ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

А. В. Васильев, В. Д. Мазуров

ВЫСШАЯ АЛГЕБРА

Конспект лекций

Часть I

Новосибирск
2010

УДК 512
ББК В14я73-2
В 191

Васильев А. В., Мазуров В. Д. Высшая алгебра: В 2 ч.: Конспект лекций / Новосиб. гос. ун-т. Новосибирск, 2010, ч. 1. 143 с.

ISBN 978-5-94356-912-8

В основе предлагаемой читателю первой части учебного пособия лежит содержание первого семестра курса «Высшая алгебра», который авторы читали на первом курсе механико-математического факультета Новосибирского государственного университета. В курсе на основе понятия алгебраической системы определяются основные алгебраические структуры: группы, кольца, поля, векторные пространства, алгебры. В дальнейшем рассматриваются примеры этих структур: группы подстановок, кольца (алгебры) матриц и многочленов, поле комплексных чисел, конечномерные векторные пространства. В рамках этого подхода изучаются классические алгебраические объекты: определители и системы линейных уравнений. Пособие предназначено для студентов математических специальностей университетов.

Рецензент
д-р физ.-мат. наук, доцент В. Г. Бардаков

ISBN 978-5-94356-912-8

Содержание

Предисловие

В основе предлагаемой читателю первой части учебного пособия лежит содержание первого семестра курса «Высшая алгебра», который авторы читали на первом курсе механико-математического факультета Новосибирского государственного университета. Нумерация определений, теорем, предложений и упражнений, принятая в пособии, соответствует его разбиению на главы и параграфы. Например, теорема 2.3.1 — это первая теорема из третьего параграфа второй главы. Нумерация вынесенных формул начинается заново внутри каждого параграфа. Упражнения, сопровождающие изложение, призваны помочь усвоению материала. Наиболее трудные из них помечены звёздочкой. Список литературы не претендует на полноту, его основная цель — предоставить читателю дополнительную возможность ознакомиться с затрагиваемыми в курсе понятиями и идеями. В приложении для удобства приводится программа курса «Высшая алгебра» на 2010–11 учебный год (два семестра). Ссылки на соответствующие места из книг, указанных в списке литературы, находятся в этой программе. Пособие снабжено предметным указателем и указателем обозначений.

Глава 1

Введение

§ 1.1. Множества и отображения

Под *множеством* понимается неупорядоченная совокупность мыслимых вместе объектов произвольной природы, которые мы умеем различать между собой. Объекты, составляющие множество, называются его *элементами*. Обычно мы будем обозначать множества заглавными, а элементы строчными латинскими буквами. Свойство объекта быть элементом некоторого множества выражается словами *элемент a принадлежит множеству A* и записывается так: $a \in A$. Если элемент a не принадлежит множеству A, пишем $a \notin A$. Два множества *равны*, если они состоят из одних и тех же элементов. Множество можно задать перечислением всех его элементов или указанием некоторого свойства, которому элементы, его составляющие, должны удовлетворять. В последнем случае, если обозначить соответствующее свойство через P, запись того факта, что множество A состоит из тех и только тех элементов, которые обладают свойством P, выглядит следующим образом: $A = \{x \mid x \text{ обладает свойством } P\}$ или кратко $A = \{x \mid P(x)\}$. Мы будем также использовать кванторы $\forall$ и $\exists$, заменяя ими выражения *для любого* и *существует* соответственно. Например, запись $\forall a \in A : P(a)$ означает, что для любого элемента $a \in A$ выполняется свойство P, а запись $\exists a \in A : P(a)$ означает, что найдётся хотя бы один элемент $a \in A$, обладающий свойством P.

Вам уже известны основные числовые множества: $\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел, $\mathbb{Z}$ — множество целых чисел, $\mathbb{Q}$ — множество рациональных чисел и $\mathbb{R}$ — множество действительных чисел.

Множество B называется *подмножеством* множества A, если каждый элемент множества B принадлежит множеству A. Мы будем обозначать этот факт так: $B \subseteq A$. В случае, если найдётся хотя бы один элемент множества A, который не принадлежит подмножеству B, множество B называется *собственным* подмножеством множества A, что можно подчеркнуть, используя следующее обозначение: $B \subset A$. Единственным множеством, не имеющим собственных подмножеств, является *пустое* множество $\varnothing$, которое по определению не содержит ни одного

элемента. Множество всех подмножеств данного множества A обозначается через $P(A)$ или 2^A.

Из двух и более множеств можно образовать новые множества. Если заданы множества $A_1, A_2, \ldots, A_n$, то множество $A_1 \cap A_2 \cap \ldots \cap A_n = \{x \mid x \in A_1 \text{ и } x \in A_2 \text{ и } \ldots \text{ и } x \in A_n\}$ называется *пересечением*, а множество $A_1 \cup A_2 \cup \ldots \cup A_n = \{x \mid x \in A_1 \text{ или } x \in A_2 \text{ или } \ldots \text{ или } x \in A_n\}$ — *объединением* множеств $A_1, A_2, \ldots, A_n$. Под *разностью* множеств A и B мы будем понимать множество $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$. Если при этом множество B является подмножеством множества A, то мы будем называть множество $A \setminus B$ *дополнением* множества B в множестве A. Если множество A фиксировано, то дополнение в A его подмножества B мы будем также обозначать через $\overline{B}$.

Напомним, что порядок элементов при записи множества не играет роли. Так, множества $\{a, b\}$ и $\{b, a\}$ равны, поскольку состоят из одних и тех же элементов. С другой стороны, в математике, как и в жизни, часто приходится рассматривать упорядоченные совокупности объектов. Упорядоченный набор из n элементов $a_1, a_2, \ldots, a_n$ мы будем обозначать $(a_1, a_2, \ldots, a_n)$ и называть *n-кой*. В случае двух объектов будем употреблять термин *упорядоченная пара*. Две n-ки $(a_1, a_2, \ldots, a_n)$ и $(b_1, b_2, \ldots, b_n)$ равны тогда и только тогда, когда $a_1 = b_1$, $a_2 = b_2, \ldots$ $\ldots, a_n = b_n$.

Упражнение 1.1.1. *Докажите, что множества* $\{\{a\}, \{a, b\}\}$ *и* $\{\{c\}, \{c, d\}\}$ *равны тогда и только тогда, когда* $a = c$ *и* $b = d$.

Определение 1.1.1. Если заданы множества $A_1, A_2, \ldots, A_n$, то их *декартовым произведением* называется множество

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Декартовой n-ой степенью множества A называется множество

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A, a_2 \in A, \ldots, a_n \in A\}.$$

В случае, когда $n = 2$, мы будем говорить о *декартовом квадрате* множества A.

Пусть заданы два множества X и Y. Правило f, по которому *каждому* элементу множества X сопоставляется *однозначно определённый* элемент множества Y, принято называть *функцией* или *отображением* из множества X в множество Y (обозначение $f : X \to Y$). Мы будем в основном использовать термин *отображение*.

Тот факт, что элемент y множества Y является образом элемента x множества X при отображении f, можно записать разными способами: $f(x) = y$, $xf = y$, $x^f = y$. Мы будем в основном использовать обозначения, при которых символ отображения располагается справа от символа элемента, т. е. предпочитать обозначение xf обозначению $f(x)$. Если $Z \subseteq X$, обозначим через Zf множество $\{y \in Y \mid \exists x \in Z : xf = y\}$, которое называется образом Z в Y. Если $Z = X$, то образ Xf мы будем также обозначать через $\operatorname{Im} f$.

