Конспект лекций по алгебре
Факультет математики и компьютерных наук
СПбГУ
2019/20 уч. г.

А.В.Степанов

Оглавление

Глава 1

Введение

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 некоторые слова и символы, встречающиеся в лекциях.

1. Обозначения и терминология

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

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

to be continued...

2. Определение основных алгебраических структур

Определение 2.1. 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 2.2. 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 2.3. *Нейтральный элемент единственен (это утверждение не зависит даже от ассоциативности).*

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

Лемма 2.4. *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 2.5. 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 2.6. *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 2.4, множество обратимых (по умножению) элементов кольца R является группой. Эта группа называется мультипликативной подгруппой кольца и обозначается через R^*.

Определение 2.7. Пусть V – абелева группа в аддитивной записи, F – поле, и задана операция (умножение) $V \times F \to V$. Предположим, что для любых $u, v \in V$ и $\alpha, \beta \in F$ выполнены следующие свойства:

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

Тогда V называется векторным пространством над полем F.

Определение 2.8. Пусть A – векторное пространство над полем F и, одновременно, кольцо с той же операцией сложения. Если выполнено свойство $(ab)\alpha = a(b\alpha)$ для любых $a, b \in A$ и $\alpha \in F$, то A называется (ассоциативной) алгеброй над полем F.

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

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

Глава 2

Векторные пространства

1. Основные определения

Далее в настоящей главе используются следующие обозначения и соглашения.

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

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

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

Пусть $u_1, \ldots, u_n \in V$, 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 α_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 α_s равны 0.

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

Предложение 1.2. $\langle S \rangle = \{\sum\limits_{k=1}^{n} u_k \alpha_k \mid u_1, \ldots, u_n \in S,\ \alpha_1, \ldots, \alpha_n \in F\}$.

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 $(u_1, \ldots, u_n)$ 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 α_s равны нулю.

Определение 1.3. Базисом называется линейно независимая система образующих.

2. Матрицы

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

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

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

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

Произведением матрицы $A \in \mathrm{M}_{m\times n}(F)$ 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 1×1, которая отождествляется с числом. Произведение же столбца на строку определено всегда, но является не числом, а матрицей соответствующего размера. Заметим, что произведение матриц некоммутативно, даже если размеры получившихся матриц равны.

Теорема 2.2. *Множество $\mathrm{M}_{m\times n}(F)$ 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

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

Множество $\mathrm{M}_n(F)$ с операциями сложения и умножения является алгеброй с единицей над полем F.

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

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

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 непосредственным вычислением. □

Заметим, что в алгебре матриц 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 $c_{ih} = \sum\limits_{j=1}^{n} a_{ij}b_{jh}$.

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

Одно из приложений описанной выше конструкции – произведение строки векторов на столбец чисел, что является просто другой записью линейной комбинации. В этих терминах линейная независимость кортежа векторов равносильна возможности сокращать на него. Действительно, если кортеж $v = (v_1, \ldots, v_n)$ 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. Другое приложение – блочное произведение матриц (это очень легко показать на доске, и очень долго писать, поэтому пока не пишу).

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

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

Теперь, если мы хотим определить умножение матрицы из $\mathrm{M}_{I\times J}(X)$ на матрицу из $\mathrm{M}_{J\times H}(Y)$ нам недостаточно иметь операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$ как в первой части параграфа, потому что мы можем получить бесконечные суммы, которые не определены. Однако мы можем определить такую сумму, если почти все слагаемые будут равны нулю. Для того чтобы гарантировать последнее условие, мы постулируем, что все операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$

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

дистрибутивны, и в каждом столбце матрицы Y почти все элементы равны 0. Аналогично, мы могли бы потребовать, чтобы в каждой строке матрицы X почти все элементы были бы нулевыми, но в нашей системе обозначений именно условие на столбцы будет выполнено. Дистрибутивность умножения нужна для того, чтобы выполнялось равенство $a \cdot 0 = 0$.

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

Определение 2.3. Предположим, что для любых $i \in I$, $j \in J$, $h \in H$ заданы операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$, причем для любых $x, x' \in X_{ij}$ и любых $y, y' \in Y_{jh}$ имеют место равенства $(x + x')y = xy + x'y$ и $x(y + y') = xy + xy'$. Из этих равенств легко вывести, что $x \cdot 0 = 0 \cdot y = 0$. Тогда определим произведение матриц $A \in \mathrm{M}_{I\times J}(X)$ и $B \in \mathrm{M}^{c.f.}_{J\times H}(Y)$ как матрицу $AB \in \mathrm{M}_{I\times H}(Z)$ с элементами

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

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

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

Лемма 2.4. *Обычные свойства умножения матриц* (1) *выполнены, как только определены все входящие в формулы операции.*

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

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

Определение 2.5. Множество обратимых элементов кольца $\mathrm{M}_n(F)$ называется полной линейной группой степени n над F и обозначается через $\mathrm{GL}_n(F)$.

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

Есть еще одна полезная унарная операция с матрицами – транспонирование.

Определение 2.6. Пусть $A \in \mathrm{M}_{I\times J}(F)$. Матрица $A^\intercal \in \mathrm{M}_{J\times I}(F)$ 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 2.7. $(AB)^\intercal = B^\intercal A^\intercal$.

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

[2] c.f. – сокращение от “column finite”, аналогично r.f. будет использоваться, как сокращение для “row finite”.

3. Другие определения базиса и его существование

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

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

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

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

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

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

Доказательство. Пусть $\mathscr{A}$ – набор всех линейно независимых подмножеств Y, содержащих X. Этот набор не пуст, так как он содержит X. Пусть $\mathscr{L}$ – линейно упорядоченный поднабор в $\mathscr{A}$. Обозначим через S объединение всех множеств из $\mathscr{L}$. Так как любое подмножество $C \in \mathscr{L}$ 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 $B_i \in \mathscr{L}$, содержащее вектор v_i. Так как набор $\mathscr{L}$ 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 $S \in \mathscr{A}$. По лемме Цорна заключаем, что $\mathscr{A}$ 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 $a \in F^Z_{fin}$ и $a_y \in F$ такие, что $y\alpha_y + Za = 0$. Коэффициент α_y не может быть равен нулю, это противоречило бы линейной независимости множества Z. Следовательно, y принадлежит линейной оболочке множества Z. Поэтому все множество Y содержится в $\langle Z \rangle$. С другой стороны, $V = \langle Y \rangle$ – наименьшее подпространство, содержащее Y. Следовательно, $\langle Z \rangle \supseteq V$, т. е. Z – система образующих, а значит и базис. □

4. Размерность пространства

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

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

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

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

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

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

Теорема 4.2 (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 (если предполагать случай конечного базиса известным). Его можно найти в курсе лекций Николая Верещагина и Александра Шеня “Введение в теорию множеств”, лекция 11, теорема 36 (в настоящий момент она доступна по ссылке `http://www.intuit.ru/studies/courses/1034/144/lecture/3994?page=4`).

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

Определение 4.3. Размерностью пространства называется мощность (любого) базиса этого пространства.

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

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

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

5. Изоморфизм и классификация векторных пространств

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

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

Другими словами, линейное отображение – это гомоморфизм векторных пространств.

Как обычно, изоморфизмом называется биективный гомоморфизм.

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

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

В этих обозначениях свойство линейности можно выразить следующей формулой:

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

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

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

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

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

6. Прямая сумма и прямое произведение

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

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

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

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

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

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

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

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

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

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

Предложение 6.4. *Для подпространств $U_1, \ldots, U_n \leqslant V$ следующие условия эквивалентны.*

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

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

Определение 6.5. Пусть I некоторое (возможно бесконечное) множество, и для каждого $i \in I$ задано подпространство $U_i \leqslant V$. Прямой суммой $\bigoplus\limits_{i \in I} U_i$ называется множество финитных функций $f : I \to \bigcup\limits_{i \in I} U_i$ таких, что $f(i) \in U_i$. Неформально это называется множество потенциально бесконечных последовательностей элементов из U_i.

В отличие от прямой суммы, прямым произведением $\underset{i \in I}{\times} U_i$ называется множество всех функций $f : I \to \bigcup\limits_{i \in I} U_i$ таких, что $f(i) \in U_i$ (множество реально бесконечных последовательностей).

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

7. Замена базиса

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

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

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

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

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

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

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

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

8. Матрица линейного отображения

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

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

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

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

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

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

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

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

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

Нетрудно проверить, что множество линейных отображений $V \to V$ 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 8.3. *Пусть f – базис n-мерного пространства V. Определим отображение $\theta_f : \mathrm{End}(V) \to \mathrm{M}_n(F)$ формулой $\theta_f(L) = L_f$. Тогда θ_f является изоморфизмом алгебр.*

Выясним связи между матрицей оператора и матрицей перехода.

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

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

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

Остальные утверждения леммы вытекают непосредственно из определений. □

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

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

$$L^{v'}_{u'} = C_{v'\to v} L^v_u C_{u\to u'}.$$

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

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

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

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

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

Определение 9.1. Пусть $L : U \to V$ – линейное отображение. Тогда

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

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

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

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

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

Теорема 9.3 (о размерности ядра и образа). *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 9.4. *Если $\dim U = \dim V$, то инъективность L равносильна сюръективности.*

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

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

Доказательство. Зададим линейное отображение L из внешней прямой суммы $U \oplus V$ в W формулой $L(u, v) = u + v$. Легко проверить, что $\operatorname{Im} L = U + V$, 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. □

10. Факторпространство

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

Определение 10.1. Множество смежных классов V по U с операциями:

$$(x + U) + (y + U) = (x + y) + U,$$
$$(x + U)\alpha = x\alpha + U$$

называется факторпространством V по U и обозначается V/U.

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

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

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

Факторпространство обладает следующим универсальным свойством.

Предложение 10.2. *Для любого линейного отображения $L : V \to W$, ядро которого содержит U существет единственное отображение $\widetilde{L} : V/U \to W$ такое, что $L = \widetilde{L} \circ \pi_U$. При этом, сюръективность $\widetilde{L}$ равносильна сюръективности L, а инъективность $\widetilde{L}$ – тому, что $\operatorname{Ker} L = U$.*

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

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

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

Таким образом, если $\operatorname{Ker} L = U$, то $\operatorname{Ker} \widetilde{L} = \{0+U\}$, и наоборот. □

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

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

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

Так как U является L-инвариантным, можно определить отображение $\overline{L} : V/U \to V/U$ формулой $\overline{L}(x+U) = L(x) + U$ (проверьте, что определение корректно). Обозначим через $\overline{w} = (w_1 + U, \ldots, w_k + U)$ базис факторпространства V/U (проверьте, что это базис). Тогда матрица B – это матрица оператора $\overline{L}$ в базисе $\overline{w}$.

11. Ранг, PDQ-разложение

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

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

Лемма 11.2. *Пусть $A \in \mathrm{M}_{m\times n}(F)$.*

1. *Набор столбцов матрицы A линейно независим тогда и только тогда, когда ее столбцовый ранг равен n.*
2. *Набор столбцов матрицы A порождает F^m тогда и только тогда, когда ее столбцовый ранг равен m.*
3. *Набор столбцов матрицы A является базисом в F^m тогда и только тогда, когда ее столбцовый ранг равен $m = n$. 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. $m = n$. □

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

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

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

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

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

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

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

где e обозначает стандартный базис пространства столбцов.

Последнее утверждение сразу следует из предыдущей леммы. □

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

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

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

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

12. Разложения Брюа и Гаусса

Матрица a называется верхней (нижней) треугольной, если $a_{ij} = 0$ при всех $i > j$ (соотв. $i < j$). Треугольная матрица с 1 на главной диагонали называется унитреугольной. Обозначим множество верхних (нижних) обратимых треугольных матриц через $B = B_n(F)$ (соотв. $B^- = B_n^-(F)$). Аналогично, множества унитреугольных матриц обозначаются через $U = U_n(F)$ и $U^- = U_n^-(F)$. В теории алгебраических групп B и B^- называются противоположными борелевскими

подгруппами, а U и U^- – их унипотентными радикалами. Через $W = W_n$ обозначим множество матриц перестановок, т. е. матриц, отличающихся от единичной перестановкой столбцов (группа Вейля).

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

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

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

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

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

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

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

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

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

является матрицей-перестановкой, а, следовательно, и

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

– также матрица-перестановка. □

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

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

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

В параграфе 7 мы докажем, что клетка Брюа BwB содержится в клетке Гаусса wB^-B. В частности, разложение Гаусса является следствием разложения Брюа. Здесь же мы дадим непосредственное доказательство разложения Гаусса. Оно сразу вытекает из следующих трех лемм. Сформулируем в двух словах основную идею. Сначала надо выбрать перестановку строк так, чтобы все квадратные подматрицы (любого размера), стоящие в левом верхнем углу, были бы обратимы. При доказательстве возможности этого ключевым замечанием является то, что ранг подматрицы, составленной из первых k столбцов матрицы a, равен k (все столбцы обратимой матрицы линейно независимы), поэтому существует k линейно независимых строк этой подматрицы. Затем матрица приводится к верхнетреугольному виду элементарными преобразованиями с ведущими элементами на главной диагонали.

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

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

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

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

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

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

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

Раскладывая $\widetilde{a}$ по индукционному предположению, получаем результат. □

Лемма 12.7. *Для любой матрицы $a \in \mathrm{GL}_n(F)$ существует матрица-перестановка w такая, что все главные подматрицы в матрице wa обратимы.*

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

Глава 3

Начала теории групп

1. Простейшие конструкции

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

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

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

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.

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

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

2. Гомоморфизмы, ядро и образ

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

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

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

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

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

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

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

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

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

Заметим, что любая подгруппа абелевой группы является нормальной.

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

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

3. Порождение, циклические группы, порядок элемента

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

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

Лемма 3.2. *$\langle X \rangle$ состоит 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, $X^{-1} = \{x^{-1} \mid x \in X\}$). Обратите внимание, что здесь элементы $x_1, \ldots, x_k$ не обязательно различны. Если групп абелева, то произведение этих элементов приводится к виду $x_1^{i_1} \cdots x_m^{i_m}$, где $x_1, \ldots, x_m$ различны, а $i_j \in \mathbb{Z}$. В аддитивной записи это превращается в линейную комбинацию элементов из X с целыми коэффициентами.*

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

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

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

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

4. Смежные классы и теорема Лагранжа

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

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

Определим отношение "сравнимости по модулю H" на множестве G по формуле: $a \equiv b \mod H \iff a \in bH$. 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 2.5 $gH = Hg$, и сравнимость слева и справа совпадают.

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

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

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

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

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

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

Доказательство. Биекция $G/H \to H\backslash G$ 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 $G = \mathbb{Z}$.

5. Факторгруппа и теорема о гомоморфизме

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

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

Определение 5.2. Группа G/H, построенная в доказательстве, называется факторгруппой G по H, а отображение π – канонической проекцией или гомоморфизмом редукции по модулю H.

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

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

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

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

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

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

□

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

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

6. Сопряженные элементы, коммутаторы и коммутант

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

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

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

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

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

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

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

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

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

Лемма 6.3. *Выполнены следующие коммутаторные формулы.*

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

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

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

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

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

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

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

Теперь результат следует из леммы 6. □

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

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

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

7. Группа унитреугольных матриц и второе доказательство разложения Гаусса

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$B_n w B_n = U_n w B_n = U_w \overline{U}_n w B_n = U_w w \overline{U}_n^w B_n \subseteq U_w w U_n B_n = U_w w B_n.$$

Обратное включение очевидно.

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

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

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

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

Доказательство. $B_nwB_n = U_wwB_n = wU_w^wB_n \subseteq wU_n^-B_n = wB_n^-B_n$. □

8. Симметрическая группа

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

Определение 8.1. Пусть X – множество. Множество биекций $X \to X$ 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.

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

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

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

Лемма 8.2. $\sigma \circ \big(i_1\,\dots\,i_k\big) \circ \sigma^{-1} = \big(\sigma(i_1)\,\dots\,\sigma(i_k)\big)$.
Следовательно, сопряжение не меняет циклического типа перестановки.

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

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

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

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

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

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

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

Следствие 8.8. *Четность перестановки циклического типа $k_1 + \dots + k_m$ равна $k_1 + \dots + k_m - m \mod 2$.*

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

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

9. Экспонента группы

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

Лемма 9.2 (свойства экспоненты группы).

(1) *Экспонента группы равна наименьшему общему кратному порядков ее элементов.*
(2) *Если группа конечна, то ее экспонента делит ее порядок.*
(3) *Экспонента прямого произведения групп $G_1 \times \cdots \times G_l$ равна наименьшему общему кратному экспонент групп $G_1, \ldots, G_l$.*
(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 $p_1, \ldots p_l$ – различные простые числа. Тогда существуют элементы $g_1, \ldots, g_l \in G$, порядки которых делятся на $p_1^{k_1}, \ldots, p_l^{k_l}$ соответственно. Ясно, что если $\operatorname{ord} g = mn$, то $\operatorname{ord} g^m = n$. Возводя элементы $g_1, \ldots, g_l$ в подходящие степени, можно считать, что $\operatorname{ord} g_i = p_i^{k_i}$ при всех $i = 1, \ldots, l$.

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 $\operatorname{ord}(g_1 \cdots g_l) = \operatorname{ord} g_1 \cdots \operatorname{ord} g_l = d$. □

Глава 4

Коммутативные кольца

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

1. Гомоморфизмы колец, ядро и образ

Определение 1.1. Пусть R и A – кольца. Функция $f : R \to A$ называется гомоморфизмом колец, если $f(a+b) = f(a) + f(b)$ и $f(a \cdot b) = f(a) \cdot f(b)$ для любых $a, b \in R$. Для гомоморфизма колец с единицей будем требовать также, чтобы $f(1_R) = 1_A$.[1]

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

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

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

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

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

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

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

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

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

2. Порождение

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

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

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

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

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

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

Лемма 2.2. *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 в виду подкольцо без 1, то $x_i \in X$).*

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

3. Факторкольцо и теорема о гомоморфизме

Теорема 3.1. *Для любого двустороннего идеала I кольца R существует кольцо A и эпиморфизм $\pi : R \to A$, 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 π задается так же, как и для групп, где уже проверено, что оно сохраняет сложение, найдено ядро π и отмечено, что это отображение сюръективно. Осталось проверить, что π сохраняет умножение, но это сразу следует из определения произведения смежных классов. □

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

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

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

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

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

4. Комплексные числа

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

Композиция отображений $\mathbb{R} \hookrightarrow \mathbb{R}[t] \twoheadrightarrow \mathbb{C}$ 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 $z \in \mathbb{R} \iff z = \overline{z}$, $z+\overline{z}, z\overline{z} \in \mathbb{R}$. Как мы узнаем позже, из неприводимости многочлена t^2+1 в $\mathbb{R}[t]$ следует, что $\mathbb{C}$ является полем. Однако нетрудно явно найти мультипликативный обратный к любому ненулевому элементу. Для этого достаточно просто домножить числитель и знаменатель на сопряженное к знаменателю:

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

Следующее утверждение проверяется непосредственно.

Лемма 4.2. *Отображение $\mathbb{C} \to \mathbb{C}$, отображающее z в $\overline{z}$ является автоморфизмом поля $\mathbb{C}$.*

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

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

Обратите внимание, что тригонометрический угол определен с точностью до целого кратного 2π, 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:

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

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

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

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

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 4.3 можно переписать в виде:

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

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

Уравнение

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

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

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

где $k \in \mathbb{Z}/nZ$. 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 $k \in (\mathbb{Z}/n\mathbb{Z})^*$.

5. Евклидовы кольца

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

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

Определение 5.2. Пусть R – область целостности. Предположим, что задана функция $f : R \to \mathbb{N} \cup \{-\infty\}$ 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" (степень 0 по определению считается равной $-\infty$).

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

Теорема 5.4. *Евклидово кольцо является ОГИ.*

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

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

6. Китайская теорема об остатках

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

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

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

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

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

Теорема 6.3. $R/IJ \cong R/I \oplus R/J$.

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

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

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

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

Следствие 6.6. *Если $x \equiv y_k \mod I_k$, $k = 1, \dots, n$, то*

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

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

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

7. Простые и максимальные идеалы

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

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

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

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

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

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

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

8. Простые и неприводимые элементы

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

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

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

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

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

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

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

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

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

Определение 8.3. Необратимый элемент p кольца R называется простым, если pR – простой идеал.

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

Доказательство. Если p – простой, то

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

т. е. p ассоциирован с a или с b.

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

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

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

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

9. Нетеровы кольца и разложение на неприводимые

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

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

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

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

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

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

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

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

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

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

10. Факториальность колец главных идеалов

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

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

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

Доказательство. Пусть

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

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

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

Индукционный переход. По условию идеал p_nR простой. Поэтому найдется l такое, что $q_l \in p_nR$. Так как q_l неприводим, то $q_l = \delta p_n$, где δ 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 $\tau : \{1, \dots, n-1\} \to \{1, \dots, m\} \setminus \{l\}$ такая, что p_k ассоциирован с $q_{\tau(k)}$ для всех k от 1 до $n - 1$. Положив $\sigma(k) = \tau(k)$ при всех k от 1 до $n - 1$, а $\sigma(n) = l$, получаем результат. □

В качестве упражнения: сформулируйте и докажите обратное утверждение.

Из предыдущей леммы и леммы 8.5 непосредственно вытекает следующий факт.

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

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

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

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

11. Наибольший общий делитель

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

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

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

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

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

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

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

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

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

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

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

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

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

Лемма 11.6. *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 $a'b'd = \frac{ab}{\gcd(a,b)}$. □

12. Локализация

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

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

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

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

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

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

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

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

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

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

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

Доказательство. Докажем, что наше определение сложения и умножения не зависит от выбора представителей классов эквивалентности. Пусть $\frac{r_1'}{s_1'} = \frac{r_1}{s_1}$ и $\frac{r_2'}{s_2'} = \frac{r_2}{s_2}$, т. е. $sr_1s_1' = sr_1's_1$ и

$s'r_2s_2' = s'r_2's_2$ для некоторых $s, s' \in S$. Перемножая последние равенства получаем $ss'r_1s_1'r_2s_2' = ss'r_1's_1r_2's_2$, откуда $\frac{r_1r_2}{s_1s_2} = \frac{r_1'r_2'}{s_1's_2'}$. Далее,

$$ss'(r_1s_2 + r_2s_1)s_1's_2' = ss'(r_1s_2s_1's_2' + r_2s_1s_1's_2') = ss'(r_1's_2s_1s_2' + r_2's_1s_1's_2) = ss'(r_1's_2' + r_2's_1')s_1s_2,$$

что доказывает равенство $\frac{r_1s_2+r_2s_1}{s_1s_2} = \frac{r_1's_2'+r_2's_1'}{s_1's_2'}$.

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

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

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

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

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

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

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

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

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

    R_P является локальным кольцом, т. е. кольцом с единственным максимальным идеалом (равносильно: множество необратимых элементов является аддитивной подгруппой).
(3) S – множество всех элементов в R, не являющихся делителями 0 (сам 0 является делителем 0). Тогда $S^{-1}R$ называется полным кольцом частных кольца R. Это максимальная локализация, для которой гомоморфизм локализации инъективен.
(4) $R = K[x]$, где K – кольцо, S – множество унитальных многочленов.

13. Поле частных и разложение на простейшие дроби

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

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

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

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

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

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

Доказательство. Разложим сначала $\frac{a}{bc}$, $a, b, c \in R$, $\gcd(b, c) = 1$ в сумму дробей со знаменателями b и c. По теореме о линейном представлении НОД существуют такие $x, y \in R$, что $1 = bx + cy$. Тогда $\frac{a}{bc} = \frac{abx+acy}{bc} = \frac{ax}{c} + \frac{ay}{b}$. По индукции легко доказать, что любая дробь со знаменателем $p_1^{k_1} \cdots p_m^{k_m}$, где $p_1, \ldots, p_m \in R$ – 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. □

14. Многочлены

Пусть F – коммутативное кольцо с 1 (которое в дальнейшем будет полем). Кольцо A с 1 (не обязательно коммутативное) вместе с гомоморфизмом $\varphi : F \to A$ называется F-алгеброй. При этом для $\alpha \in F$ и $x \in A$ мы определяем произведение $\alpha x = \varphi(\alpha)x$. Нетрудно видеть, что в случае, когда F – поле, это определение совпадает с определением 2.8. Гомоморфизм θ алгебры (A, φ) на алгебру (B, ψ) – это гомоморфизм колец $\theta : A \to B$ такой, что $\psi = \theta \circ \varphi$.

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

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

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

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

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

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

$$\varepsilon_a : F[t] \to A, \qquad \varepsilon_a(p) = p(a)$$

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

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

Доказательство. Существование: $\varepsilon = \varepsilon_a$.

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

Далее F является полем.

Теорема 14.3. *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 14.4 (теорема Безу). *Пусть $\alpha \in F$, а $p \in F[t]$, где F – поле. Остаток от деления многочлена p на $t - \alpha$ равен $p(\alpha)$.*

Элемент α является корнем многочлена p тогда и только тогда, когда p делится на $t - \alpha$.

Многочлен степени n не может иметь больше, чем n корней.

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

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

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

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

Теорема 14.6. *Пусть $t_0, y_0, \ldots, t_n, y_n \in F$, 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 $w(t) = \prod_{i=0}^{n}(t - t_j)$ 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 λ. Поэтому λ можно найти из условия $p_{k+1}(t_k) = y_k$. Очевидно, что тогда все требования к p_{k+1} будут выполнены.

15. Формальная производная и кратность корня

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

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

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

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

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

Непосредственное доказательство. Линейность формальной производной очевидна. Учитывая это, второе свойство достаточно проверить для одночленов:

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

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

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

□

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

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

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

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

Доказательство. Для того чтобы выполнялись требуемые равенства мы должны положить $\varphi(z) = z(c_0, \dots, c_n)$ для любого многочлена $z \in \mathbb{Z}[z_1, \dots, z_n]$. С другой стороны, ясно, что значение в данной точке суммы (произведения) многочленов равно сумме (соотв. произведению) его значений. Поэтому приведенная формула для φ задает требуемый гомоморфизм $\varphi : \mathbb{Z}[z_1, \dots, z_n] \to R$ 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 $\hat{\varphi}\big(\sum_{k=0}^{l} c_k t^k\big) = \sum_{k=0}^{l} \varphi(c_k) t^k$ и назовем его гомоморфизмом, индуцированным φ.

Доказательство леммы 15.2 методом общего элемента. Я не смогу сейчас объяснить, что такое "общий элемент для некоторой задачи", придется ограничиться определением общего элемента для нашей конкретной задачи – доказательства свойств формальной производной.

Зафиксируем степени m и n многочленов p и q. Тогда свойства производной включают в себя элементы $a_0, \dots, a_n, b_0, \dots, b_m$ (коэффициенты многочленов p и q) и α 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, β) и будет общим элементом для нашей задачи.

По лемме 15.4 для любого кольца R, элемента $\alpha \in R$ и многочленов $p, q \in R[t]$ степеней не превосходящих n и m, соответственно, существует единственный гомоморфизм $\varphi : P \to R$ 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, β) 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 15.3 кольцо P вкладывается в поле вещественных чисел, а над полем вещественных чисел свойства производной известны из математического анализа. Так как свойства сохраняются при изоморфизме, то можно считать, что $P \subseteq \mathbb{R}$, поэтому свойства производной выполнены для общего элемента, а, значит, и в общем случае. □

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

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

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

Лемма 15.6. *Пусть α – корень многочлена p кратности k. Кратность α в p' не меньше $k-1$. Если $k \neq 0$ в поле F, то α 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 15.7. *(о рациональных корнях многочлена) Пусть $p(t) = a_n t^n + \cdots + a_0$ – многочлен с целыми коэффициентами. Тогда рациональными корнями p могут быть только числа вида $\frac{c}{d}$, где c – делитель свободного члена a_0, а d – делитель старшего коэффициента a_n.*

16. Основная теорема алгебры

Следствие 16.1. *Пусть $g \in \mathbb{C}[t]$, а $w \in \mathbb{C}$. Обозначим через $\overline{g}$ 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 16.2. Поле F называется алгебраически замкнутым, если любой многочлен из $F[t]$ степени $\geqslant 1$ имеет хотя бы один корень в F.

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

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

Следствие 16.5. *Любой многочлен степени $\geqslant 3$ 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 4.2 $p(\overline{w}) = 0$. 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. □

17. Экспонента мультипликативной группы кольца вычетов

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

Если числа $n_1, \ldots, n_l$ – 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 17.1. Порядок мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^*$ обозначается $\varphi(n)$. Функция $\varphi : \mathbb{N} \to \mathbb{N}$ называется функцией Эйлера.

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

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

Второе утверждение очевидно. □

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

Теорема 17.4. *Если $\gcd(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.*
Если p – простое число, а $k \in \mathbb{N}$, то $\varphi(p^k) = p^k - p^{k-1}$.

Пусть $p_1, \ldots, p_l$ – различные простые числа, $k_1, \ldots, k_l \in \mathbb{N}$, 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 17.5 (теорема Эйлера). *Если a взаимно просто с n, то $a^{\varphi(n)} \equiv 1 \mod n$.*

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

Определим функцию $\varphi' : \mathbb{N} \to \mathbb{N}$ 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 17.6. *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 леммы 9.2 экспонента группы $(\mathbb{Z}/n\mathbb{Z})^*$ равна наименьшему общему кратному экспонент групп $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^*$, а, значит, делит $\varphi'(n)$. Последнее означает, что $x^{\varphi'(n)} = 1$ для любого $x \in (\mathbb{Z}/n\mathbb{Z})^*$, что и требуется. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. О простых числах

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

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

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

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

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

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

Теорема 18.3 (распределение простых чисел). *Обозначим через $\pi(n)$ количество простых чисел от 2 до n. Тогда $\frac{\pi(n)}{n/\ln n} \to 1$ 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 $\frac{|T|}{n}$ для данного непростого n показывает, насколько хорош наш тест для данного n. На самом деле, можно оценить $\sup \frac{|T|}{\varphi(n)}$ по всем непростым n. Если этот супремум не меньше 1, то тест плохой и применять его в коммерческих целях нецелесообразно. Те числа n, для которых $\frac{|T|}{\varphi(n)} \geqslant 1$ (т. е. любое число, взаимно простое с n, принадлежит T), называются псевдопростыми для данного теста.

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

Название	Множество T	Псевдопростые числа	$\sup \frac{\lvert T\rvert}{\varphi(n)}$
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,...	$\leqslant 1/2$
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	$\varnothing$	$\leqslant 1/4$

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

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

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

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

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

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

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

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

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*

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

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. Второе вытекает из следующего вычисления:

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

□

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

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

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

Доказательство. Так как f антисимметрична, то $f(v_{i_1}, \ldots, v_{i_m}) = 0$ 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 $(i_1, \ldots, i_n)$. Пусть $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ – функция, заданная равенством $\sigma(k) = i_k$. Так как $i_k \neq i_l$ при $k \neq l$, а область определения σ совпадает с ее множеством значений, то σ – биекция, т. е. $\sigma \in S_n$. Заметим, что за счет антисимметричности $f(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = (-1)^{\varepsilon(\sigma)} f(v_1, \ldots, v_n)$. 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* $\alpha \in F$

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

2. Определение определителя

Определение 2.1. Определитем матрицы $A \in \mathrm{M}_n(F)$ называется число

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

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 $b \in {}^nF$. 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 τ можно взять любую нечетную перестановку. Для наших целей удобно взять транспозицию $\tau = (ij)$. Тогда

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

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 (4), 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,

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

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

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

Так как ε 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 σ^{-1} пробегает все множество S_n. Таким образом,

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

□

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

Предложение 3.3.

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

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

Доказательство. Пусть сначала $A = \begin{pmatrix} E & * \\ 0 & E \end{pmatrix}$. Так как эта матрица легко получается из единичной с помощью серии первых преобразований Гаусса, то ее определитель равен 1.

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

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

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

Наконец, пусть

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

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

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

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

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

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-го слагаемого последней суммы переставим i-ую строку на первое место так, чтобы порядок следования остальных строк не изменился. Очевидно, это можно сделать с помощью $i-1$ транспозиций строк. По свойству антисимметричности получим

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

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

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

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

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

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

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

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

Доказательство второго равенства (для строк) совершенно аналогично. □

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^{ad}, транспонированная к матрице из алгебраических дополнений матрицы B, т.е. элемент матрицы B^{ad} в позиции (i, j) равен $A_{ji}(B)$.

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

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

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

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

ДОКАЗАТЕЛЬСТВО. Положим $B = A \cdot A^{\mathrm{ad}}$. Элемент матрицы A^{ad} в позиции (k, j) равен A_{jk}. Получаем: $b_{ij} = \sum_{k=1}^{n} a_{ik}A_{jk}$. При $i = j$, по свойству 3.6, $b_{ij} = \det A$, а при $i \neq j$, по свойству 4.1, $b_{ij} = 0$. Таким образом, $B = E \det A$. Аналогично, $A^{\mathrm{ad}}A = E \det A$. 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 Δ определитель матрицы A, а через Δ_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 $x = \frac{1}{\Delta}A^{\mathrm{ad}}b$ или $x_i = \frac{1}{\Delta}\sum_{k=1}^{n} A_{ki}b_k$. Осталось заметить, что по теореме 3.6 $\sum_{k=1}^{n} A_{ki}b_k = \Delta_i$. □

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

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

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

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

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

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 λ 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 $\det(A - \lambda E) = 0$. Действительно, определитель равен нулю тогда и только тогда, когда столбцы матрицы линейно зависимы, а линейная зависимость – это и есть ненулевое решение уравнения. □

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 $(-1)^n t^n$).

Определение 1.4. Многочлен $\det(A-tE)$ называется характеристическим многочленом матрицы A и обозначается через χ_A.

