алгебраически замкнутое поле, $V$ – векторное пространство над $F$, $L : V \to V$ – 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 $R$ – евклидово кольцо, то по теореме 6.4 $V$ 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[3] $\sum_{i=0}^{k-1} \alpha_i (t-\lambda)^i$, где $\alpha_i \in F$. Таким образом, элементы $(t-\lambda)^i$, $i = 0, \ldots, k-1$, образуют базис $M$, как векторного пространства над $F$. Если $v_0, \ldots, v_{k-1}$ – элементы $V$, соответствующие $(t-\lambda)^0, \ldots, (t-\lambda)^{k-1}$ 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 $\langle v_0, \ldots, v_{k-1} \rangle$ 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. □

[3]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 $k$.

Глава 11

# Многочлены

В будущем предполагается успеть рассказать здесь несколько вещей, которые сейчас вынесены только в заголовки (пустых) параграфов. В курсе 2015-2016 года я не успеваю ничего из этой главы.

**1. Многочлены над факториальным кольцом, лемма Гаусса**

**2. Симметрические многочлены**

**3. Нетеровы кольца, теорема Гильберта о базисе**

**4. Теорема Гильберта о нулях, идеи алгебраической геометрии**

**5. Базисы Гребнера**

Глава 12

# Поля и элементы теории Галуа

## 1. Расширение полей

Пусть $F \subseteq K$ – два поля. Говорят, что $K$ является расширением $F$ и пишут "пусть $K/F$ – расширение полей". Обозначение нехорошее, потому что можно перепутать с факторгруппой аддитивных групп этих полей, но общепринятое. Поле $K$ можно рассматривать как векторное пространство над $F$. Размерность этого пространства называется степенью расширения $K/F$ и обозначается $[K : F]$. Расширение называется конечным в случае, когда его степень конечна.

Расширение $K/F$ называется простым, если существует элемент $\theta \in K$ такой, что $K$ – наименьшее расширение $F$, содержащее $\theta$. Полем дробно-рациональных функций $F(t)$ называется поле частных кольца многочленов $F[t]$.

Лемма 1.1. *Простое расширение изоморфно либо полю дробно-рациональных функций $F(t)$, и тогда оно бесконечно, либо факторкольцу $F[t]/(p)$, где $p \in F[t]$ – неприводимый многочлен, и тогда оно конечно, и его степень равна* $\deg p$.

Доказательство. Рассмотрим канонический гомоморфизм $K$-алгебр $\varepsilon : F[t] \to K$, посылающий $t$ в $\theta$. Если ядро равно нулю, то образ изоморфен $F[t]$. По универсальному свойству поля частных существует гомоморфизм $F(t) \to K$, который по определению простого расширения будет эпиморфизмом. Так как любой гомоморфизм полей является мономорфизмом, то в этом случае $F(t) \cong K$.

Пусть $\operatorname{Ker}\varepsilon \neq 0$. Так как $F[t]$ – область главных идеалов, то $\operatorname{Ker}\varepsilon = (p)$ для некоторого многочлена $p \in F[t]$. Так как $\operatorname{Im}\varepsilon$ – область целостности, то $(p)$ – простой идеал, т. е. $p$ неприводим. Ненулевой простой идеал является максимальным, таким образом $\operatorname{Im}\varepsilon$ – поле. По определению простого расширения $K = \operatorname{Im}\varepsilon \cong F[t]/(p)$. □

Определение алгебраического и трансцендентного элемента над $F$ (в произвольной $F$-алгебре)!!!.

Лемма 1.2. *Пусть $p \in F[t]$ – неприводимый многочлен. Если $K$ – расширение $F$, в котором $p$ имеет корень, то существует мономорфизм полей $F[t]/(p) \rightarrowtail K$.*

Лемма 1.3. *Если $L/K/F$ – расширения полей, то $[L : F] = [L : K] \cdot [K : F]$.*

Доказательство. Если $X$ – базис $L$ над $K$, а $Y$ – базис $K$ над $F$, то $\{kl \mid k \in Y, l \in X\}$ является базисом $L$ над $F$. □

## 2. Поле разложения

Пусть $p \in F[t]$ – (не обязательно неприводимый) многочлен над $F$. Мы хотим построить универсальное расширение $K/F$, в котором многочлен $p$ раскладывается на линейные множители. К сожалению, универсальности добиться не удастся, потому что не удастся соблюсти единственность. Это видно уже на примере $F = \mathbb{R}$ и $p = t^2+1$, так что $K = \mathbb{C}$, но у поля $\mathbb{C}$ есть автоморфизм, оставляющий $\mathbb{R}$ на месте – комплексное сопряжение. Несмотря на эту неудачу, такое расширение все же будет единственным с точностью до (неединственного) изоморфизма.

Определение 2.1. Полем разложения многочлена $p \in F[t]$ над полем $F$ называется такое расширение $K/F$, что многочлен $p$ раскладывается над $K$ на линейные множители, и для любого другого расширения $L/F$, обладающего тем же свойством, существует гомоморфизм полей $K \to F$ тождественный на $F$.