Пусть имеется два отображения $f : X \to Y$ и $g : Y \to Z$. *Композицией* (или *произведением*) отображений f и g называется отображение $f * g : X \to Z$, определяемое $\forall x \in X$ равенством $x(f * g) = (xf)g$. Таким образом, отображение $f * g$ есть результат последовательного выполнения сначала отображения f, а затем отображения g. Иногда по аналогии с умножением чисел мы будем опускать символ $*$ и писать просто fg вместо $f * g$.

Замечание. При расположении символа отображения слева от символа элемента запись $f * g$ композиции отображений f и g уже означала бы, что сначала выполняется отображение g, а потом f: $(f * g)x = f(g(x))$. Таким образом, нам пришлось бы читать запись $f * g$ справа налево, что не слишком удобно. Это одна из причин, почему мы отдаём предпочтение правостороннему расположению символа отображения. Отметим, что с другой стороны имеются достаточно веские причины и для использования левосторонней записи.

Вернёмся к определению отображения. Оно требует, чтобы *каждый* элемент x множества X имел образ $y = xf$ в Y. Обратное верно не всегда: могут существовать элементы множества Y, которые не имеют прообразов в X. Те отображения, для которых таких элементов в Y нет, носят специальное название.

Определение 1.1.2. Отображение $f : X \to Y$ называется отображением множества X *на* множество Y или *сюръекцией*, если для каждого элемента $y \in Y$ существует элемент $x \in X$ такой, что $y = xf$. Соответствующее обозначение: $f : X \underset{\text{на}}{\longrightarrow} Y$.

Определение отображения также требует, чтобы каждый элемент множества X имел *ровно один* образ в Y. Иными словами, если $xf = y_1$ и $xf = y_2$, то $y_1 = y_2$. Обратное снова в общем случае неверно: у одного элемента из Y может быть несколько прообразов в X. Например, если рассмотреть отображение $f : \mathbb{R} \to \mathbb{R}$, действующее по правилу $xf = x^2$, то у числа 4 имеется два прообраза: 2 и -2. Мы опять выделим отображения, для которых такая ситуация невозможна.

Определение 1.1.3. Отображение $f : X \to Y$ называется *взаимно однозначным* отображением из множества X в множество Y или *инъекцией*, если для любых элементов $x_1, x_2 \in X$ из равенства $x_1 f = x_2 f$ следует равенство $x_1 = x_2$. Соответствующее обозначение: $f : X \xrightarrow{1\text{-}1} Y$.

Отображения, которые удовлетворяют определениям 1.1.2 и 1.1.3 одновременно, также имеют специальное название.

Определение 1.1.4. Отображение $f : X \to Y$ называется *взаимно однозначным* отображением множества X *на* множество Y или *биекцией*, если оно является сюръекцией и инъекцией одновременно. Соответствующее обозначение: $f : X \xrightarrow[\text{на}]{1\text{-}1} Y$.

Если отображение $f : X \to Y$ является биекцией, то, как следует из определения отображения, существует *обратное* к нему отображение $f^{-1} : Y \to X$, действующее по правилу: $x = yf^{-1}$ тогда и только тогда, когда $y = xf$. Обратное отображение снова является биекцией. Множества X и Y, между которыми можно установить биекцию, принято называть *равномощными*.

Упражнение 1.1.2. *Приведите пример отображения, которое*

1) *не является ни сюръекцией, ни инъекцией;*

2) *является сюръекцией, но не является инъекцией;*

3) *является инъекцией, но не является сюръекцией;*

4) *является биекцией.*

Упражнение 1.1.3. *Докажите, что композиция двух биекций снова является биекцией.*

Упражнение 1.1.4. *Пусть $m, n \in \mathbb{N}$, множество X состоит из m элементов, а множество Y — из n элементов. Докажите, что следующие утверждения эквивалентны.*

1. *Существует биекция $\varphi : X \to Y$.*

2. *Выполняется равенство $m = n$.*

Из утверждения, приведённого в упражнении, в частности, следует, что если множество X конечно (состоит из конечного числа элементов), то между ним и любым его собственным подмножеством установить биекцию не удастся. Это неверно в случае, когда множество X бесконечно, как показывает следующее упражнение.

Упражнение 1.1.5. *Пусть множество X бесконечно. Тогда найдётся по крайней мере одно собственное подмножество Y множества X такое,*

что существует биекция $\varphi : X \to Y$. Более точно, выполняются следующие утверждения:

1. *Для любого конечного подмножества Z множества X существует биекция $\varphi : X \to Y$, где $Y = X \setminus Z$.*

2. *Найдётся бесконечное число бесконечных подмножеств Z множества X таких, что существует биекция $\varphi : X \to Y$, где $Y = X \setminus Z$.*

Замечание. Как следует из утверждений упражнений 1.1.4 и 1.1.5, множество X конечно тогда и только тогда, когда оно не содержит собственных подмножеств, равномощных X. Любопытно, что интуитивно ясное понятие конечного множества удаётся формализовать в рамках теории множеств, положив в качестве определения именно указанный выше критерий.

§ 1.2. Алгебраические системы

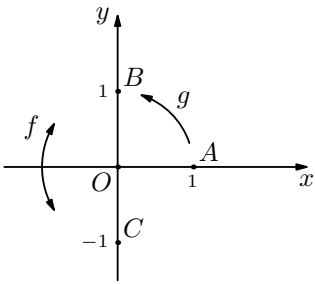
Алгебра, как вам известно из опыта, имеет дело с операциями на множествах. Например, если рассмотреть множество $\mathbb{N}$ натуральных чисел, то для любых двух чисел m и n вы сумеете определить их сумму и произведение, которые в свою очередь являются натуральными числами. Не проводя вычислений, вы способны предсказать, что сумма $n+m$ совпадёт с суммой $m+n$. Если $m < n$, то вы сумеете найти единственное натуральное число x, удовлетворяющее уравнению $x + m = n$ и т. д. В течение долгого времени именно решение уравнений (или систем уравнений) считалось основным предметом алгебры. Решению уравнений (в том числе и квадратных) был посвящен и труд «Китаб аль-джебр валь-мукабала» арабского математика Эль Хорезми (Хорезми Мухаммед бен Муса), жившего около 800 г. н.э., в котором впервые появился термин *аль-джебр*, давший в латинизированном варианте название всей математической дисциплине. Однако полезно помнить, что этим термином Эль Хорезми называл не конкретное уравнение, а одно из двух основных преобразований, используемых им при решении уравнений. Иными словами, свойство операции, заданной на множестве (в данном случае, числовом). Взгляд на алгебру как на науку, изучающую свойства операций на множествах, возобладавший с развитием математики, оказался весьма плодотворным. Оказалось, что полезно рассматривать не только различные числовые множества, но и множества функций, преобразований (в том числе преобразований геометрических объектов) и даже множества произвольной природы. В соответствии с этим взглядом расширилось и понятие алгебраической операции. Например, если

рассмотреть множество *движений* плоскости, т. е. множество биекций плоскости на себя, сохраняющих расстояние между точками, то композиция, т. е. последовательное выполнение двух движений, результатом которой снова является движение, также может быть рассмотрена как естественная *алгебраическая операция* на множестве всех движений плоскости. Наша первая задача — сформулировать по возможности наиболее общее определение алгебраической операции. С этой целью мы рассмотрим несколько примеров и попытаемся выделить то главное, что их объединяет.