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

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

Доказательство. Пусть $C = C_{u\to v}$. Тогда $L_v = C^{-1}L_uC$ и

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

□

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

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

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

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

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

Применяя к этому равенству оператор L, получим

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

а умножая его на λ_m:

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

Вычитая последнее равенство из предпоследнего, имеем:

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

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

[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.

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

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

Собственным подпространством, соответствующим собственному числу λ, 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 $k = \dim \mathrm{Ker}(L - \lambda I)$ геометрическую кратность собственного числа λ. Выберем базис $(u_1, \dots, u_k)$ пространства $\mathrm{Ker}(L-\lambda I)$ 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 λE. Поэтому $\chi_L = \det(L_u - tE)$ делится на $(\lambda - t)^k$, следовательно, алгебраическая кратность λ 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 теорема Гамильтона–Кэли

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

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

Теорема 2.2. *Пусть V – конечномерное векторное пространство над алгебраически замкнутым полем F, а $L : V \to V$ – 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 после изучении модулей над областями главных идеалов, а сейчас мы выведем некоторые следствия этой теоремы. Для этого нам понадобится несколько простых утверждений.

Лемма 2.3. *Матрица J_n^m имеет 1 во всех позициях $(k, k+m)$, $1 \leqslant k \leqslant n-m$.*
Если $N \in \mathrm{M}_m(F)$ – верхнетреугольная матрица с нулями по главной диагонали, то $N^m = 0$.

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

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

Следующее утверждение показывает, как работать с блочно-диагональными матрицами. Обозначим через $\mathrm{diag}(A^{(1)}, \dots, A^{(m)})$ диагональную матрицу с квадратными диагональными блоками $A^{(1)}, \dots, A^{(m)}$.

Лемма 2.5. *Множество блочно диагональных матриц с квадратными диагональными блоками фиксированного размера является подкольцом матричного кольца, изоморфным прямой сумме матричных колец соответствующих размеров. В частности, для любого многочлена p*

$$p\big(\mathrm{diag}(A^{(1)}, \dots, A^{(m)})\big) = \mathrm{diag}\big(p(A^{(1)}), \dots, p(A^{(m)})\big).$$

Первое применение жордановой формы – доказательство следующего утверждения.

Теорема 2.6 (теорема Гамильтона–Кэли). *Пусть A – квадратная матрица или линейный оператор на конечномерном пространстве. Тогда $\chi_A(A) = 0$.*

Доказательство. Ясно, что доказывать можно только для случая матриц. Пусть $A \in \mathrm{M}_n(F)$. Как мы узнаем позже, любое поле F вкладывается в алгебраически замкнутое поле $\overline{F}$. Поэтому $A \in \mathrm{M}_n(\overline{F})$, и по теореме 2.2 существует $C \in \mathrm{M}_n(\overline{F})$ такая, что $A = C^{-1}A'C$, где A' – жорданова форма матрицы A (матрица оператора умножения на A в жордановом базисе). По лемме 2.4 равенство $\chi_A(A) = 0$ равносильно равенству $\chi_A(A') = 0$, а так как A и A' – матрицы одного и того же оператора в разных базисах, то $\chi_A = \chi_{A'}$. По определению $A' = \mathrm{diag}(\lambda_1 E_{k_1} + J_{k_1}, \dots, \lambda_m E_{k_m} + J_{k_m})$ для некоторых $m, k_1, \dots, k_m \in \mathbb{N}$ и $\lambda_1, \dots, \lambda_m \in \overline{F}$. Тогда

$\chi_{A'}(t) = \prod_{i=1}^{m}(\lambda_i - t)^{k_i}$. Если подставить i-й диагональный блок матрицы A' в i-й сомножитель многочлена $\chi_{A'}$, то в соответствие с леммой 2.3 получится 0 (напомним, что при подстановке матрицы в многочлен свободный член многочлена умножается на единичную матрицу). Следовательно, значение $\chi_{A'}$ на любом диагональном блоке матрицы A' равно 0. Теперь требуемое равенство следует из леммы 2.5 □

Полезно знать и непосредственное доказательство теоремы Гамильтона–Кэли, без использования жордановой формы.

ВТОРОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ГАМИЛЬТОНА–КЭЛИ. Заметим, что матричное кольцо $\mathrm{M}_n(F[t])$ над кольцом многочленов изоморфно кольцу $\mathrm{M}_n(F)[t]$ многочленов с матричными коэффициентами.[2] Рассмотрим матрицу $A - tE \in \mathrm{M}_n(F[t])$. По теореме 4.5 главы 5

$$(A - tE)(A - tE)^{\mathrm{ad}} = (A - tE)^{\mathrm{ad}}(A - tE) = \det(A - tE)E = \chi_A(t)E. \tag{5}$$

Переписывая это равенство в кольце $\mathrm{M}_n(F)[t]$ получаем

$$(A - tE)(B_0 + B_1 t + \cdots + B_{n-1}t^{n-1}) = \chi_A(t)E,$$

где $B_i \in \mathrm{M}_n(F)$ – коэффициенты в разложении матрицы $(A - tE)^{\mathrm{ad}}$ по степеням t.

Как видно, для доказательства теоремы достаточно подставить в это равенство A вместо t. Однако, такая подстановка законна только если A лежит в центре кольца коэффициентов. Действительно, формально, подстановка элемента a алгебры R в многочлен – это вычисление значения гомоморфизма $\varphi_a : R[t] \to R$, посылающего t в a и оставляющего на месте все элементы R. Но t коммутирует со всеми элементами кольца R, а гомоморфизм сохраняет это свойство. Обратно, если a коммутирует со всеми элементами из R, то простая проверка показывает, что формула $\varphi_a(r_0 + \cdots + r_m t^m) = r_0 + \cdots + r_m a^m$ задает требуемый гомоморфизм (это небольшое обобщение универсального свойства кольца многочленов 14.2 главы 4).

Определим R, как минимальную F-подалгебра в $\mathrm{M}_n(F)$, содержащую матрицы A и $B_1, \ldots, B_{n-1}$. Так как $A - tE$ коммутирует с $(A - tE)^{\mathrm{ad}}$, то и A коммутирует с этой матрицей. Следовательно, $A(B_0 + \cdots + B_{n-1}t^{n-1}) = (B_0 + \cdots + B_{n-1}t^{n-1})A$, откуда сразу следует, что $AB_i = B_iA$ при всех i. Таким образом, A лежит в центре алгебры R и, значит, ее можно подставить вместо t в равенство (5). В левой части этого равенства, очевидно, получается 0, следовательно, и правая часть $\chi_A(A)E = 0$. □

Пусть R – ассоциативная (возможно некоммутативная) алгебра с 1 над полем F. Напомним, что для любого $r \in R$ существует единственный гомоморфизм F-алгебр

$$\varepsilon_r : F[t] \to R, \qquad p \mapsto p(r),$$

отображающий независимую переменную t в r. Ядро этого гомоморфизма – идеал кольца $F[t]$. Так как $F[t]$ – область главных идеалов, то $\operatorname{Ker}\varepsilon_r$ – главный идеал. Образующая этого идеала называется минимальным многочленом элемента r и обозначается φ_r. Этот многочлен определен однозначно с точностью до умножения на обратимый элемент кольца $F[t]$, т. е. ненулевую константу.

По теореме о гомоморфизме наименьшая подалгебра с 1 в R, содержащая r, изоморфна $F[t]/(\varphi_r)$. Она обозначается через $F[r]$. Таким образом, каждому многочлену от r (элементу $F[r]$) однозначно сопоставляется смежный класс этого многочлена в $F[t]/(\varphi_r)$. Как мы знаем, этот смежный класс имеет единственного представителя наименьшей степени, а именно, остаток от деления на φ_r.

Пусть теперь $R = M_n(F)$, а $A \in R$.

ЛЕММА 2.7. *Характеристический многочлен матрицы A делится на минимальный. Любое собственное число является корнем минимального многочлена.*

[2]Мы определяли только кольцо многочленов над коммутативным кольцом, но определение над некоммутативным кольцом ничем не отличается. Важно только понимать, что независимая переменная t коммутирует со всеми элементами кольца.

Доказательство. Первое утверждение сразу следует из теоремы Гамильтона–Кэли. Второе также несложно вывести из теоремы о жордановой форме, но мы дадим непосредственное доказательство. Действительно, если $Ax = \lambda x$, то $A^n x = \lambda^n x$ и, следовательно, $p(A)x = p(\lambda)x$ для любого многочлена $p \in F[t]$. Следовательно, $0 = \varphi_A(A)x = \varphi_A(\lambda)x$, откуда (т. к. $x \neq 0$) следует, что $\varphi_A(\lambda) = 0$. □

Замечание 2.8. С использованием жордановой формы нетрудно доказать, что кратность собственного числа в минимальном многочлене матрицы равна размеру наибольшей жордановой клетки с этим собственным числом.

3. Разложение Жордана

Элемент r кольца R называется нильпотентным, если $r^m = 0$ для некоторого натурального m. Наименьшее такое m называется степенью нильпотентности элемента r. Из того, что матрица J_n нильпотентна, а сопряжение при помощи обратимой матрицы является автоморфизмом матричного кольца, следует существование аддитивного и мультипликативного разложения Жордана над замкнутым полем.

Для формулировки и доказательства аддитивного разложения Жордана над незамкнутым полем нам понадобится небольшой экскурс в теорию Галуа, т. е. некоторые сведения о расширениях полей. Доказательства приведенных утверждений появятся позже, в главе **??**. Если даны два поля $F \subseteq K$, то обычно пишут "дано расширение полей K/F" (читается "K над F"; обозначение не имеет никакого отношения к факторгруппе) или "пусть K – расширение поля F". Элемент $a \in K$ называется алгебраическим над F, если он является корнем некоторого многочлена с коэффициентами из F.

Теорема 3.1. *Для любого поля F существует алгебраически замкнутое поле $\overline{F}$, которое содержит F, а каждый его элемент алгебраичен над F. Такое поле единственно с точностью до изоморфизма.*

Поле $\overline{F}$ из формулировки теоремы называется *алгебраическим замыканием* поля F.

Поле F называется совершенным, если любой неприводимый многочлен из $F[t]$ не имеет кратных корней в алгебраическом замыкании поля F. Вспомнив, что кратные корни – это общие корни многочлена и его производной, нетрудно видеть, что поле совершенно, если производная неприводимого многочлена не может быть равна нулю. Действительно, неприводимый многочлен взаимно прост с любым ненулевым многочленом меньшей степени. Отсюда сразу следует, что любое поле характеристики 0 совершенно. В поле F характеристики p отображение $F \to F$, $x \mapsto x^p$, сохраняет не только операцию умножения, но и сложения (так как $\binom{p}{n}$ делится на p при любом n от 1 до $p-1$). Оно называется *эндоморфизмом Фробениуса*. Ясно, что эндоморфизм Фробениуса инъективен ($x^p = y^p \iff (x-y)^p = 0 \iff x = y$). Нетрудно доказать, что поле F совершенно тогда и только тогда, когда эндоморфизм Фробениуса биективен. В частности, любое конечное поле совершенно. Простейший пример несовершенного поля дает поле рациональных функций $\mathbb{F}_p[t]$, где неприводимый многочлен $t^p - 1$ над алгебраическим замыканием имеет один корень кратности p.

Группа Галуа расширения K/F – это группа автоморфизмов поля K действующих тождественно на F. Следующая лемма является ключевой для перехода от случая замкнутого поля к любому совершенному во многих ситуациях.

Теорема 3.2. *Пусть F – совершенное поле, а $\overline{F}$ – его алгебраическое замыкание. Тогда множество элементов, неподвижных под действием любого элемента группы Галуа расширения $\overline{F}/F$, совпадает с F.*

Квадратная матрица называется полупростой, если оператор умножения на нее диагонализуем.

Теорема 3.3 (аддитивное разложение Жордана). *Предположим, что поле F совершенно. Тогда для любой матрицы $A \in \mathrm{M}_n(F)$ существуют единственные матрицы $A^{(s)}, A^{(n)} \in \mathrm{M}_n(F)$ такие, что:*

(1) *$A^{(s)}$ – полупростая, $A^{(n)}$ – нильпотентная;*
(2) *$A = A^{(s)} + A^{(n)}$;*
(3) *$A^{(s)}A^{(n)} = A^{(n)}A^{(s)}$.*

При этом матрицы $A^{(s)}$ и $A^{(n)}$ выражаются, как многочлены от матрицы A.

Доказательство. Пусть сначала F алгебраически замкнуто. Тогда по теореме 2.2 существует обратимая матрица C такая, что

$$C^{-1}AC = \operatorname{diag}(\mu_1 E, \dots, \mu_m E) + \operatorname{diag}(N_1, \dots, N_m),$$

где $\mu_1, \dots, \mu_m$ – все различные собственные числа матрицы A, а N_i – матрица с некоторым количеством единиц непосредственно над главной диагональю и нулями в остальных местах. Обозначим первое слагаемое (диагональную матрицу) через S, а второе – через N. Ясно, что $\mu_i E$ коммутирует с N_i, поэтому $SN = NS$. Очевидно также, что S полупроста, а N нильпотентна. Таким образом,

$$A = CSC^{-1} + CNC^{-1}$$

является аддитивным разложением Жордана.

Второй шаг доказательства – утверждение о том, что полупростая и нильпотентная части матрицы A являются многочленами от A. Так как сопряжение при помощи C является автоморфизмом матричного кольца, достаточно доказать, что S – многочлен от $B = C^{-1}AC$ (тогда $N = B - S$ – тоже многочлен от B). Докажем, что $\operatorname{diag}(0, \dots, 0, \mu_i E, 0, \dots, 0)$ является многочленом от B, этого достаточно, так как S равно сумме этих матриц. Утверждение не требует доказательства при $\mu_i = 0$. Пусть $\mu_i \neq 0$. Рассмотрим многочлен $f(t) = \prod_{j \neq i}(t - \mu_j)^{k_j}$, где k_j – размер j-го блока. Тогда

$$f(B) = \operatorname{diag}\big(f(\mu_1 E + N_1), \dots, f(\mu_m E + N_m)\big)$$

Так как $N_j^{k_j} = 0$, то для любого $j \neq i$ в произведении $f(\mu_j E + N_j)$ есть нулевой сомножитель. С другой стороны, матрица $f(\mu_i E + N_i)$ является верхнетреугольной с числом $\mu = \prod_{j \neq i}(\mu_i - \mu_j)$ на диагонали. Так как $\mu_i \neq \mu_j$ при $i \neq j$, то $\mu \neq 0$. Получаем,

$$f(\mu_i E + N_i) = \mu E + U,$$

где U – верхнетреугольная матрица с 0 на главной диагонали. Нетрудно видеть, что $U^{k_i} = 0$. Положим $g(t) = (\mu - t)^{k_i} - \mu^{k_i}$. Тогда $g(0) = 0$ и $g(\mu E + U) = -\mu^{k_i} E$. Следовательно,

$$g\big(f(B)\big) = g\big(\operatorname{diag}(0, \dots, 0, \mu E + U, 0, \dots, 0)\big) = \operatorname{diag}(0, \dots, 0, -\mu^{k_i} E, 0, \dots, 0).$$

Таким образом, многочлен $\frac{\mu_i}{-\mu^{k_i}} g \circ f$ отображает B в требуемую диагональную матрицу.

Третий шаг – доказательство единственности разложения. Снова достаточно доказать это для матрицы B. Заметим сначала, что любая матрица, коммутирующая с B, коммутирует также и с любым многочленом от B, в частности, с N и S. Пусть $B = S' + N'$, где S' полупростая, N' нильпотентная, и $S'N' = N'S'$. Из последнего равенства следует, что S' и N' коммутируют с B, следовательно, все 4 матрицы N, S, N' и S' коммутируют друг с другом.

Так как $S = \operatorname{diag}(\mu_1 E, \dots, \mu_m E)$, где все μ_i различны, а $SS' = S'S$, то простое матричное вычисление показывает, что $S' = \operatorname{diag}(S^{(1)}, \dots, S^{(m)})$, где размеры диагональных блоков равны размерам диагональных блоков, на которые разбита матрица S. Заметим, что сумма коммутирующих между собой нильпотентных элементов кольца нильпотентна. Действительно, если $y^k = z^r = 0$, то в сумме

$$(y + z)^{k+r-1} = \sum_{i=0}^{k+r-1} \binom{k + r - 1}{i} y^i z^{k+r-1-i},$$

каждое слагаемое равно нулю, потому что либо $i \geqslant k$, либо $k + r - 1 - i \geqslant r$. Таким образом, матрица $S' - S = N - N'$ нильпотентна.

Пусть $J^{(i)} = (C^{(i)})^{-1} S^{(i)} C^{(i)}$ – жорданова форма матрицы $S^{(i)}$. Положим

$$C' = \operatorname{diag}(C^{(1)}, \ldots, C^{(m)}) \text{ и } J' = \operatorname{diag}(J^{(1)}, \ldots, J^{(m)}).$$

Тогда $(C')^{-1} S' C' = J'$. Так как S' диагонализуема, то этим свойством обладает и матрица J'. Но J' – блочно диагональная матрица с жордановыми блоками по диагонали. Если не все эти блоки имеют размер 1 на 1, то алгебраическая кратность какого-то собственного числа не совпадает с геометрической, что противоречит диагонализуемости. Таким образом, матрица J' диагональна. Заметим, что C' коммутирует с S, потому что S коммутирует с любой блочно диагональной матрицей с такими размерами блоков. Следовательно, матрица $S - J' = (C')^{-1}(S - S')C$ диагональна и нильпотентна. Легко видеть, что она нулевая. Таким образом, $S = S'$, откуда следует единственность.

Четвертый шаг доказательства – существование аддитивного разложения Жордана над незамкнутым полем. Пусть $\overline{F}$ – алгебраическое замыкание поля F. Тогда по доказанному существуют единственные матрицы $A^{(s)}, A^{(n)} \in \mathrm{M}_n(\overline{F})$, удовлетворяющие условиям теоремы. Необходимо показать, что все элементы матриц $A^{(s)}$ и $A^{(n)}$ лежат в исходном поле F. Пусть σ – элемент группы Галуа расширения $\overline{F}/F$, т. е. автоморфизм поля $\overline{F}$, тождественный на F. Нетрудно видеть, что он индуцирует автоморфизм матричного кольца $\mathrm{M}_n(\overline{F})$, тождественный на $\mathrm{M}_n(F)$, который мы, допуская вольность записи, будем также обозначать через σ. А именно, для матрицы $X \in \mathrm{M}_n(\overline{F})$ положим $\sigma(X)_{ij} = \sigma(x_{ij})$. Очевидно, что любой автоморфизм матричного кольца сохраняет свойства коммутирования, нильпотентности и диагонализуемости. Следовательно, $A = \sigma(A) = \sigma(A^{(s)}) + \sigma(A^{(n)})$ является аддитивным разложением Жордана матрицы A. Из единственности разложения следует, что $\sigma(A^{(s)}) = A^{(s)}$ и $\sigma(A^{(n)}) = A^{(n)}$. Таким образом, все элементы матриц $A^{(s)}$ и $A^{(n)}$ неподвижны под действием любого элемента σ группы Галуа $\overline{F}/F$. По теореме 3.2 все эти элементы принадлежат F.

Наконец, последний **пятый шаг** – доказать, что коэффициенты многочленов p и q, для которых $A^{(s)} = p(A)$ и $A^{(n)} = q(A)$, лежат в F. По доказанному на втором шаге такие многочлены существуют в $\overline{F}[t]$. Давайте считать, что они имеют минимально возможную степень, тогда они определены единственным образом, см. текст перед леммой 2.7. Элемент σ группы Галуа $\overline{F}/F$ индуцирует автоморфизм кольца многочленов $\sum \alpha_i t^i \mapsto \sum \sigma(\alpha_i) t^i$, который мы будем снова обозначать через σ. Ясно, что

$$p(A) = A^{(s)} = \sigma\big(A^{(s)}\big) = \sigma\big(p(A)\big) = \sigma(p)\big(\sigma(A)\big) = \sigma(p)(A).$$

Так как σ не меняет степень многочлена, а $p(A) = \sigma(p)(A)$, то $\sigma(p) = p$. По теореме 3.2 все коэффициенты многочлена p лежат в F, т. е. $p \in F[t]$ □

Элемент r кольца с 1 называется унипотентным, если $r - 1$ нильпотентен.

Следствие 3.4 (мультипликативное разложение Жордана). *Для любой матрицы $A \in \mathrm{GL}_n(F)$ над совершенным полем F существуют матрицы $S, U \in \mathrm{M}_n(F)$ такие, что S – полупростая, U – унипотентная, $A = SU$, и $SU = US$.*

При этом матрицы S и U выражаются, как многочлены от матрицы A.

Доказательство. Пусть $A = S + N$ – аддитивное разложение Жордана матрицы A. Так как A – обратимая матрица, то и $S = A - N$ обратима. Действительно, $(A - N)A^{-1} = E - NA^{-1}$, матрица $\tilde{N} = NA^{-1}$ нильпотентна, так как N нильпотентна и коммутирует с A^{-1}, а $(E - \tilde{N})(E + \tilde{N} + \cdots + \tilde{N}^{k-1}) = E - \tilde{N}^k = E$ для достаточно большого k. Таким образом, $A = SU$, где $U = (E + S^{-1}N))$ и есть мультипликативное разложение Жордана.

Осталось доказать, что U – многочлен от A. Пусть $S = p(A)$, где $p \in F[t]$ – многочлен, существование которого утверждается в предыдущей теореме, а x – собственный вектор матрицы A, соответствующий собственному числу $\lambda \in \overline{F}$. Тогда $Sx = p(A)x = p(\lambda)x$ (последнее равенство

достаточно проверить на одночленах, для которых оно очевидно). Так как S обратима, а $x \neq 0$, то $p(\lambda) \neq 0$. Так как только собственные числа являются корнями минимального многочлена φ_A матрицы A, то p взаимно прост с φ_A. Напишем линейное представление НОД: $1 = pf + \varphi_A g$ и подставим туда A. Получим $E = p(A)f(A) + \varphi_A(A)g(A) = Sf(A)$. Таким образом, $S^{-1} = f(A)$, и $U = AS^{-1} = Af(A)$. □

4. Функции от матриц

Пусть $f : D \to \mathbb{C}$ – дифференцируемая функция комплексной переменной, где D – открытый круг в $\mathbb{C}$. Из теории функций комплексной переменной следует, что она раскладывается в степенной ряд в окрестности любой точки $\mu \in D$:

$$f(z) = \sum_{k=0}^{\infty} \alpha_k(\mu)(z-\mu)^k.$$

При этом радиус сходимости этого ряда не меньше, чем расстояние от μ до границы круга. Как и в случае числового ряда, для матрицы $A \in \mathrm{M}_n(\mathbb{C})$ положим по определению,

$$f(A) = \lim_{m\to\infty} \sum_{k=0}^{m} \alpha_k(\mu)(A-\mu E)^k,$$

где предел берется поэлементно (впрочем, можно брать предел по любой норме на векторном пространстве $\mathrm{M}_n(\mathbb{C})$ так как в конечномерном пространстве предел не зависит от выбора нормы). Естественно, этот предел не всегда существует. Вскоре мы докажем, что при некоторых предположениях он не зависит от точки μ.

Умножение матриц задается многочленами и, поэтому, непрерывно, как функция $\mathbb{C}^{2n^2} \to \mathbb{C}^{n^2}$. Для $A \in \mathrm{M}_n(\mathbb{C})$ и $C \in \mathrm{GL}_n(\mathbb{C})$ имеем:

$$f(C^{-1}AC) = \lim_{m\to\infty} \sum_{k=0}^{m} \alpha_k(C^{-1}AC-\mu E)^k \overset{2.4}{=} \lim_{m\to\infty} C^{-1}\Big(\sum_{k=0}^{m} \alpha_k(A-\mu E)^k\Big)C \overset{\text{непр.}}{=} C^{-1}f(A)C.$$

Равенство означает, что либо ряды в обеих частях расходятся, либо эти выражения равны. Предположим, что $C^{-1}AC = \mathrm{diag}(\lambda_1 E + J_{k_1}, \ldots, \lambda_l E + J_{k_l})$ – жорданова форма матрицы A. По лемме 2.5 для вычисления многочлена от блочно диагональной матрицы достаточно вычислить его от каждого диагонального блока. Аналогичное утверждение очевидно верно и с заменой слова "многочлен" на слово "предел". Докажем, что для жорданова блока результат применения функции не зависит от того, в окрестности какой точки мы раскладываем эту функцию в ряд.

Лемма 4.1. *Пусть $\lambda, \mu \in D$, а $J = J_s$ – жорданов блок размера $s \times s$ с собственным числом 0. Тогда*

$$f(\lambda E + J) = \sum_{k=0}^{\infty} \alpha_k(\mu)((\lambda-\mu)E + J)^k = \sum_{k=0}^{s-1} \alpha_k(\lambda)J^k$$

не зависит от выбора точки $\mu \in D$.

Доказательство. Раскладывая $f(z)$ в ряд в окрестностях точек λ и μ получаем

$$f(z) = \sum_{k=0}^{\infty} \alpha_k(\lambda)(z-\lambda)^k = \sum_{j=0}^{\infty} \alpha_j(\mu)\big((z-\lambda)+(\lambda-\mu)\big)^j =$$

$$\sum_{j=0}^{\infty} \alpha_j(\mu)\Big(\sum_{k=0}^{j} \binom{j}{k}(z-\lambda)^k(\lambda-\mu)^{j-k} = \sum_{k=0}^{\infty}\Big(\sum_{j=k}^{\infty} \alpha_j(\mu)\binom{j}{k}(\lambda-\mu)^{j-k}\Big)\big(z-\lambda\big)^k$$

(так как внутри круга сходимости ряд сходится абсолютно, мы имеем право менять порядок суммирования). Нетрудно доказать, что коэффициенты при соответствующих степенях $z-\lambda$ должны быть равны. Следовательно,

$$\alpha_k(\lambda) = \sum_{j=k}^{\infty} \alpha_j(\mu)\binom{j}{k}(\lambda-\mu)^{j-k}.$$

Подставляя $\lambda E + J$ вместо z в предыдущее вычисление, получим[3]

$$f(\lambda E + J) = \sum_{k=0}^{\infty} \alpha_k(\mu)\big((\lambda-\mu)E + J\big)^k = \cdots = \sum_{k=0}^{s-1} \alpha_k(\lambda) J^k.$$

□

Теорема 4.2. *Пусть $A \in \mathrm{M}_n(\mathbb{C})$ имеет собственные числа $\lambda_1, \ldots, \lambda_l \in D$ (не обязательно различные), а $C = C_{e\to u}$ – матрица перехода от стандартного базиса $\mathbb{C}^n$ к жорданову базису матрицы A. Тогда ряд для $f(A)$ сходится и*

$$f(A) = C\,\mathrm{diag}\big(f(\lambda_1 E + J_{s_1}), \ldots, f(\lambda_l E + J_{s_l})\big)C^{-1},$$

а значение f на жордановом блоке вычисляется по формуле

$$f(\lambda E + J_s) = \sum_{k=0}^{s-1} \alpha_k(\lambda) J_s^k.$$

Вычисление экспоненты от матрицы применяется при решении системы дифференциальных уравнений $y' = Ay$, где $y = (y_1, \ldots, y_n)^\intercal$, y_k – дифференцируемые функции $\mathbb{C} \to \mathbb{C}$, а $A \in \mathrm{M}_n(\mathbb{C})$. Общее решение этой системы имеет вид $y = e^{At}c$, где c пробегает множество столбцов $\mathbb{C}^n$.

5. Другое доказательство жордановой формы

Основным доказательством теоремы о жордановой форме в нашем курсе будет доказательство, использующее строение конечнопорожденных модулей над кольцом многочленов. Это будет сделано в параграфе 9. А сейчас мы приведем набросок другого доказательства. Первым шагом является теорема о ядре произведения многочленов от оператора. Напомним, что умножение в алгебре операторов на векторном пространстве – это композиция.

Теорема 5.1. *Пусть $L : V \to V$ – линейный оператор на векторном пространстве V над полем F (V не предполагается конечномерным), а $p, q \in F[t]$ – взаимно простые многочлены. Тогда*

$$\mathrm{Ker}\big(p(L)q(L)\big) = \mathrm{Ker}\, p(L) \oplus \mathrm{Ker}\, q(L).$$

Доказательство. Так как p и q взаимно просты, существуют многочлены $f, h \in F[t]$ такие, что $pf + qh = 1$. Подставляя в это равенство оператор L, получим $f(L)p(L) + h(L)q(L) = \mathrm{id}$. Действуя на вектор $x \in V$, получим $f(L)p(L)(x) + h(L)q(L)(x) = x$. Если $x \in \mathrm{Ker}\big(p(L)q(L)\big)$, то первое слагаемое лежит в ядре оператора $q(L)$, так как $q(L)f(L)p(L)(x) = f(L)\big(p(L)q(L)\big)(x) = f(L)(0) = 0$. Аналогично второе слагаемое лежит в ядре оператора $p(L)$. Таким образом, $\mathrm{Ker}\big(p(L)q(L)\big) = \mathrm{Ker}\, p(L) + \mathrm{Ker}\, q(L)$. Если же $x \in \mathrm{Ker}\, p(L) \cap \mathrm{Ker}\, q(L)$, то $x = f(L)p(L)(x) + h(L)q(L)(x) = 0$, следовательно, сумма прямая. □

[3] Доказательство выглядит, как жульничество, но смысл его таков. Кольцо R дифференцируемых функций в некотором открытом круге вкладывается в кольцо формальных степенных рядов $\mathbb{C}[[t]]$ (определения этого кольца нет в конспекте, но этот пример был в лекциях первого семестра). Подкольцо $\mathbb{C}[J_s]$ матричного кольца $M_s(\mathbb{C})$ изоморфно кольцу усеченных многочленов $\mathbb{C}[t]/(t^s)$, потому что t^s – минимальный многочлен матрицы J^s. Любой элемент из $\mathbb{C}[[t]]$ единственным образом представляется в виде суммы многочлена степени, меньшей s, и ряда, делящегося на t^s. Поэтому $\mathbb{C}[[t]]/(t^s) \cong \mathbb{C}[t]/(t^s) \cong \mathbb{C}[J_s]$. Поэтому равенство в $\mathbb{C}[[t]]$ выполнено и для образов левой и правой части в $\mathbb{C}[J_s]$.

Пусть теперь поле алгебраически замкнуто. Используя теорему Гамильтона–Кэли (или минимальный многочлен оператора вместо характеристического) и последнюю теорему, разложим пространство в прямую сумму подпространств

$$V = \operatorname{Ker} \varphi_L(L) = \bigoplus_{i=1}^{m} \operatorname{Ker}(L - \lambda_i \mathrm{id})^{k_i}.$$

Подпространство $\operatorname{Ker}(L - \lambda_i \mathrm{id})^{k_i}$ называется корневым подпространством оператора L, соответствующим собственному числу λ_i.

Обозначим через A сужение оператора $L - \lambda_i \mathrm{id}$ на корневое подпространство $U = \operatorname{Ker}(L - \lambda_i \mathrm{id})^{k_i}$. Для окончания доказательства теоремы о жордановой форме достаточно научиться выбирать базис u пространства U такой, что A_u состоит из жордановых блоков. Так как оператор A нильпотентен, то его собственные числа равны 0. Таким образом, необходимо выбрать базис, удовлетворяющий условиям $A(u_j) = u_{j-1}$ или $A(u_j) = 0$ для всех $j = 1, \ldots, k_j$. Набор векторов $v_1, \ldots, v_k$ таких, что $A(v_1) = 0$, а $A(v_j) = v_{j-1}$ при $j = 2, \ldots, k$ называется жордановой цепочкой. Следующее утверждение заканчивает доказательство.

Теорема 5.2. *Для любого нильпотентного оператора существует базис, состоящий из жордановых цепочек (это верно над любым полем).*

Доказательство этой теоремы не очень сложно, но требует аккуратной организации индукции по размерности пространства.

6. Дифференциальные и рекуррентные уравнения

Приведем еще одно приложение теоремы 5.1. Пусть дано линейное однородное уравнение с постоянными коэффициентами

$$y^{(n)} + a_{n-1} y^{(n-1)} + \cdots + a_0 y = 0. \tag{6}$$

Это уравнение можно записать в виде $p(D)(y) = 0$, где D – оператор дифференцирования на множестве дифференцируемых функций $\mathbb{C} \to \mathbb{C}$, а $p = t^n + a_{n-1} t^{n-1} + \cdots + a_0$. Другими словами, нам надо найти ядро дифференциального оператора $p(D)$.

Аналогично, пусть F^∞ обозначает векторное пространство бесконечных последовательностей $x : \mathbb{N}_0 \to F$, где F алгебраически замкнутое поле. Рекуррентное уравнение

$$x_{m+n} + a_{n-1} x_{m+n-1} + \cdots + a_0 x_m = 0 \text{ при любом } m \in \mathbb{N}_0 \tag{7}$$

сводится к нахождению ядра оператора $p(S)$, где S – оператор сдвига номеров, т. е. $S(x)_k = x_{k+1}$ при всех $k \in \mathbb{N}_0$.

По теореме 5.1 для решения обоих задач над замкнутым полем (в случае дифференциальных уравнений над $\mathbb{C}$) достаточно рассмотреть случай $p(t) = (t - \lambda)^k$. При $\lambda = 0$ мы умеем решать такую задачу: решение дифференциального уравнения $y^{(k)} = 0$ – множество многочленов степени $\leqslant k-1$, а для рекуррентного уравнения $x_{m+k} = 0$ при любом $m \in \mathbb{N}$ – множество конечных последовательностей длины k, дополненных нулями. Общий случай для дифференциальных уравнений следует из теоремы сдвига.

Теорема 6.1. *Пусть D – оператор дифференцирования, определенный выше, а p – многочлен. Тогда*

$$\operatorname{Ker} p(D - \lambda \mathrm{id}) = e^{\lambda t} \operatorname{Ker} p(D).$$

Для рекуррентного уравнения теорему сдвига написать не удается.