ТЕОРЕМА 2.2. *Поле разложение многочлена $p$ над $F$ существует и единственно с точностью до изоморфизма, тождественного на $F$.*

ДОКАЗАТЕЛЬСТВО. Проведем доказательство существования индукцией по $\deg p$. База очевидна (при $\deg p = 1$). Пусть $p = fg$, где $f$ неприводим. Тогда над полем $\tilde{F} = F[t]/(f)$ многочлен $f$ имеет корень и, следовательно, раскладывается на множители $f = (t-\theta)\tilde{f}$. Таким образом, над $\tilde{F}$ имеем $p = (t-\theta)\tilde{p}$, где $\tilde{p} = \tilde{f}g$. По индукционному предположению существует поле разложение $K$ многочлена $\tilde{p}$ над $\tilde{F}$. Это поле и будет полем разложения $p$ над $F$.

Ясно, что $p$ раскладывается над $K$ на линейные множители. Докажем "версальное" свойство поля $K$.[1] Пусть $L/F$ другое расширение, в котором $p$ раскладывается на линейные множители. По единственности разложения на неприводимые, $f$ должен делиться хотя бы на один линейный сомножитель, т. е. иметь корень в поле $L$. По лемме существует вложение $\tilde{F} \rightarrowtail L$. Отождествляя элементы $\tilde{F}$ с их образами в $L$, и используя версальное свойство поля разложения $\tilde{f}$ над $\tilde{F}$, убеждаемся, что существует вложение $K \rightarrowtail L$, что и доказывает, что $K$ – поле разложения $p$ над $F$.

По лемме 1.3, только что построенное расширение $K/F$ имеет конечную степень, как последовательное выполнение конечного числа конечных расширений. Пусть $\hat{K}$ – другое поле разложения $p$ над $F$. По определению поля разложения существуют гомоморфизмы $\varphi : K \to \hat{K}$ и $\hat{\varphi} : \hat{K} \to K$, тождественные на $F$. Любой гомоморфизм полей инъективен, а при инъективном отображении размерность векторного пространства не падает. Следовательно, $\dim_F K = \dim_F \hat{K}$. Инъективные отображения между векторными пространствами одинаковой размерности являются биективными, поэтому $\varphi$ и $\hat{\varphi}$ – изоморфизмы (не обязательно взаимно обратные, но это и не требуется). □

## 3. Существование и единственность конечных полей

ТЕОРЕМА 3.1. *Любое конечное поле имеет содержит $p^n$ элементов, где $p$ – простое число, а $n \in \mathbb{N}$.*

*Обратно, для любого простого числа $p$ и натурального $n$ существует поле из $p^n$ элементов, и любые два таких поля изоморфны.*

ДОКАЗАТЕЛЬСТВО. Пусть $K$ – конечное поле, а $F$ – аддитивная подгруппа в $K$, порожденная 1. Как и любая циклическая группа $F \cong \mathbb{Z}/p\mathbb{Z}$ для некоторого $p \in \mathbb{N}$. Сейчас мы будем использовать натуральные числа в двух смыслах: как собственно натуральные числа и как элементы множества $F \subseteq K$, где $k = \underbrace{1_K + \cdots + 1_K}_{k \text{ раз}}$. Ясно, что $F$ – подкольцо в $K$, изоморфное $\mathbb{Z}/p\mathbb{Z}$. Так как в $K$ нет делителей нуля, то $p$ – простое число (иначе делители нуля есть уже в $F$). Из этого следует, что $F$ – поле. Поле $K$ можно рассматривать, как векторное пространство над $F$. Ясно, что оно конечномерно. По теореме о классификации векторных пространств оно изоморфно $F^n$ для некоторого $n$ и, следовательно, $|K| = |F^n| = p^n$.

Пусть, теперь, $q = p^n$, а $L$ – поле разложения многочлена $t^q - t$ над $\mathbb{Z}/p\mathbb{Z}$. Заметим, что $\operatorname{char} L = p$, т. е. $p = 0$ в $L$. Обозначим через $K$ множество корней этого многочлена. Формальная производная $(t^q - t) = qt^{q-1} - 1 = -1$ в поле $L$. Следовательно, многочлен $t^q - t$ не имеет кратных корней, поэтому $|K| = q$. Пусть $x, y \in K$. Тогда $(xy)^q = x^q y^q = xy$, то $xy \in K$, аналогично $x^{-1} \in K$ при $x \neq 0$. Так как биномиальные коэффициенты $\binom{p}{k}$ делятся на $p$, то из бинома Ньютона следует, что $(x+y)^p = x^p + y^p$. Применяя эту формулу $n$ раз, получаем $(x+y)^q = x^q + y^q = x + y$, откуда $x + y \in K$. Таким образом, $K$ является подполем в $L$, содержащим все корни многочлена $t^q - t$. По определению поля разложения $L$ вкладывается в $K$, откуда $L = K$.

Пусть, наконец, $\tilde{K}$ – произвольное поле из $q$ элементов. Его мультипликативная группа состоит из $q-1$ элемента, поэтому $x^{q-1} = 1$ для любого $x \in \tilde{K}^* = \tilde{K} \setminus \{0\}$. Следовательно, все элементы

[1] Версальное – это универсальное, но без "уни", т. е. без единственности.

поля $\tilde{K}$ являются корнями многочлена $t^q - t$. По определению поля разложения оно вкладывается в $\tilde{K}$, а в предыдущем абзаце мы показали, что оно имеет $q$ элементов. Следовательно, $\tilde{K}$ изоморфно полю разложения многочлена $t^q - t$, и единственность следует из единственности поля разложения. □

## 4. Существование примитивного элемента

## 5. Соответствие Галуа