Примеры. 1. Операция сложения на множестве $\mathbb{N}$ натуральных чисел сопоставляет каждой паре натуральных чисел m и n однозначно определённое натуральное число $k = m + n$, которое называется суммой чисел m и n. Вспомним определение отображения. Несложно сообразить, что сложение можно рассматривать как отображение множества $\mathbb{N}^2$ в множество $\mathbb{N}$ (или $+ : \mathbb{N}^2 \to \mathbb{N}$). Правда, тогда, следуя нашим обозначениям для отображений, логичнее было бы писать $(m, n)+ = k$ вместо привычного $m + n = k$, но суть дела от этого не меняется. Более существенным выглядит другой вопрос: стоит ли считать, что пара элементов (в нашем случае это числа m и n), к которой мы применяем операцию, упорядочена? Ведь, как мы хорошо знаем, сложение натуральных чисел обладает тем свойством, что $m + n = n + m$, а значит, результат данной операции не зависит от порядка слагаемых. Но не стоит забывать, что мы стремимся к тому, чтобы дать по возможности общее определение алгебраической операции. Скажем, если мы зададим операцию $f : \mathbb{N}^2 \to \mathbb{N}$ по правилу $(m, n)f = m^n$ (возведение m в степень n), то при перемене мест аргументов результат, очевидно, изменится, поскольку m^n, вообще говоря, не равно n^m. То же самое мы увидим и в следующем примере.

2. Рассмотрим множество S всех отображений непустого множества A в себя. Мы будем называть такие отображения *преобразованиями* множества A. Поскольку композиция $f * g$ двух преобразований $f : A \to A$ и $g : A \to A$ снова является преобразованием множества A, отображение $* : S^2 \to S$, ставящее в соответствие паре преобразований их композицию, можно рассматривать как естественную алгебраическую операцию на множестве S. Легко заметить, что эта операция может оказаться некоммутативной ($f * g \neq g * f$). Рассмотрим, к примеру, следующие преобразования координатной плоскости $\mathbb{R}^2$. Пусть f — осевая симметрия плоскости относительно оси абсцисс, а g — поворот на угол $90°$ относительно начала координат. Композиция двух данных

преобразований, взятых в любом порядке, снова является преобразованием плоскости, однако результат зависит от порядка, в котором мы производим преобразования.



Действительно, образ точки A с координатами $(1,0)$ под действием преобразования $f * g$ есть точка B с координатами $(0,1)$:

$$A(f * g) = (Af)g = Ag = B.$$

С другой стороны, образ точки A под действием преобразования $g * f$ есть точка C с координатами $(0,-1)$:

$$A(g * f) = (Ag)f = Bf = C.$$

Таким образом, преобразования $f * g$ и $g * f$ различны.

Первые два примера приводят нас к определению операции на множестве A (вообще говоря, произвольной природы) как произвольного отображения из A^2 в A. Однако естественное желание продолжить обобщение приводит нас к мысли, что можно рассматривать операции от иного количества аргументов.

3. Операция вычитания на множестве $\mathbb{Z}$ целых чисел может быть успешно определена через операцию сложения, если мы предварительно введём операцию f *взятия противоположного элемента*. А именно, положим, что $\forall x \in \mathbb{Z}$ выполняется $xf = -x$. Тогда правило $x - y = (x,y) - = (x,yf) + = x + (-y)$ определяет вычитание для любых $x, y \in \mathbb{Z}$. Операция f взятия противоположного элемента зависит от одного, а не от двух аргументов, как это было в предыдущих примерах. Мы будем называть такие операции *унарными*, а операции, зависящие от двух аргументов, — *бинарными*.

4. В физике часто рассматривается центр масс системы тел. Пусть в пространстве V заданы три произвольные материальные точки A, B, C

одинаковой массы. Задача состоит в том, чтобы определить точку D пространства, которая является центром масс данной системы. Эта задача решается достаточно просто. Скажем, если точки A, B, C не лежат на одной прямой, то D — точка пересечения медиан треугольника ABC. Отображение $f : V^3 \to V$, ставящее в соответствие набору из трёх точек пространства точку, которая является центром масс указанной системы, можно рассматривать как алгебраическую операцию на множестве V. Естественно, можно рассмотреть аналогичную систему, состоящую из n материальных точек, что приведёт нас к операции от n аргументов.

Рассмотренные примеры приводят нас к следующему общему определению алгебраической операции.

Определение 1.2.1. Пусть A — непустое множество. Отображение $f : A^n \to A$ называется *n-арной* (или *n-местной) алгебраической операцией* на множестве A. Иными словами, n-арная алгебраическая операция, заданная на множестве A, ставит в соответствие каждому упорядоченному набору из n элементов множества A некоторый однозначно определённый элемент множества A. Число n называется *арностью* или *местностью* операции f.

Теперь мы готовы определить основной объект алгебры.

Определение 1.2.2. *Алгебраической системой* называется объект $\mathfrak{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots \rangle$, являющийся совокупностью непустого множества A и непустого набора алгебраических операций $f_1, f_2, \ldots, f_k, \ldots$, заданных на этом множестве. Множество A называется *носителем* или *основным множеством* системы $\mathfrak{A}$, а его элементы — *элементами системы* $\mathfrak{A}$.

Используя данное определение, можно сказать, что предметом алгебры является изучение алгебраических систем.

Примеры. 1. $\mathfrak{A} = \langle \mathbb{Z}, +, \cdot, f \rangle$, где $+$, $\cdot$ — обычные операции сложения и умножения целых чисел, а f — унарная операция взятия противоположного элемента.

2. $\mathfrak{A} = \langle S, * \rangle$, где S — множество всех преобразований непустого множества A, а $*$ — композиция двух преобразований.

3. $\mathfrak{A} = \langle \mathbb{R}[x], +, \cdot \rangle$, где $\mathbb{R}[x]$ — множество всех многочленов от одной переменной с коэффициентами из множества $\mathbb{R}$ действительных чисел, а сложение и умножение заданы естественным образом.

4. $\mathfrak{A} = \langle F, +, * \rangle$, где F — множество всех функций из $\mathbb{R}$ в $\mathbb{R}$, $*$ — композиция двух функций, а операция сложения определяется правилом $x(f + g) = xf + xg$.

5. $\mathfrak{A} = \langle P(A), \cap, \cup, \setminus, \neg \rangle$, где $P(A)$ — множество всех подмножеств некоторого непустого множества A, а операции пересечения, объединения, разности и взятия дополнения определяются в соответствии с нашими определениями из предыдущего параграфа. При этом $\cap, \cup, \setminus$ — бинарные операции, а операция $\neg$ взятия дополнения унарна.

6. Следующие объекты нельзя рассматривать как алгебраические системы: $\langle \mathbb{N}, - \rangle$, $\langle \mathbb{Z}, : \rangle$, так как результат операции не лежит в соответствующем множестве. Отметим, что даже на множестве $\mathbb{Q}$ не удаётся корректно определить операцию деления, поскольку на 0 делить нельзя. Однако если мы обозначим через $\mathbb{Q}^*$ множество $\mathbb{Q} \setminus \{0\}$ ненулевых рациональных чисел, то $\langle \mathbb{Q}^*, : \rangle$ — алгебраическая система. То же самое верно и для множества действительных чисел.

Упражнение 1.2.1. *Являются ли алгебраическими системами следующие объекты:*

1. *Множество $\mathbb{Z}$ целых чисел*?

2. $\langle \mathbb{Q}^+, \sqrt{\ } \rangle$, *где $\mathbb{Q}^+$ — множество положительных рациональных чисел, а $\sqrt{\ }$ — унарная операция извлечения арифметического корня*? *Тот же вопрос, если в качестве носителя выбрано множество $\mathbb{R}^+$ положительных действительных чисел.*

3. $\langle \mathbb{N}, f \rangle$, *где $f : \mathbb{N}^2 \to \mathbb{N}$ по правилу $(m, n)f = $ Н.О.Д.(m, n) — наибольший общий делитель чисел m и n*?