Решение дифференциального уравнения (6) можно найти и с помощью вычисления экспоненты от матрицы. Для этого надо переписать это уравнение в виде системы

$$y_0' = y_1; \quad y_1' = y_2; \quad \ldots \quad y_{n-1}' = y_n; \quad y_n' = -\sum_{k=0}^{n-1} a_k y_k$$

и решить ее помощью экспоненты от матрицы, как было описано в параграфе 4.

Аналогично, решение рекуррентного уравнения (7) можно найти возводя некоторую матрицу в степень, что делается с помощью жордановой формы. А именно, уравнение (7) можно записать в виде

$$\begin{pmatrix} x_{m+1} \\ x_{m+2} \\ \vdots \\ x_{m+n-1} \\ x_{m+n} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & 0 \\ \dots & \dots & \dots & \ddots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix} \cdot \begin{pmatrix} x_m \\ x_{m+1} \\ \vdots \\ x_{m+n-2} \\ x_{m+n-1} \end{pmatrix},$$

или короче $x^{(m+1)} = Ax^{(m)}$. Тогда для нахождения формулы для $x^{(m)}$ надо просто возвести матрицу A в степень m и умножить на произвольный столбец $x^{(0)}$.

7. Модули над кольцами

Определение 7.1. Пусть R – (не обязательно коммутативное) кольцо с 1. Аддитивная абелева группа M с заданной операцией "умножения" $M \times R \to M$ называется правым R-модулем, если для любых $\alpha, \beta \in R$ и $u, v \in M$:

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

Аналогично определяется левый R-модуль.

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

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

Примеры.

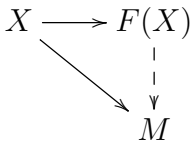
(1) Идеал является модулем.
(2) Абелева группа – $\mathbb{Z}$-модуль, векторное пространство – F-модуль.
(3) Кольцо является модулем над самим собой. Этот модуль называется регулярным. Это аналог одномерного векторного пространства.
(4) Если $\varphi : R \to A$ – гомоморфизм колец, то A является (левым) 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) Множество R^n является правым R-модулем и левым $\mathrm{M}_n(R)$-модулем.

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

Определение 7.2. Модуль называется свободным, если он имеет базис.

Свободный модуль $F(X)$ с базисом X обладает следующим универсальным свойством.

Предложение 7.3. *Для любого R-модуля M и функции $X \to M$ существует единственный гомоморфизм модулей $F(X) \to M$ такой, что диаграмма*



коммутативна.

Доказательство. Из условия коммутативности диаграммы мы знаем образы базисных элементов. Так как любой элемент $F(X)$ является линейной комбинацией базисных, а гомоморфизм модулей переводит линейные комбинации в линейные комбинации, то образы всех элементов $F(X)$ определены однозначно. Проверка того, что таким образом мы действительно получим гомоморфизм модулей тривиальна. □

Следующее утверждение – конструкция свободного модуля.

Предложение 7.4. *Пусть $F(X)$ – 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 $i : X \to F(X)$ формулой $i(x) = \mathbb{1}_x$ – характеристическая функция множества $\{x\}$, т. е. $\mathbb{1}_x(y) = \begin{cases} 1, & y = x \\ 0, & y \neq x \end{cases}$. Тогда $F(X)$ вместе с отображением i – свободный модуль с базисом X.*

Предложение 7.5. *Если X конечно, то $F(X) \cong R^{|X|} \cong \underbrace{R \oplus \cdots \oplus R}_{|X| \text{ раз}}$.*

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

8. Подмодули свободного модуля над ОГИ

Следующие два параграфа лежат на стыке теории коммутативных колец и линейной алгебры. Мы докажем теорему классификации конечнопорожденных модулей над кольцами главных идеалов, из которой затем выведем теорему о Жордановой форме оператора. В качестве бесплатного приложения мы получим теорему о строении конечнопорожденных абелевых групп.

Пусть R – коммутативное кольцо, а M – конечнопорожденный R-модуль, т. е. в M существует конечная система образующих $X = \{x_1, \ldots, x_k\}$. По универсальному свойству свободного модуля существует единственный гомоморфизм свободного модуля $F(X)$ в M, тождественный на X. Так как X – система образующих, то этот гомоморфизм сюръективен. По теореме о гомоморфизме $M \cong F(X)/N$ для некоторого подмодуля N в $F(X)$. Учитывая, что $F(X) \cong R^{|X|}$, для описания произвольного конечнопорожденного R-модуля достаточно описать подмодули в R^k для произвольного натурального k.

Прежде, чем перейти к классификации подмодулей, определим аналог размерности векторных пространств для конечнопорожденных свободных модулей. Если u и v – конечные базисы свободного модуля, то, также как и для векторных пространств, существуют взаимно обратные матрицы перехода $C_{u \to v}$ и $C_{v \to u}$. Неквадратная матрица над коммутативным кольцом не может быть двусторонне обратима. Действительно, если бы она была двусторонне обратима, то ее образ над любым факторкольцом обладал бы тем же свойством. С другой стороны, в любом коммутативном кольце существует максимальный идеал, фактор по которому – поле, а для поля результат

известен из линейной алгебры. Поэтому любой базис свободного модуля имеет одинаковое число элементов, которое называется рангом этого модуля.[4]

Специфика области главных идеалов, необходимая для классификации подмодулей конечнопорожденного свободного модуля, выражена в следующей лемме.

Лемма 8.1. *Пусть R – область главных идеалов. Для любого столбца $x \in R^k$ существует матрица $A \in \mathrm{GL}_k(R)$ такая, что $Ax = e_{*1}\alpha$. При этом α является наибольшим общим делителем элементов столбца x.*

Доказательство. Проведем доказательство индукцией по k. Для $k = 1$ доказывать нечего. При $k > 1$ положим $d = \gcd(x_{k-1}, x_k)$, $a = \frac{x_{k-1}}{d}$ и $b = \frac{x_k}{d}$. По теореме о линейном представлении НОД существуют $r, s \in R$ такие, что $x_{k-1}r + x_k s = d$, откуда $ar + bs = 1$. Тогда

$$\begin{pmatrix} E & 0 & 0 \\ 0 & r & s \\ 0 & -b & a \end{pmatrix} \begin{pmatrix} x' \\ x_{k-1} \\ x_k \end{pmatrix} = \begin{pmatrix} x' \\ d \\ 0 \end{pmatrix},$$

где $x' = (x_1, \ldots, x_{k-2})^\intercal$. Заметим, что определитель первого сомножителя равен 1, следовательно, эта матрица обратима. По индукционному предположению существует обратимая матрица A' такая, что $A' \binom{x'}{d} = \binom{\alpha}{0}$, где $\alpha = \gcd(x_1, \ldots, x_{k-2}, d) = \gcd(x_1, \ldots, x_k)$. □

Если R – нетерова область целостности, то свойство из предыдущей леммы равносильно тому, что любой идеал в R является главным.

Теорема 8.2 (классификации подмодулей конечнопорожденного свободного модуля). *Пусть R – кольцо главных идеалов, а N – подмодуль свободного модуля R^k. Существует базис $u = (u_1, \ldots, u_k)$ модуля R^k и элементы $\alpha_1, \ldots, \alpha_k \in R$ такие, что*

(1) *элементы $u_1\alpha_1, \ldots, u_k\alpha_k$ лежат в N и порождают его;*
(2) *α_{i+1} делится на α_i при всех $i = 1, \ldots, k-1$ (мы считаем, что 0 делится на 0).*

Схема доказательства.

$$\begin{pmatrix} n_1 & * \\ n_2 & * \\ \vdots & * \\ n_k & * \end{pmatrix} \to \begin{pmatrix} \alpha & y_1 & * \\ 0 & y_2 & * \\ \vdots & \vdots & * \\ 0 & y_k & * \end{pmatrix} = \begin{pmatrix} \alpha & y_1 & \gcd(\alpha, y_1) & * \\ 0 & y_2 & * & * \\ \vdots & \vdots & * & * \\ 0 & y_k & * & * \end{pmatrix} \to \begin{pmatrix} \alpha & 0 & \ldots \\ 0 & * & * \\ \vdots & * & * \\ 0 & * & * \end{pmatrix} \to \cdots \to \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & 0 & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \alpha_k \end{pmatrix}.$$

□

Доказательство. Проведем доказательство индукцией по рангу k свободного модуля, в котором лежит изучаемый подмодуль. При $k = 1$ подмодуль в R^1 – это идеал кольца R, а любой идеал в R – главный. Таким образом, достаточно взять $u_1 = 1$, а α_1 – образующая этого идеала.[5]

Пусть $k > 1$. Обозначим через $I(x)$ идеал, порожденный элементами столбца x. Положим $S = \{I(x) \mid x \in N\}$. Пусть $I(n) = \alpha R$ максимальный из идеалов множества S. Можно считать, что $\alpha \neq 0$, иначе $N = 0$ и утверждение очевидно. По лемме 8.1 существует $A \in \mathrm{GL}_k(R)$ такая,

[4]Для некоммутативных колец это утверждение неверно, т. е. существует некоммутативное кольцо Λ для которого модули Λ^n и Λ^m изоморфны при $m \neq n$. Простейший пример такого кольца – кольцо эндоморфизмов бесконечномерного векторного пространства. Кольца, для которых ранг свободного модуля определен однозначно, называются ИБЧ или IBN-кольцами (Invariant Basis Number). Нетрудно доказать, что из не-ИБЧ-кольца не существует ни одного гомоморфизма ни в одно ИБЧ-кольцо, т. е. в каком-то смысле класс не-ИБЧ-колец – это черная дыра: попав туда, выбраться уже невозможно.

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

что $An = e_{*1}\alpha$. Возьмем $x \in N$, обозначим $y = Ax$ и докажем, что y_1 делится на α. Пусть $\gamma = \gcd(y_1, \alpha)$. Существуют элементы $\lambda, \mu \in R$ такие, что $y_1\lambda + \alpha\mu = \gamma$. Тогда первый элемент столбца $Ax\lambda + An\mu$ равен γ. Имеем

$$\alpha R \leqslant \gamma R \leqslant I(Ax\lambda + An\mu) = I(x\lambda + n\mu).$$

Так как $x\lambda + n\mu \in N$, то идеал $I(x\lambda + n\mu)$ принадлежит S. Максимальность идеала αR влечет равенство $\alpha R = I(x\lambda + n\mu)$, откуда $y_1 \in \gamma R = \alpha R$.

Таким образом, $y_1 = \alpha\beta$ для некоторого $\beta \in R$, и

$$Ax = An\beta + \sum_{i=2}^{k} e_{*i}y_i = e_{*1}\alpha\beta + \sum_{i=2}^{k} e_{*i}y_i.$$

Домножая на A^{-1} получаем

$$x = u'_1\alpha\beta + \sum_{i=2}^{k} u'_i y_i \in \langle u'_1\alpha, u'_2, \ldots, u'_k\rangle,$$

где $u'_i = a'_{i*}$ – столбцы матрицы A^{-1}. Так как x – произвольный элемент из N, то мы доказали, что $N \leqslant \langle u'_1\alpha, u'_2, \ldots, u'_k\rangle$. Более того, из формулы для x следует,что $\sum_{i=2}^{k} u'_i y_i = x - u'_1\alpha\beta \in N$, откуда

$$N = \langle u'_1\alpha\rangle \oplus (\langle u'_2, \ldots, u'_k\rangle \cap N)$$

(сумма прямая, потому что уже $\langle u'_1\rangle \cap \langle u'_2, \ldots, u'_k\rangle = \{0\}$).

Модуль $N' = N \cap \langle u'_2, \ldots, u'_k\rangle$ содержится в свободном модуле $\langle u'_2, \ldots, u'_k\rangle$ ранга $k-1$, поэтому к нему можно применить индукционное предположение. Другими словами, существует базис $u_2, \ldots, u_k$ модуля $\langle u'_2, \ldots, u'_k\rangle$ и элементы $\alpha_2, \ldots, \alpha_k \in R$ такие, что N' порожден элементами $u_2\alpha_2, \ldots, u_k\alpha_k$ и α_{i+1} делится на α_i при всех $i = 2, \ldots, k-1$. Положим $\alpha_1 = \alpha$ и $u_1 = u'_1$. Легко проверить, что $u_1, \ldots, u_k$ – базис модуля R^k, а $u_1\alpha_1, \ldots, u_k\alpha_k$ порождает N.

Осталось доказать, что α_2 делится на α_1. Обозначим через $C = C_{e\to u}$ матрицу, составленную из столбцов $u_1, \ldots, u_n$. Элемент $u_1\alpha_1 + u_2\alpha_2$ принадлежит N, поэтому

$$I(u_1\alpha_1 + u_2\alpha_2) = I(C^{-1}u_1\alpha_1 + C^{-1}u_2\alpha_2) = \alpha_1 R + \alpha_2 R \in S.$$

Так как $\alpha_1 R$ – максимальный среди идеалов из S, то $\alpha_1 R + \alpha_2 R = \alpha_1 R$, откуда следует, что $\alpha_2 \in \alpha_1 R$, т. е. α_2 делится на α_1. □

Следствие 8.3. *Любой подмодуль конечнопорожденного свободного модуля над областью главных идеалов является свободным, причем ранг подмодуля не превосходит ранга модуля.*

Следствие 8.4 (Нормальная форма Смита). *Для любой матрицы $A \in \mathrm{M}_{k,l}(R)$ над областью главных идеалов 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.*

Формально это утверждение не следует из теоремы, так как “матрица перехода” от одной системы образующих к другой не обязана быть обратимой. Для доказательства достаточно повторить рассуждения из доказательства теоремы с N равным линейной оболочке столбцов матрицы A, с необходимыми уточнениями.

9. Конечнопорожденные модули над кольцами главных идеалов

Модуль M над кольцом R называется циклическим, если он порожден одним элементом. Любой циклический модуль изоморфен R/I для некоторого идеала I кольца R. Действительно, если $M = \langle m\rangle$, то отображение $\pi : R \to M$, 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 (если R – область целостности, то I может быть равен 0).

Теорема 9.1 (Классификация конечнопорожденных модулей). *Любой конечнопорожденный модуль над областью главных идеалов изоморфен прямой сумме примарных модулей. При этом набор примарных модулей определен однозначно.*

Доказательство. В этом параграфе мы докажем только существование такого разложения и выведем несколько следствий. Единственность будет доказана в следующем разделе.

Пусть M – конечнопорожденный модуль над областью главных идеалов R. Как уже говорилось, существует эпиморфизм $R^k \to M$. Обозначим его ядро через N По теореме 8.2 существует базис $u_1, \dots, u_k$ модуля R^k и элементы $\alpha_1, \dots, \alpha_k \in R$ такие, что $N = \langle u_1\alpha_1, \dots, u_n\alpha_n\rangle$. Зададим гомоморфизм $\rho : R^k \to \bigoplus_{i=1}^{k} R/\alpha_i R$ формулой

$$\rho(u_1\beta_1 + \dots + u_k\beta_k) = (\beta_1 \mod \alpha_1, \dots, \beta_k \mod \alpha_k)$$

(так как u – базис, то эта формула однозначно задает отображение). Легко видеть, что ρ – 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. □

Следствие 9.2 (Классификация конечнопорожденных абелевых групп). *Любая конечнопорожденная абелева группа изоморфна прямой сумме циклических групп бесконечного порядка и порядка p^n, где p – простое число. При этом такое разложение единственно с точностью до перестановки прямых слагаемых.*

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

Из теоремы о строении конечнопорожденных модулей, примененной к кольцу многочленов, получаем доказательство существования нормальных форм матрицы оператора. Клеткой Фробениуса называется матрица $A \in \mathrm{M}_n(F)$ с элементами $a_{i+1,i} = 1$ при $i = 1, \dots, n-1$, произвольными a_{in}, $i = 1, \dots, n$, и остальными нулями.

Теорема 9.3 (нормальная форма Фробениуса). *Для любого линейного оператора $L : V \to V$ существует базис и пространства V такой, что матрица L_u клеточно диагональная с клетками Фробениуса по диагонали.*

Доказательство. Рассмотрим V как $F[t]$-модуль, полагая $t^k v = L^k(v)$ и продолжая это определение по линейности на все кольцо $F[t]$. Так как $F[t]$ – кольцо главных идеалов, то по теореме 9.1 V изоморфно прямой сумме циклических модулей (допуская вольность речи будем считать, что V равно прямой сумме циклических модулей). Заметим, что $F[t]$ не может встречаться в прямой сумме, потому что V конечномерно над F, а $F[t]$ – нет.

Каждый из циклических модулей является L-инвариантным подпространством, поэтому в F-базисе V, состоящем из F-базисов циклических модулей, матрица оператора L будет клеточно диагональной. В каждом циклическом модуле $F[t]/pF[t]$ выберем базис из смежных классов $\overline{t^k} = t^k + pF[t]$. Тогда $L(\overline{t^k}) = t \cdot \overline{t^k} = \overline{t^{k+1}}$. Если $k < \deg p - 1$, то оператор L отображает базисный вектор в следующий. Следовательно, в соответствующих столбцах матрицы оператора L появляются единицы под главной диагональю и остальные нули. Таким образом, в диагональных блоках стоят клетки Фробениуса. □

В предыдущей теореме единственности не было, потому что клетки Фробениуса соответствуют циклическим модулям, которые не обязательно примарны. Заметим, что характеристический многочлен фробениусовой клетки A равен $\pm(t^n + a_{nn}t^{n-1} + \dots + a_{2n}t + a_{1n})$.

Доказательство существования жордановой формы. Пусть F – алгебраически замкнутое поле, V – векторное пространство над F, $L : V \to V$ – 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 – область главных идеалов, то по теореме 9.1 V изоморфно прямой сумме примарных модулей. Заметим, что R не может встречаться в прямой сумме, потому что V конечномерно над F, а R – нет.

Так как F замкнуто, то неприводимыми элементами кольца R являются только многочлены $t-\lambda$. Таким образом, осталось изучить модули $M = R/(t-\lambda)^k R$. Элементы этого модуля взаимно однозначно соответствуют многочленам степени, меньшей k. Поэтому любой элемент M может быть единственным образом представлен в виде F-линейной комбинации[6] $\sum_{i=0}^{k-1} \alpha_i (t-\lambda)^i$, где $\alpha_i \in F$. Таким образом, элементы $(t-\lambda)^i$, $i = 0, \dots, k-1$, образуют базис M, как векторного пространства над F. Если $v_0, \dots, v_{k-1}$ – элементы V, соответствующие $(t-\lambda)^0, \dots, (t-\lambda)^{k-1}$ при изоморфизме, то ясно, что $(t-\lambda)v_i = v_{i+1}$ при $i < k-1$, а $(t-\lambda)v_{k-1} = 0$. По определению действия t на V получаем:

$$L(v_i) = v_{i+1} + \lambda v_i \text{ при } i < k-1, \text{ и } L(v_{k-1}) = \lambda v_{k-1}.$$

Другими словами, матрица сужения оператора L на подпространство $\langle v_0, \dots, v_{k-1} \rangle$ в выбранном базисе – это жорданова клетка. Таким образом, пространство V разбилось в прямую сумму подпространств, в каждом из которых матрица сужения L в подходящем базисе является жордановой клеткой. Объединение базисов прямых слагаемых является базисом пространства. Ясно, что в объединении подходящих базисов матрица оператора L будет клеточно-диагональной с жордановыми блоками по диагонали.

Утверждение о единственности следует из единственности разложения конечнопорожденного модуля в прямую сумму примарных модулей. □

10. Единственность разложения на примарные

Пусть R – область целостности, а M – R-модуль. Множество элементов из M, которые при умножении на какой-нибудь ненулевой элемент кольца обращаются в 0, называется подмодулем кручения. Это действительно подмодуль, потому что если $m_1 r_1 = 0$ и $m_2 r_2 = 0$, то $(m_1+m_2)r_1 r_2 = 0$ (здесь $m_1, m_2 \in M$, а $r_1, r_2 \in R \setminus \{0\}$). Говорят, что M – модуль без кручения, если его подмодуль кручения нулевой. Фактормодуль по подмодулю кручения является модулем без кручения. Действительно, Обозначим через $T = T(M)$ подмодуль кручения. Тогда $x + T$ содержится в $T(M/T)$ тогда и только тогда, когда $xr \in T$ для некоторого ненулевого $r \in R$. Но тогда по определению подмодуля кручения $xrr' = 0$ для какого-то $r' \in R \setminus \{0\}$, при этом $rr' \neq 0$, так как R – область целостности. Следовательно, $x \in T$, т. е. $x + T = 0_{M/T}$.

Пусть теперь R – область главных идеалов, а $p \in R$ – неприводимый элемент. Тогда R/pR – поле. Для натурального числа k рассмотрим фактормодуль $p^{k-1}M/p^k M$. Так как умножение на p аннулирует любой элемент этого модуля, то можно естественным образом определить на этом модуле структуру R/pR-векторного пространства: $(r + pR)(p^{k-1}m + p^k M) = p^{k-1}rm + p^k M$. Оказывается числа $l_{p,k} = l_{p,k}(M) = \dim_{R/pR} p^{k-1}M/p^k M$ по всем неприводимым $p \in R$ и всем $k \in \mathbb{N}$ полностью определяют строение подмодуля кручения $T(M)$.

Лемма 10.1. *Пусть $M = R/p^n R$ – примарный модуль, а $q \neq p$ – неприводимый элемент в R. Тогда $l_{q,k} = 0$, $l_{p,k} = 1$ при $n \geqslant k$, и $l_{p,k} = 0$ в противном случае.*

$l_{p,k}(M_1 \oplus M_2) = l_{p,k}(M_1) + l_{p,k}(M_2)$.

Если M – прямая сумма примарных модулей не изоморфных R, то $l_{p,k}(M)$ равно количеству прямых слагаемых в разложении M, изоморфных $R/p^h R$ с $h \geqslant k$.

[6] Здесь мы отождествляем многочлен степени, меньшей k, с его смежным классом, также как мы часто делаем в группе $\mathbb{Z}/k\mathbb{Z}$, отождествляя смежный класс целого числа с остатком от деления на k.

Доказательство. Так как q обратим в кольце R/p^nR, то умножение на q является автоморфизмом модуля M, откуда $q^kM = q^{k-1}M$. Фактормодуль циклического модуля циклический, поэтому если он ненулевой, то он порожден 1 элементом. При $n \geqslant k$ модуль $p^{k-1}(R/p^nR)$ порожден элементом p^{k-1}, отсюда первое утверждение.

Ясно, что $p^k(M_1 \oplus M_2) = p^kM_1 \oplus p^kM_2$. Следовательно,

$$p^{k-1}(M_1 \oplus M_2)/p^k(M_1 \oplus M_2) \cong p^{k-1}M_1/p^kM_1 \oplus p^{k-1}M_2/p^kM_2,$$

откуда вытекает второе утверждение леммы. Третье утверждение сразу вытекает из двух первых. □

Замечание 10.2. В предыдущей лемме можно заменить идеалы вида p^nR на $\mathfrak{m}^n$, где $\mathfrak{m}$ – максимальный идеал. Тогда можно не накладывать никаких ограничений на коммутативное кольцо R.

Доказательство единственности разложения из теоремы 9.1. Пусть R – область главных идеалов, а

$$M = R^k \oplus M_1 \oplus \cdots \oplus M_s, \text{ где } M_i = \bigoplus_{j=1}^{t_i} R/p_i^{h_{ij}}R \text{ при всех } i = 1, \ldots, s,$$

а $p_1, \ldots, p_s$ – различные неприводимые элементы R. Мы хотим доказать, что набор $p_1, \ldots, p_s$, а также числа k, s, t_i и h_{ij} зависят только от самого модуля M, а не от разложения в прямую сумму.

Ясно, что $T(M) = M_1 \oplus \cdots \oplus M_s$ является подмодулем кручения в M, а $R^k \cong M/T(M)$. Так как ранг свободного модуля определен однозначно, то k определено однозначно.

Числа $l_{q,k} = l_{q,k}\big(T(M)\big)$ также не зависят от разложения. Количество прямых слагаемых в разложении модуля M на примарные, изоморфных R/p^hR, равно $l_{p,h} - l_{p,h+1}$. Действительно, по предыдущей лемме $l_{p,h+1}$ – количество слагаемых R/p^nR, где $n \geqslant h+1$, а $l_{p,h}$ количество слагаемых R/p^nR, где $n \geqslant h$. Таким образом, количество слагаемых изоморфных R/p^hR также определяется модулем M однозначно, что завершает доказательство. □

Глава 7

Билинейные и квадратичные формы

Везде в этой главе мы считаем, что характеристика основного поля не равна 2. Изучение квадратичных форм в характеристике 2 – это существенно более сложная задача, даже на уровне определений.

1. Формы и их матрицы

Пусть V – векторное пространство над полем F.

Напомним, что функция $B : V \times V \to F$ 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 1.1. $\mathrm{Bil}(V) = \mathrm{Bil}^{(s)}(V) \oplus \mathrm{Bil}^{(a)}(V)$.

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 $\mathrm{Bil}^{(s)}(V) \cap \mathrm{Bil}^{(a)}(V) = \{0\}$ очевиден (и тоже использует условие, что $2 \neq 0$ в поле F). □

Определение 1.2. Функция $Q : V \to F$ называется квадратичной формой, если существует билинейная форма $B : V \times V \to F$ такая, что $Q(x) = B(x, x)$.

Теорема 1.3 (поляризация квадратичной формы). *Пусть Q – квадратичная форма на V, соответствующая билинейной форме B. Положим*

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

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, которая на самом деле является изоморфизмом векторных пространств.

В некоторых ситуациях приходится рассматривать чуть более общий случай. Пусть $\bar{\cdot} : F \to F$ – инволюция, т. е. автоморфизм поля порядка 2. Иными словами, для любых $\alpha, \beta \in F$ выполнены равенства

(1) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;
(2) $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$ и
(3) $\overline{\overline{\alpha}} = \alpha$.

Определение 1.4. Функция $B : V \times V \to F$ называется полуторалинейной формой, если для любых $x, y, z \in V$ и $\alpha, \beta \in F$ имеют место равенства:

$$B(x\alpha + y\beta, z) = B(x, z)\overline{\alpha} + B(y, z)\overline{\beta} \text{ и } B(z, x\alpha + y\beta) = B(z, x)\alpha + B(z, y)\beta.$$

Полуторалинейная форма B называется эрмитовой, если $B(x,y) = \overline{B(y,x)}$ для любых $x, y \in V$.

Симметричная билинейная форма является частным случаем эрмитовой формы, если инволюция тривиальна. Поэтому в дальнейшем, везде где можно, мы будем рассматривать эрмитовы формы вместо симметричных билинейных.

Для матрицы $A \in \mathrm{M}_{m,n}(F)$ обозначим $A^* = \overline{A}^\intercal$. Другими словами, $a^*_{ij} = \overline{a_{ji}}$.

Предложение 1.5. *Пусть B полуторалинейная форма на V, а $v = (v_1, \dots, v_n)$ – базис V. Тогда существует матрица $A \in \mathrm{M}_n(F)$ такая, что $B(x,y) = x_v^* A y_v$ для любых $x, y \in V$. При этом $a_{ij} = B(v_i, v_j)$.*

Доказательство. Пусть $x_v = (x_1, \dots, x_n)^\intercal$ и $y_v = (y_1, \dots, y_n)^\intercal$. Тогда

$$B(x,y) = B(\sum_{i=1}^{n} v_i x_i, \sum_{j=1}^{n} v_j y_j) = \sum_{i,j=1}^{n} \overline{x}_i B(v_i, v_j) y_j = x_v^* A y_v.$$

□

Определение 1.6. Матрица A, построенная в предыдущей лемме, называется матрицей формы B в базисе v и обозначается через B_v. Матрицей квадратичной формы называется матрица ассоциированной с ней симметричной билинейной формы.

Определение 1.7. Полуторалинейная форма называется вырожденной, если существует $y \in V \setminus \{0\}$ такой, что $B(y,x) = 0$ при всех $x \in V$.

Если форма вырождена, то $y_v^* B_v x_v = 0$ для любого столбца $x_v \in F^n$, откуда система линейных уравнений $z B_v = 0$ имеет ненулевое решение. Таким образом, вырожденность формы равносильна вырожденности матрицы этой формы (в любом базисе). Следовательно, вырожденность "слева" эквивалентна вырожденности "справа":

$$\exists\, y \in V \setminus \{0\}\ \forall x \in V:\ B(x,y) = 0.$$

Ясно, что матрица квадратичной формы симметрична, т. е. $B_v^\intercal = B_v$, а матрица эрмитовой формы эрмитова, т. е. $B_v^* = B_v$ (другое название такой матрицы самосопряженная).

Замечание 1.8. Пусть F – поле с инволюцией, а $K = \{\alpha \in F \mid \overline{\alpha} = \alpha\}$. Нетрудно проверить, что K – подполе в F. Диагональные элементы и определитель любой эрмитовой матрицы A лежит в K. Действительно, $A = A^* \implies \det A = \det A^* = \det \overline{A} = \overline{\det A}$, а утверждение про диагональные элементы очевидно.

Предложение 1.9. *Пусть B полуторалинейная форма на V, а u и v – базисы пространства V. Тогда $B_v = C^*_{u\to v} B_u C_{u\to v}$.*

2. Диагонализация эрмитовой формы

В этом параграфе мы начинаем классификацию эрмитовых (квадратичных) форм. Сначала для этого надо определить, какие формы мы считаем одинаковыми. Вместо квадратичной формы можно всегда рассматривать соответствующую симметричную билинейную форму, являющуюся эрмитовой формой с тривиальной инволюцией поля. Поэтому в дальнейшем мы в основном формулируем все для эрмитовых форм.

Определение 2.1. Если B – квадратичная (эрмитова) форма на векторном пространстве V, то пара (V, B) называется квадратичным (соотв. эрмитовым) пространством. Квадратичное или эрмитово пространство называется невырожденным, если форма B невырождена.

Изометрией эрмитовых пространств $(V, B) \to (V', B')$ называется биективное линейное отображение $L : V \to V'$, обладающее свойством $B'\big(L(x), L(y)\big) = B\big(x, y\big)$ для всех $x, y \in V$.

Предложение 2.2. *Пусть B эрмитова форма на V. Положим*

$$V^\perp = \{x \in V \mid B(x,y) = 0 \,\forall y \in V\}.$$

Если $V = V^\perp \oplus U$ (заметим, что такое U всегда существует), то сужение формы B на $U \times U$ невырождено. При этом, если $V = V^\perp \oplus U'$, то U и U' изометричны.

Доказательство. Пусть $x \in U$ такой, что $B(x,y) = 0$ для любого $y \in U$. Любой вектор $z \in V$ представляется в виде суммы $z = y + w$ для некоторых $y \in U$ и $w \in V^\perp$. Тогда $B(x,z) = B(x,y) + B(x,w) = 0$. Таким образом, $x \in U \cap V^\perp = \{0\}$, следовательно, сужение B на $U \times U$ невырождено.

Пусть $V^\perp \oplus U = V^\perp \oplus U' = V$. Тогда для любого $x' \in U'$ существует единственный $x \in U$ такой, что $x' \in x + V^\perp$ (такой x называется проекцией x' на U параллельно $V^\perp$). Нетрудно проверить, что такое проектирование (т. е. сопоставление $x' \mapsto x$) является линейным отображением, а обратным к нему является проектирование U на U' параллельно $V^\perp$. Так что это изоморфизм векторных пространств и

$$B(x',x') = B(x+w, x+w) = B(x,x) + B(w,x) + B(x,w) + B(w,w) = B(x,x),$$

откуда следует, что этот изоморфизм – изометрия. □

Задача теории эрмитовых форм – классификация всех конечномерных эрмитовых пространств над данным полем с точностью до изометрии. Ясно, что пространства разной размерности не могут быть изометричными. Очевидно также, что изометрия сохраняет подпространство $V^\perp$ из предложения 2.2. Таким образом, достаточно классифицировать невырожденные эрмитовы пространства любой фиксированной размерности.

Лемма 2.3. *Эрмитовы пространства (V,B) и (V',B') изометричны тогда и только тогда, когда существуют такие базисы v и v' пространств V и V' соответственно, что $B_v = B'_{v'}$.*

Доказательство. Пусть $L : V \to V'$ – изометрия эрмитовых пространств, а $v = (v_1, \dots, v_n)$ – базис пространства V. Тогда $v' = \big(L(v_1), \dots, L(v_n)\big)$ является базисом V'. По определению изометрии $B'\big(L(x), L(y)\big) = B\big(x,y\big)$ для любых $x, y \in V$, откуда $B_v = B'_{v'}$.

Обратно, если $B_v = B'_{v'}$, то отображение $L(x) = v'x_v$ является изометрией эрмитовых пространств. Действительно, $L(x)_{v'} = x_v$, поэтому

$$B'\big(L(x), L(y)\big) = L(x)^*_{v'} B'_{v'} L(y)_{v'} = x_v^* B_v y_v.$$

□

Лемма 2.4. *Пусть B – ненулевая эрмитова форма на V. Тогда существует вектор $x \in V$ такой, что $B(x,x) \neq 0$.*

Доказательство. Так как форма ненулевая, существует пара векторов $y, z \in V$ таких, что $B(y,z) \neq 0$. Если $B(y,y)$ или $B(z,z)$ не равно нулю, то все доказано. Иначе

$$B(y + \lambda z, y + \lambda z) = B(y,y) + B(z,z) + B(y,\lambda z) + B(\lambda z, y) = B(y,z)\lambda + \overline{\lambda} \cdot \overline{B(y,z)}$$

При $\lambda = \overline{B(y,z)}$ получим $B(y + \lambda z, y + \lambda z) = 2B(y,z)\overline{B(y,z)} \neq 0$. □

Теорема 2.5 (диагонализация матрицы эрмитовой формы). *Для любой эрмитовой формы существует базис, в котором ее матрица диагональна.*

Доказательство. Пусть B – эрмитова форма на V. Мы должны доказать, что существует базис v пространства V ортогональный относительно формы B. По предложению 2.2 $V = V^\perp \oplus U$, и сужение формы B на $U \times U$ невырождено. Для доказательства достаточно найти B-ортогональный базис пространства U (вектора из V_0 по определению ортогональны всем векторам).

Проведем доказательство индукцией по $n = \dim U$. Если $n = 1$, то доказывать нечего. Пусть $n > 1$. По предыдущей лемме существует $u_1 \in U$ такой, что $B(u_1, u_1) \neq 0$. Дополним u_1 до базиса $u = (u_1, \ldots, u_n)$ пространства U. Положим $w_k = u_k - \frac{B(u_k,u_1)}{B(u_1,u_1)}u_1$ при $2 \leqslant k \leqslant n$. Тогда

$$B(w_k, u_1) = B\Big(u_k - \frac{B(u_k, u_1)}{B(u_1, u_1)}u_1, u_1\Big) = B(u_k, u_1) - \frac{B(u_k, u_1)}{B(u_1, u_1)}B(u_1, u_1) = 0.$$

Таким образом, u_1 B-ортогонален всем векторам w_k при $2 \leqslant k \leqslant n$, а, следовательно, и всему подпространству $W = \langle w_2, \ldots, w_n\rangle$. По индукционному предположению существует B-ортогональный базис $(v_2, \ldots, v_n)$ подпространства W. Положив $v_1 = u_1$, получим ортогональный базис $(v_1, \ldots, v_n)$ пространства U. □

Покажем, как алгоритм диагонализации, приведенный в доказательстве теоремы, работает на практике. Путь u – произвольный базис пространства V, и $A = B_u$. При переходе к другому базису матрица A меняется на C^*AC. Если C – трансвекция, то умножение справа на C производит преобразование Гаусса со столбцами, а умножение слева на C^* – такое же преобразование со строками, но с сопряженными коэффициентами. Если $a_{11} = B(u_1, u_1) \neq 0$, то

$$\begin{pmatrix} a_{11} & c \\ c^* & \star \end{pmatrix} \approx \begin{pmatrix} 1 & 0 \\ -c^*/a_{11} & E \end{pmatrix} \begin{pmatrix} a_{11} & c \\ c^* & \star \end{pmatrix} \begin{pmatrix} 1 & -c/a_{11} \\ 0 & E \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ 0 & \star \end{pmatrix},$$

где $c = (a_{12}, \ldots, a_{1n})$, а знак "$\approx$" стоит между матрицами одной и той же формы в разных базисах. После этого мы работаем с получившейся матрицей $(n-1) \times (n-1)$, обозначенной звездочкой.

Если $a_{11} = 0$, но какой-нибудь другой диагональный элемент матрицы A не равен нулю, то проделываем аналогичные преобразования используя этот элемент вместо a_{11}. Если же все диагональные элементы равны нулю, но $a_{ij} = \alpha \neq 0$ (такой элемент всегда найдется в ненулевой матрице), то по лемме 2.4 сумма $u_i + u_j\overline{\alpha}$ не аннулируется квадратичной формой, ассоциированной с B. Значит достаточно прибавить $u_j\overline{\alpha}$ к u_i и проделать операции, как в вынесенной формуле. Матрица перехода между такими базисами отличается от единичной только в позиции (j, i), в которой стоит $\overline{\alpha}$. Проиллюстрируем сказанное на примере матрицы 2×2 с $a_{11} = a_{22} = 0$.

$$\begin{pmatrix} 0 & \alpha \\ \overline{\alpha} & 0 \end{pmatrix} \approx \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \alpha \\ \overline{\alpha} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \overline{\alpha} & 1 \end{pmatrix} = \begin{pmatrix} 2\alpha\overline{\alpha} & \alpha \\ \overline{\alpha} & 0 \end{pmatrix} \approx \begin{pmatrix} 2\alpha\overline{\alpha} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix}.$$

Пусть Q – квадратичная форма. Если матрица Q_v диагональна, а $u_k = v_k\lambda_k$, то матрица Q_u также диагональна, причем ее диагональные элементы отличаются от диагональных элементов Q_v умножением на λ_k^2. Таким образом, для невырожденных форм, играют роль только классы вычетов диагональных элементов Q_v в $F^*/(F^*)^2$. В частности, если из любого элемента поля F можно извлечь квадратный корень, то классификация совсем простая.

Определение 2.6. Поле F называется квадратично замкнутым, если для любого $\alpha \in F$ уравнение $x^2 = \alpha$ имеет хотя бы одно решение. В частности, алгебраически замкнутое поле является квадратично замкнутым.

Следствие 2.7. *Любые два невырожденных квадратичных пространства одинаковой размерности над квадратично замкнутым полем изоморфны.*

3. Вещественные квадратичные формы

В этом параграфе V обозначает вещественное векторное пространство размерности m. В общем случае неверно, что любые две диагональные матрицы Q_u и Q_v квадратичной формы Q отличаются только перестановкой диагональных элементов и умножением их на квадраты. Однако, для поля вещественных чисел это так, и роль играют только знаки диагональных элементов.

Определение 3.1. Сигнатурой последовательности вещественных чисел называется пара чисел (p, n), где p – количество положительных среди этих чисел, а n – отрицательных.

Сигнатурой вещественной диагональной матрицы называется сигнатура последовательности ее диагональных элементов.

Лемма 3.2. *Пусть B – симметричная билинейная форма на V, а $v_1, \dots, v_k \in V$. Если $B(v_i, v_i) > 0$ при всех i, а $B(v_i, v_j) = 0$ при всех $j \neq i$, то форма B положительно определена на подпространстве $\langle v_1, \dots, v_k \rangle$.*

Теорема 3.3 (закон инерции квадратичных форм). *Пусть Q – квадратичная форма на вещественном векторном пространстве V, а u, v – базисы V такие, что матрицы Q_u и Q_v диагональны. Тогда сигнатуры матриц Q_u и Q_v равны.*

Доказательство. По предложению 2.2 можно считать, что форма Q невырождена. Пусть (p_u, n_u) – сигнатура матрицы Q_u, а (p_v, n_v) – сигнатура матрицы Q_v. Перенумеровав при необходимости базисные элементы, можно считать, что положительные диагональные элементы матриц Q_u и Q_v стоят выше (и левее) отрицательных.

Предположим, что $p_u > p_v$. По предыдущей лемме форма Q положительно определена на подпространстве $U = \langle u_1, \dots, u_{p_u} \rangle$. Аналогично, Q отрицательно определена на $W = \langle v_{p_v+1}, \dots, v_m \rangle$. Но по теореме о размерности суммы и пересечения

$$\dim U \cap W = p_u + (m - p_v) - \dim(U + W) \geqslant p_u + (m - p_v) - m = p_u - p_v > 0.$$

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

В соответствие с законом инерции можно дать следующее определение. Сигнатурой квадратичной формы называется сигнатура ее матрицы в таком базисе, в котором эта матрица диагональна. Сигнатуру квадратичной формы Q будем обозначать через $\operatorname{Sign} Q$.

Следствие 3.4 (классификация вещественных квадратичных форм). *Два вещественных квадратичных пространства (V, Q) и (V', Q') изометричны тогда и только тогда, когда $\dim V = \dim V'$, а $\operatorname{Sign} Q = \operatorname{Sign} Q'$.*

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

Теорема 3.5 (критерий Сильвестра). *Пусть Q – квадратичная форма на V, а A – матрица формы Q. Предположим, что главные миноры $\Delta_1, \dots, \Delta_m$ матрицы A не равны нулю. Тогда сигнатура формы Q равна сигнатуре последовательности $(\frac{\Delta_1}{\Delta_0}, \dots, \frac{\Delta_m}{\Delta_{m-1}})$.*

В частности, форма положительно определена тогда и только тогда, когда все ее главные миноры больше 0.

Доказательство. По лемме 12.6 главы 2 матрица A лежит в главной клетке Гаусса, т. е. $A = BDC$, где B – нижняя унитреугольная матрица, C – верхняя унитреугольная, а D – диагональная. Так как A симметрична, то $BDC = (BDC)^\intercal = C^\intercal D B^\intercal$, откуда $B^{-1} C^\intercal D = D C (B^\intercal)^{-1}$. Но последняя матрица одновременно нижняя и верхняя треугольная, следовательно $B^{-1} C^\intercal = E$, т. е. $B = C^\intercal$. Это означает, что D – матрица той же квадратичной формы Q в другом базисе, а ее сигнатура совпадает с сигнатурой формы Q.

Аналогично лемме 12.5 главы 2 главные миноры матриц A и D совпадают. Действительно, при умножении матрицы слева на унитреугольную главные подматрицы также умножаются на унитреугольные (это просто блочное умножение матриц) и, значит, их определители не меняются. Следовательно, $\Delta_k = d_{11} \dots d_{kk}$, откуда $d_{kk} = \Delta_k/\Delta_{k-1}$. Таким образом, последовательность из формулировке равна последовательности диагональных элементов матрицы D.

Если все главные миноры положительны, то в любой диагонализации формы Q все диагональные элементы положительны. По лемме 3.2 из этого следует, что форма положительно определена. Обратно, если Q положительно определена, то все диагональные элементы матрицы этой формы в любом базисе положительны. □

Замечание 3.6. Рассмотрим эрмитову форму B на комплексном векторном пространстве (инволюция – комплексное сопряжение). В соответствие с замечанием 1.8 диагональные элементы и главные миноры любой матрицы этой формы лежат в $\mathbb{R}$, поэтому для этой формы имеют смысл все утверждения настоящего параграфа. На самом деле все эти утверждения верны, а доказательства повторяют доказательства для вещественного случая с необходимыми уточнениями.

4. Пространства со скалярным произведением

В этом параграфе мы рассмотрим случай вещественных (комплексных) векторных пространств с положительно определенной симметричной билинейной (соотв. эрмитовой) формой, при этом инволюция на поле комплексных чисел – это обычное комплексное сопряжение. Можно рассматривать эти 2 случая одновременно, считая, что V – векторное пространство над полем $F = \mathbb{R}$ или $\mathbb{C}$, а в вещественном случае инволюция тривиальна. Для эрмитовой формы B и $x \in V$ имеем $B(x,x) = \overline{B(x,x)}$, откуда $B(x,x) \in \mathbb{R}$.

Определение 4.1. Эрмитова форма называется положительно определенной, если $B(x,x) > 0$ для любого вектора $x \neq 0$. Положительно определенная эрмитова форма называется (эрмитовым) скалярным произведением. В вещественным случае эрмитовость означает симметричность и билинейность, а скалярное произведение называется евклидовым. Конечномерное векторное пространство со скалярным произведением называется евклидовым или (классическим) эрмитовым пространством.

Квадратичная форма Q над произвольным полем называется анизотропной, если $Q(x) \neq 0$ при $x \neq 0$. Аналогично, мы будем говорить, что эрмитова форма B анизотропна, если $B(x,x) \neq 0$ при $x \neq 0$. В частности, скалярное произведение, является анизотропной формой. Позже мы узнаем, что для классификации квадратичных форм достаточно классифицировать анизотропные формы, так что они занимают особое место в теории квадратичных форм. По определению скалярное произведение является анизотропной формой, поэтому все утверждения, в которых не используется специфика поля вещественных или комплексных чисел[1] будут доказаны для произвольных анизотропных форм.

В дальнейшем скалярное произведение будет обозначаться просто (x,y) вместо $B(x,y)$, а матрица этой формы будет называться матрицей Грама и обозначаться через Γ или Γ_v, где v – базис. Соответствующая квадратичная форма будет обозначаться через $\|x\|^2 = (x,x)$. Другими словами, $\|x\| = \sqrt{(x,x)}$, что имеет смысл за счет положительной определенности.

Как следует из предложения 1.5, любое скалярное произведение на F^n имеет вид $(x,y) = x^*\Gamma y$, где $\Gamma \in \mathrm{M}_n(F)$ – матрица Грама в стандартном базисе. Эта формула всегда задает полуторалинейную форму, эрмитовость такой формы равносильна эрмитовости матрицы Γ, а положительная определенность, как мы узнаем чуть позже, – положительности собственных чисел Γ. В случае $\Gamma = E$ такое скалярное произведение называется стандартным.

Теорема 4.2. *Пусть V – векторное пространство (не обязательно конечномерное) со скалярным произведением. Тогда для любых $x, y \in V$ имеют место неравенства:*

[1] Эта специфика чаще всего проявляется в наличии неравенств.

(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 $(x,y) + (y,x) \leqslant 2\|x\|\|y\|$. Так как $(y,x) = \overline{(x,y)}$, левая часть равна $2\operatorname{Re}(x,y)$. Но $\operatorname{Re}(x,y) \leqslant |(x,y)| \leqslant \|x\| \cdot \|y\|$ по неравенству КБШ, откуда следует последнее неравенство. □

Следующие несколько утверждений верны для произвольной анизотропной эрмитовой формы B.

Лемма 4.3. *Набор ненулевых попарно B-ортогональных векторов линейно независим.*

Теорема 4.4 (ортогонализация Грама–Шмидта). *Пусть B – анизотропная форма на V, $u_1, \dots, u_n \in V$. Положим*

$$\begin{aligned} v_1 &= u_1 \\ v_2 &= u_2 - v_1\frac{B(v_1,u_2)}{B(v_1,v_1)} \\ &\dots\dots\dots\dots \\ v_n &= u_n - \sum_{i=1}^{n-1} v_i\frac{B(v_i,u_n)}{B(v_i,v_i)} \end{aligned}$$

(если $v_i = 0$, то соответствующее слагаемое отсутствует; строго говоря, надо было бы писать, что коэффициент при v_i в формуле для v_k равен 0, в случае $v_i = 0$, и $\frac{B(v_i,u_k)}{B(v_i,v_i)}$ в противном случае). Тогда для любых $i, j, k \in \{1, \dots, n\}$, $i \neq j$ выполнены следующие утверждения.

(1) $B(v_i, v_j) = 0$.
(2) $\langle u_1, \dots, u_k\rangle = \langle v_1, \dots, v_k\rangle$.
(3) *Если $u_1, \dots, u_k$ линейно независимы, то и $v_1, \dots, v_k$ линейно независимы, в частности, $v_m \neq 0$ при всех $m = 1, \dots, k$.*
(4) *Если $u_k \in \langle u_1, \dots, u_{k-1}\rangle$, то $v_k = 0$.*
(5) *Если $(u_1, \dots, u_n)$ – система образующих V, то ненулевые из векторов $v_1, \dots, v_n$ образуют базис.*
(6) *Если $(u_1, \dots, u_n)$ – базис V, то $(v_1, \dots, v_n)$ – B-ортогональный базис V.*

Процесс ортогонализации – конструктивный способ построения ортогонального базиса пространства, существование которого мы уже доказали для произвольной эрмитовой формы в теореме 2.5. На самом деле доказательство теоремы 2.5 для анизотропной формы совпадает с процессом ортогонализации. В случае скалярного произведения можно сделать нормы всех базисных векторов равными 1. Такой базис будет называться ортонормированным.

В следующем утверждении в качестве B традиционно рассматривается стандартное скалярное произведение на F^m, хотя на самом деле это не имеет никакого значения. Для доказательства достаточно применить процесс ортогонализации к столбцам матрицы A.

Следствие 4.5 (QR-разложение). *Пусть B – анизотропная эрмитова форма на F^m. Для любой матрицы $A \in \mathrm{M}_{m,n}(F)$ существует матрица $Q \in \mathrm{M}_{m,n}(F)$ с B-ортогональными столбцами и верхняя унитреугольная матрица $R \in \mathrm{M}_n(F)$ такие, что $A = QR$.*

Для подпространства $U \leqslant V$ определим ортогональное дополнение U формулой

$$U^{\perp_B} = U^\perp = \{x \in V \mid B(y,x) = 0 \,\forall y \in U\}.$$

Нетрудно видеть, что сужение формы B на U невырождено тогда и только тогда, когда $U \cap U^\perp = \{0\}$. В конечномерном пространстве из подсчета размерностей сразу следует, что в этом случае ортогональное дополнение является и прямым дополнением.

Предложение 4.6. *Пусть B невырожденная эрмитова форма на конечномерном пространстве V, а $U \leqslant V$. Тогда $\dim U^\perp = \dim V - \dim U$ и $(U^\perp)^\perp = U$.*

Если сужение B на U невырождено, то $V = U \oplus U^\perp$. В частности, если B анизотропна, то равенства выполнены для любого подпространства U.

Доказательство. Пусть $u = (u_1, \dots, u_k)$ – базис U, а $L : V \to F^k$ – линейное отображение, заданное формулой $L(x) = \big(B(u_1,x), \dots, B(u_k,x)\big)^\intercal$. Ясно, что $U^\perp = \operatorname{Ker} L$. Если v – базис V, то можно записать наше отображение в координатной форме: $L(x) = CB_v x_v$, где $C = \big(\overline{(u_1)_v}, \dots, \overline{(u_k)_v}\big)^\intercal$. Так как набор u линейно независим, ранг матрицы C равен k. Так как B невырождена, матрица B_v обратима и умножение на нее не меняет ранга матрицы. Следовательно, размерность образа оператора L равна k, а по теореме о размерности ядра и образа $\dim \operatorname{Ker} L = \dim V - k$.

Очевидно, что $U \leqslant (U^\perp)^\perp$. С другой стороны, из доказанного следует, что их размерности равны, откуда вытекает второе равенство.

Если $B|_U$ невырождена, то $U \cap U^\perp = \{0\}$, откуда $U \oplus U^\perp \leqslant V$. Но мы уже доказали, что $\dim U + \dim U^\perp = \dim V$, следовательно, $U \oplus U^\perp = V$. □

Вернемся к ситуации, когда форма анизотропна. Тогда другое доказательство того, что $V = U + U^\perp$ дает процесс ортогонализации, примененный к последовательности $(u_1, \dots, u_k, x)$, где x произвольный элемент из V. Действительно, на последнем шаге мы получим вектор $y \in x + U$, ортогональный U, откуда $x \in y + U \subseteq U^\perp + U$.

Из последнего предложения следует, что каждый вектор $x \in V$ единственным образом представляется в виде $x = z + y$, где $z \in U$, а $y \in U^\perp$. В этом случае элемент z называется ортогональной проекцией x на U. Мы будем обозначать его $\operatorname{pr}_U x$. Проекция на вектор – это проекция на подпространство, порожденное этим вектором. Легко видеть, что

$$\operatorname{pr}_z x = \frac{(z,x)}{(z,z)} z.$$

В этих терминах формулу процесса ортогонализации можно произнести следующим образом: новый вектор v_k равен разности старого u_k и его проекций на все вектора, найденные на предыдущих шагах.

Обратите внимание, что если u является ортогональным базисом подпространства U, то $\operatorname{pr}_U x = \sum_{j=1}^k \operatorname{pr}_{u_j} x$, если же базис u не ортогонален, то такое равенство может выполняться только случайно.[2]

Предложение 4.7 (равенство Парсеваля и неравенство Бесселя). *Пусть $u_1, \dots, u_k$ – ортогональный набор ненулевых векторов пространства V со скалярным произведением, а $x \in V$. Обозначим через U линейную оболочку векторов $u_1, \dots, u_k$. Тогда*

(1) $\operatorname{pr}_U x = \sum\limits_{j=1}^k \operatorname{pr}_{u_j} x = \sum\limits_{j=1}^k \frac{(u_j,x)}{(u_j,u_j)} u_j$;

(2) $\|x\|^2 \geqslant \|\operatorname{pr}_U x\|^2 = \sum\limits_{j=1}^k \frac{|(u_j,x)|^2}{(u_j,u_j)}$ *(неравенство Бесселя);*

(3) *равенство в последней формуле имеет место тогда и только тогда, когда $x \in U$ (равенство Парсеваля).*

[2] *Упражнение.* Найдите условие на u равносильное существованию ненулевого x, для которого равенство верно.

Доказательство. Пусть $z = \mathrm{pr}_U x = \sum_{j=1}^{k} u_j \alpha_j$. Тогда $x = z + y = \sum_{j=1}^{k} u_j \alpha_j + y$ для некоторого $y \in U^\perp$. Домножая выражение для x скалярно (слева) на u_l, получаем формулу для α_l, откуда следует первый пункт предложения.

Так как набор $u_1, \ldots, u_k$ ортогонален, то скалярный квадрат правой части выражения для z равен сумме скалярных квадратов слагаемых. Следовательно, правая часть неравенства Бесселя равна $\|z\|^2$. Но $\|x\|^2 = \|z + y\|^2 = \|z\|^2 + \|y\|^2 \geqslant \|z\|^2$, причем равенство достигается, только если $y = 0$. □

Неравенство Бесселя является всего лишь выражением того факта, что длина гипотенузы не меньше длины катета. Следующее утверждение сравнивает длину гипотенузы того же прямоугольного треугольника с длиной другого катета.

Предложение 4.8. *Для любого $u \in U$ выполнено неравенство $\|x - u\| \geqslant \|x - \mathrm{pr}_U x\|$.*

Доказательство. Пусть $x = z + y$, где $z = \mathrm{pr}_U x$, а $y \in U^\perp$. Тогда для любого $u \in U$:

$$\|x - u\|^2 = \|y + (z - u)\|^2 = \|y\|^2 + \|z - u\|^2 \geqslant \|y\|^2 = \|x - \mathrm{pr}_U x\|^2.$$

□

До конца параграфа $V = F^m$ пространство со стандартным скалярным произведением.

Лемма 4.9. *Пусть $A \in \mathrm{M}_{m,n}(F)$ – матрица с линейно независимыми столбцами. Тогда матрица A^*A невырождена.*

Доказательство. Если $U \leqslant V$ – подпространство, порожденное столбцами матрицы A, то A^*A – матрица Грама сужения скалярного произведения на $U \times U$. Так как наше скалярное произведение невырождено на любом подпространстве, то эта матрица невырождена. □

Теорема 4.10 (метод наименьших квадратов). *Пусть $A \in \mathrm{M}_{m,n}(F)$ – матрица с линейно независимыми столбцами, а $b \in F^m$. Тогда $\|Ax - b\|$ минимальна, если $x \in F^n$ удовлетворяет уравнению $A^*Ax = A^*b$. (заметим, что по предыдущей лемме такой вектор x всегда существует и единственный).*

Доказательство. Для любого $y \in F^n$

$$(Ay, Ax - b) = y^*(A^*Ax - A^*b) = 0.$$

Таким образом, вектор $Ax - b$ ортогонален подпространству, порожденному столбцами матрицы A, т. е. Ax является ортогональной проекцией b на это подпространство. Теперь результат следует из предложения 4.8. □

5. Нормальные операторы

Определение 5.1. Пусть V – векторное пространство над произвольным полем F. Множество линейных отображений из V в F

$$V^* := \mathrm{Hom}_F(V, F)$$

с поточечными операциями называется пространством, двойственным к V (dual space).

Пусть U и V – векторные пространства, а $L : U \to V$ – линейное отображение. Тогда сопряженное отображение $L^* : V^* \to U^*$ задается формулой $L^*(\varphi) = \varphi \circ L$.

Если V конечномерно, то при помощи выбора базиса его можно отождествить с F^n. Тогда любое линейное отображение $V \to F$ – это умножение слева на строку длины n, следовательно, V^*

отождествляется с ${}^nF$. Так как эти пространства имеют одинаковую размерность, то они изоморфны.[3] В случае бесконечномерных пространств это совсем не так, например базис пространства, двойственного к счетномерному, имеет мощность континуум.

Далее на протяжении этого параграфа пространство V конечномерно. Любая невырожденная полуторалинейная форма B задает полулинейную биекцию пространства на его сопряженное. А именно, для $x \in V$ положим $\varphi_x(y) = B(x,y)$. Тогда $\varphi_x \in V^*$, а $x \mapsto \varphi_x$ – искомая биекция. Действительно, невырожденность формы B равносильна тривиальности ядра этого отображения; ясно, что отображение полулинейно, т. е. $\varphi_{x+z} = \varphi_x + \varphi_z$ и $\varphi_{\alpha x} = \overline{\alpha}\varphi_x$; а сюръективность следует из теоремы о размерности ядра и образа, которая верна и для полулинейных отображений. Большую часть утверждений настоящего параграфа можно сформулировать для эрмитовых пространств над произвольным полем. Мы, однако, оставим эти обобщения в качестве упражнения и будем рассматривать только евклидовы и классические эрмитовы пространства.

Если U и V эрмитовы пространства, то мы можем отождествить их со своими двойственными при помощи полулинейной биекции, определенной в предыдущем абзаце. Тогда L^* отождествляется с линейным отображением $L^\star : V \to U$, для которого следующая диаграмма коммутативна.

$$\begin{array}{ccc} V & \xrightarrow{L^\star} & U \\ {\scriptstyle x\mapsto\varphi_x}\downarrow & & \downarrow{\scriptstyle y\mapsto\varphi_y} \\ V^* & \xrightarrow{L^*} & U^* \end{array}$$

Обратите внимание, что пока мы различаем $L^* : V^* \to U^*$ и $L^\star : V \to U$ (у них разные символы “звездочка”).

Лемма 5.2. *Определенное выше отображение $L^\star$ удовлетворяет равенству*

$$\big(L^\star(x), y\big)_U = \big(x, L(y)\big)_V \tag{8}$$

и $L^{\star\star} = L$.

Доказательство. Пусть $x \in V$. Тогда коммутативность диаграммы говорит, что $L^*(\varphi_x) = \varphi_{L^\star(x)}$. Применяя обе части равенства к элементу $y \in U$ получим

$$L^*(\varphi_x)(y) = \varphi_x\big(L(y)\big) = \big(x, L(y)\big)_V = \varphi_{L^\star(x)}(y) = \big(L^\star(x), y\big)_U.$$

Далее,

$$\big(x, L(y)\big)_V = \big(L^\star(x), y\big)_U = \overline{\big(y, L^\star(x)\big)_U} = \overline{\big(L^{\star\star}(y), x\big)_V} = \big(x, L^{\star\star}(y)\big)_V.$$

Так как последнее равенство выполнено для любого $x \in V$, а скалярное произведение невырождено, то $L(y) = L^{\star\star}(y)$ для любого $y \in U$, что и означает $L^{\star\star} = L$. □

Последняя лемма говорит в частности, что отображение $L^\star$, удовлетворяющее равенству (8) существует. Единственность такого отображения очевидна (см. конец доказательства предыдущей леммы). Таким образом, мы получаем 2 равносильных определения оператора $L^\star$, ни одно из которых не выглядит конструктивным, так как в каждом из них надо искать вектор, скалярное умножение на который реализует данный линейный функционал. В действительности же, для нахождения такого вектора надо просто решить систему линейных уравнений.

В дальнейшем, мы меняем обозначение $L^\star$ на общепринятое L^*. Какой из операторов имеется в виду $V \to U$ или $V^* \to U^*$, всегда будет ясно из контекста. Обратите внимание, что первая версия L^* употребляется, только если зафиксированы изоморфизмы между пространствами и сопряженными к ним, в частности, если U и V – эрмитовы (квадратичные) пространства или если там зафиксированы базисы. В этом и следующем параграфах L^* обозначает оператор $V \to U$.

Лемма 5.3. *Пусть u – ортонормированный базис эрмитова пространства V, а $L : V \to V$. Тогда $(L^*)_u = (L_u)^*$.*

[3] Это первый пример в нашем курсе неканонического изоморфизма, т. е. изоморфизма, который зависит от какого-то выбора.

Доказательство. $\big(y, L^*(x)\big) = \big(L(y), x\big)$. Так как базис u ортонормирован, то $(z,t) = z_u^* t_u$. Используя это и определение матрицы оператора получим $y_u^*(L^*)_u x_u = (L_u y_u)^* x_u = y_u^*(L_u)^* x_u$. Так как x_u и y_u – произвольные столбцы, получаем требуемое равенство матриц. □

Определение 5.4. Оператор $L : V \to V$ называется самосопряженным или эрмитовым, если $L^* = L$.

Изоморфизм $L : U \to V$ называется унитарным или изометрией, если $L^* = L^{-1}$.

Оператор $L : V \to V$ называется нормальным, если $L^*L = LL^*$.

Таким образом, нормальные операторы является одновременным обобщением таких важных типов, как самосопряженные и унитарные операторы (а на самом деле еще и косоэрмитовы, т. е. те, для которых $L^* = -L$). Следующее утверждение говорит о связи эрмитовых форм и самосопряженных операторов.

Лемма 5.5. *Пусть $L : V \to V$ – линейный оператор, а $B = B_L$ – полуторалинейная форма, заданная равенством $B(x,y) = \big(x, L(y)\big)$. Оператор L является самосопряженным тогда и только тогда, когда форма B эрмитова. При этом $B_u = L_u$ в любом ортонормированном базисе u.*

Теорема 5.6. *Для любого нормального оператора существует ортонормированный базис из собственных векторов.*

Собственные вектора нормального оператора, соответствующие различным собственным числам, ортогональны.

Собственные числа самосопряженного оператора вещественны.

Собственные числа унитарного оператора по модулю равны 1.

Доказательство первого утверждения опирается на 2 леммы.

Лемма 5.7. *Если $AB = BA$, то собственное подпространство оператора A инвариантно относительно B.*

Доказательство. Если $Ax = \lambda x$, то $A(Bx) = B(Ax) = B(\lambda x) = \lambda Bx$, т. е. Bx принадлежит тому же собственному подпространству, что и x. □

Лемма 5.8. *Если $U \leqslant V$ инвариантно относительно оператора $L : V \to V$, то $U^\perp$ инвариантно относительно L^*.*

Доказательство. Пусть $x \in U^\perp$, а y – произвольный вектор из U. Так как $L(y) \in U$, то $\big(L^*(x), y\big) = \big(x, L(y)\big) = 0$. Таким образом, $L^*(x) \in U^\perp$. □

Доказательство теоремы 5.6. Пусть L – нормальный оператор в эрмитовом пространстве V. Проведем доказательство индукцией по $\dim V$. Так как $\mathbb{C}$ алгебраически замкнуто, то существует хотя бы один корень характеристического многочлена, следовательно, хотя бы одно ненулевое собственное подпространство V_λ. Так как $LL^* = L^*L$, то по лемме 5.7 V_λ инвариантно относительно L^*. Теперь по лемме 5.8 $V_\lambda^\perp$ инвариантно относительно $L^{**} = L$. Размерность пространства $V_\lambda^\perp$ строго меньше $\dim V$, поэтому к нему можно применить индукционное предположение. Выберем ортогональный базис $(v_1, \dots, v_k)$ подпространства $V_\lambda^\perp$ из собственных векторов оператора L и ортогональный базис $(v_{k+1}, \dots, v_n)$ подпространства V_λ. Тогда $(v_1, \dots, v_n)$ – искомый базис пространства V.

Из доказанного следует, что собственные подпространства нормального оператора попарно ортогональны, откуда вытекает второе утверждение.

Пусть $L(x) = \lambda x$ для некоторого $x \neq 0$. Если $L = L^*$, то

$$\bar\lambda\big(x,x\big) = \big(L(x), x\big) = \big(x, L(x)\big) = \lambda\big(x,x\big),$$

откуда $\bar\lambda = \lambda$, т. е. $\lambda \in \mathbb{R}$.

Аналогично, если $L^{-1} = L^*$, то

$$\bar\lambda\lambda\big(x,x\big) = \big(L(x),L(x)\big) = \big(x,x\big).$$

Сокращая на (x,x), получаем $|\lambda|^2 = \bar\lambda\lambda = 1$. □

На самом деле условия, собранные в теореме 5.6 являются характеризациями соответствующих типов операторов. Следствие в одну сторону доказано в теореме, а обратное сразу следует из леммы 5.3.

Следствие 5.9. *Оператор L является нормальным тогда и только тогда, когда существует ортогональный базис из его собственных векторов. При этом он самосопряжен тогда и только тогда, когда его собственные числа вещественные, и является унитарным тогда и только тогда, когда его собственные числа по модулю равны* 1.

Следующее утверждение является частным случаем спектральной теоремы, которая говорит о строении самосопряженных операторов в гильбертовых пространствах. Она формулируется в терминах ортогональных проекторов.

Определение 5.10. Оператор $P : V \to V$ называется проектором, если $P^2 = P$. Если $\operatorname{Ker} P \perp \operatorname{Im} P$, то проектор P называется ортогональным.

Если P – проектор в произвольном векторном пространстве V, то $V = \operatorname{Ker} P \oplus \operatorname{Im} P$. Действительно, $P(x-P(x)) = 0$, т. е. $x - P(x) \in \operatorname{Ker} P$, следовательно, $x = x - P(x) + P(x) \in \operatorname{Ker} P + \operatorname{Im} P$; с другой стороны, $P(x) \in \operatorname{Ker} P \implies P(x) = P^2(x) = 0$, откуда $\operatorname{Im} P \cap \operatorname{Ker} P = \{0\}$. Отсюда следует, что для ортогонального проектора P имеет место равенство $\operatorname{Ker} P = (\operatorname{Im} P)^\perp$. Нетрудно видеть, что ортогональный проектор является самосопряженным оператором.