Определение 1.2.3. Пусть на множестве A задана n-арная алгебраическая операция f. Если непустое подмножество B множества A таково, что $B^n f \subseteq B$ (т. е. результат операции f, произведённой над произвольными элементами множества B, снова принадлежит B), то B называется *замкнутым* относительно операции f. При этом на множестве B определена n-арная алгебраическая операция $f|_B : B^n \to B$, действующая по правилу $(b_1, b_2, \ldots, b_n)f|_B = (b_1, b_2, \ldots, b_n)f$, которую мы назовём *сужением* (или *ограничением) f на B*.

Замечание. Если подмножество B множества A замкнуто относительно операции f, то в случаях, не вызывающих недоразумений, будем использовать для сужения f на B то же самое обозначение f, что и для операции на основном множестве A.

Примеры. 1. Подмножества $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ множества $\mathbb{R}$ замкнуты относительно операции сложения $+$, заданной на $\mathbb{R}$. С другой стороны, первые два из упомянутых подмножеств замкнуты относительно операции вычитания $-$, заданной на том же множестве, а третье — множество $\mathbb{N}$ натуральных чисел — нет.

2. Как следует из упражнения 1.1.3, подмножество всех биекций множества всех преобразований непустого множества A замкнуто относительно операции композиции.

Упражнение 1.2.2. *Обозначим через $2\mathbb{Z}$ и $2\mathbb{Z}+1$ множества чётных и нечётных целых чисел соответственно. Относительно каких операций, заданных на множестве $\mathbb{Z}$ целых чисел, замкнуты эти множества? Рассмотреть бинарные операции: сложение, умножение, вычитание, деление, взятие наибольшего общего делителя; а также унарные операции: взятие противоположного элемента, удвоение, утроение. Под удвоением (утроением) понимается операция, сопоставляющая каждому целому числу n число $2n$ ($3n$ соответственно).*

Упражнение 1.2.3. *Даны два взаимно простых натуральных числа a и b. Пусть подмножество M множества $\mathbb{Z}$ целых чисел таково, что $a, b \in M$ и M замкнуто относительно операций сложения и взятия противоположного элемента. Докажите, что $M = \mathbb{Z}$.*

Определение 1.2.4. Непустое подмножество B основного множества A системы $\mathfrak{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots\rangle$ называется *замкнутым* в системе $\mathfrak{A}$, если оно замкнуто относительно каждой алгебраической операции системы $\mathfrak{A}$. Система $\mathfrak{B} = \langle B, f_1|_B, f_2|_B, \ldots, f_k|_B, \ldots\rangle$ называется *подсистемой* системы $\mathfrak{A}$.

Примеры. 1. Система $\mathfrak{B} = \langle \mathbb{N}, +, \cdot, \rangle$ является подсистемой системы $\mathfrak{A} = \langle \mathbb{Z}, +, \cdot, \rangle$. Но если в $\mathfrak{A}$ добавить операцию вычитания (или взятия противоположного элемента), то образовать подсистему, используя в качестве носителя множество $\mathbb{N}$, уже не удастся.

2. Пусть $\mathfrak{A} = \langle F, +, * \rangle$, где F — множество всех функций из $\mathbb{R}$ в $\mathbb{R}$, $*$ — композиция двух функций, а операция сложения определяется правилом $x(f+g) = xf + xg$. Пусть $\widehat{F}$ — подмножество всех возрастающих функций множества F. Тогда $\mathfrak{B} = \langle \widehat{F}, +, * \rangle$ — подсистема системы $\mathfrak{A}$.

Упражнение 1.2.4. *Определите все конечные подсистемы (т. е. подсистемы с носителями, содержащими конечное число элементов) следующих алгебраических систем:*

1. $\langle \mathbb{Z}, f \rangle$, *где f — операция удвоения.*

2. $\langle \mathbb{Z}, \cdot \rangle$.

3. $\langle P, f \rangle$, *где P — множество точек плоскости, а f — 3-арная операция, сопоставляющая трём точкам пространства их центр масс.*

§ 1.3. Изоморфизм алгебраических систем

В математике очень важно иметь возможность выяснить, когда две на первый взгляд различные задачи по существу совпадают. В алгебре нас занимают только те свойства алгебраических систем и их основных множеств, которые могут быть выражены в терминах заданных операций. Если две алгебраические системы имеют одни и те же алгебраические свойства, то с точки зрения алгебраиста их можно рассматривать как идентичные. Этот подход приводит нас к понятию *изоморфизма* — биективного отображения носителя одной алгебраической системы на носитель другой, *сохраняющего* заданные операции.

Определение 1.3.1. Пусть заданы две алгебраические системы $\mathfrak{A} = \langle A, f_1, f_2, \ldots, f_k, \ldots\rangle$ и $\mathfrak{B} = \langle B, g_1, g_2, \ldots, g_k, \ldots\rangle$ с одним и тем же числом алгебраических операций, причём операции f_i и g_i с одним и тем же индексом имеют одинаковую арность n_i. Системы $\mathfrak{A}$ и $\mathfrak{B}$ называются *изоморфными* (запись $\mathfrak{A} \simeq \mathfrak{B}$), если существует биекция $\varphi : A \to B$ такая, что для любого индекса i и любого упорядоченного набора элементов $(a_1, a_2, \ldots, a_{n_i}) \in A^{n_i}$ выполняется равенство

$$((a_1, a_2, \ldots, a_{n_i})f_i)\varphi = (a_1\varphi, a_2\varphi, \ldots, a_{n_i}\varphi)g_i.$$

Биекция φ, удовлетворяющая указанному свойству, называется *изоморфизмом системы* $\mathfrak{A}$ *на систему* $\mathfrak{B}$.

Замечание. Поскольку изоморфизм φ системы $\mathfrak{A}$ на систему $\mathfrak{B}$ является биекций их носителей A и B, корректно определено обратное отображение $\varphi^{-1} : B \to A$, которое также является биекцией. Нетрудно проверить, что это отображение тоже сохраняет операции, а значит, является изоморфизмом системы $\mathfrak{B}$ на систему $\mathfrak{A}$. Таким образом, если система $\mathfrak{A}$ изоморфна системе $\mathfrak{B}$, то и система $\mathfrak{B}$ изоморфна системе $\mathfrak{A}$, т. е. понятие изоморфизма *симметрично* относительно $\mathfrak{A}$ и $\mathfrak{B}$.

Примеры. 1. Пусть $\mathfrak{A} = \langle \mathbb{R}, + \rangle$, $\mathfrak{B} = \langle \mathbb{R}^+, \cdot \rangle$, здесь $\mathbb{R}^+$ — множество положительных действительных чисел. Рассмотрим отображение $\varphi : \mathbb{R} \to \mathbb{R}^+$, заданное правилом $x\varphi = 2^x$. Докажем, что φ — изоморфизм $\mathfrak{A}$ на $\mathfrak{B}$. Тот факт, что φ — биекция множества $\mathbb{R}$ на множество $\mathbb{R}^+$, известен из школьного курса математики. С другой стороны, $\forall x, y \in \mathbb{R}$ имеем

$$(x + y)\varphi = 2^{x+y} = 2^x \cdot 2^y = (x\varphi) \cdot (y\varphi),$$

откуда следует, что φ сохраняет операцию, а следовательно, является изоморфизмом. Аналогично, обратное отображение, действующее по правилу $x\varphi^{-1} = \log_2(x)$, есть изоморфизм $\mathfrak{B}$ на $\mathfrak{A}$.

2. Пусть $\mathfrak{A} = \langle \mathbb{Z}, + \rangle$, $\mathfrak{B} = \langle 2\mathbb{Z}, + \rangle$, здесь, как и в предыдущем параграфе, $2\mathbb{Z}$ — множество всех чётных чисел. Рассмотрим отображение $\varphi : \mathbb{Z} \to 2\mathbb{Z}$, заданное правилом $x\varphi = 2x$. Это отображение, очевидно, является биекцией, а цепочка равенств $(x + y)\varphi = 2(x + y) = 2x + 2y = x\varphi + y\varphi$ показывает, что оно к тому же сохраняет операцию. Следовательно, $\mathfrak{A} \simeq \mathfrak{B}$.