Следствие 5.11 (спектральная теорема). *Оператор L в евклидовом (эрмитовом) пространстве V является самосопряженным тогда и только тогда, когда он представляется в виде линейной комбинации ортогональных проекторов на попарно ортогональные подпространства с вещественными коэффициентами.*

Эти ортогональные подпространства можно считать одномерными, порожденными собственными векторами $u_1, \dots, u_n$ оператора L. Тогда

$$L = \sum_{k=1}^{n} \lambda_k P_k, \ \text{где } P_k(x) = \operatorname{pr}_{u_k} x = \frac{(u_k,x)}{(u_k,u_k)} u_k.$$

Доказательство. Очевидно, что линейная комбинация самосопряженных операторов с вещественными коэффициентами является самосопряженным оператором. Обратно, по теореме 5.6 существует ортогональный базис из собственных векторов $u_1, \dots, u_n$ оператора L. По формуле "координаты в ортогональном базисе" (теорема 4.7(1)) $x = \sum_{k=1}^{n} \frac{(u_k,x)}{(u_k,u_k)} u_k$, откуда

$$L(x) = \sum_{k=1}^{n} \frac{(u_k,x)}{(u_k,u_k)} L(u_k) = \sum_{k=1}^{n} \lambda_k \frac{(u_k,x)}{(u_k,u_k)} u_k.$$

При этом мы уже доказывали, что формула $P_k(x) = \operatorname{pr}_{u_k} x = \frac{(u_k,x)}{(u_k,u_k)} u_k$ задает ортогональный проектор на $\langle u_k \rangle$, что доказывает оба утверждения. □

Проекторы на собственные вектора, соответствующие одному и тому же собственному числу, можно собрать в один проектор на собственное подпространство. Так что можно выразить самосопряженный оператор через линейную комбинацию проекторов на его собственные подпространства.

Следствие 5.12. *Для любой эрмитовой формы в эрмитовом пространстве V существует ортонормированный базис, в котором матрица этой формы диагональна.*

Для любой квадратичной формы в евклидовом пространстве V существует ортонормированный базис, в котором матрица этой формы диагональна.

Доказательство. Пусть $L : V \to V$ – самосопряженный оператор, соответствующий данной форме. По теореме 5.6 существует ортогональный базис из собственных векторов этого оператора. Нормируя эти вектора (что не портит их ортогональности и "собственности") получаем ортонормированный базис из собственных векторов. В этом базисе из собственных векторов матрица оператора диагональна, а по лемме 5.5 она равна матрице исходной формы.

В евклидовом пространстве надо только заметить, что, так как собственные числа оператора L вещественны, то и у него существуют собственные вектора в исходном пространстве, а дальше повторить доказательство теоремы 5.6 для евклидова случая. □

6. Матричные разложения

В этом параграфе снова F – это поле вещественных или комплексных чисел.

Определение 6.1. Самосопряженный оператор называется положительно (неотрицательно) определенным, если все его собственные числа положительны (неотрицательны). Это равносильно тому, что эрмитова форма, заданная этим оператором, положительно (неотрицательно) определена.

Эрмитова матрица $A \in \mathrm{M}_n(\mathbb{C})$ называется положительно (неотрицательно) определенной, если эрмитова форма $B(x, y) = x^*Ay$ положительно (неотрицательно) определена.

Для диагональной матрицы $D \in \mathrm{M}_n(\mathbb{R})$ с неотрицательными диагональными элементами положим $\sqrt{D} = \mathrm{diag}(\sqrt{d_{11}}, \ldots, \sqrt{d_{nn}})$ (берутся арифметические квадратные корни). Сейчас мы определим, точнее, докажем корректность определения квадратного корня из произвольной неотрицательно определенной эрмитовой матрицы. Это утверждение понадобится для доказательства единственности полярного разложения. Обобщение этого утверждения на другие полиномиальные матричные уравнения (вместо $X^2 = A$) оставляется читателю в качестве упражнения.

Лемма 6.2. *Пусть $A \in \mathrm{M}_n(\mathbb{C})$ – неотрицательно определенная эрмитова матрица. Тогда существует единственная неотрицательно определенная эрмитова матрица $H \in \mathrm{M}_n(\mathbb{C})$ такая, что $H^2 = A$.*

Доказательство. По теореме 5.6 существует матрица $C \in \mathrm{GL}_n(\mathbb{C})$ такая, что $A = C^{-1}DC$, где D диагональна с неотрицательными диагональными элементами. Тогда $H = C^{-1}\sqrt{D}C$ удовлетворяет условиям леммы.

Обратно, если H удовлетворяет условиям леммы, то $H = G^{-1}\bar{D}G$ для некоторой матрицы $G \in \mathrm{GL}_n(\mathbb{C})$ и диагональной $\bar{D}$ с неотрицательными элементами по диагонали. Тогда $H^2 = G^{-1}\bar{D}^2G = C^{-1}DC$. Поэтому собственные числа матриц $\bar{D}^2$ и D и их кратности совпадают. Меняя при необходимости порядок собственных векторов матриц A и H можно считать, что $\bar{D}^2 = D = \mathrm{diag}(\lambda_1 E, \ldots, \lambda_k E)$, где $\lambda_j \neq \lambda_l$ при $j \neq l$. Из выражения для H^2 получаем $(CG^{-1})D = D(CG^{-1})$. Вычисление показывает, что CG^{-1} – блочно диагональная матрица с блоками тех же размеров, что и диагональные блоки матрицы D. Заметим, что $\bar{D} = \mathrm{diag}(\sqrt{\lambda_1}E, \ldots, \sqrt{\lambda_k}E)$ также коммутирует с любой такой блочно диагональной матрицей, откуда $H = G^{-1}\bar{D}G = C^{-1}\bar{D}C$ – единственная матрица с неотрицательными собственными числами, удовлетворяющая равенству $H^2 = A$. □

Теорема 6.3 (разложение Холецкого). *Любая положительно определенная эрмитова матрица $A \in \mathrm{M}_n(\mathbb{C})$ представляется в виде произведения $A = C^*C$, для некоторой верхнетреугольной матрицы C с положительными диагональными элементами. При этом матрица C определена единственным образом.*

Доказательство. Пусть $B(x, y) = x^*Ay$ – эрмитова форма на $\mathbb{C}^n$. Ее матрица в стандартном базисе $B_e = A$. По определению положительная определенность A равносильна положительной определенности B. По теореме 2.5 существует базис, в котором эта форма диагональна, а так как она положительно определена, то диагональные элементы вещественны и положительны. Домножая базисные вектора на соответствующие вещественные константы можно

добиться того, чтобы эта матрица стала единичной. Если u такой базис $\mathbb{C}^n$, что $B_u = E$, то $A = B_e = C^*_{u\to e} B_u C_{u\to e} = C^*_{u\to e} C_{u\to e}$. По QR-разложению $C_{u\to e} = QC$ для некоторой матрицы Q с ортонормированными столбцами и верхнетреугольной матрицы C с положительными элементами по диагонали. Тогда $A = (QC)^*QC = C^*Q^*QC = C^*C$.

На самом деле, это доказательство равносильно применению процесса ортогонализации Грама–Шмидта относительно скалярного произведения B к векторам стандартного базиса. Действительно, процесс ортогонализации (вместе с нормированием) говорит, что умножая стандартный базис на верхнетреугольную матрицу с положительными диагональными элементами, можно получить базис v, ортонормированный относительно B. Это означает, что $B_v = E$, а $C_{e\to v}$ верхнетреугольная, откуда $A = B_e = C^*_{e\to v} C_{e\to v}$.

Другое доказательство существования вытекает из разложения Гаусса и совпадает с началом доказательства критерия Сильвестра. А именно, так как форма $B(x, y) = x^*Ay$ положительно определена, то все главные миноры ее матрицы в любом базисе положительны. Следовательно, по лемме 12.6 главы 2 A лежит в главной клетке Гаусса, т. е. $A = GDH$ для некоторой верхней унитреугольной матрицы H, диагональной матрицы D и нижней унитреугольной матрицы G. Так как $A = A^*$, то $GDH = H^*D^*G^*$ откуда $(H^*)^{-1}GD = D^*G^*H^{-1}$. Последняя матрица является одновременно верхней и нижней треугольной, следовательно, $G = H^*$ и $D = D^*$. Из положительной определенности сразу следует, что диагональные элементы матрицы D положительны. Следовательно, $A = (H^*\sqrt{D})(\sqrt{D}H)$ – искомое разложение.

Единственность следует из единственности разложения Гаусса. Если $C^*C = \bar{C}^*\bar{C}$ для некоторых верхнетреугольных матриц $C, \bar{C}$ с положительными диагональными элементами, то матрица $(\bar{C}^*)^{-1}C^* = \bar{C}C^{-1}$ верхнетреугольна и нижнетреугольна одновременно, следовательно, она диагональна. То есть $\bar{C} = LC$ для некоторой диагональной матрицы L. Так как диагональные элементы C и $\bar{C}$ положительны, то L обладает тем же свойством. Кроме того, $C^*C = \bar{C}^*\bar{C} = (LC)^*LC = C^*(L^*L)C$, откуда $L^*L = L^2 = E$. Таким образом, $L = E$ и $\bar{C} = C$. □

Теорема 6.4 (сингулярное разложение). *Любая матрица $A \in \mathrm{M}_{m,n}(\mathbb{C})$ представляется в виде произведения $A = BDC$, где B и C – квадратные унитарные матрицы, а $D \in \mathrm{M}_{m,n}(\mathbb{C})$ диагональна (т. е. $d_{ij} = 0$ при всех $i \neq j$) с неотрицательными элементами по диагонали.*

На языке линейных отображений это же утверждение звучит следующим образом.

Для любого линейного отображения $L : U \to V$, где U и V – классические эрмитовы пространства, существуют ортонормированные базисы u и v пространств U и V соответственно, в которых матрица $D = L^u_v$ оператора L диагональна с неотрицательными элементами по диагонали.

При этом диагональные элементы матрицы D определены однозначно с точностью до перестановки и равны корням из собственных чисел матрицы A^*A (соотв. оператора L^*L) или 0.

Доказательство. Пусть u и v ортонормированные базисы пространств U и V соответственно. Матрица L^u_v диагональна с элементами α_i по диагонали тогда и только тогда, когда $L(u_i) = \alpha_i v_i$ или $L(u_i) = 0$ (последнее существенно, если $\dim U > \dim V$). Ортогональность базиса v влечет $\big(L(u_i), L(u_j)\big) = 0$ при всех $i \neq j$. Перепишем последнее равенство в виде $\big(L^*L(u_i), u_j\big) = 0$, т. е. вектор $L^*L(u_i)$ лежит в ортогональном дополнении подпространства, порожденного всеми u_j при $j \neq i$. Заметим, что это ортогональное дополнение одномерно и содержит u_i. Следовательно, $L^*L(u_i) = \lambda_i u_i$. Таким образом, если сингулярное разложение оператора существует, то u_i – собственные вектора оператора L^*L. Этот оператор самосопряженный и неотрицательно определенный, поэтому все λ_i – вещественные неотрицательные числа. Так как $\|v_i\| = 1$, а $\alpha_i > 0$, то $\alpha_i = \|L(u_i)\|$. Имеем

$$\alpha_i^2 = \big(L(u_i), L(u_i)\big) = \big(L^*L(u_i), u_i\big) = \lambda_i\big(u_i, u_i\big) = \lambda_i.$$

Мы доказали, что если сингулярное разложение существует, то матрица D определена единственным образом с точностью до перестановки диагональных элементов.

По теореме 5.6 существует ортонормированный базис из собственных векторов оператора L^*L. Расположим эти вектора так, чтобы $u_1, \dots, u_k$ соответствовали ненулевым собственным числам, а остальные – собственному числу 0. Тогда при $i > k$ имеем $0 = \big(L^*L(u_i), u_i\big) = \big(L(u_i), L(u_i)\big)$, откуда $L(u_i) = 0$. Вектора $v_j = \frac{L(u_j)}{\|L(u_j)\|}$ при $j \leqslant k$ образуют базис образа оператора L. Как было показано выше, $L(u_j) \perp L(u_h)$ при $j \neq h$, поэтому этот базис образа ортонормированный. Дополним его до ортонормированного базиса v пространства V (это можно сделать, дополнив до произвольного базиса, применив процесс ортогонализации и нормировав полученные вектора). Таким образом, в ортонормированных базисах u и v матрица оператора L диагональна, что завершает доказательство. □

Следствие 6.5 (полярное разложение). *Любая матрица $A \in \mathrm{M}_n(\mathbb{C})$ представляется в виде произведения $A = GH$, где G – унитарная матрицы, а $H \in \mathrm{M}_n(\mathbb{C})$ – неотрицательно определенная эрмитова. При этом матрица H определена единственным образом, а если A обратима, то и G единственна.*

Доказательство. Пусть $A = BDC$ – сингулярное разложение матрицы A. Тогда $A = (BC)(C^{-1}DC)$ – ее полярное разложение. Действительно, произведение унитарных матриц унитарно, а $C^{-1}DC = C^*DC$ – эрмитова.

Если $A = GH$, где G унитарная, а H эрмитова, то $A^*A = H^*G^*GH = H^2$. Но по лемме 6.2 такая положительно определенная матрица H единственна. Если же A обратима, то обратима и H, поэтому $G = AH^{-1}$ единственна. □

Очевидно, что унитарность (самосопряженность) оператора равносильна унитарности (самосопряженности) его матрицы в ортонормированном базисе. Таким образом, можно говорить о полярном разложении оператора.

Следствие 6.6. *Пусть V – евклидово или эрмитово пространство. Линейный оператор $L : V \to V$ является нормальным тогда и только тогда, когда унитарный и эрмитов операторы в его полярном разложении коммутируют.*

Доказательство. Если $L = GH$, где G – унитарный, а H – эрмитов, то $L^*L = H^*G^*GH = H^2$, а $LL^* = GHH^*G^* = GH^2G^{-1}$. Таким образом, $L^*L = LL^*$ тогда и только тогда, когда G коммутирует с H^2. В этом случае $(GHG^{-1})^2 = H^2$, и по лемме 6.2 $GHG^{-1} = H$, т. е. G и H коммутируют. Обратная импликация очевидна. □

7. Гильбертово пространство

Не вдаваясь в подробности, в этом параграфе мы обсудим, какие утверждения этой главы про евклидовы (эрмитовы) пространства выживают в бесконечномерных пространствах со скалярным произведением. Мы будем рассматривать только одно (с точностью до изометрии) бесконечномерное пространство, а именно то, которым в основном интересуется функциональный анализ – сепарабельное гильбертово пространство.

Пусть V – (бесконечномерное) векторное пространство над $\mathbb{R}$ или $\mathbb{C}$ с евклидовым (соотв. эрмитовым) скалярным произведением. Также как в предыдущих параграфах мы будем обозначать основное поле буквой F, а в вещественном случае черта будет тождественной инволюцией. Скалярное произведение задает норму в пространстве V, которая в соответствие с неравенством треугольника превращает его в нормированное, а, следовательно, и топологическое пространство. Оно называется полным, если любая фундаментальная последовательность имеет предел. Оно называется сепарабельным, если в нем существует плотное счетномерное подпространство. Гильбертово пространство – это полное пространство со скалярным произведением. Для простоты мы считаем наше гильбертово пространство сепарабельным. Все сепарабельные гильбертовы пространства над F изометричны.

Моделью сепарабельного гильбертова пространства является множество ℓ_2 бесконечных последовательностей $x = (x_n)_{n=0}^{\infty}$, для которых ряд $\sum_{n=0}^{\infty} |x_n|^2$ сходится, с естественными операциями

сложения и умножения на число и со скалярным произведением

$$(x, y) = \sum_{n=0}^{\infty} \overline{y_n} x_n.$$

Другой пример (приведем только вещественную версию) – $L_2([a, b])$. Пусть V – множество измеримых функций $f : [a, b] \to \mathbb{R}$ таких, что интеграл Лебега $\int_a^b f(t)^2\, dt$ сходится, с поточечными операциями. Зададим симметричную билинейную форму B на V формулой

$$B(f, g) = \int_a^b f(t)g(t)\, dt.$$

Ясно, что эта форма неотрицательно определена, но вырождена, скажем, функция, отличающаяся от нуля на множестве меры 0 (например, в конечном числе точек), ортогональна всему пространству. Положим $L_2([a, b]) = V/V^{\perp_B}$. Тогда B индуцирует скалярное произведение на этом пространстве. Можно доказать, что набор функций 1, $\sin nt$, $\cos nt$ ($n \in \mathbb{N}$) являются ортогональным базисом плотного подпространства в $L_2([-\pi, \pi])$, поэтому $L_2([a, b])$ является сепарабельным (чтобы перевести $[-\pi, pi]$ в $[a, b]$ достаточно сделать линейную замену переменных).

В анализе базисом гильбертова пространства называют базис плотного подпространства, т. е. базис – это набор v такой, что любой вектор представляется в виде бесконечной линейной комбинации базисных векторов $\sum_{n=0}^{\infty} v_n \alpha_n$ единственным образом (как обычно, сумма ряда – это предел последовательности частичных сумм, а понятие предела в нормированном пространстве существует). Тот базис, который изучается в курсе линейной алгебре, в гильбертовом пространстве, конечно же, также существует. Он называется алгебраическим базисом или базисом Гамеля. Заметим, что счетного базиса Гамеля в гильбертовом пространстве не существует.

Неравенство треугольника, КБШ, и процесс ортогонализации естественно имеют место и в гильбертовом пространстве, так как работают с конечномерными подпространствами. Процесс ортогонализации работает и с бесконечными базисами.

А вот дальше начинаются неожиданности, связанные с наличием незамкнутых линейных подпространств, не непрерывных линейных отображений и инъективных, но не сюръективных эндоморфизмов. В ℓ_2 незамкнутым линейным подпространством является множество ℓ_2^{fin} финитных последовательностей. Оно как раз является счетномерным плотным подпространством, наличие которого доказывает сепарабельность. Базис этого подпространства можно дополнить до алгебраического базиса всего гильбертова пространства, следовательно, $\ell_2 = \ell_2^{fin} \oplus U$ для некоторого подпространства U. Отображение $L : \ell_2 \to F$, заданное равенствами $L(x + y) = \sum_{n=0}^{\infty} n x_n$, где $x \in \ell_2^{fin}$, а $yinU$, не является непрерывным. Инъективным, но не сюръективным является сдвиг $S(x)_1 = 0$, $S(x)_n = x_{n-1}$. Сдвиг в обратную сторону: $S'(x)_n = x_{n+1}$ является примером сюръективного, но не инъективного оператора в ℓ_2. Заметим, что $S' \circ S = \mathrm{id} \neq S \circ S'$, то есть в алгебре операторов существуют односторонне обратимые элементы.

В анализе под подпространством гильбертова пространства по умолчанию считают *замкнутое* подпространство, а под линейным оператором – непрерывный линейный оператор. С такой оговоркой разложение в прямую сумму подпространства и его ортогонального дополнения и равенство $(U^{\perp})^{\perp} = U$ имеют место и в гильбертовых пространствах (для незамкнутого подпространства $(U^{\perp})^{\perp}$ является замыканием U).

Формула для координат в ортогональном базисе, неравенство Бесселя и равенство Парсеваля имеют место в гильбертовых пространствах и для бесконечных ортогональных наборов. Выполнена также лемма о расстоянии от точки до (замкнутого) подпространства.

Двойственное пространство к гильбертову пространству H – это пространство *непрерывных* линейных функционалов, т. е. непрерывных линейных отображений $H \to F$. С таким соглашением можно доказать, что H^* канонически изоморфно H (это называется теоремой Рисса). Оба определения сопряженного оператора теперь переносятся и на гильбертовы пространства.

Изучение собственных чисел операторов становится существенно сложнее из за наличия инъективных, но не сюръективных операторов. Далее $F = \mathbb{C}$, потому что даже в конечномерных пространствах над $\mathbb{R}$ все доказательства проходят через $\mathbb{C}$. Множество тех чисел $\lambda \in \mathbb{C}$, для которых оператор $L - \lambda\mathrm{id}$ не обратим, называется спектром оператора L. При этом λ называется собственным числом, если (также как и в конечномерном случае) этот оператор не инъективен. Множество собственных чисел называется точечным спектром. Для компактного самосопряженного оператора верен аналог следствия 5.11 (с бесконечной линейной комбинацией проекторов). Если же самосопряженный оператор не компактен, то он может вообще не иметь собственных чисел и теорема о его строении гораздо сложнее.

Некоторые из матричных разложений имеют место и для операторов в гильбертовых пространствах с соответствующими оговорками. Таково, например, полярное разложение.

8. Кватернионы и движения трехмерного пространства

К теории квадратичных и эрмитовых форм примыкает теория конечномерных алгебр с делением. Алгебра A над полем F называется телом или алгеброй с делением, если любой ее ненулевой элемент обратим. Она называется центральной, если F является ее центром, т. е. множеством элементов, коммутирующих со всеми элементами A. Легко доказать, что над замкнутым полем любая такая алгебра совпадает с самим полем. Действительно, для любого элемента $a \in A$ алгебра $F[a]$ изоморфна $F[t]/(f)$ для некоторого многочлена f. Если f приводим, то $F[a]$ содержит делители нуля, что невозможно. В противном случае, так как F замкнуто, то $\deg f = 1$, откуда $a \in F$.

Над полем вещественных чисел существует ровно одна центральная алгебра с делением. Она называется алгеброй кватернионов. Алгебра кватернионов $\mathbb{H}$ – это 4-мерное векторное пространство над $\mathbb{R}$ с базисом $e = (1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ и таблицей умножения

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,\ \mathbf{ij} = -\mathbf{ji} = \mathbf{k},\ \mathbf{jk} = -\mathbf{kj} = \mathbf{i},\ \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Легко проверить, что эта алгебра ассоциативна (достаточно проверить это на базисных элементах).

Кватернион $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ можно представить как сумму скалярной части a и векторной части $v = b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$. Если отождествить векторную часть с трехмерным вектором, то умножение векторных частей выглядит следующим образом:

$$uv = u \times v - (u, v),$$

где $\times$ обозначает векторное произведение. Кватернион с нулевой скалярной частью называется чистым кватернионом.

Отображение $\bar{\cdot} : \mathbb{H} \to \mathbb{H},\ a + v \to a - v$, называется сопряжением и является антиинволюцией на $\mathbb{H}$. Действительно,

$$(b+u)(a+v) = ba-(u,v)+(u\times v+au+bv),\ \text{а}\ (a-v)(b-u) = ab-(v,u)+(v\times u-au-bv) = \overline{(b+u)(a+v)},$$

а остальные свойства антиинволюции очевидны. Кроме того

$$(a + v)(a - v) = a^2 - vv = a^2 - v \times v + (v, v) = a^2 + (v, v).$$

Для ненулевого кватерниона это число является положительным вещественным числом и квадратный корень из него называется модулем кватерниона. Таким образом, мы видим, что $h\frac{\bar{h}}{|h|^2} = 1$, т. е. $\mathbb{H}$ – алгебра с делением.

Легко видеть, что модуль является гомоморфизмом мультипликативной группы кватернионов в мультипликативную группу положительных вещественных чисел. Действительно,

$$|h|^2|g|^2 = h\bar{h}g\bar{g} = gh\bar{h}\bar{g} = gh\overline{gh} = |gh|^2.$$

Сопоставление кватерниону $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ матрицы умножения на этот кватернион в стандартном базисе $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

задает гомоморфизм алгебры кватернионов в алгебру матриц $\mathrm{M}_4(\mathbb{R})$, а определитель этой матрицы – гомоморфизм мультипликативной группы кватернионов в $\mathbb{R}^*$, который является нормой[4] из $\mathbb{H}$ в $\mathbb{R}$. Вычисление показывает, что этот определитель равен $(a^2 + b^2 + c^2 + d^2)^2$, т. е. четвертой степени модуля кватерниона.

Другое матричное представление кватернионов получается при рассмотрении $\mathbb{H}$, как векторного пространства над $\mathbb{C}$ с умножением $h(a + bi) = h(a + b\mathbf{i})$, где $h \in \mathbb{H}$, а $a, b \in \mathbb{R}$. Тогда $\mathbb{H}$ будет 2-мерным векторным пространством над $\mathbb{C}$ с базисом $(1, \mathbf{j})$: любой кватернион единственным образом представляется в виде $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = 1 \cdot (a + b\mathbf{i}) + \mathbf{j} \cdot (c - d\mathbf{i})$. Умножение на кватернион $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ слева является линейным оператором на этом векторном пространстве, матрица которого равна

$$\begin{pmatrix} a + bi & -c - di \\ c - di & a - bi \end{pmatrix}.$$

Нетрудно проверить, что это отображение задает вложение мультипликативной группы кватернионов в группу $\mathrm{GL}_2(\mathbb{C})$. Определитель указанной матрицы равен $a^2 + b^2 + c^2 + d^2$ и называется редуцированной нормой $\mathrm{nrd}(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})$. Заметим, что кватернионы с модулем 1 отображаются в унитарные матрицы с определителем 1. Это совершенно не удивительно, потому что умножение на кватернион с модулем 1 является изометрией 4-мерного пространства кватернионов, норма кватерниона равна норме столбца его координат в выбранном базисе (относительно стандартного скалярного произведения в $\mathbb{C}^2$), а умножение на матрицу сохраняет нормы столбцов тогда и только тогда, когда она унитарна. Более удивительно, что это отображение биективно, чуть позже мы сформулируем это в виде изоморфизма групп. Заметим, что это не все изометрии 4-мерного вещественного пространства $\mathbb{H}$, а только $\mathbb{C}$-линейные изометрии.

Интересно также рассмотреть операцию сопряжения кватернионом: $c_h(z) = hzh^{-1}$. Эта операция тоже не меняет модуль кватерниона z, а кроме того оставляет инвариантным пространство чистых кватернионов. Это можно доказать вычислением, а можно воспользоваться идеями параграфа 5. Действительно, множество вещественных чисел инвариантно относительно оператора сопряжения любым кватернионом, а подпространство чистых кватернионов является его ортогональным дополнением (относительно евклидова скалярного произведения, ассоциированного с выбранной нормой). По лемме 5.8 оно инвариантно относительно сопряженного оператора. Так как оператор сопряжения является унитарным, то сопряженный с ним равен обратному. Таким образом, подпространство чистых кватернионов инвариантно относительно сопряжения обратным к любому кватерниону.

Если $h = a + v$ – разложение кватерниона на вещественную часть и чистый кватернион, то $c_h(v) = v$, и нетрудно видеть, что $\langle 1, v\rangle_{\mathbb{R}}$ – собственное подпространство оператора c_h, соответствующее 1. По леммам 5.7 и 5.8 ортогональное дополнение этого подпространства (плоскость в пространстве чистых кватернионов) c_h-инвариантно. Непосредственное вычисление показывает, что любой поворот в этой плоскости реализуется, а отношение $a/|v|$ определяет угол этого поворота,

[4]Понятие нормы в алгебре отличается от понятия нормы в анализе. В алгебре нормой называют определитель матрицы умножения на элемент F-алгебры.

Действительно, можно считать, что $|h| = 1$, а тогда

$$(a+v)w(a-v) = a^2w + a(vw - wv) + vwv = a^2w + 2av \times w - (v \times w - (v,w))v =$$
$$a^2w + 2av \times w - v \times w \times v + (v,w)v = a^2w + 2av \times w - (v,v)w + 2(v,w)v.$$

Пусть $a = \cos\frac{\alpha}{2}$, $|v| = \sin\frac{\alpha}{2}$, а $e_1 = w - \mathrm{pr}_v w$, $e_2 = \frac{v\times w}{|v|}$, $e_3 = \mathrm{pr}_v w$ – ортогональный базис. Тогда

$$(a+v)w(a-v) = w(\cos^2\frac{\alpha}{2} - \sin^2\frac{\alpha}{2}) + 2\,\mathrm{pr}_v w \cdot \sin^2\frac{\alpha}{2} + 2e_2 \cdot \cos\frac{\alpha}{2}\sin\frac{\alpha}{2} =$$
$$w\cos\alpha - \mathrm{pr}_v w \cdot \cos\alpha + \mathrm{pr}_v w + e_2 \cdot \sin\alpha = e_1\cos\alpha + e_2\sin\alpha + e_3.$$

Заметим, что третья координата w в этом базисе не изменилась, а длины векторов e_1 и e_2 равны. Следовательно, $(a+v)w(a-v)$ – вектор, полученный поворотом w на угол α вокруг прямой, натянутой на вектор v. Таким образом, сопряжение кватернионом реализует любой поворот трехмерного пространства.

Несколько слов об обозначениях групп изометрий эрмитова пространства. В общем виде, если F – поле с инволюцией, V – конечномерное векторное пространство над F, а B – невырожденная эрмитова форма на V, то группа изометрий формы B называется унитарной группой и обозначается $\mathrm{U}(B)$ или $\mathrm{U}_n(F)$, где $n = \dim V$, если инволюция и форма известны из контекста. Если инволюция тривиальна, то эта группа называется ортогональной группой и обозначается через $\mathrm{O}(B)$ или $\mathrm{O}_n(F)$. Подгруппы этих групп, состоящие из преобразований с определителем 1, называются специальной унитарной и специальной ортогональной группой и обозначаются через SU и SO, соответственно.

Для стандартных скалярных произведений в $\mathbb{C}^n$ и $\mathbb{R}^n$ соответствующие группы обычно обозначаются просто через U_n, SU_n, O_n и SO_n. Как мы видели, определитель унитарной матрицы по модулю равен 1. Следовательно, определитель вещественной ортогональной матрицы равен ± 1. Поэтому группа O_{2k+1} раскладывается в прямое произведение $\mathrm{SO}_{2k+1} \times \{\pm E\}$.

Собственные числа матрицы из SO_3 по модулю равны 1, одно из них вещественно, а два других комплексно сопряженные (если все 3 вещественны, то одно равно 1, а два других равны между собой). Так как произведение комплексно сопряженных чисел равно 1, то одно из собственных чисел должно быть равно 1, т. е. ортогональное преобразование действует на некоторой прямой тривиально. Ортогональное дополнение этой прямой инвариантно. Легко видеть, что ортогональная матрица 2×2 с определителем 1 – это матрица поворота. Если же определитель преобразования из O_3 равен -1, то композиция его с любым зеркальным отражением будет лежать в SO_3, т. е. будет вращением. Таким образом, мы доказали хорошо известный из геометрии факт.

Предложение 8.1. *Любое движение трехмерного пространства с неподвижной точкой является поворотом или композицией поворота с (любой) зеркальной симметрией.*

Повороты называются собственными движениями, а композиция поворота и симметрии – несобственными. Таким образом, SO_3 – это группа собственных движений трехмерного пространства.

Теперь можно сформулировать связь кватернионов с унитарными и ортогональными группами.

Предложение 8.2. *Мультипликативная группа кватернионов с модулем* 1 *изоморфна группе* SU_2*, а всех кватернионов* $\mathbb{H}^* \cong \mathbb{R}^*_{>0} \times \mathrm{SU}_2$.

Факторгруппа $\mathbb{H}^*/\mathbb{R} \cong \mathrm{SU}_2/\{\pm E\} \cong \mathrm{SO}_3$.

Модуль кватерниона задает на $\mathbb{H}^*$ *структуру нормированного топологического пространства, которая индуцирует топологию на* $\mathbb{H}^*/\mathbb{R}$. *Ясно, что* $\mathbb{H}^*/\mathbb{R}$ *с этой топологией гомеоморфно проективному пространству* $\mathbb{RP}^3$. *Изоморфизм* $\mathbb{H}^*/\mathbb{R} \to \mathrm{SO}_3$ *является гомеоморфизмом и, следовательно,* SO_3 *гомеоморфно* $\mathbb{RP}^3$.

9. Теоремы Витта

Этот параграф посвящен основам классификации квадратичных пространств над произвольным полем F характеристики не 2. Мы увидим, что любая квадратичная форма является суммой нескольких экземпляров гиперболической плоскости и анизотропной формы. Начнем с определения суммы форм и гиперболической плоскости.

Будем говорить, что две формы изоморфны, если соответствующие квадратичные пространства изометричны. Пусть (V, Q) и (V', Q') – квадратичные пространства. Обозначим через $Q \oplus Q'$ квадратичную форму на $V \oplus V'$, действующую по правилу $Q \oplus Q'(x, x') = Q(x) + Q'(x')$ (проверьте, что это действительно квадратичная форма). Если подпространства V и V' невырождены, то в пространств $V \oplus V'$ они являются ортогональными дополнениями друг друга относительно формы $Q \oplus Q'$. Поэтому в текстах про квадратичные формы чаще используют обозначение $Q \perp Q'$ вместо $Q \oplus Q'$ и называют такую форму ортогональной суммой форм Q и Q'.

Обозначим через $\langle \alpha_1 \rangle \oplus \cdots \oplus \langle \alpha_n \rangle = \langle \alpha_1, \ldots, \alpha_n \rangle$ форму, которая в некотором базисе имеет матрицу $\operatorname{diag}(\alpha_1, \ldots, \alpha_n)$. Форма $\mathbb{H} \cong \langle 1, -1 \rangle$ (точнее двумерное пространство с этой формой) называется гиперболической плоскостью. Ненулевой вектор x называется изотропным относительно формы Q, если $Q(x) = 0$, в противном случае x называется анизотропным. Напомним, что форма Q называется изотропной, если существует Q-изотропный вектор, и анизотропной в противном случае.

Лемма 9.1. *Любая невырожденная изотропная квадратичная форма Q изоморфна $\mathbb{H} \oplus Q'$ для некоторой невырожденной формы Q'.*

Доказательство. Так как Q изотропна, существует $x \in V \smallsetminus \{0\}$ такой, что $Q(x) = 0$. Обозначим через B симметричную билинейную форму, ассоциированную с Q. Поскольку Q невырождена, найдется $y \in V$ такой, что $B(x, y) \neq 0$. Домножая y на подходящий скаляр, можно считать, что $B(x, y) = 2$. Для любого $\lambda \in F$ вектора x и $z = y + \lambda x$ линейно независимы, причем $B(x, z) = B(x, y) + \lambda B(x, x) = 2$. Наконец, $Q(z) = B(y + \lambda x, y + \lambda x) = B(y, y) + 2\lambda B(x, y) + B(x, x) = Q(y) + 4\lambda$. Значит, если положить $\lambda = -Q(y)/4$, получим $Q(z) = 0$. Возьмем теперь $v_1 = (x + z)/2$, а $v_2 = (x - z)/2$. Тогда $B(v_1, v_2) = 0$, а $Q(v_1) = -Q(v_2) = 1$.