Подчеркнём ещё раз, что изоморфизм систем влечёт полное совпадение их алгебраических свойств. Иными словами, любое утверждение, которое можно записать в терминах алгебраических операций, заданных на одной из изоморфных систем, будет верно и для второй системы (естественно, в терминах соответствующих операций второй системы).

Предположим теперь, что две алгебраические системы $\mathfrak{A}$ и $\mathfrak{B}$ не изоморфны. Вопрос состоит в том, как это доказать. Если носители A и B этих систем не равномощны, то всё очевидно, так как между ними не удастся установить биекцию. Однако если множества A и B равномощны, то проблема сложнее, поскольку проверка того факта, что некоторая биекция не сохраняет операции, не даёт права утверждать, что системы не изоморфны. Требуется проверить все биекции, а их может быть очень много. Например, если равномощные множества A и B бесконечны, то и биекций между ними бесконечно много. Тем не менее обращение к сути понятия изоморфизма подсказывает способ доказательства неизоморфности систем. Напомним, что изоморфизм систем влечёт полное совпадение их алгебраических свойств. Следовательно, если мы укажем свойство операции (операций) одной системы, которое не имеет места для соответствующей операции (операций) второй системы, то отсюда будет вытекать неизоморфность этих систем. Поясним сказанное на простом примере.

Пример. Пусть $\mathfrak{A} = \langle \mathbb{Z}, \cdot \rangle$, $\mathfrak{B} = \langle 2\mathbb{Z}, \cdot \rangle$. В множестве $\mathbb{Z}$ есть элемент 1, который обладает тем свойством, что $\forall x \in \mathbb{Z}$ имеет место равенство $1 \cdot x = x$. В множестве $2\mathbb{Z}$ элемента с таким свойством нет. Воспользуемся этим для доказательства того факта, что системы $\mathfrak{A}$ и $\mathfrak{B}$ не изоморфны. Предположим противное, и пусть φ — биекция, устанавливающая изоморфизм. Положим $1\varphi = 2k$, $2\varphi = 2n$, где k, n — некоторые целые числа. Поскольку φ должна сохранять операцию, выполняется цепочка равенств: $4kn = (2k) \cdot (2n) = 1\varphi \cdot 2\varphi = (1 \cdot 2)\varphi = 2\varphi = 2n$. Если $n \neq 0$, то $2k = 1$, что невозможно. Если же предположить, что $2\varphi = 0$, то можно записать аналогичную цепочку равенств для элементов 1φ и $3\varphi = 2m$, последний из которых в данном случае не может быть равен 0, поскольку φ — взаимно однозначное отображение и $3\varphi \neq 2\varphi = 0$.

Имеем $4km = (2k) \cdot (2m) = 1\varphi \cdot 3\varphi = (1 \cdot 3)\varphi = 3\varphi = 2m$. Отсюда снова $2k = 1$; противоречие. Таким образом, никакая биекция не сохраняет операцию, а значит, системы $\mathfrak{A}$ и $\mathfrak{B}$ не изоморфны.

Упражнение 1.3.1. *Изоморфны ли следующие алгебраические системы:*

1) $\langle \mathbb{Z}, + \rangle$ *и* $\langle \mathbb{Z}, \cdot \rangle$;

2) $\langle P(A), \cap \rangle$ *и* $\langle P(A), \cup \rangle$, *здесь* A — *произвольное непустое множество;*

3) $\langle \mathbb{Q}, + \rangle$ *и* $\langle \mathbb{Q}^+, \cdot \rangle$, *здесь* $\mathbb{Q}^+$ — *множество положительных рациональных чисел* (*сравните с примером* 1 *к определению изоморфизма*);

4) $\langle \mathbb{N}, f \rangle$ *и* $\langle \mathbb{N}, g \rangle$, *здесь* f *и* g — *унарные операции удвоения и утроения*?

Упражнение 1.3.2.* *Пусть* a, b — *два произвольных действительных числа. Обозначим через* $\mathfrak{A}_{ab}$ *алгебраическую систему* $\langle \mathbb{R}, f \rangle$ *с одной унарной операцией* f, *действующей по правилу* $xf = ax + b$. *Сколько попарно неизоморфных алгебраических систем в множестве* $\{\mathfrak{A}_{ab} \mid a, b \in \mathbb{R}\}$?

Глава 2

Группы, кольца, поля

§ 2.1. Определения основных алгебраических структур

В силу общности определений алгебраической операции и алгебраической системы можно придумать массу примеров алгебраических систем. Далеко не все из них будут представлять реальный интерес. В этом параграфе мы определим наиболее существенные классы алгебраических систем: группы, кольца и поля. Мы сделаем это, выделив естественные алгебраические свойства, которыми системы из этих классов должны обладать. Поэтому сначала мы обсудим, какие свойства можно считать наиболее существенными. Рассмотрим следующее выражение: $(x+y)-x$. Одного взгляда на него достаточно, чтобы уверенно заявить, что оно равно y (предполагается, что x и y — числа). Однако та легкость, с которой был сделан вывод, основана на хорошем знакомстве со свойствами сложения чисел. Попробуем вспомнить эти свойства, выписав подробно все шаги, которые мы совершили при преобразовании выражения:

$$(x + y) - x = (x + y) + (-x), \tag{1}$$

$$(x + y) + (-x) = (y + x) + (-x), \tag{2}$$

$$(y + x) + (-x) = y + (x + (-x)), \tag{3}$$

$$y + (x + (-x)) = y + 0, \tag{4}$$

$$y + 0 = y. \tag{5}$$

Шаг (1) соответствует определению операции вычитания через сложение с противоположным элементом. В свою очередь, определение *противоположного* элемента: $x + (-x) = 0$ — явным образом использовалось на шаге (4). Основное свойство 0, или, как говорят в алгебре, *нейтрального элемента* по сложению, — основа шага (5). Шаг (2) — знакомый с первого класса переместительный закон сложения. Его общеупотребительное алгебраическое название — закон *коммутативности*. Наконец, шаг (3) основан на законе *ассоциативности* сложения (в элементарной математике его называют сочетательным законом). Если

добавить к указанным свойствам аналогичные свойства операции умножения, а также связывающий между собой сложение и умножение распределительный закон (свойство *дистрибутивности*), то мы получим набор базовых свойств основных операций на числовых множествах. Разумно определённые алгебраические системы (необязательно числовые) также обладают аналогичными свойствами (или некоторыми из них). Сначала мы займёмся алгебраическими системами с одной бинарной операцией. Наиболее важный класс таких систем — *группы*.

Определение 2.1.1. Алгебраическая система $\mathfrak{G} = \langle G, * \rangle$ с одной бинарной операцией называется *группой*, если выполняются следующие условия (*аксиомы группы*):

1. Для любых элементов $a, b, c \in G$ выполняется $(a * b) * c = a * (b * c)$ (аксиома ассоциативности).

2. Существует элемент $e \in G$ такой, что для любого элемента $a \in G$ выполняется $a * e = e * a = a$ (аксиома нейтрального элемента).

3. Для любого $a \in G$ существует элемент $a^{-1} \in G$ такой, что выполняется $a * a^{-1} = a^{-1} * a = e$ (аксиома обратного элемента).

Замечание. Подчеркнём, что термин *группа* — это не название конкретной алгебраической системы. Любая алгебраическая система с одной бинарной операцией, удовлетворяющей перечисленным аксиомам, является группой. Таким образом, с помощью термина группа мы выделяем целый класс алгебраических систем.

Примеры. 1. $\mathfrak{G} = \langle \mathbb{Z}, + \rangle$. В данном случае групповая операция — сложение. Нейтральным элементом является число 0, а обратным элементом к целому числу a, очевидно, будет число с противоположным знаком. Группами также являются следующие числовые алгебраические системы: $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{Q}^*, \cdot \rangle$, $\langle \mathbb{R}^*, \cdot \rangle$.

2. Если S — множество всех движений плоскости, а $*$ — операция композиции, заданная на этом множестве, то система $\mathfrak{G} = \langle S, * \rangle$ является группой. Относительно той же операции композиции группы образуют и множество всех параллельных переносов, и множество всех поворотов плоскости относительно заданной точки.

Несложно заметить, что все числовые алгебраические системы из примера 1 помимо аксиом группы обладают свойством коммутативности: $a * b = b * a$. С другой стороны, группа движений плоскости из примера 2 этим свойством не обладает (см. пример с композицией поворота и осевой симметрии из § 1.2).

Определение 2.1.2. Группа $\mathfrak{G} = \langle G, * \rangle$ называется *абелевой* (или

коммутативной), если для любых двух элементов $a, b \in G$ выполняется равенство $a * b = b * a$ (аксиома коммутативности).

Замечание. Обычно операцию в группе называют *умножением* и вместо $a*b$ пишут просто ab. Стоит, однако, помнить, что носитель группы может не являться числовым множеством, а групповая операция может не иметь никакого отношения к обычному умножению чисел. Иногда, если речь идет о коммутативной группе, в качестве символа операции используют знак $+$, операцию называют *сложением*, нейтральный элемент называют нулём и обозначают 0, а обратный элемент к элементу a называют противоположным и обозначают $-a$. В зависимости от обозначения групповой операции говорят о *мультипликативной* (операция — умножение) или *аддитивной* (операция — сложение) группе. В тех ситуациях, когда групповая операция заранее известна, обозначение группы отождествляют с обозначением основного множества, на котором она задана, т. е. вместо записи *группа* $\mathfrak{G} = \langle G, * \rangle$ пишут просто *группа* G.

Упражнение 2.1.1. *Пусть G — мультипликативная группа (группа с операцией умножения), g — некоторый элемент этой группы. Докажите, что отображение $\varphi_g : G \to G$, действующее по правилу $x\varphi_g = xg$ для любого элемента $x \in G$, является биекцией множества G на себя.*

Упражнение 2.1.2. *Пусть G — группа. Докажите, что нейтральный элемент группы, определённый аксиомой 2, единствен. Докажите, что для каждого элемента $g \in G$ его обратный элемент, определённый аксиомой 3, единствен.*

Пусть $g_1, g_2, \ldots, g_n$ — элементы группы G. Определим

$$\prod_{i=1}^{n} g_i = (\ldots(g_1 \cdot g_2) \cdot \ldots) \cdot g_n.$$

Упражнение 2.1.3. *Докажите, что*

$$\prod_{i=1}^{n} g_i = \prod_{i=1}^{k} g_i \cdot \prod_{i=k+1}^{n} g_i.$$

Замечание. Вывод, который следует из утверждения упражнения 2.1.3, можно сформулировать так: произведение элементов группы не зависит от расстановки скобок в этом произведении (*обобщённый ассоциативный закон*).

При определении абелевой группы мы добавили к аксиомам группы дополнительную аксиому коммутативности. С другой стороны, иногда бывает полезно рассматривать алгебраические системы с одной бинарной операцией, в которых выполняются только некоторые из аксиом группы.

Определение 2.1.3. Алгебраическая система $\mathfrak{G} = \langle G, * \rangle$ с одной бинарной операцией называется *полугруппой*, если она удовлетворяет аксиоме ассоциативности. Полугруппа называется *моноидом*, если в ней есть нейтральный элемент.

Пример. Примером полугруппы служит множество $\mathbb{N}$ натуральных чисел с операцией сложения (или умножения), а моноидом является множество всех преобразований произвольного непустого множества, если в качестве операции взять композицию двух преобразований (подробнее об этом позже).

Упражнение 2.1.4. *Пусть A — непустое множество. Докажите, что система $\langle P(A), \cap \rangle$ — полугруппа. Является ли она моноидом*?

Используя определение 2.1.3, можно определить понятие группы следующим образом: группа — это моноид, в котором каждый элемент обратим.

Определение 2.1.4. Пусть алгебраическая система $\mathfrak{G} = \langle G, * \rangle$ является группой. Её подсистема $\mathfrak{H} = \langle H, *|_H \rangle$ называется *подгруппой*, если она является группой относительно сужения $*|_H$ групповой операции $*$ на множество H.

Замечание. Отметим, что не каждая подсистема группы является подгруппой. Например, $\langle \mathbb{N}, + \rangle$ является подсистемой группы $\langle \mathbb{Z}, + \rangle$, но не является её подгруппой, поскольку в ней не выполняются аксиомы нейтрального элемента и обратного элемента.

Как и в случае с группой, мы будем отождествлять обозначение подгруппы $\mathfrak{H} = \langle H, *|_H \rangle$ с обозначением её основного множества H. В частности, тот факт, что H — подгруппа группы G, мы будем кратко записывать следующим образом: $H \leqslant G$.

Примеры. 1. В любой группе G всегда есть две подгруппы: сама G и *единичная подгруппа* $1 = \{e\}$, состоящая из нейтрального элемента e группы G.

2. Для данного натурального числа n множество $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ всех целых чисел, кратных n, является подгруппой группы $\mathbb{Z}$ целых чисел с операцией сложения.

Упражнение 2.1.5. *Пусть G — группа. Докажите, что непустое подмножество H является подгруппой группы G, если $\forall a, b \in H$ выполняются свойства:*

1) $ab \in H$; 2) $a^{-1} \in H$.

Порядком группы G называется количество элементов множества G. Мы будем обозначать порядок группы через $|G|$. Аналогично определяется порядок подгруппы. Пусть g — элемент мультипликативной группы G. Если n — натуральное число, то через g^n мы обозначим элемент группы G, который получается в результате умножения g на себя n раз:

$$g^n = \underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ раз}}.$$

Порядком элемента g группы G называется наименьшее натуральное число n такое, что $g^n = e$, где e — нейтральный элемент группы G, если такое число n существует. В противном случае мы говорим, что элемент g имеет бесконечный порядок. Порядок элемента g обозначается через $|g|$.

Упражнение 2.1.6. *Докажите, что в конечной группе каждый элемент имеет конечный порядок.*

Для удобства мы также положим, что $g^0 = e$ и $g^{-n} = (g^{-1})^n$, где n — натуральное число, определив таким образом любую целую степень элемента группы.

Упражнение 2.1.7. *Пусть h — произвольный элемент группы G. Докажите, что множество $H = \{h^n \mid n \in \mathbb{Z}\}$ является подгруппой группы G.*

Теперь мы определим два важнейших класса алгебраических систем с двумя бинарными операциями. Мы будем называть эти операции сложением и умножением и обозначать через $+$ и $\cdot$, не забывая о том, что они могут существенно отличаться от сложения и умножения чисел в обычном смысле.

Определение 2.1.5. Алгебраическая система $\mathfrak{R} = \langle R, +, \cdot \rangle$ с двумя бинарными операциями — сложением и умножением — называется *кольцом*, если выполняются следующие условия:

1. Множество R является абелевой группой относительно сложения.

2. Для любых $a, b, c \in R$ выполняются равенства $(a + b)c = ac + bc$ (*правый закон дистрибутивности*) и $c(a + b) = ca + cb$ (*левый закон дистрибутивности*).