Дополнив v_1, v_2 до базиса $(v_1, v_2, u_3, \ldots, u_n)$ при $i \geqslant 3$ положим

$$v_i = u_i - B(v_1, u_i)v_1 + B(v_2, u_i)v_2.$$

Так как $B(v_1, v_i) = B(v_2, v_i) = 0$, то $Q \cong \mathbb{H} \oplus Q'$, где Q' – сужение формы Q на подпространство, порожденное векторами $v_3, \ldots, v_n$. □

Из леммы следует в частности, что все невырожденные изотропные двумерные формы изоморфны $\mathbb{H}$. Большая часть алгебраистов предпочитает выбирать базис $\mathbb{H}$ так, чтобы матрица квадратичной формы была равна $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, а не $\operatorname{diag}(1, -1)$, то есть в координатах: $Q(x) = 2x_1x_2$, а не $Q(x) = x_1^2 - x_2^2$.

Из леммы следует также, что любое квадратичное пространство представляется в виде суммы нескольких экземпляров гиперболической плоскости и анизотропного подпространства. Наша следующая цель – доказать, что анизотропное подпространство определено единственным образом с точностью до изометрии. Для этого мы докажем теорему о сокращении, которая говорит о том, что изометрию $U \oplus V \cong U \oplus W$ можно сокращать на U.

Пусть Q – квадратичная форма на V, соответствующая симметричной билинейной форме B, а x – Q-анизотропный вектор. Определим отражение S_x относительно вектора[5] x формулой

$$S_x(y) = y - 2\frac{B(x, y)}{Q(x)}x.$$

Простое вычисление показывает, что отражение является изометрией, а $S_x^2 = \mathrm{id}$.

[5]Геометрически, это является отражением относительно гиперплоскости, ортогональной x.

Лемма 9.2. *Пусть $x_1, x_2 \in V$ и $Q(x_1) = Q(x_2) \neq 0$. Тогда существует композиция отражений, переводящая x_1 в x_2.*

Доказательство. Если $Q(x_1 - x_2) \neq 0$, то подойдет отражение относительно этого вектора:

$$S_{x_1-x_2}(x_1) = x_1 - 2\frac{B(x_1 - x_2, x_1)}{Q(x_1 - x_2)}(x_1 - x_2) = \\ x_1 - 2\frac{Q(x_1) - B(x_2, x_1)}{Q(x_1) + Q(x_2) - 2B(x_2, x_1)}(x_1 - x_2) = x_1 - (x_1 - x_2) = x_2.$$

Если $Q(x_1 + x_2) \neq 0$, то $S_{x_1+x_2}(x_1) = -x_2$, а $S_{x_2}(-x_2) = x_2$. Если же $Q(x_1 - x_2) = Q(x_1 + x_2) = 0$, то

$$0 = Q(x_1 - x_2) + Q(x_1 + x_2) = Q(x_1) + Q(x_2) + Q(x_1) + Q(x_2) = 4Q(x_1),$$

что противоречит предположению. □

Следствие 9.3. *Любая изометрия невырожденного пространства есть композиция отражений.*

Доказательство. Пусть $L : V \to V$ – изометрия невырожденного квадратичного пространства (V, Q). Доказываем индукцией по $n = \dim V$; база $n = 1$ очевидна. Пусть $n > 1$. Возьмем $x \in V$ такой, что $Q\big(L(x)\big) = Q\big(x\big) \neq 0$. По лемме найдется композиция отражений $S\colon V \to V$ такая, что $S(x) = L(x)$. Отображение $S^{-1}L$, таким образом, является изометрией и оставляет x на месте; значит, $S^{-1}L$ оставляет на месте и $W = x^\perp$ – подпространство размерности $n - 1$. По предположению индукции изометрия $S^{-1}L|_W$ является композицией отражений (относительно векторов из W). Заметим, что любое отражение относительно вектора из W оставляет на месте x, поскольку $x \perp W$. Значит, изометрия $S^{-1}L$ является композицией тех же самых отражений, рассматриваемых уже как преобразований всего пространства V. Перенося S в другую часть, получаем, что и L является композицией отражений. □

Теорема 9.4 (Витта о сокращении). *Если $Q \oplus Q_1 \cong Q \oplus Q_2$, то $Q_1 \cong Q_2$.*

Доказательство. Предложение 2.2 дает возможность сокращать на ортогональное дополнение ко всему пространству, поэтому можно считать, что форма Q невырождена. Докажем сначала, что из $\langle\alpha\rangle \oplus Q_1 \cong \langle a\rangle \oplus Q_2$ следует, что $Q_1 \cong Q_2$. Пусть при $i = 1, 2$ форма $Q_i' = \langle\alpha\rangle \oplus Q_i$ задана на пространстве $\langle x_i\rangle \oplus W_i$, причем $Q_i'(x_i) = \alpha$. Изометричность этих форм означает, что существует линейное отображение $L\colon \langle x_1\rangle \oplus W_1 \to \langle x_2\rangle \oplus W_2$, для которого $Q_2'\big(L(x)\big) = Q_1'\big(x\big)$. Так как $Q_2'\big(L(x_1)\big) = Q_1'\big(x_1\big) = \alpha$, то по лемме 9.2 найдется изометрия $S\colon \langle x_2\rangle \oplus W_2 \to \langle x_2\rangle \oplus W_2$ такая, что $S(x_2) = L(x_1)$. Ясно, что $S^{-1}L$ является изометрией $\langle x_1\rangle \oplus W_1 \to \langle x_2\rangle \oplus W_2$ и $S^{-1}L(x_1) = x_2$. Так как изометрия сохраняет ортогональность векторов, то она сохраняет и ортогональные дополнения. Поэтому $S^{-1}L$ отображает $W_1 = x_1^\perp$ на $W_2 = x_2^\perp$. Это означает, что ограничение $S^{-1}L$ на W_1 и дает нужную изометрию между Q_1 и Q_2.

В общем случае по теореме 2.5 $Q \cong \langle\alpha_1\rangle \oplus \cdots \oplus \langle\alpha_n\rangle$, и доказательство проводится очевидной индукцией по n. □

Следствие 9.5. *Любая невырожденная форма Q представляется в виде*

$$Q \cong \underbrace{\mathbb{H} \oplus \cdots \oplus \mathbb{H}}_{r \text{ раз}} \oplus Q_{an},$$

где анизотропная часть Q_{an} *определена однозначно с точностью до изометрии, и* индекс Витта $i(Q) := r$ *определен однозначно.*

Доказательство. По лемме 9.1 если форма изотропна, из нее можно выделить $\mathbb{H}$. Продолжая этот процесс, дойдем до какой-то анизотропной формы (потому что размерность все время убывает). Единственность легко выводится из теоремы о сокращении. □

Для доказательства теоремы о продолжении изометрии в случае, когда мы продолжаем изометрию с вырожденного подпространства, нам понадобится следующее утверждение.

Лемма 9.6. *Пусть B невырожденная симметричная билинейная форма на V, а W вырожденное подпространство в V. Пусть $w = (w_1, \dots, w_k)$ – базис пространства $W \cap W^\perp$, а $v = (v_1, \dots, v_m)$ – дополнение w до базиса пространства W. Тогда существует набор векторов $u = (u_1, \dots, u_k)$ пространства V таких, что подпространство $U = \langle w \cup u \rangle$ ортогонально подпространству $\langle v \rangle$, а матрица сужения B на U в базисе $w \cup u$ равна $\left(\begin{smallmatrix} 0 & E \\ E & 0 \end{smallmatrix}\right)$.*

Заметим, что тогда подпространство $\langle w \cup u \cup v \rangle$ невырождено.

Доказательство. Так как B невырождена, то по лемме 4.6 размерность ортогонального дополнения подпространства W строго меньше, чем размерность ортогонального дополнения подпространства $W' = \langle w_1, \dots, w_{k-1}, v_1, \dots, v_m \rangle$. Поэтому существует вектор $x \in V$, ортогональный всем векторам из набора $w \cup v$, кроме w_k. Таким образом, подпространство, порожденное w_k и x двумерно, изотропно и ортогонально W'. Также как в доказательстве леммы 9.1, найдем в этом подпространстве изотропный вектор u_k такой, что $B(u_k, w_k) = 1$.

Теперь в пространстве $\overline{W} = W + \langle u_k \rangle$ имеем: $\overline{W} \cap \overline{W}^\perp = \langle w_1, \dots, w_{k-1} \rangle$. Индукцией по k найдем изотропные вектора $u_1, \dots, u_k$ такие, что u_i ортогонален w_j при всех $j \neq i$, всем u_j и всем v_j. При этом $B(u_i, w_i) = 1$, а это и означает, что u – искомый набор.

По лемме 2.2 подпространство $\langle v \rangle$ невырождено. Подпространство $\langle w \cup u \rangle$ невырождено, так как матрица сужения формы B на него невырождена. Наконец ортогональная сумма двух невырожденных подпространств невырождена. □

Следствие 9.7 (Теорема о продолжении изометрии). *Пусть (V, Q) – невырожденное квадратичное пространство, W_1, W_2 – подпространства в V такие, что существует изометрия $L\colon W_1 \to W_2$. Тогда существует изометрия $M\colon V \to V$ такая, что $M|_{W_1} = L$.*

Доказательство. В случае, когда W_1 невырождено, утверждение следует из теоремы Витта о сокращении. Действительно, в этом случае по предложению 4.6 V раскладывается в прямую сумму W_i и его ортогонального дополнения ($i = 1, 2$). По теореме о сокращении существует изометрия $L' : W_1^\perp \to W_2^\perp$. Тогда изометрия $M : V = W_1 \oplus W_1^\perp \to W_2 \oplus W_2^\perp = V$ задается формулой $M(x + y) = L(x) + L'(y)$ при $x \in W_1$, $y \in W_1^\perp$.

Пусть теперь W_1 – вырожденное подпространство в невырожденном пространстве V. Выберем базис $w = (w_1, \dots, w_k)$ пространства $W_1 \cap W_1^\perp$ и дополним его до базиса $w \cup v$ пространства W_1. Выберем набор $u = (u_1, \dots, u_k)$, удовлетворяющий условиям леммы 9.6. Так как L изометрия, то $L(w)$ является базисом пространства $W_2 \cap W_2^\perp$, а $L(w) \cup L(v)$ – базисом W_2. Выберем набор $u' = (u'_1, \dots, u'_k)$, удовлетворяющий условиям леммы 9.6 с $W = W_2$. Продолжим L на пространство $W_1' = W_1 + \langle u \rangle$, положив $L(u) = u'$ и продолжив по линейности. Так как матрицы сужений формы Q на $\langle w \cup u \rangle$ и $\langle L(w) \cup L(u) \rangle$ в базисах $w \cup u$ и $L(w) \cup L(u)$ совпадают, то сужение L на эти подпространства является изометрией. С другой стороны, сужение L на $\langle v \rangle$ и было изометрией этого пространства на $\langle L(v) \rangle$. Так как $\langle w \cup u \rangle \perp \langle v \rangle$, а $\langle L(w) \cup L(u) \rangle \perp \langle L(v) \rangle$, то определенное выше продолжение L является изометрией $W_1' \to W_2' = W_2 + \langle u' \rangle$. Наконец, по той же самой лемме 9.6 пространство W_1' невырождено, и по первому абзацу доказательства L можно продолжить с него на все пространство V. □

Следствие 9.8. *Индекс Витта равен размерности максимального полностью изотропного подпространства (т. е. подпространства, сужение формы на которое нулевое). Более того, все масимальные изотропные подпространства переводятся друг в друга изометриями.*

10. Симплектические формы

Симплектическая форма – это билинейная антисимметричная форма. В отличие от квадратичных форм, определение симплектической формы не зависит от характеристики поля, надо только

правильно определять понятие антисимметричности, см. параграф 1. Некоторая часть теории эрмитовых форм переносится и на симплектические формы,[6] основным же отличием является то, что любой вектор изотропен и, следовательно, нет никаких шансов диагонализовать матрицу симплектической формы. К счастью, любая симплектическая форма приводится к очень простому каноническому виду, причем все симплектические пространства (т. е. пространства с симплектической формой) одной размерности изометричны. Группа линейных преобразований, сохраняющих симплектическую форму, называется симплектической группой. Наряду с полной линейной, унитарной, ортогональной группами и некоторыми их модификациями, симплектическая группа является *классической* группой. Классические группы являются примерами полупростых групп Ли (над $\mathbb{R}$ или $\mathbb{C}$) и алгебраических групп (над произвольным полем), и играют огромную роль во многих отраслях математики от чистой алгебры до механики. В частности, из классических групп над конечными полями строится большая часть простых конечных групп (обычно, факторгруппа коммутанта классической группы по центру проста), а симплектические многообразия (нечто, склеенное из кусков симплектических пространств) и симплектическая группа являются чуть ли не основой гамильтоновой механики.

В этом параграфе мы докажем только классификацию конечномерных невырожденных симплектических пространств. Заметим сначала, что матрица симплектической формы в любом базисе кососимметрическая, т. е. $A^\intercal = -A$. Пусть V – двумерное пространство с ненулевой симплектической формой B. Существует пара векторов v_1, v_2 для которых $B(v_1, v_2) \neq 0$. Домножая v_2 на подходящую константу, можно считать, что $B(v_1, v_2) = 1$. Так как $B(v_1, v_1) = 0$, то отсюда сразу следует линейная независимость v_1 и v_2. В базисе $v = (v_1, v_2)$ матрица формы B имеет вид

$$B_v = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Таким образом, все двумерные невырожденные симплектические пространства изометричны между собой. Такое пространство будем называть симплектической плоскостью.

Теорема 10.1. *Любое невырожденное симплектическое пространство имеет четную размерность и изометрично ортогональной сумме симплектических плоскостей.*

Доказательство. Из сказанного выше следует, что любая пара векторов пространства V, на которых симплектическая форма B не равна нулю, порождают симплектическую плоскость S. Также как в доказательстве леммы 4.6 легко видеть, что $\dim S^{\perp_B} = \dim V - 2$ и $S \cap S^{\perp_B} = \{0\}$. Поэтому $V = S \oplus S^{\perp_B}$ и $(S^{\perp_B})^{\perp_B} = S$. Так как $S^{\perp_B} \cap (S^{\perp_B})^{\perp_B} = \{0\}$, то подпространство $S^{\perp_B}$ невырождено, можно применить индукцию по размерности пространства V. Так как размерность падает на 2, то база индукции – случай размерности 0 или 1. Первый из них тривиален, а во втором надо только заметить, что любая симплектическая форма на одномерном пространстве нулевая, откуда следует, что невырожденных симплектических форм нечетной размерности не бывает. □

[6] Кусок теории эрмитовых форм переносится на полуторалинейные формы с довольно слабым условием симметрии: $B(x, y) = 0 \iff B(y, x) = 0$.

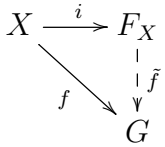
Глава 8

Теория групп

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

1. Свободные группы, задание группы образующими и соотношениями

Универсальное свойство свободной группы аналогично определению свободного модуля. Пусть X – множество. Группа F_X вместе с отображением $i : X \to F_X$ называется *свободной группой с множеством образующих* X (или порожденной X, или свободной группой множества X), если для любой функции f из X в группу G существует единственный гомоморфизм групп $\tilde{f} : F_X \to G$ такой, что диаграмма



коммутативна.

Как обычно, это определение ничего не говорит о существовании универсального объекта. Сейчас мы построим свободную группу и покажем, что она удовлетворяет сформулированному универсальному свойству. Пусть $\bar{X} = \{\bar{x} \mid x \in X\}$ – множество символов. Для $x \in X$ положим $\bar{\bar{x}} = x$. Рассмотрим множество $W = W_X$, состоящее из слов (включая пустое слово) в алфавите $X \cup \bar{X}$. Пусть Q – подмножество в $W \times W$, состоящее из всех пар $(w_1 x \bar{x} w_2, w_1 w_2)$, $w_1, w_2 \in W$, $x \in X \cup \bar{X}$. Обозначим через $\sim$ наименьшее отношение эквивалентности на W, содержащее Q. Другими словами, $u \sim v$ тогда и только тогда, когда u приводится к v при помощи вставки и стирания фрагментов вида $x\bar{x}$.

Пусть $F_X = W/\sim$ – множество классов эквивалентности $\sim$. Определим операцию на $F(X)$, как конкатенацию слов. Точнее, $[w_1]\cdot[w_2] = [w_1 w_2]$, где $w_1, w_2 \in W$, а квадратные скобки означают класс эквивалентности, содержащий данное слово. Нетрудно проверить, что результат операции не зависит от выбора представителей классов эквивалентности. Очевидно, что операция ассоциативна, а нейтральным элементом является класс эквивалентности пустого слова. Обратный к $[x_1 \dots x_n]$ – это элемент $[\bar{x}_n \dots \bar{x}_1]$, где $x_1, \dots, x_n \in X \cup \bar{X}$. Таким образом, F_X – группа.

Теорема 1.1. *Группа F_X вместе с отображением $X \to F_X$, $x \mapsto [x]$ является свободной группой с множеством образующих X.*

Доказательство. Заметим, что по определению умножения в F_X для $x \in X$ имеем $[x]^{-1} = [\bar{x}]$. Для удобства обозначений, допуская вольность речи, будем писать x^{-1} вместо $\bar{x}$. Пусть $f : X \to G$ – функция из X в группу G. Зададим отображение $f' : W \to G$ формулой

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

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

$$\tilde{f} : F_X \to G, \qquad \tilde{f}([w]) = f'(w)$$

задана корректно. Теперь очевидно, что $\tilde{f}$ является гомоморфизмом, причем $\tilde{f}([x]) = f(x)$ для любого $x \in X$, что равносильно коммутативности диаграммы. Так как любой гомоморфизм $F_X \to$

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 $\tilde{f}$. □

Обычно элементы множества X отождествляют с их образами в F_X, т. е. с классами эквивалентности однобуквенных слов. Слово из W называется редуцированным, если оно не содержит вхождений $x\bar{x}$ при $x \in X \cup \bar{X}$. Нетрудно выбрать редуцированного представителя в каждом классе эквивалентности.[1]

Предложение 1.2. *В каждом классе эквивалентности $W/\sim$ есть ровно одно редуцированное слово. Оно имеет наименьшую длину среди всех слов из этого класса.*

Доказательство. Возьмем произвольное слово из фиксированного класса эквивалентности. Если оно не редуцированное, то выкинув из него вхождение $x\bar{x}$ получим более короткое слово из того же класса. Доказательство существования заканчивает индукция по длине слова.

Доказательству единственности мешает неоднозначность алгоритма удаления вхождений $x\bar{x}$ из нередуцированного слова. Значит, для однозначности надо придумать детерминированный алгоритм, который является проекцией на множество редуцированных слов, т. е. редуцированное слово переводит в себя, а нередуцированное – в редуцированное. Кроме того, надо доказать, что применение этого алгоритма к эквивалентным словам возвращает одно и то же. Так как эквивалентные слова связаны цепочкой вставок и удалений фрагментов $x\bar{x}$, то достаточно доказывать, что алгоритм возвращает одинаковые значения на словах w_1w_2 и $w_1x\bar{x}w_2$, где $w_1, w_2 \in W$, а $x \in X \cup \bar{X}$.[2]

Определим функцию $f : W \times W \to W \times W$ следующими равенствами:

$$\begin{aligned} f(w, \varnothing) &= (w, \varnothing); \\ f(\varnothing, xw) &= (x, w); \\ f(vy, xw) &= (vyx, w), \text{ если } y \neq \bar{x}; \\ f(v\bar{x}, xw) &= (v, w), \end{aligned}$$

где $v, w \in W$, а $x, y \in X \cup \bar{X}$. Так как длина второго слова под действием f убывает ровно на 1, пока оно не пустое, то $f^k(\varnothing, w) = (w', \varnothing)$ для достаточно большого k (здесь f^k обозначает композицию f с собой k раз). В этом случае положим $g(w) = w'$. Это и есть наш алгоритм, он называется W-процессом. Легко проверить, что если v редуцированное слово, то первое слово в $f(v, w)$ также является редуцированным. Поэтому g всегда возвращает редуцированное слово. Также очевидно, что редуцированное слово отображается в себя под действием g, потому что последнее правило из определения f ни разу не применяется.

Осталось доказать, что $g(w_1w_2) = g(w_1x\bar{x}w_2)$. Ясно, что

$$f^k(\varnothing, w_1w_2) = (g(w_1), w_2) \text{ и } f^k(\varnothing, w_1x\bar{x}w_2) = (g(w_1), x\bar{x}w_2),$$

где k – длина слова w_1. Далее, если $g(w_1) = \varnothing$ или $g(w_1) = vy$ при $y \neq \bar{x}$, то $f^2(g(w_1), x\bar{x}w_2) = f(g(w_1)x, \bar{x}w_2) = (g(w_1), w_2)$. В случае $g(w_1) = v\bar{x}$, $f^2(v\bar{x}, x\bar{x}w_2) = f(v, \bar{x}w_2) = (g(w_1), w_2)$. Итак, в любом случае $f^{k+2}(\varnothing, w_1x\bar{x}w_2) = f^k(\varnothing, w_1w_2)$, следовательно, $g(w_1w_2) = g(w_1x\bar{x}w_2)$. □

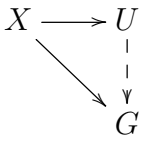
Соотношением в группе называется равенство $w = 1$, где w элемент свободной группы на некотором множестве X. В дальнейшем мы иногда будем говорить "соотношение w" вместо "соотношение $w = 1$". Если соотношение выполняется в группе для всех элементов (как, например,

[1] Следующее утверждение – из серии "очевидно, потому что очевидно". Доказывать такие утверждения бывает, однако, нелегко, а главное, очень противно. Зачем доказывать то, что и так понятно? К сожалению уровень абстракции современной математики таков, что некоторые утверждения из этой серии оказываются неверными. Почти любой математик испытал это на себе, найдя контрпример к "очевидному" утверждению в начале своего доказательства какой-нибудь классной теоремы.

[2] Другими словами, если $g(v) = g(w)$ при всех $(v, w) \in Q$, то эквивалентность $v \overset{g}{\sim} w \iff g(v) = g(w)$ содержит эквивалентность $\sim$. Это соображение мы уже использовали выше.

$x^{-1}y^{-1}xy = 1$ в абелевой группе), то оно называется групповым тождеством. Мы же сейчас рассмотрим соотношения, которые выполнены для конкретных элементов. Пусть R – подмножество свободной группы на множестве X, G группа, а $f : X \to G$ – функция. Говорят, что в G выполняются соотношения R, если при подстановке в элементы из R вместо элементов множества X их образов в G получается верное равенство. Более строго, по универсальному свойству свободной группы существует единственный гомоморфизм $\tilde{f} : F_X \to G$ такой, что $f = \tilde{f} \circ i$, где i – вложение X в F_X. Говорят, что в G выполняются соотношения R, если $R \subseteq \operatorname{Ker} \tilde{f}$.[3]

Универсальная группа, удовлетворяющая соотношениям R, называется группой, заданной образующими X и соотношениями R, и обозначается через $\langle X \mid R\rangle$. Точнее, группа $U = \langle X \mid R\rangle$ вместе с функцией $X \to U$ называется группой заданной образующими X и соотношениями R, если в ней выполнены соотношения R и для любой группы G с соотношениями R существует единственный гомоморфизм $U \to G$, для которого диаграмма

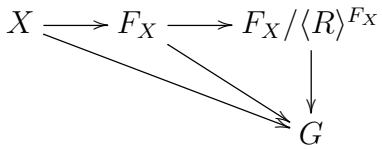


коммутативна.

Пусть $P \leqslant Q$ – группы, а S – подмножество в Q. Напомним, что подгруппа, порожденная S, – это наименьшая подгруппа $\langle S\rangle$ в Q, содержащая S. Наименьшая нормальная подгруппа группы Q, содержащая подгруппу P называется нормальным замыканием P в Q и обозначается P^Q. Нетрудно видеть, что она порождена всеми элементами вида p^q, $p \in P$, $q \in Q$.

Теорема 1.3. *$\langle X \mid R\rangle \cong F_X/\langle R\rangle^{F_X}$. Отображение из X в эту группу – это композиция канонического отображения $X \to F_X$ с канонической проекцией $F_X \to F_X/\langle R\rangle^{F_X}$.*

Доказательство. Пусть G – группа с соотношениями R. Функция $X \to G$ индуцирует единственный гомоморфизм $F_X \to G$. По определению R лежит в ядре этого гомоморфизма. Так как ядро – это нормальная подгруппа, то подгруппа $\langle R\rangle$ и ее нормальное замыкание также лежат в ядре. По универсальному свойству факторгруппы (теорема 5.3 главы 3) существует единственный гомоморфизм $F_X/\langle R\rangle^{F_X} \to G$, делающий следующую диаграмму коммутативной:



Таким образом, группа $F_X/\langle R\rangle^{F_X}$ вместе с указанным отображением из множества X удовлетворяет определению группы, заданной образующими X и сотношениями R. □

Примеры групп, заданных образующими и соотношениями.

(1) $\mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid [x, y]\rangle = \langle x, y \mid [x, y] = 1\rangle = \langle x, y \mid xy = yx\rangle$.
(2) $D_n \cong \langle x, y \mid x^2 = y^2 = (xy)^n = 1\rangle$.

2. Подгруппы свободной группы

Теорема 2.1 (теорема Нильсена–Шрайера). *Любая подгруппа свободной группы свободна.*

Замечание 2.2. При этом количество образующих подгруппы свободной группы с двумя образующими может быть любым от 1 до (счетной) бесконечности.

[3]Второе определение, в отличие от первого, не апеллирует к конструкции свободной группы, а только к ее универсальному свойству. Также как и для многочленов, подстановка значений вместо переменных – это образ элемента свободной группы, являющегося аналогом многочлена, под действием некоторого канонического гомоморфизма.

Существует несколько доказательств теоремы Нильсена–Шрайера. Мы приведем идеи двух геометрических доказательств и полностью изучим алгебраическое доказательство Шрайера, в котором явно строятся свободные образующие.

Топологическое доказательство теоремы Нильсена—Шрайера. Рассмотрим свободную группу F со свободной системой образующих X. Пусть, далее, Y — букет окружностей, занумерованных элементами множества X. Тогда F является фундаментальной группой Y. Каждая подгруппа $H \leqslant F$ является фундаментальной группой какого-то накрытия пространства Y. Однако каждое накрытие Y само гомотопно букету окружностей. Но это и значит, что H свободна. □

Комбинаторно-геометрическое доказательство, приведенное в книге J.-P. Serre "Trees", сразу следует из теоремы о свободном действии группы на дереве. Представим граф, как множество вершин V, множество ребер E, и функции $s, t : E \to V$, сопоставляющие ребру его начало (source) и конец (target). Говорят, что группа G действует на графе (V, E, s, t), если задан гомоморфизм из G в группу автоморфизмов графа. Другими словами, задано действие G на множествах V и E, удовлетворяющие условиям:

$$gs(v) = s(gv) \text{ и } gt(v) = t(gv) \text{ для любых } g \in G \text{ и } v \in V.$$

Граф называется неориентированным, если задан автоморфизм $\bar{\cdot}$ этого графа порядка 2 такой, что $s(\bar{v}) = t(v)$ для любого ребра $v \in V$ (в этом случае ребра v и $\bar{v}$ рассматриваются как одно неориентированное ребро. Будем говорить, что группа G действует свободно на неориентированном графе $(V, E, s, t, \bar{\cdot})$, если она действует свободно на множестве вершин и $gv \neq \bar{v}$ для всех $g \in G$ и $v \in V$. Неориентированный граф без циклов называется деревом.

Графом Кэли группы G относительно системы образующих S называется неориентированный граф, вершинами которого являются элементы группы, а неориентированные ребра соответствуют парам (g, gs) по всем $g \in G$ и $s \in S$. Группа очевидным образом действует на своем графе Кэли: действие на вершинах – это левое умножение, при этом ребро (g, gs) переходит в ребро (hg, hgs) под действием элемента h. Заметим, что это действие свободно тогда и только тогда, когда S не содержит инволюций (т. е. элементов порядка 2).

Лемма 2.3. *Граф Кэли группы G является деревом, на котором группа действует свободно, тогда и только тогда, когда S свободно порождает G.*

Доказательство. Пусть $s_1, \ldots, s_n \in S \cup S^{-1}$, а $w = s_1 \ldots s_n \in F_S$ – редуцированное слово. Канонический образ w в G равен e_G тогда и только тогда, когда ребра, соединяющие вершины $e_G, s_1, s_1 s_2, \ldots, s_1 \ldots s_n = e_G$ образуют цикл. Условие свободы действия необходимо для того, чтобы исключить образующие порядка 2, которые по нашему соглашению образуют не цикл, а определяют неориентированное ребро. □

Таким образом, свободная группа свободно действует на некотором дереве. Оказывается, верно и обратное.

Теорема 2.4. *Группа свободно действует на дереве тогда и только тогда, когда она свободная.*

Отсюда сразу следует теорема Нильсена–Шрайера, потому что любая подгруппа свободной группы свободно действует на том же дереве, на котором свободно действует вся группа.

Третье доказательство теоремы Нильсена–Шрайера основано на следующих двух утверждениях. Пусть $X \subseteq G$ — порождающее множество группы G, $H \leqslant G$, а Y — система представителей левых смежных классов G по H, т. е. $G = HY$, причем, если $Hy_1 = Hy_2$ для $y_1, y_2 \in Y$, то $y_1 = y_2$. Будем считать, что $H \cap Y = \{1\}$. Рассмотрим проекцию $G \to Y$, $g \mapsto \overline{g}$, которая каждому $g \in G$ сопоставляет тот единственный $\overline{g} \in Y$, для которого $H\overline{g} = Hg$. По нашему соглашению относительно представителя H для любого $h \in H$ имеем $\overline{h} = 1$.

Теорема 2.5 (Теорема Шрайера). *Подгруппа H порождается множеством*

$$Z = \{yx \cdot (\overline{yx})^{-1} \mid y \in Y,\, x \in X\}.$$

Доказательство. Так как $Hyx = H\overline{yx}$, все элементы из Z действительно лежат в H. Для доказательства того, что они порождают H, воспользуемся "трюком накопления". Запишем элемент $h \in H$ в виде произведения образующих: $h = x_1 \dots x_l$, где $x_1, \dots, x_l \in X \cup X^{-1}$. Так как $\overline{x_1 \dots x_l} = \overline{h} = 1$, то можно переписать выражение для h в виде

$$h = \big(1 \cdot x_1(\overline{1 \cdot x_1})^{-1}\big)\big(\overline{x_1}x_2(\overline{x_1x_2})^{-1}\big)\big(\overline{x_1x_2}x_3(\overline{x_1x_2x_3})^{-1}\big) \dots \big(\overline{x_1 \dots x_{l-1}}x_l(\overline{x_1 \dots x_l})^{-1}\big),$$

Докажем, что все сомножители в правой части лежат в $Z \cup Z^{-1}$. Прежде всего, заметим, что, так как $H\overline{g_1} = Hg_1$, то $H\overline{g_1}g_2 = Hg_1g_2$, откуда $\overline{\overline{g_1}g_2} = \overline{g_1g_2}$ для любых $g_1, g_2 \in G$. Если $x_k \in X$, то

$$\overline{x_1 \dots x_{k-1}}x_k(\overline{x_1 \dots x_k})^{-1} = yx_k \cdot (\overline{yx_k})^{-1} \in Z,$$

где $y = \overline{x_1 \dots x_{k-1}} \in Y$.

Пусть теперь $x_k = x^{-1}$ для некоторого $x \in X$, а $y \in Y$. Положим $\tilde{y} = \overline{yx^{-1}}$. Тогда $\overline{\tilde{y}x} = \overline{yx^{-1}x} = y$. Следовательно,

$$\Big(yx^{-1} \cdot (\overline{yx^{-1}})^{-1}\Big)^{-1} = \tilde{y}x \cdot y^{-1} = \tilde{y}x \cdot (\overline{\tilde{y}x})^{-1} \in Z.$$

Таким образом, $yx_k \cdot (\overline{yx_k})^{-1} \in Z^{-1}$, что завершает доказательство. □

Следствие 2.6. *Подгруппа конечного индекса в конечнопорожденной группе конечно порождена.*

Следующее утверждение, также принадлежащее Шрайеру, говорит о выборе "хорошего" множества представителей смежных классов по подгруппе H свободной группы F_X. Пусть $U \subseteq F_X$, а $g \in F_X$. Обозначим через $l(g)$ длину редуцированного слова в алфавите $X \cup X^{-1}$ равного g и положим $l(U) = \min\limits_{g \in U} l(g)$. Система представителей Y смежных классов F_X по H называется минимальной, если для любого $g \in F_X$ длина представителя $\overline{g}$ смежного класса Hg равна $l(Hg)$. Система Y называется шрайеровской трансверсалью, если любой начальный отрезок редуцированного слова из Y принадлежит Y (в частности, пустое слово принадлежит Y). Ясно, что достаточно требовать, чтобы для каждого редуцированного слова $x_1 \dots x_n \in Y$ слово $x_1 \dots x_{n-1}$ также лежало бы в Y (т. е. брать отрезки на 1 меньшей длины).

Лемма 2.7. *Для любой подгруппы $H \leqslant F_X$ существует минимальная шрайеровская трансверсаль Y.*

Доказательство. Строим представитель $Y \cap Hg$ индукцией по $n = l(Hg)$. При $n = 0$ выбираем нейтральный элемент (пустое слово). Пусть теперь $n > 0$, а $h = x_1 \dots x_n$, $x_i \in X \cup X^{-1}$, – слово наименьшей длины в Hg. Пусть $u = x_1 \dots x_{n-1}$ — начальный отрезок этого слова. Так как $l(Hu) < n$, то по индукционному предположению мы уже выбрали представителя Hu в Y. Пусть, скажем, $H\overline{u} = Hu$, где $\overline{u}$ – такой представитель, $l(\overline{u}) = m \leqslant n-1$, а $\overline{u} = t_1 \dots t_m$, $t_i \in X \cup X^{-1}$, – его приведенное разложение. Тогда $H\overline{u}x_n = Hux_n = Hh = Hg$. Так как h – элемент наименьшей длины в своем смежном классе, то $m + 1 \geqslant l(\overline{u}x_n) \geqslant l(h) = n$. Таким образом, $m = n - 1$ и значит, $y = \overline{u}x_n = t_1 \dots t_{n-1}x_n$ является приведенным разложением y. Выберем y в качестве представителя смежного класса Hg. Очевидно, что для него выполняется условие, фигурирующее в определении минимальной шрайеровской системы. □

Пусть H произвольная группа, а Z – произвольная система образующих H такая, что $Z \cap Z^{-1} = \varnothing$. Для того чтобы доказать, что $H \cong F_Z$, достаточно проверить, что непустое редуцированное слово в алфавите $Z \cup Z^{-1}$ не равно 1 в H. Действительно, по универсальному свойству свободной группы существует единственный гомоморфизм $\varphi : F_Z \to H$, отображающий однобуквенные слова в соответствующие элементы множества Z. Так как система образующих группы H лежит в образе φ, то φ сюръективно. Ядро φ – это множество редуцированных слов (точнее, их классов эквивалентности), которые отображаются в 1_H, а приведенное выше условие как раз и говорит,

что таких непустых слов не существует. Это простое соображение вместе с двумя предыдущими леммами лежит в основе нашего доказательства теоремы Нильсена–Шрайера.

Доказательство теоремы Нильсена–Шрайера. Пусть H – подгруппа свободной группы F_X, Y – шрайеровская трансверсаль к H (не обязательно минимальная), существование которой обеспечивает предыдущая лемма, а $\bar{\cdot} : F_X \to Y$ – проекция из теоремы 2.5. Также как в теореме 2.5 возьмем систему образующих

$$Z = Z(X) = \{yx(\overline{yx})^{-1} \mid y \in Y,\, x \in X\} \smallsetminus \{1\}$$

группы H (естественно, единичный элемент можно выбросить из системы образующих) и докажем, что множество Z свободно порождает H.

Легко видеть (это уже было в доказательстве теоремы Шрайера), что $Z(X)^{-1} \subseteq Z(X^{-1})$. Аналогично, $Z(X^{-1})^{-1} \subseteq Z(X)$, откуда $Z(X)^{-1} = Z(X^{-1})$. Таким образом, $Z \cup Z^{-1} = Z(X \cup X^{-1})$.

Начнем с доказательства того, что естественное представление элемента из $Z(X \cup X^{-1})$ несократимо. Пусть $x \in X \cup X^{-1}$, а $y \in Y$. Ясно, что

$$yx \in Y \iff yx = \overline{yx} \iff yx(\overline{yx})^{-1} = 1.$$

Пусть $y = x_1 \dots x_n$ и $\tilde{y} = \overline{yx} = t_1 \dots t_m$ представлены редуцированными словами, где $x_i, t_i \in X \cup X^{-1}$. Если $yx \notin Y$, то слово $x_1 \dots x_n x t_m^{-1} \dots t_1^{-1}$, представляющее элемент $yx\tilde{y}^{-1}$ из $Z(X \cup X^{-1})$, также редуцировано. Действительно, если $x = x_n^{-1}$, то $yx = x_1 \dots x_{n-1} \in Y$, так как система представителей шрайеровская, а если $x = t_m$, то $\tilde{y}x^{-1} = t_1 \dots t_{m-1} \in Y$, по той же причине. Но тогда $\tilde{y}x^{-1} = \overline{\tilde{y}x^{-1}} = \overline{yxx^{-1}} = y$, откуда опять $yx = \tilde{y} \in Y$, что противоречит предположению. В других же местах сокращения не могут произойти.

Далее рассмотрим произведения двух элементов $z = yx(\overline{yx})^{-1}$ и $z' = uv(\overline{uv})^{-1}$ из $Z \cup Z^{-1}$ (т. е. $x, v \in X \cup X^{-1}$, а $y, u \in Y$). Положим, $\tilde{u} = \overline{uv}$ и предположим, что $z' \neq z^{-1}$. Докажем, что при этом условии

$$v\tilde{u}^{-1}yx = vwx, \qquad \text{т. е.} \qquad z'z = uvwx(\overline{yx})^{-1},$$

где w и vwx несократимые слова (при этом w может быть пустым). Пусть $\tilde{u} = t_1 \dots t_k$ и $y = x_1 \dots x_m$ – редуцированные слова (здесь $x_i, t_i \in X \cup X^{-1}$). Так как z и z' не равны 1, то их естественные представления несократимы, т. е. $v \neq t_k$, а $x \neq x_m^{-1}$. Для определенности предположим, что $k \geqslant m$ (ситуация $m < k$ аналогична случаю $m > k$). Если $y \neq t_1 \dots t_m$, то $v\tilde{u}^{-1}yx = vwx$, где w – несократимое слово начинающееся с t_k^{-1} и заканчивающееся x_m. Следовательно, слово vwx также редуцировано.

Пусть теперь $y = t_1 \dots t_m$. Если $k = m$, то $v\tilde{u}^{-1}yx = vx$. Если $v = x^{-1}$, то $(\overline{yx})^{-1} = (\overline{\tilde{u}v^{-1}})^{-1} = u^{-1}$, следовательно, $z' = z^{-1}$, что противоречит предположению. В противном случае возьмем в качестве w пустое слово. Наконец, если $k > m$, то $v\tilde{u}^{-1}yx = vt_k^{-1} \dots t_{m+1}^{-1}x$. Если $x \neq t_{m+1}$, то последнее слово несократимо. В противном случае $yx = t_1 \dots t_{m+1}$, что лежит в Y, так как это начало слова $v \in Y$, а Y шрайеровская. Но это противоречит предположению о том, что $z \neq 1$.

Из доказательства следует, что если $z' = z^{-1}$, то $v = x^{-1}$, а это невозможно при $v, x \in X$. Поэтому пересечение $Z(X) \cap Z(X)^{-1}$ пусто.

Доказательство заканчивает индукция по длине произведения элементов из $Z \cup Z^{-1}$. Пусть $z_i = y_i x_i (\overline{y_i x_i})^{-1} \in Z \cup Z^{-1}$. Индукцией по n докажем, что редуцированная форма элемента $z_1 \dots z_n$ оканчивается на $x_n(\overline{y_n x_n})^{-1}$ и, следовательно, это произведение не равно 1. База $n = 1$ уже доказана там, где говорится, что $xy(\overline{yx})^{-1}$ либо равно 1, либо несократимо (естественно, везде предполагается, что $(\overline{yx})^{-1}$ записано редуцированным словом).

По индукционному предположению $z_1 \dots z_{n-1} = tx_{n-1}(\overline{y_{n-1}x_{n-1}})^{-1}$. По доказанному ранее $x_{n-1}(\overline{y_{n-1}x_{n-1}})^{-1}y_n x_n = x_{n-1}wx_n$, причем последняя запись несократима. Следовательно,

$$z_1 \dots z_n = tx_{n-1}(\overline{y_{n-1}x_{n-1}})^{-1}y_n x_n (\overline{y_n x_n})^{-1} = tx_{n-1}wx_n(\overline{y_n x_n})^{-1}.$$

□

Рассмотрим следующий пример. Пусть $X = \{t, x\}$ и $F = F_X$ – свободная группа с двумя образующими. Построим множество шрайеровских образующих коммутанта группы F. Ясно, что факторгруппа по коммутанту – это свободная абелева группа (т.е. свободный $\mathbb{Z}$-модуль) с двумя образующими. Короче, $F/[F,F] \cong \mathbb{Z} \oplus \mathbb{Z}$. Естественный представитель класса эквивалентности, отображающегося в (n,k) – элемент $t^n x^k$. Ясно, что трансверсаль $Y = \{t^n x^k \mid n,k \in \mathbb{Z}\}$ является шрайеровской. Далее, $(t^n x^k)x \in Y$, поэтому из таких произведений не возникают элементы шрайеровской системы образующих. Зато $(t^n x^k)t \notin Y \iff k \neq 0$, и $\overline{(t^n x^k)t} = t^{n+1}x^k$. Таким образом,

$$(t^n x^k)t(t^{n+1}x^k)^{-1} = t^n x^k t x^{-k} t^{-n-1} \in Z$$

(заметим, что последний элемент является коммутатором $[t^n x^k t^{-n}, t]$). Легко видеть, что все такие слова являются редуцированными и, следовательно, различны в F. По доказательству теоремы Нильсена–Шрайера получаем, что подгруппа $[F,F]$ свободно порождена множеством $Z = \{t^n x^k t x^{-k} t^{-n-1} \mid k,n \in \mathbb{Z},\ k \neq 0\}$ и является свободной группой со счетным числом образующих.

3. Действие группы на множестве и лемма Бернсайда

Определение 3.1. Пусть G – группа, а X – множество. Будем говорить, что G действует на X и писать $G \curvearrowright X$, если задана операция $G \times X \to X$ (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 $\theta : G \to S_X$ задает действие группы G на множестве X по правилу $gx = \theta(g)(x)$ (проверьте, что эта операция действительно удовлетворяет условиям определения 3.1). Обратно, если задано действие G на X, то можно задать гомоморфизм $\theta : G \to S_X$ формулой $\theta(g)(x) = gx$ (проверьте, что $\theta(g)$ – биекция, и что θ – 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 3.2. 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 3.3. *Орбитой* элемента $x \in X$ под действием G называется множество $Gx = \{gx \mid g \in G\}$. Количество элементов в данной орбите называется *длиной орбиты* (в разных орбитах может быть разное количество элементов).

Лемма 3.4. *Любые две орбиты либо не пересекаются, либо совпадают. Таким образом, множество X разбивается в дизъюнктное объединение орбит.*

Доказательство этого утверждения практически совпадает с доказательством аналогичного утверждения для смежных классов.

Определение 3.5. Неподвижными точками элемента $g \in G$ называются те $x \in X$, для которых $gx = x$. *Множество неподвижных точек* элемента g мы будем обозначать через $\mathrm{Fix}_X(g)$.

Определение 3.6. Множество элементов группы G, оставляющих на месте данный элемент $x \in X$ называется *стабилизатором* элемента x и обозначается через G_x. Другими словами, $G_x = \{g \in G \mid gx = x\}$. Очевидно, что стабилизатор является подгруппой в G.

Замечание 3.7. Обратите внимание на то, что количество пар $(g, x) \in G \times X$, для которых $gx = x$ можно вычислить двумя способами, которые указаны в разных частях следующего равенства:

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

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 3.8. *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 3.9. 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 $gx = x \implies g = 1$, другими словами, если $\forall x \in X$: $G_x = \{1\}$.
- Действие называется транзитивным, если $\forall x, y \in X\, \exists g \in G : gx = y$, другими словами, $\forall x \in X :\ Gx = X$ (квантор не имеет значения, равносильно можно написать $\exists x \in X : Gx = X$).

Примеры.

- $S_n \curvearrowright \{1, \dots, n\}$.
- $\mathrm{GL}_n(R) \curvearrowright R^n$.
- $G \curvearrowright G$, 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 3.10 (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 3.8 получим $N=\sum_{x\in X}\frac{|G_x|}{|G|}=\frac{1}{|G|}\sum_{x\in X}|G_x|$. Используя формулу из замечания 3.7 получим $N=\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}_X(g)|$, что и требовалось доказать. □

4. Классификация G-множеств

Перейдем теперь к классификации действий данной группы G на множестве. При этом удобно будет говорить, что если G действует на множестве X, то X является G-множеством (по аналогии с R-модулем). Во-первых, надо понять, с точностью до чего будет происходить классификация, т. е. что такое изоморфизм G-множеств.

Определение 4.1. Пусть X,Y – G-множества. Функция $f:X\to Y$ называется G-эквивариантной, если $f(gx)=g\,f(x)$ для любых $x\in X$ и $g\in G$.

Изоморфизмами G-множеств являются G-эквивариантные биекции.

В этом параграфе мы дадим классификацию G-множеств с точностью до изоморфизма.

Лемма 4.2. *Стабилизаторы точек из одной орбиты сопряжены.*

Доказательство. Пусть $x\in X$, а $y\in Gx$, т. е. существует $g\in G$ такое, что $y=gx$. Тогда

$$h\in G_y \iff hy=y \iff hgx=gx \iff g^{-1}hgx=x \iff g^{-1}hg\in G_x.$$

Таким образом, $G_x=g^{-1}G_yg$, что и требовалось. □

Определение 4.3. Если $G\curvearrowright X$ транзитивно, то X называется однородным G-множеством.

Если H – подгруппа в G, то G действует на множестве левых смежных классов G/H по формуле $g(xH)=(gx)H$, $g,x\in G$. Такое действие называется стандартным однородным G-множеством.

Теорема 4.4. *Любое однородное G-множество X изоморфно стандартному однородному G-множеству. Точнее, $X\cong G/G_x$ для любой точки $x\in X$.*

G-множества G/H и G/F изоморфны тогда и только тогда, когда подгруппы H и F сопряжены.

Доказательство. Рассмотрим функцию $\varphi:G/G_x\to Gx=X$, $\varphi(gG_x)=gx$, заданную в лемме 3.8, где проверено, что это отображение биективно. Проверка того, что это отображение G-эквивариантно, не составляет труда.

Пусть $F=gHg^{-1}$. Докажем, что $F=G_{gH}$ – стабилизатор элемента gH при действии G на G/H. Действительно,

$$f(gH)=gH \iff g^{-1}fgH=H \iff g^{-1}fg\in H \iff f\in gHg^{-1}=F.$$

Следовательно, по первой части доказательства $G/H\cong G/F$.

Обратно, пусть φ – изоморфизм G-множеств $G/H\xrightarrow{\sim}G/F$, а $\varphi(H)=gF$. Для любого $h\in H$ имеем: $gF=\varphi(H)=\varphi(hH)=h\varphi(H)=hgF$, откуда $g^{-1}hg\in F$. Таким образом, $g^{-1}Hg\subseteq F$.

Для доказательства обратного включения заметим, что $\varphi(H) = gF \iff F = \varphi(g^{-1}H) \iff \varphi^{-1}(F) = g^{-1}H$. Следовательно, для любого $f \in F$ имеем $g^{-1}H = \varphi^{-1}(fF) = f\varphi^{-1}(F) = fg^{-1}H$, откуда $gfg^{-1} \in H$. □

Следствие 4.5 (классификация G-множеств). *Любое G-множество изоморфно $\bigsqcup\limits_{i\in\mathscr{I}} G/H_i$, где $\mathscr{I}$ – некоторое множество индексов, а H_i – подгруппа в G. Такое представление единственно, с точностью до перестановки элементов множества $\mathscr{I}$ и замены каждой H_i на сопряженную. Точнее, если*

$$\bigsqcup_{i\in\mathscr{I}} G/H_i \cong \bigsqcup_{j\in\mathscr{J}} G/F_j,$$

то существует биекция $\sigma : \mathscr{I} \to \mathscr{J}$ и элементы $g_i \in G$ такие, что $g_i H_i g_i^{-1} = F_{\sigma(i)}$.

5. Несколько приложений действия группы на множестве

Естественное приложение леммы Бернсайда – задачи о раскрасках. Оно подробно описаны в моем тексте `http://alexei.stepanov.spb.ru/students/algebra3/Bernside.pdf`. Такие задачи естественно разбирать на практических занятиях. В этом же параграфе мы рассмотрим менее очевидные приложения действия групп на множествах. На самом деле, все утверждения этого параграфа являются несложными задачами, которые показывают, как можно использовать изученный в предыдущих двух параграфах материал.

Пусть $H \leqslant G$. *Сердцевиной* подгруппы H называется наибольшая нормальная подгруппа в G, содержащаяся в H. Сердцевина H равна

$$\operatorname{Core} H = \bigcap_{g\in G} H^g.$$

Предложение 5.1. *Ядро транзитивного действия $G \curvearrowright X$ равно $\operatorname{Core} G_x = \cap_{y\in X} G_y$, где $x \in X$.*

Доказательство. Ядро действия по определению есть пересечение стабилизаторов всех точек из X. По лемме 4.2 все эти стабилизаторы сопряжены в G. Легко проверить также, что $gG_xg^{-1} = G_{gx}$, т. е. все подгруппы, сопряженные с G_x являются стабилизаторами точек. □

Теорема 5.2. *Пусть H – подгруппа индекса n в G. Тогда индекс $\operatorname{Core} H$ конечен и делит $n!$. В частности, если в бесконечной группе есть подгруппа конечного индекса, то есть и нормальная подгруппа конечного индекса.*

Доказательство. Стандартное однородное пространство G/H задает гомоморфизм $\theta : G \to S_n$. Порядок образа этого гомоморфизма равен индексу ядра, т. е. $|G : \operatorname{Core} H|$. □

Следующее утверждение – задача, которую я услышал от А. С. Меркурьева, показывает еще один трюк, связанный с гомоморфизмом $G \to S_n$, который возникает при действии G на n-элементном множестве.

Упражнение 5.3. Пусть G – группа четного порядка. Зададим функцию $\varphi : G \to \mathbb{Z}_2$ формулой $\varphi(g) = |G|/\operatorname{ord} g \mod 2$. Докажите, что эта функция – гомоморфизм.

Решение. Пусть $|G| = 2n$. Рассмотрим действие G на себе левыми трансляциями, соответствующее отображение $\theta : G \to S_{2n}$ и его композицию с четностью перестановки $\varepsilon : S_{2n} \to \mathbb{Z}_2$. Если $k = \operatorname{ord} g$, то g отображается в перестановку, состоящую из k-циклов (эти циклы – соответствуют правым смежным классам по $\langle g\rangle$). Четность такой перестановки равна $(k-1)\cdot\frac{2n}{k} = 2n - \frac{2n}{k} \equiv \frac{2n}{k} \mod 2$. Таким образом, функция из условия задачи – это и есть гомоморфизм $\varepsilon \circ \theta$. □

Вот еще одна задача, которую в разных вариациях любят давать на мат-меховских экзаменах.

Упражнение 5.4. Пусть p – наименьшее простое число, делящее порядок группы G. Тогда подгруппа индекса p нормальна в G. В частности, подгруппа индекса 2 всегда нормальна, подгруппа индекса 3 нормальна в группе нечетного порядка и т. п.

Решение. Пусть $|G : H| = p$ – простое, а $|G|$ не делится на простые, меньшие p. Тогда $|G|$ взаимно просто с $(p-1)!$, а индекс $|G : \operatorname{Core} H|$ делит $|G|$ и $p!$. Так как $\gcd(|G|, p!) = p$, то $|G : H| \leqslant |G : \operatorname{Core} H| = p$, откуда $\operatorname{Core} H = H$. □

6. Теоремы о гомоморфизме и лемма о бабочке

В этом параграфе мы докажем несколько технических утверждений, несложно вытекающих из теоремы о гомоморфизме. В следующем утверждении сформулирован наиболее общий факт типа второй теоремы об изоморфизме. Сама теорема, также как и чуть более сложное утверждение, лемма о бабочке, являются его простыми следствиями.

Будем говорить, что подгруппа A нормализует подгруппу B, если $a^{-1}Ba = B$ для любого $a \in A$. Другими словами, A нормализует B, если она содержится в нормализаторе

$$N_G(B) := \{g \in G \mid B^g = B\}$$

подгруппы в B в группе G. В этом случае $AB = \{ab \mid a \in A,\, b \in B\}$ является подгруппой в G, в которой B нормальна.

Лемма 6.1. *Пусть $C \leqslant B$ и A – подгруппы группы G такие, что $B \trianglelefteq \langle A \cup C\rangle$. Тогда*

$$\frac{\langle A \cup C\rangle}{B} \cong \frac{A}{A \cap B}.$$

Доказательство. Обозначим $D = \langle A \cup C\rangle$. Из условия $B \trianglelefteq D$ следует, что A нормализует B, и, следовательно, $D \leqslant \langle A \cup B\rangle = AB$. Рассмотрим гомоморфизм $\varphi : A \to D/B$, являющийся композицией вложения и канонической проекции $A \hookrightarrow D \twoheadrightarrow D/B$. Любой элемент $d \in D$ представляется в виде $d = ab$ для некоторых $a \in A$ и $b \in B$. Тогда $\varphi(a) = dB$, откуда следует сюръективность φ. Условие $\varphi(a) = 1_{D/B} = B$ равносильно тому, что $a \in A \cap B$, т. е. ядро φ равно $A \cap B$. По теореме о гомоморфизме получаем искомый изоморфизм. □

При $C = B$ из предыдущей леммы получаем следующее утверждение.

Теорема 6.2 (2-я теорема о гомоморфизме). *Если A нормализует B, то*

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

Теорема 6.3 (3-я теорема о гомоморфизме). *Пусть $K \trianglelefteq G$, а $\pi : G \to G/K$ – канонический гомоморфизм. Тогда отображение $H \mapsto \pi(H)$ является биекцией множества подгрупп в G, содержащих K, на множество подгрупп в G/K. При этом H нормальна в G тогда и только тогда, когда $\pi(H)$ нормальна в G/K и*

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

(здесь $\pi(H)$ обозначена за H/K, так как эти группы даже не просто изоморфны, а равны).

Доказательство. Обратным к заданному отображению будет взятие полного прообраза. Очевидно, что $\pi\big(\pi^{-1}(F)\big) = F$ и $\pi^{-1}\big(\pi(H)\big) \supseteq H$. Если $g \in \pi^{-1}\big(\pi(H)\big)$, т. е. $\pi(g) = \pi(h)$ для некоторого $h \in H$, то $gh^{-1} \in \operatorname{Ker}\pi = K \leqslant H$, откуда $g \in hH = H$.

Так как при нашей биекции сопряженные подгруппы переходят в сопряженные, утверждение о нормальности очевидно. Для доказательства изоморфизма зададим гомоморфизм $\pi' : G \to \frac{G/K}{H/K}$ как композицию двух канонических проекций. Композиция сюръекций сюръективна, с другой стороны $\operatorname{Ker}\pi' = \pi^{-1}(H/K) = H$. Теперь результат следует из первой теоремы о гомоморфизме. □

Теорема 6.4 (лемма о бабочке). *Пусть $A' \trianglelefteq A$ и $B' \trianglelefteq B$ – подгруппы некоторой группы G. Тогда*

$$\frac{A \cap B}{(A \cap B')(B \cap A')} \cong \frac{A'(A \cap B)}{A'(A \cap B')} \cong \frac{B'(B \cap A)}{B'(B \cap A')}.$$

Доказательство. Легко видеть, что $A \cap B$ нормализует A', B', $A \cap B'$ и $B \cap A'$, поэтому все произведения подгрупп в формуле, которую требуется доказать, корректно определены. По лемме 6.1 $\frac{A'(A\cap B)}{A'(A\cap B')} \cong \frac{A\cap B}{F}$, где $F = \big(A'(A \cap B')\big) \cap A \cap B$. Так как $A'(A \cap B') \subseteq A$, то $F = \big(A'(A\cap B')\big)\cap B$. Любой элемент из $A'(A\cap B')$ записывается в виде ab, где $a \in A'$, а $b \in A\cap B' \subseteq B$. Если этот элемент лежит в $F \subseteq B$, то $a \in A' \cap B$. Таким образом, $F \subseteq (A' \cap B)(A \cap B')$. Обратное включение очевидно. Итак, мы доказали, что первая факторгруппа в формуле изоморфна второй. Аналогично доказывается, что первая факторгруппа изоморфна третьей. □

7. Теоремы Силова

Далее в этом параграфе G – конечная группа, а p – простое число. Группа порядка p^k называется p-группой.

Определение 7.1. p-Подгруппа $S \leqslant G$ называется силовской p-подгруппой, если ее индекс взаимно прост с p.

Целью этого параграфа является доказательство существования силовских подгрупп и их основных свойств. Для этого нам потребуется несколько вспомогательных утверждений.

Лемма 7.2. *Если A, B – p-подгруппы в G, причем A нормализует B, то AB также является p-подгруппой.*

Доказательство. По второй теореме об изоморфизме 6.2 $\frac{AB}{B} \cong \frac{A}{A\cap B}$, отуда $|AB| = |B|\cdot|\frac{A}{A\cap B}|$, что очевидно является степенью числа p. □

Лемма 7.3. *Пусть $G \curvearrowright X$. Предположим, что индекс любой собственной подгруппы G делится на p. Тогда количество неподвижных точек под действием G сравнимо с $|X|$ по модулю p.*

Доказательство. Длина орбиты равна индексу стабилизатора точки. Если этот стабилизатор – собственная подгруппа, т. е. если точка не является неподвижной, то по условию длина ее орбиты делится на p. Количество элементов в X равно сумме длин орбит, следовательно, по модулю p оно сравнимо с суммой длин одноэлементных орбит, т. е. с количеством неподвижных точек. □

Напомним, что центром группы G называется множество элементов, коммутирующих со всеми элементами группы G:

$$\mathrm{Center}(G) = \{c \in G \mid cg = gc \forall g \in G\}.$$

Следствие 7.4. *Любая p-группа имеет нетривиальный центр.*

Доказательство. Рассмотрим действие p-группы G на себе сопряжениями. По лемме 7.3 количество неподвижных точек сравнимо с порядком группы по модулю p, а значит, делится на p. Но оно ненулевое, так как одна из неподвижных точек – нейтральный элемент группы. □

Теорема 7.5 (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 $|G| = p^n m$, где m не делится на p.

Пусть существует собственная подгруппа H в G, индекс которой взаимно прост с p. Тогда по индукционному предположению в H существует силовская p-подгруппа, которая будет силовской p-подгруппой в G. В противном случае рассмотрим действие G на себе сопряжениями. По лемме 7.3 количество неподвижных точек этого действия делится на p, т. е. порядок центра группы G

делится на p. Предположим, что он равен $p^k l$, где l не делится на p. По теореме о строении конечнопорожденных абелевых групп в центре существует подгруппа C порядка p^k. По индукционному предположению в группе G/C, имеющей порядок $p^{n-k}m$, существует силовская p-подгруппа $\overline{P}$, которая имеет порядок p^{n-k}. Обозначим через P полный прообраз группы $\overline{P}$ под действием гомоморфизма редукции $\rho : G \to G/C$. Пусть $\pi : P \to \overline{P}$ – сужение ρ на P. Тогда $|\operatorname{Ker}\pi| = |C| = p^k$, а $|\operatorname{Im}\pi| = |\overline{P}| = p^{n-k}$. Следовательно, $|P| = p^n$, и P является силовской p-подгруппой в G.

$\mathbf{C}_p$+$\mathbf{D}_p$. Пусть H – p-подгруппа, а S – силовская p-подгруппа. Рассмотрим действие H на G/S левыми трансляциями. По лемме существует неподвижная точка этого действия, скажем, $HxS = xS$. Тогда $x^{-1}Hx \subseteq S$, что доказывает, что H содержится в силовской p-подгруппе xSx^{-1}. С другой стороны, если H была силовской, то мы доказали, что H и S сопряжены.

$\mathbf{F}_p$. Рассмотрим действие силовской p-подгруппы S на множестве X всех силовских p-подгрупп сопряжением. Если $\{P\}$ – неподвижный элемент этого действия, то S нормализует P. Тогда по лемме 7.2 PS является p-подгруппой и, следовательно, совпадает с S. Таким образом, у этого действия ровно одна неподвижная точка. Теперь, по лемме 7.3 $1 \equiv |X| \mod p$, что и требовалось доказать. □

Лемма 7.6 (аргумент Фраттини). *Пусть H – конечная нормальная подгруппа группы G, а P – силовская подгруппа в H. Тогда $G = N_G(P) \cdot H$.*

Доказательство. Для любого $g \in G$ рассмотрим подгруппу P^g. Так как $P \leqslant H \trianglelefteq G$, то $P^g \leqslant H$, и, следовательно, является силовской подгруппой в H. Так как силовские подгруппы сопряжены, существует элемент $h \in H$ такой, что $P^h = P^g$, откуда $P^{gh^{-1}} = P$, т. е. $gh^{-1} \in N_G(P)$. Таким образом, $g \in N_G(P)h \subseteq N_G(P) \cdot H$. □

Следствие 7.7. *Любая подгруппа, содержащая нормализатор силовской подгруппы, самонормализуема.*

Доказательство. Пусть P – силовская подгруппа группы F. Пусть H содержит ее нормализатор $N_F(P)$, и положим $G = N_F(H)$. Заметим, что силовская подгруппа P группы F является силовской подгруппой и в любой промежуточной между P и F подгруппой, в частности, P – силовская в H. В соответствие с аргументом Фраттини $G = N_G(P) \cdot H \leqslant N_F(P) \cdot H = H$. □

Упражнение 7.8. Для подгруппы B группы G следующие условия эквивалентны.

(1) Любая надгруппа группы B самонормализуема, и никакие 2 различные надгруппы не сопряжены.
(2) $x \in \langle B, B^x\rangle$ для любого $x \in G$.
(3) $B \not\subseteq H^x$ для любых $B \leqslant H \leqslant G$ и $x \in G \setminus H$.

Подгруппа B, удовлетворяющая условиям последнего упражнения, называется абнормальной.

Упражнение 7.9. Докажите, что нормализатор силовской подгруппы абнормален.

Упражнение 7.10. Докажите, что в полной линейной группе $\mathrm{GL}_n(F)$ над конечным полем F характеристики p одна из силовских p-подгрупп – это группа верхних унитреугольных матриц $U_n(F)$,[4] а ее нормализатор – это группа всех обратимых верхнетреугольных матриц $B_n(F)$.

Из двух последних утверждений следует, что $B_n(F)$ абнормальна. Оказывается, что это верно над любым полем.

Упражнение 7.11. Пусть K – произвольное поле. Докажите, что $B_n(K)$ абнормальна в $\mathrm{GL}_n(K)$.

[4]Все остальные силовские p-подгруппы с ней сопряжены, т. е. становятся группой верхних унитреугольных матриц после замены базиса.

8. Полупрямое произведение

В категории $\mathscr{C}$ рассмотрим морфизмы $A \xrightarrow{\varphi} B \xrightarrow{\psi} A$, композиция которых равна id_A. В этом случае морфизм ψ называется ретракцией, а φ называется сечением морфизма ψ. Заметим, что в этом случае φ обязано быть мономорфизмом, а ψ – 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 8.1. *Пусть H, K – подгруппы в G, причем K нормальна. Следующие условия эквивалентны.*

(1) *Существует 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 6.2).*
(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 ψ – 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. ψ – 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 ψ тождественна. □

Определение 8.2. Если выполнены условия предложения 8.1, то G называется (внутренним) полупрямым произведением подгрупп H и K; это обозначается через $G = K \rtimes H$.

Пусть $G = K \rtimes H$, а $\theta : H \to S_K$ – гомоморфизм, определяющий действие H на K левым сопряжением, т. е. $\theta(h)(k) = hkh^{-1}$. Легко проверить, что сопряжение является автоморфизмом, т. е. образ θ 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 8.3. Пусть G – декартово произведение множеств A и B. Определим умножение на G формулой

$$(a, b) \cdot (a', b') = (a\theta(b)(a'), bb').$$

Тогда G называется (внешним) полупрямым произведением групп A и B, соответствующим θ и обозначается $G = A \rtimes_\theta B$.

Также как и в случае прямого произведения, внешнее полупрямое произведение после некоторых отождествлений становится внутренним.

Предложение 8.4. *Пусть $G = A \rtimes_\theta B$. Положим $A' = A \times \{1_B\}$ и $B' = \{1_A\} \times B$. Тогда G является внутренним полупрямым произведением $A' \rtimes B'$.*

Обратно, если G – внутреннее полупрямое произведение своих подгрупп $K \rtimes H$, а $\theta : H \to \mathrm{Aut}(K)$ – действие H на K левыми сопряжениями, то $G \cong K \rtimes_\theta H$.

Одним из простых геометрических примеров полупрямого произведения является группа автоморфизмов аффинного пространства.

Определение 8.5. Пусть V – векторное пространство над произвольным полем F. Если аддитивная группа V свободно и транзитивно действует на множестве A, то пара (A, V) называется аффинным пространством над F. Действие V на A обычно обозначается сложением: $(a, v) \mapsto a+v$.

Аффинным отображением $\varphi : (A, V) \to (A', V')$ называется пара (φ_v, φ_a), состоящая из линейного отображения $\varphi_v : V \to V'$ и функции $ph_a : A \to A'$, для которых имеет место тождество $\varphi_a(a + v) = \varphi_a(a) + \varphi_v(v)$. Нетрудно видеть, что φ_a однозначно определяется заданием образа одной точки $a \in A$ и линейным отображением φ_v. Действительно, по условию для любой $b \in A$ существует единственный вектор $v \in V$ такой, что $b = a+v$, следовательно, $\varphi_a(b) = \varphi_a(a)+\varphi_v(v)$. Аффинное отображение φ называется изоморфизмом, если φ_v изоморфизм (тогда φ_a автоматически является биекцией).

Пара (B, W) называется аффинным подпространством пространства (A, V), если $B \subseteq A$, $W \leqslant V$, и эта пара сама является аффинным пространством относительно той же операции. Пара (B, W), $B \subseteq A$, $W \leqslant V$, является аффинным подпространством тогда и только тогда, когда $b + w \in B$ для любых $b \in B$ и $w \in W$ и W действует транзитивно на B.

Если мы рассмотрим регулярное действие V на себе, то получим *стандартное* аффинное пространство (V, V).[5] Нетрудно видеть, что любое аффинное пространство изоморфно стандартному. Если $\varphi_v : V \to V$ тождественное отображение, то изоморфизм φ однозначно определяется выбором базовой точки множества A, т. е. образом нуля при отображении φ_a. Давайте изучим строение группы автоморфизмов стандартного аффинного пространства.