Замечание. Как и в случае с группой, мы будем зачастую использовать обозначение носителя R для самого кольца $\mathfrak{R}$.

Кольцо называется *ассоциативным*, если операция умножения, заданная в кольце, ассоциативна. Поскольку в нашем курсе алгебры мы будем иметь дело только с ассоциативными кольцами, договоримся, что под термином *кольцо* мы будем всегда понимать именно ассоциативное кольцо.

Кольцо называется *коммутативным*, если операция умножения, заданная в кольце, коммутативна. Кольцо называется *кольцом с единицей*, если в нём существует нейтральный по умножению элемент, который мы будем записывать как 1. Отметим, что мы всегда полагаем, что в кольце с единицей $1 \neq 0$, в частности, кольцо с единицей содержит по крайней мере два различных элемента. Элемент кольца называется *обратимым*, если для него существует обратный по умножению элемент. Множество всех обратимых элементов кольца R обозначим через R^*.

Определение 2.1.6. Алгебраическая система $\mathfrak{F} = \langle F, +, \cdot \rangle$ с двумя бинарными операциями — сложением и умножением — называется *полем*, если она является коммутативным (и, по нашей договорённости, ассоциативным) кольцом с единицей, в котором каждый ненулевой элемент обратим.

Перед тем как перейти к примерам, приведём для удобства полный список аксиом кольца и поля.

1. $\forall a, b, c$: $(a + b) + c = a + (b + c)$ — ассоциативность сложения.
2. $\forall a, b$: $a + b = b + a$ — коммутативность сложения.
3. $\exists 0\ \forall a$: $a + 0 = 0 + a = a$ — существование нуля.
4. $\forall a\ \exists(-a)$: $a + (-a) = (-a) + a = 0$ — существование противоположного элемента.
5. $\forall a, b, c$: $(a + b)c = ac + bc$ — правая дистрибутивность.
6. $\forall a, b, c$: $c(a + b) = ca + cb$ — левая дистрибутивность.
7. $\forall a, b, c$: $(ab)c = a(bc)$ — ассоциативность умножения.
8. $\forall a, b$: $ab = ba$ — коммутативность умножения.
9. $\exists 1\ \forall a$: $a \cdot 1 = 1 \cdot a = a$ — существование единицы.

10. $\forall a \neq 0\ \exists a^{-1}$: $aa^{-1} = a^{-1}a = 1$ — существование обратного элемента.

Таким образом, алгебраическая система с операциями сложения и умножения, удовлетворяющими аксиомам 1–7 (или 1–6, если не предполагать, что кольцо ассоциативно), является кольцом, а система с операциями, удовлетворяющими аксиомам 1–10, является полем.

Примеры. 1. Числовые алгебраические системы $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ являются кольцами. Первая из них является коммутативным кольцом с единицей, но не является полем. Вторая и третья системы являются полями.

2. Определим на множестве $P(A)$ всех подмножеств непустого множества A операцию *симметрической разности* $\triangle$ по правилу: $\forall B, C \subseteq A$ имеем $B \triangle C = (B \setminus C) \cup (C \setminus B)$. Система $\langle P(A), \triangle, \cap \rangle$ является коммутативным кольцом с единицей.

3. Множество всех векторов трёхмерного пространства относительно операций сложения и векторного произведения образует неассоциативное кольцо (и некоммутативное).

Как и в случае с группой, *подкольцо* (*подполе*) определяется как подсистема кольца (поля), которая сама является кольцом (полем) относительно сужений операций сложения и умножения, заданных в кольце (в поле).

Пример. Подмножество $n\mathbb{Z}$ образует подкольцо кольца целых чисел относительно обычных операций сложения и умножения. Поле рациональных чисел, очевидно, является подполем поля действительных чисел.

Как и в случае с группой, под *порядком* кольца (поля) мы понимаем количество элементов в его носителе.

Пример. Поле из двух элементов можно определить, записав для его элементов, а это по необходимости 0 и 1 (не путать с числами!), таблицы сложения и умножения:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Это поле, которое мы обозначим через $\mathbb{Z}_2$, — частный пример кольца $\mathbb{Z}_n$ вычетов по модулю n (см. упражнения в конце этого параграфа).

Если взглянуть на таблицу умножения поля $\mathbb{Z}_2$, обнаруживается, что для любого элемента $a \in \mathbb{Z}_2$ выполняется $a \cdot 0 = 0 \cdot a = 0$. Это же

свойство, как известно, присуще и числовым кольцам (см. примеры). Сейчас мы докажем, что это свойство имеет место в любом кольце (в том числе и неассоциативном).

Предложение 2.1.1. *Пусть R — кольцо. Для любого элемента $a \in R$ имеет место равенство $a \cdot 0 = 0 \cdot a = 0$.*

Доказательство. Мы докажем только равенство $a0 = 0$, поскольку второе доказывается аналогично. Пусть $a0 = b$. Тогда

$$b + b = a0 + a0 = a(0 + 0) = a0 = b.$$

Прибавляя к обеим частям равенства $b + b = b$ противоположный к b элемент, получаем $(b + b) + (-b) = b + (-b)$. Откуда $b + (b + (-b)) = 0$, а значит, $b + 0 = 0$, и окончательно $b = 0$. □

Отметим, что в произвольном кольце из равенства $ab = 0$, вообще говоря, не следует, что $a = 0$ или $b = 0$. Ненулевые элементы кольца, для которых имеет место равенство $ab = 0$, называют *делителями нуля*. Кольцо, в котором таких делителей нет, называют *кольцом без делителей нуля*. Примером кольца без делителей нуля может служить произвольное поле.

Предложение 2.1.2. *В поле нет делителей нуля.*

Доказательство. Пусть F — поле и элементы $a, b \in F$ таковы, что $ab = 0$, но $a \neq 0$ и $b \neq 0$. Умножим каждую часть равенства $ab = 0$ справа на элемент b^{-1}, обратный к элементу b (его существование следует из аксиомы 10). Имеем $(ab)b^{-1} = 0b^{-1}$. Левая часть этого равенства в силу ассоциативности умножения равна $a(bb^{-1})$, а значит, в силу аксиом 9 и 10 она равна a. Правая часть равенства в силу предложения 2.1.1 равна 0. Полученное противоречие доказывает наше утверждение. □

Утверждение предложения 2.1.1 выполняется для любой алгебраической системы, являющейся кольцом, а утверждение предложения 2.1.2 — для любой алгебраической системы, являющейся полем. Поэтому, доказав эти предложения, мы получили результаты, касающиеся не одной конкретной системы, а целого класса алгебраических систем. В этом состоит значение абстрактного подхода к алгебре.

Упражнение 2.1.8. *Зафиксируем натуральное число n. Для произвольного целого числа k обозначим через $\overline{k}$ множество всех целых чисел, сравнимых с k по модулю n. Пусть $\mathbb{Z}_n = \{\overline{k} \mid k \in \mathbb{Z}\}$. Покажите, что операции сложения и умножения, заданные формулами: $\overline{i} + \overline{j} = \overline{i + j}$, $\overline{i} \cdot \overline{j} = \overline{i \cdot j}$, корректно определены на $\mathbb{Z}_n$, и докажите, что относительно*

указанных операций множество $\mathbb{Z}_n$ образует кольцо. Это кольцо называется кольцом вычетов по модулю n.

Упражнение 2.1.9. *Докажите, что кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.*

Упражнение 2.1.10. *Сформулируйте определение изоморфизма для колец и докажите, что любой изоморфизм кольца целых чисел на себя является тождественным.*

§ 2.2. Группа подстановок

Определение 2.2.1. Биективное преобразование π непустого множества M, т. е. взаимно однозначное отображение M на себя, называется *подстановкой* множества M.