Предложение 8.6. *Группа автоморфизмов аффинного пространства (V, V) изоморфна полупрямому произведению $V \rtimes \mathrm{Aut}(V)$. Если $\dim V = n < \infty$, то эта группа изоморфна подгруппе в $\mathrm{GL}_{n+1}(F)$, состоящей из всех матриц, у которых последняя строка совпадает с последней строкой единичной матрицы.*

Доказательство. Сопоставим автоморфизму φ его векторную часть φ_v. Ясно, что это гомоморфизм групп $\pi : \mathrm{Aut}(V, V) \to \mathrm{Aut}(V)$. Ядро этого гомоморфизма состоит из аффинных изоморфизмов вида (ψ, id), которые, как мы заметили выше, однозначно определяются образом нуля. Так как $\psi(v) = \psi(0 + v) = \psi(0) + v$ (здесь v в выражении $\psi(v)$ играет роль точки, а в остальных – роль вектора), то ψ – это сдвиг на $\psi(0)$. Поэтому отображение $(\psi, \mathrm{id}) \mapsto \psi(0)$ задает изоморфизм $\mathrm{Ker}\,\psi \cong V$.

С другой стороны, $\mathrm{Aut}(V)$ вкладывается в $\mathrm{Aut}(V, V)$ по правилу $\theta \mapsto (\theta, \theta)$. Таким образом, имеем последовательность гомоморфизмов $\mathrm{Aut}(V) \to \mathrm{Aut}(V, V) \to \mathrm{Aut}(V)$, композиция которых тождественная. Кроме того,

$$(\theta, \theta) \circ (\psi, \mathrm{id}) \circ (\theta^{-1}, \theta^{-1}) = (\theta \circ \psi \circ \theta^{-1}, \mathrm{id}), \text{ а } \theta \circ \psi \circ \theta^{-1}(0) = \theta\big(\psi(0)\big),$$

так что образ автоморфизма θ действует на сдвиг, соответствующий вектору $\psi(0)$ естественным образом.

□

На основании теорем Силова и строения полупрямого произведения можно классифицировать все группы порядка pq, где p и q – простые числа. Напомним, что $C_k \cong \mathbb{Z}/k\mathbb{Z}$ обозначает циклическую группу порядка k. Докажем сначала две простые леммы.

Лемма 8.7. *Группа автоморфизмов аддитивной группы $\mathbb{Z}/p\mathbb{Z}$ равна $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$.*

Доказательство. Автоморфизм φ аддитивной группы $\mathbb{Z}/p\mathbb{Z}$ однозначно определен образом 1: если $\varphi(1) = m+p\mathbb{Z}$, то $\varphi(x) = mx+p\mathbb{Z}$. Для того чтобы заданный таким образом гомоморфизм

[5] Рассмотрение стандартного аффинного пространства вместо векторного пространства – это способ формализовать отождествление точек и векторов.

φ был автоморфизмом, необходимо и достаточно, чтобы m было взаимно просто с p, т. е. $m \in (\mathbb{Z}/p\mathbb{Z})^*$ (таким образом, элемент группы $(\mathbb{Z}/p\mathbb{Z})^*$ отождествляется с автоморфизмом умножения на этот элемент). В этой части доказательства p не обязательно простое число. Если же p простое, то кольцо $\mathbb{Z}/p\mathbb{Z}$ является полем, следовательно, группа $(\mathbb{Z}/p\mathbb{Z})^*$ циклическая. □

Лемма 8.8. *Множество элементов циклической группы, порядок которых делит фиксированное число q, является циклической подгруппой, порядок которой делит q.*

Если q простое число, то любой неединичный элемент порождает эту подгруппу.

Доказательство. Возведение в степень q является эндоморфизмом абелевой группы, а рассматриваемая подгруппа – его ядро. Любая подгруппа циклической группы циклическая. Порядок циклической группы равен порядку образующей, который по условию делит q. □

Предложение 8.9. *Пусть $p > q$ – простые числа, а G – группа порядка pq. Тогда $G \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/q\mathbb{Z})$.*

Если гомоморфизм θ тривиален, то $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$. В частности, если $p-1$ не делится на q, то существует единственная группа порядка pq (с точностью до изоморфизма).

Если гомоморфизмы θ, η оба нетривиальны, то $(\mathbb{Z}/p\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_\eta (\mathbb{Z}/q\mathbb{Z})$. В частности, если $p-1$ делится на q, то существует ровно 2 группы порядка pq (с точностью до изоморфизма).

Доказательство. По теореме Силова количество силовских p-подгрупп равно $pk+1$ для некоторого целого неотрицательного k. Так как в группе порядка p нет собственных подгрупп, две различных силовских p-подгруппы пересекаются по нейтральному элементу. Тогда количество элементов во всех силовских p-подгруппах равно $1 + (p-1)(pk+1) = p(pk-k+1) \leqslant pq$, откуда $k(p-1) \leqslant q-1$. Но по условию $q < p$, поэтому это неравенство возможно только при $k = 0$. Таким образом, существует только одна силовская p-подгруппа $P \cong \mathbb{Z}/p\mathbb{Z}$. Так как P^g является силовской p-подгруппой, то $P^g = P$ для любого $g \in G$. Следовательно, P нормальна в G. Если $S \cong \mathbb{Z}/q\mathbb{Z}$ – силовская q-подгруппа, то SP является группой, а $S \cap P = \{1_G\}$. Легко видеть (например, по второй теореме об изоморфизме), что $SP/P \cong S$, откуда $|SP| = pq$ и $SP = G$. Таким образом, $G = P \rtimes S \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes (\mathbb{Z}/q\mathbb{Z})$.

По предложению 8.4 $G \cong (\mathbb{Z}/p\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/q\mathbb{Z})$. Если θ отображает любой элемент $\mathbb{Z}/q\mathbb{Z}$ в тождественный автоморфизм, то полупрямые сомножители поэлементно коммутируют, т. е. произведение прямое. В случае, если $p-1$ не делится на q, никаких других гомоморфизмов из $\mathbb{Z}/q\mathbb{Z}$ в $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong C_{p-1}$ нет, что доказывает второе утверждение нашего предложения.

Пусть теперь $p-1 \vdots q$, а $\theta, \eta : \mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$ – два нетривиальных гомоморфизма. Так как группа $(\mathbb{Z}/p\mathbb{Z})^*$ циклическая, то по лемме 8.8 существует $k \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$ такое, что $\eta(k) = \eta(1)^k = \theta(1)$. Тогда $\theta(y) = \eta(ky)$ при любом $y \in \mathbb{Z}/q\mathbb{Z}$. Зададим отображение

$$\varphi : (\mathbb{Z}/p\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/q\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z}) \rtimes_\eta (\mathbb{Z}/q\mathbb{Z}) \text{ по формуле } \varphi(x,y) = (x, ky).$$

Тогда

$$\varphi\big((x_1,y_1)(x_2,y_2)\big) = \varphi\big(x_1 + x_2 \cdot \theta(y_1), y_1 + y_2\big) = \big(x_1 + x_2 \cdot \theta(y_1), k(y_1+y_2)\big)$$
$$\varphi(x_1,y_1)\varphi(x_2,y_2) = (x_1, ky_1)(x_2, ky_2) = (x_1 + x_2 \cdot \eta(ky_1), ky_1 + ky_2)$$

Эта выкладка доказывает, что φ – гомоморфизм, а его биективность очевидна. □

9. Субнормальные ряды

Определение 9.1. Цепочка подгрупп $\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = G$ называется нормальным (субнормальным) рядом, если H_i нормально в G (соответственно в H_{i+1}) для любого $i = 1, \ldots, n-1$. Длиной ряда называется количество включений (в данном случае n). Факторгруппы H_{i+1}/H_i называются факторгруппами ряда.

Два ряда называются эквивалентными, если их длины равны, а факторгруппы изоморфны с точностью до перестановки, т. е. существует перестановка $\sigma \in S_n$ такая, что факторгруппа первого ряда с номером i изоморфна факторгруппе второго ряда с номером $\sigma(i)$.

Ряд не имеет повторов, если $H_i \neq H_{i+1}$ при всех $i = 1, \ldots, n-1$.

Уплотнение ряда подгрупп – это другой ряд подгрупп, содержащий каждый элемент первоначального ряда.

Субнормальный ряд без повторов, для которого любое его уплотнение без повторов совпадает с ним самим, называется композиционным рядом.

Напомним, что группа называется простой, если она не содержит нетривиальных нормальных подгрупп (т. е. нормальных подгрупп, не совпадающих с самой группой и с единицей). Эквивалентное определение композиционного ряда – это ряд без повторов, у которого все факторгруппы просты.

Ясно, что композиционный ряд существует не для любой группы, но для конечных групп он, конечно, существует. Более общо, композиционный ряд существует тогда и только тогда, когда выполнены условия обрыва возрастающих и убывающих цепей подгрупп данной группы. Сейчас мы докажем, что любые 2 композиционных ряда изоморфны (если существуют). Этот факт легко следует из теоремы Шрайера о том, что любые 2 субнормальных ряда имеют эквивалентные уплотнения.

Теорема 9.2 (теорема Шрайера об уплотнении). *Любые 2 субнормальных ряда имеют эквивалентные уплотнения.*

Доказательство. Пусть

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_n = G \text{ и } \{1\} = K_0 \leqslant K_1 \leqslant \cdots \leqslant K_m = G$$

субнормальные ряды группы G. Для всех допустимых i, j положим

$$H_{ij} = H_i(H_{i+1} \cap K_j) \text{ и } K_{ji} = K_j(K_{j+1} \cap H_i)$$

(так как $H_i \trianglelefteq H_{i+1}$ и $K_j \trianglelefteq K_{j+1}$, произведения являются подгруппами). Получаем композиционные ряды

$$\begin{aligned}\{1\} = H_{00} \leqslant H_{01} \leqslant \cdots \leqslant H_{0\,m-1} \leqslant \ldots \\ \leqslant H_{i-1\,m} = H_i = H_{i0} \leqslant H_{i1} \leqslant \cdots \leqslant H_{i\,m-1} \leqslant \ldots \\ \leqslant H_{n-2\,m} = H_{n-1} = H_{n-1\,0} \leqslant H_{n-1\,1} \leqslant \cdots \leqslant H_{n-1\,m-1} \leqslant H_{n-1\,m} = G\end{aligned}$$

и аналогично

$$\begin{aligned}\{1\} = K_{00} \leqslant K_{01} \leqslant \cdots \leqslant K_{0\,n-1} \leqslant \ldots \\ \leqslant K_{j-1\,n} = K_j = K_{j0} \leqslant K_{j1} \leqslant \cdots \leqslant K_{j\,n-1} \leqslant \ldots \\ \leqslant K_{m-2\,n} = K_{m-1} = K_{m-1\,0} \leqslant K_{m-1\,1} \leqslant \cdots \leqslant K_{m-1\,n-1} \leqslant K_{m-1\,n} = G\end{aligned}$$

Очевидно, эти ряды являются уплотнениями исходных рядов. Для доказательства того, что они эквивалентны, докажем изоморфизм $H_{i\,j+1}/H_{ij} \cong K_{j\,i+1}/K_{ji}$, другими словами,

$$\frac{H_i(H_{i+1} \cap K_{j+1})}{H_i(H_{i+1} \cap K_j)} \cong \frac{K_j(K_{j+1} \cap H_{i+1})}{K_j(K_{j+1} \cap H_i)}.$$

Но последний изоморфизм – это в точности лемма о бабочке. □

Из теоремы следует, что любые 2 композиционных ряда имеют эквивалентные уплотнения. Если из этих уплотнений выкинуть повторения, то получатся исходные композиционные ряды, которые, естественно, также будут эквивалентны.

Следствие 9.3. *Любые 2 композиционных ряда группы эквивалентны.*

Факторы композиционного ряда называются композиционными факторами группы. Как мы только что доказали, набор (но не последовательность!) композиционных факторов определен однозначно. Это и означает, что любая конечная группа строится из кирпичиков, которыми являются простые группы. При этом набор кирпичиков, но не их порядок, определен группой однозначно. И, как мы уже видели при изучении групп порядка pq, из одного набора кирпичиков, даже сложенного в одном порядке, можно получить разные группы.

Простейшими примерами простых групп являются группы A_n, $n \geqslant 5$, и $\mathrm{PSL}_n(F)$, где $n \geqslant 3$ или $n = 2$, а поле F содержит больше 3 элементов.

10. Примеры простых групп

Исторически первым примером простой неабелевой группы была знакопеременная группа A_n, $n \geqslant 5$.

Назовем элемент i подвижным под действием перестановки σ, если $\sigma(i) \neq i$. Использование стандартного термина: "i неподвижная точка $\iff \sigma(i) = i$" привело бы к необходимости произносить "не неподвижная точка", что явно неблагозвучно.

Лемма 10.1. *Группа A_n порождена 3-циклами.*

Доказательство. Пусть $\sigma \in A_n$. Докажем, что σ раскладывается в произведение 3-циклов индукцией по количеству элементов, подвижных под действием σ. Если это количество равно 0, то σ – тождественная перестановка, и доказывать нечего. Ясно, что это количество не может быть равно 1, а если оно было бы равно 2, то σ была бы транспозицией, которая не лежит в A_n. Поэтому можно считать, что $\sigma(i_1) \neq i_1$, $\sigma(i_2) \neq i_2$, $\sigma(i_3) \neq i_3$ для некоторых различных $1 \leqslant i_1, i_2, i_3 \leqslant n$. Заметим, что $\sigma^{\pm 1}(i_k)$ также подвижны под действием σ. Предположим для определенности, что $\sigma(i_2) \neq i_1$ (иначе заменим i_2 на i_3). Положим $\tau = (\sigma(i_1)\ i_1\ \sigma(i_2))\sigma$. Тогда $\tau(m) = \sigma(m)$ для любого $m \neq i_1, \sigma^{-1}(i_1), i_2$. Следовательно, любая неподвижная точка перестановки σ осталась неподвижной точкой перестановки τ, а кроме того $\tau(i_1) = i_1$. Таким образом, неподвижных точек у τ строго больше, чем у σ и можно воспользоваться индукционным предположением. □

Следствие 10.2. *Если подгруппа $H \trianglelefteq A_n$ содержит 3-цикл, но она совпадает с A_n.*

Доказательство. При $n = 3$ утверждение очевидно. Пусть $n \geqslant 4$ и $(i\ j\ k) \in H$. Возьмем $l \neq i, j, k$ и рассмотрим перестановку $\tau(i\ j\ k)\tau^{-1} = (\tau(i)\ \tau(j)\ \tau(k)) \in H$ при $\tau = (i\ j\ l)$. Получим $(j\ l\ k) \in H$ и $(j\ k\ l) = (j\ l\ k)^{-1} \in H$. Таким образом, мы можем заменить один любой индекс в 3-цикле на любой другой. Ясно, что делая так несколько раз, мы докажем, что любой 3-цикл лежит в H. Доказательство заканчивает лемма 10.1. □

Лемма 10.3. *Пусть $n > 3$. Для любой $\sigma \in S_n \smallsetminus \{\mathrm{id}\}$ существует $\tau \in A_n$ такая, что $[\sigma, \tau] \neq \mathrm{id}$ и имеет не более 5 подвижных точек.*

Доказательство. Пусть $\sigma(i) \neq i$. Возьмем $k \neq i, \sigma(i), \sigma^2(i)$. Тогда

$$\rho := [\sigma, (i\ \sigma(i)\ k)] = {}^{\sigma}(i\ \sigma(i)\ k) \cdot (i\ \sigma(i)\ k)^{-1} = (\sigma(i)\ \sigma^2(i)\ \sigma(k))(i\ k\ \sigma(i)),$$

а эта перестановка двигает максимум 5 элементов $i, \sigma(i), \sigma^2(i), k, \sigma(k)$. Если $\rho = \mathrm{id}$, то $(\sigma(i)\ \sigma^2(i)\ \sigma(k)) = (\sigma(i)\ k\ i)$, что противоречит неравенству $k \neq \sigma^2(i)$. □

Теорема 10.4. *Группа A_n является простой при $n \geqslant 5$.*

Доказательство. Пусть H – нетривиальная нормальная подгруппа в A_n. По лемме 10.3 она содержит нетождественную перестановку, двигающую не более 5 элементов. Есть всего 3 циклических типа таких четных перестановок: 3, $2 + 2$, и 5. Далее считаем, что i_1, i_2, i_3, i_4, i_5 – различные индексы от 1 до n. Если $(i_1\ i_2)(i_3\ i_4) \in H$, то

$$[(i_1\ i_2)(i_3\ i_4), (i_1\ i_2)(i_3\ i_5)] = [(i_3\ i_4), (i_3\ i_5)] = (i_3\ i_4\ i_5) \in H$$

Если же 5-цикл $\sigma = (i_1\ i_2\ i_3\ i_4\ i_5) \in H$, то

$$[(i_1\ i_2)(i_3\ i_4), (i_1\ i_2\ i_3\ i_4\ i_5)] = (i_2\ i_1\ i_4\ i_3\ i_5)(i_1\ i_2\ i_3\ i_4\ i_5) = (i_2\ i_5\ i_4) \in H$$

Как видно, в любом случае наша нормальная подгруппа содержит 3-цикл и следствие 10.2 заканчивает доказательство. □

Другой пример простой группы – проективная специальная линейная группа. Напомним, что $\mathrm{PSL}_n(F)$ обозначает факторгруппу группы $\mathrm{SL}_n(F)$, состоящей из матриц с определителем 1, по центру, т. е. по подгруппе скалярных матриц.

Теорема 10.5. *Пусть F – поле, а $n \geqslant 2$. При $n = 2$ предположим дополнительно, что $|F| > 3$. Тогда группа $\mathrm{PSL}_n(F)$ проста.*

Если поле конечно, то $\mathrm{PSL}_n(F)$ – конечная простая группа. Большая часть конечных простых групп – это проективные линейные группы, т.е. факторгруппы по центру матричных групп над конечными полями. Они называются группами типа Ли, потому что в каком-то смысле они похожи на группы Ли. Группы типа Ли классифицируются некоторыми комбинаторными структурами, называемыми системами корней (система корней – это конечный набор точек в евклидовом пространстве, обладающий большой группой симметрий). Теорема классификации простых конечных групп утверждает, что кроме знакопеременных групп и групп типа Ли существует ровно 26 простых конечных групп, которые называются спорадическими группами.

11. Разрешимые и нильпотентные группы

Глава 9

Начала теории категорий

Чем раньше математик начинает пользоваться языком теории категорий, тем проще ему потом изучать любые области математики, хотя бы потому что он видит формальные взаимосвязи между ними. Весь курс алгебры буквально пронизан категориями, функторами, естественными (и неестественными!) преобразованиями, универсальными конструкциями и сопряженными функторами. Поэтому прочитав настоящую главу вы сможете лучше увидеть взаимосвязи между различными понятиями и утверждениями.

1. Категория, универсальные объекты, типы морфизмов

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

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

удовлетворяющих следующим условиям:

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

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

Часто мы будем писать:

- $X \in \mathscr{C}$ вместо $X \in \operatorname{Obj}\mathscr{C}$;
- $\operatorname{Mor}\mathscr{C}(X, Y)$ вместо $\operatorname{Mor}(X, Y)$, если из контекста неясно, про какую категорию идет речь;
- $\varphi : X \to Y$ вместо $\varphi \in \operatorname{Mor}(X, Y)$;
- $\phi \in \operatorname{Mor}\mathscr{C}$ для любого морфизма категории $\mathscr{C}$ (т. е. $\operatorname{Mor}\mathscr{C}$ – это класс всех морфизмов категории $\mathscr{C}$;
- $X = \operatorname{source}\varphi$ и $Y = \operatorname{target}\varphi$ для морфизма $\varphi : X \to Y$.

Определение 1.2. Категория $\mathscr{B}$ называется подкатегорией категории $\mathscr{C}$, если $\operatorname{Obj}\mathscr{B} \subseteq \operatorname{Obj}\mathscr{C}$ и $\operatorname{Mor}_{\mathscr{B}}(X, Y) \subseteq \operatorname{Mor}_{\mathscr{C}}(X, Y)$ для любых $X, Y \in \operatorname{Obj}\mathscr{B}$. Подкатегория $\mathscr{B}$ называется полной, если последнее включение всегда является равенством.

Определение 1.3. Пусть $\mathscr{C}$ – категория. Противоположной категорией к $\mathscr{C}$ называется категория $\mathscr{C}^{op}$:

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

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

- $\operatorname{Obj}(\mathscr{C} \times \mathscr{B}) = \operatorname{Obj}\mathscr{C} \times \operatorname{Obj}\mathscr{B}$;

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

Определение 1.5. Морфизм φ 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 $\mathfrak{Set}$, пунктированных множеств $\mathfrak{Set}_*$.
(2) Категория множеств с инъективными (сюръективными) отображениями.
(3) Алгебраические и геометрические структуры.
   - Категория моноидов $\mathfrak{Mon}$.
   - Категория групп $\mathfrak{Grp}$.
   - Категория абелевых групп $\mathfrak{Ab}$.
   - Категория F-векторных пространств $\mathfrak{Vect} = F - \mathfrak{Vect}$, конечномерных векторных пространств $\mathfrak{Vect}_{f.d.}$.
   - Категория R-модулей $R - \mathfrak{Mod}$.
   - Категория R-алгебр $R - \mathfrak{Alg}$.
   - Категория коммутативных колец с 1 $\mathfrak{Ring}$
   - Категория коммутативных колец без 1 $\mathfrak{Rng}$
   - Категория полей (автоматом все морфизмы – мономорфизмы).
   - Категория топологических пространств $\mathfrak{Top}$, пунктированных топологических пространств $\mathfrak{Top}_*$.
   - Гомотопическая категория: объекты – топологические пространства, иногда обладющие какими-то хорошими свойствами, например CW-комплексы, морфизм из A в B – последовательность отображений

     $$A = A_0 \xrightarrow{\varphi_0} B_0 \xleftarrow{\psi_0} A_1 \longrightarrow \ldots \longrightarrow B_n = B,$$

     где φ_i – непрерывны, а ψ_i – гомотопические эквивалентности. При композиции таких морфизмов соответствующие последовательности пририсовываются друг к другу, а фрагменты $X \xleftarrow{\psi} Y \xrightarrow{\psi}$ вычеркиваются.
(4) Моноид – категория с одним объектом.
(5) Группоид – малая категория, все морфизмы которой являются изоморфизмами. Обобщение понятия группы. Полезно, например, при изучении фундаментальной группы несвязных пространств. Строится фундаментальный группоид: объекты – точки данного топологического пространства, Морфизм из точки a в точку b – класс гомотопных путей из a в b. Копозиция – конкатенация путей, как она опредеяется в топологии (с точности до гомотопии).
(6) Категория матриц над кольцом R: объекты – натуральные числа, $\mathrm{Mor}(m,n) = \mathrm{M}_{m\times n}(R)$. Композиция морфизмов – произведение матриц.
(7) Частично упорядоченное множество, из a в b есть ровно 1 морфизм $\iff a \leqslant b$.
(8) Ориентированный граф: объекты – вершины, морфизмы пути (категория путей) или из a в b есть ровно 1 морфизм $\iff$ из a существует путь в b (категория достижимости).

(9) Категория морфизмов $\mathrm{Mor}\,\mathscr{C}$. Объекты – морфизмы в категории $\mathscr{C}$, морфизмы из $\varphi : X \to Y$ в $\varphi' : X' \to Y'$ – коммутативные квадраты

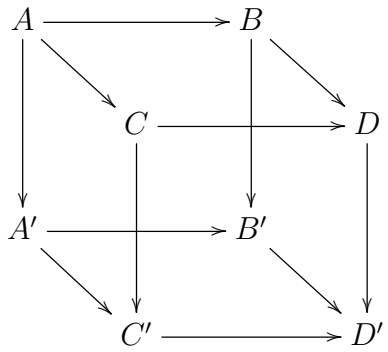
$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ \downarrow & & \downarrow \\ X' & \xrightarrow{\varphi'} & Y' \end{array}$$

(10) Γ – ориентированный граф. Определим категорию (коммутативных) $\mathscr{C}_\Gamma$ диаграмм в $\mathscr{C}$ типа Γ. Диаграмма в $\mathscr{C}$ типа Γ – это функция, сопоставляющая вершинам Γ объекты $\mathscr{C}$, а ребрам Γ – морфизмы $\mathscr{C}$. Даграмма называется коммутативной, если для любых двух вершин и для любых двух путей, соединяющих эти вершины, композиции морфизмов вдоль этих путей совпадают.

Морфизм η диаграмм F и G – набор морфизмов $\eta_a : F(a) \to G(a)$, где a пробегает вершины графа Γ, такой что для любого ребра α из вершины a в вершину b квадрат

$$\begin{array}{ccc} F(a) & \xrightarrow{F(\alpha)} & F(b) \\ {\scriptstyle \eta_a}\downarrow & & \downarrow{\scriptstyle \eta_b} \\ G(a) & \xrightarrow{G(\alpha)} & G(b) \end{array}$$

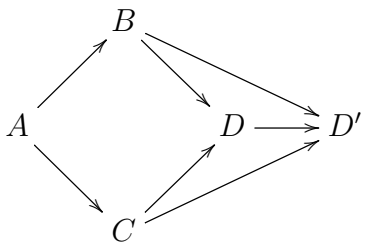
коммутативен. Например, если Γ – это квадрат со стрелками слева направо и сверху вниз, то морфизм диаграмм типа Γ – это коммутативный куб



(11) Часто рассматривают подкатегорию в категории коммутативных диаграмм, состоящую из диаграмм, у которых объекты в нескольких вершинах и несколько морфизмов между ними фиксированы. В этом случае морфизмы – это морфизмы диаграмм, тождественные на зафиксированных вершинах. Например, для данных объектов $A, B, C \in \mathscr{C}$ и морфизмов $C \leftarrow A \to B$ можно рассмотреть категорию квадратов вида

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ C & \longrightarrow & D \end{array}$$

морфизмами в которой являются коммутативные диаграммы



Инициальный объект в этой категории называется пушаутом диаграммы $C \leftarrow A \rightarrow B$ или копроизведением B и C над A. Позже мы рассмотрим несколько важных примеров пушаутов, а также двойственного понятия – пулбэка ([расслоенного] произведения).

2. Функторы

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

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

Индексы в обозначении отображения $\mathscr{F}_{X,Y}$ обычно опускают, потому что они однозначно восстанавливаются по аргументу. В таких обозначениях свойства в определении означают, что $\mathscr{F}$ сохраняет композицию морфизмов и тождественные морфизмы. Для функторов используется такое же обозначение, что и для функций: запись $\mathscr{F} : \mathscr{B} \to \mathscr{C}$ означает, что $\mathscr{F}$ является функтором из категории $\mathscr{B}$ в категорию $\mathscr{C}$.

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

Примеры.

(1) Забывающие функторы. Формально, забывающий функтор – это тот, который действует инъективно на каждом множестве морфизмов.
(2) Функтор вложения подкатегории в категорию.
(3) M_n, GL_n, обратимые элементы моноида.
(4) Центр группы $Z(G) = \{a \in G \mid ag = ga \,\forall g \in G\}$ не определяет функтор, потому что образ центра не обязательно лежит в центре. Он будет функтором, если в качестве морфизмов в категории групп рассматривать только сюръективные гомоморфизмы.
(5) Отображение, сопоставляющее группе ее коммутант, 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).
(6) Пусть Γ – ориентированный граф, а $\mathscr{C}_\Gamma$ – категория достижимости, связанная с этим графом. Функтор из $\mathscr{C}_\Gamma$ в произвольную категорию $\mathscr{B}$ называется коммутативной диаграммой типа Γ в категории $\mathscr{B}$.
(7) $\operatorname{Mor} : \mathscr{C}^{op} \times \mathscr{C} \to \mathfrak{Set}$. Если $\mathscr{C}$ – категория векторных пространств, то вместо категории множеств можно написать категорию векторных пространств. Можно зафиксировать первый или второй аргумент.

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

3. Естественные преобразования

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

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

для любых объектов $X, Y \in \operatorname{Obj}\mathscr{B}$ и любого морфизма $\alpha \in \operatorname{Mor}(X, Y)$.

Последнее условие в определении означает коммутативность следующей диаграммы:

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

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

Категории $\mathscr{B}$ и $\mathscr{C}$ называются эквивалентными, если существуют функторы $\mathscr{F} : \mathscr{B} \to \mathscr{C}$ и $\mathscr{F}' : \mathscr{C} \to \mathscr{B}$ такие, что композиция $\mathscr{F} \circ \mathscr{F}'$ естественно изоморфна $id_{\mathscr{C}}$, а $\mathscr{F}' \circ \mathscr{F}$ естественно изоморфна $id_{\mathscr{B}}$. Другими словами, существуют естественные изморфизмы $X \cong \mathscr{F}\big(\mathscr{F}'(X)\big)$ и $Y \cong \mathscr{F}'\big(\mathscr{F}(Y)\big)$, где $X \in \operatorname{Obj}\mathscr{C}$, а $Y \in \operatorname{Obj}\mathscr{B}$. 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) $\operatorname{Mor}(X, \operatorname{Mor}(Y, Z)) \cong \operatorname{Mor}(X \times Y, Z)$ в категории множеств. Аналог этого естественного изоморфизма выполнен в разных других категориях $\mathscr{C}$, если множество $\operatorname{Mor}(Y, Z)$ естественным образом превращается в объект категории $\mathscr{C}$. При этом вместо прямого произведения возникают другие универсальные конструкции.
(5) В категории векторных пространств над полем F множество $\operatorname{Mor}(Y, Z)$ имеет естественную структуру векторного пространства. Поэтому можно считать, что $\operatorname{Mor}_{\mathscr{V}ect/F}(\_\,,\_)$ является функтором $(\mathscr{V}ect/F)^{op} \times \mathscr{V}ect/F \to \mathscr{V}ect/F$. Тогда $\operatorname{Mor}\big(X, \operatorname{Mor}(Y, Z)\big)$ естественно изоморфно пространству $\operatorname{Bil}(X \times Y, Z)$ билинейных отображений из $X \times Y$ в Z. В следующем параграфе мы определим тензорное произведение $X \otimes Y$ так, чтобы $\operatorname{Bil}(\mathrm{X} \times \mathrm{Y}, \mathrm{Z})$ было бы естественно изоморфно $\operatorname{Mor}(X \otimes Y, Z)$.
(6) Рассмотрим контравариантный функтор $V \mapsto V^*$ на категории векторных пространств из примера 7. Ясно, что его композиция с самим собой будет ковариантным функтором. Построим естественное преобразование η 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 η – естественное преобразование, является рутинной. Заметим, что отображение η_V является инъективным (нетрудно посчитать его ядро).

    Пусть теперь $\mathscr{V} = \mathscr{V}ect_{fd}/F$ обозначает категорию конечномерных векторных пространств и их линейных отображений. Рассмотрим сужения функторов $* : \mathscr{V} \to \mathscr{V}^{op}$ и $** : \mathscr{V} \to \mathscr{V}$. Так как размерности пространств V, V^* и V^{**} совпадают, то построенные выше отображения η_V являются изоморфизмами векторных пространств. Это доказывает, что функтор $** : \mathscr{V} \to \mathscr{V}$ естественно изоморфен тождественному, а функтор $*$ – квазиобратен сам себе. В частности, категория конечномерных векторных пространств эквивалентна своей противоположной.
(7) Пусть Γ – ориентированный граф, $\mathscr{C}_\Gamma$ – категория достижимости в этом графе, а $\mathscr{B}$ – произвольная категория. Тогда естественное преобразование функторов $\mathscr{F} \to \mathscr{G}$, где $\mathscr{F},\mathscr{G} : \mathscr{C}_\Gamma \to \mathscr{B}$, – это просто морфизм соответствующих диаграмм (см. пример функторов номер 6).
(8) Пусть $\mathscr{F} : \mathscr{B} \to \mathscr{C}$ – функтор. Он определяет естественное преобразование функторов $\eta^{\mathscr{F}} : \operatorname{Mor}\big(\_\,,\_\big) \to \operatorname{Mor}\big(\mathscr{F}(\_), \mathscr{F}(\_)\big)$ по правилу: $\eta^{\mathscr{F}}_{(X,Y)}(\alpha) = \mathscr{F}(\alpha)$, где $\alpha \in \operatorname{Mor}(X, Y)$.

4. Универсальные квадраты

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

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

Формально:

$$\operatorname{Obj}\mathscr{S} = \{(X, \varphi, \psi) \mid X \in \operatorname{Obj}\mathscr{C},\ \varphi \in \operatorname{Mor}(X, B),\ \psi \in \operatorname{Mor}(X, A),\ \beta \circ \varphi = \alpha \circ \psi\},$$
$$\operatorname{Mor}\big((X, \varphi, \psi), (X', \varphi', \psi')\big) = \{\lambda \in \operatorname{Mor}(X, X') \mid \varphi' \circ \lambda = \varphi,\ \psi' \circ \lambda = \psi\}.$$

При этом композиция морфизмов задана очевидным образом. Тогда финальный объект в этой категории называется пулбэком морфизмов α и β или, чаще, пулбэком диаграммы

$$A \xrightarrow{\alpha} C \xleftarrow{\beta} B$$

.

Двойственным образом определяется пушаут, т. е. пушаут в категории $\mathscr{C}$ – это пулбэк в категории $\mathscr{C}^{op}$.

Примеры.

5. Сопряженные функторы

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

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

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

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

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

– естественный изоморфизм. Рассмотрим биекцию

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

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

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

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

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

Посмотрев на определение g видим, что в левой части стоит f. По определению f_X получаем

$$f = \mathscr{F}(g) \circ f_X,$$

что и означает, что g является морфизмом $(\mathscr{G}(X), f_X) \to (Y, f)$ в категории $\mathscr{M}_X$.

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

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

то есть $g' = \eta_{X,Y}(f) = g$.

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

Определим функцию

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

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