Примеры. 1. Преобразование π множества $\mathbb{N}$ натуральных чисел, определённое правилом

$$n\pi = \begin{cases} 2k-1, & \text{при } n = 2k, \\ 2k, & \text{при } n = 2k-1, \end{cases}$$

является подстановкой, а преобразование χ того же множества по правилу $n\chi = 2n$ — нет, поскольку это отображение — инъекция, но не сюръекция.

2. Преобразование π множества $M = \{1, 2, 3\}$ по правилу $1\pi = 2$, $2\pi = 3$, $3\pi = 1$, будет подстановкой, а преобразование χ того же множества M по правилу $1\chi = 2$, $2\chi = 3$, $3\chi = 2$, — нет.

В случае, когда множество M конечно, подстановку удобно записывать в виде таблицы из двух строк. Например, подстановка π из примера 2 при такой форме записи будет выглядеть следующим образом:

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

При этом в первой строке перечисляются все элементы множества, а затем под каждый из них *подставляется* его образ при отображении π. Термин *подстановка* появился именно из-за этой формы записи. Отметим, что элементы в первой строке подстановки могут располагаться в любом порядке. В частности,

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Теорема 2.2.1. *Множество $S(M)$ всех подстановок непустого множества M образует группу относительно операции композиции.*

Доказательство. Пусть π, σ — две подстановки множества $S(M)$. Докажем, во-первых, что их композиция $\pi * \sigma$ тоже является подстановкой. Заметим, что $\pi * \sigma$ — преобразование множества M. Поэтому нам остаётся показать, что $\pi * \sigma$ — биективное преобразование. Для любых $x, y \in M$ из равенства $x(\pi * \sigma) = y(\pi * \sigma)$ следует равенство $(x\pi)\sigma = (y\pi)\sigma$. Поскольку σ – биекция, имеем $x\pi = y\pi$. Но π — тоже биекция, откуда $x = y$. Следовательно, $\pi * \sigma$ — инъекция. С другой стороны, подстановки π и σ, как биекции, имеют обратные отображения π^{-1} и σ^{-1}, которые тоже являются биекциями, а значит, подстановками. Для произвольного элемента $x \in M$ элемент $y = (x\sigma^{-1})\pi^{-1} \in M$ обладает тем свойством, что $y(\pi * \sigma) = ((x\sigma^{-1})\pi^{-1})(\pi * \sigma) = ((x\sigma^{-1})(\pi^{-1} * \pi))\sigma = (x\sigma^{-1})\sigma = x$. А значит, $\pi * \sigma$ — сюръекция. Поэтому $\pi * \sigma$ — подстановка. Таким образом, $\langle S(M), \cdot \rangle$ — алгебраическая система.

Проверим теперь, что эта система является группой. Нейтральным элементом этой системы является тождественная подстановка ε, действующая на каждом элементе $x \in M$ по правилу $x\varepsilon = x$. С другой стороны, для каждой подстановки π существует обратное преобразование π^{-1}, которое тоже является биекцией, а значит, подстановкой. Поэтому аксиомы 2 и 3 группы выполнены. Осталось доказать, что операция композиции подстановок ассоциативна. Мы докажем более общее утверждение:

Предложение 2.2.1. *Пусть $f : X \to Y$, $g : Y \to U$, $h : U \to W$ — произвольные отображения, тогда $(f * g) * h = f * (g * h)$.*

Доказательство предложения. Пусть x — произвольный элемент множества X. Утверждение предложения следует из следующей цепочки равенств:

$$x((f * g) * h) = (x(f * g))h = ((xf)g)h = (xf)(g * h) = x(f * (g * h)).$$

Поскольку подстановка — частный случай отображения, ассоциативность композиции подстановок следует из предложения 2.2.1. □

Поскольку $S(M)$ — группа, мы будем называть композицию подстановок π и σ *произведением*, называть операцию композиции *умножением* подстановок и писать $\pi \cdot \sigma$ или $\pi\sigma$ вместо $\pi * \sigma$.

Пример. Пусть $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Тогда

$$\pi\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Упражнение 2.2.1.

1. *Перемножить подстановки π и σ из примера в обратном порядке и убедиться, что $\pi\sigma \neq \sigma\pi$.*

2. *Найти порядки подстановок π и σ как элементов группы.*

3. *Найти подстановки π^{100} и σ^{100}.*

4. *Найти подстановки π^{-1} и σ^{-1}, обратные к подстановкам π и σ.*

Определение 2.2.2. Группа $S(M)$ всех подстановок множества M называется *симметрической группой подстановок* множества M. Произвольную подгруппу этой группы будем называть *группой подстановок* множества M.

Поскольку свойства группы подстановок множества M не зависят от природы элементов из M, симметрические группы подстановок равномощных множеств изоморфны. В случае, когда множество M конечно и состоит из n элементов, будем обозначать симметрическую группу подстановок множества M через S_n (*симметрическая группа степени* n) и полагать, что $M = \{1, 2, \ldots, n\}$. Элементы множества M будем называть *символами*. В нашем курсе мы будем иметь дело прежде всего с группами подстановок, заданных на конечных множествах.

Упражнение 2.2.2. *Доказать, что $|S_n| = n!$. Выписать все подстановки из группы S_3. Составить таблицу умножения для группы S_3. Найти все подгруппы группы S_3.*

Будем записывать произвольную подстановку π группы S_n как

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

подразумевая, что $\{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$ и $1\pi = i_1, 2\pi = i_2, \ldots, n\pi = i_n$. Иногда мы будем нарушать порядок элементов в первой строке и записывать произвольную подстановку как

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}.$$

В частности, подстановка π^{-1} может быть записана следующим образом:

$$\pi^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Теперь мы рассмотрим вопрос о структуре множества символов $M = \{1, 2, \dots, n\}$ относительно действия на нём некоторой подстановки $\pi \in S_n$. Пусть i — произвольный символ из M. Если $i\pi = i$, т. е. i остаётся на месте под действием подстановки π, то мы будем называть i *неподвижным символом* относительно π. Если $i\pi \neq i$, то будем говорить, что i — *перемещаемый символ*. Множество всех перемещаемых подстановкой π символов обозначим через $\operatorname{supp}(\pi)$ и назовём *носителем* или *суппортом* подстановки π. Таким образом, подстановка

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_s & k_1 & \dots & k_t \\ j_1 & j_2 & \dots & j_s & k_1 & \dots & k_t \end{pmatrix},$$

где $i_l \neq j_l$ для любого $l \in \{1, 2, \dots, s\}$, имеет носитель $\operatorname{supp}(\pi) = \{i_1, i_2, \dots, i_s\}$. Несложно заметить, что образ $\operatorname{supp}(\pi)\pi = \{j_1, j_2, \dots, j_s\}$ носителя $\operatorname{supp}(\pi)$ под действием π совпадает с самим носителем, т. е. $\operatorname{supp}(\pi)\pi = \operatorname{supp}(\pi)$. Кроме того, $\operatorname{supp}(\varepsilon) = \varnothing$ и $\operatorname{supp}(\pi^{-1}) = \operatorname{supp}(\pi)$, где ε — тождественная, а π^{-1} — обратная к π подстановки.

Пусть $i_1 \in \operatorname{supp}(\pi)$ и $i_1\pi = i_2$, $i_2\pi = i_3$ и т. д., а s — наименьшее натуральное число такое, что $i_s\pi \in \{i_1, i_2, \dots, i_s\}$. Указанное число s существует из-за конечности множества M, а значит, и множества $\operatorname{supp}(\pi)$. Несложно заметить, что $i_s\pi = i_1$, поскольку элементы $i_2, \dots, i_s$ уже имеют прообразы $i_1, \dots, i_{s-1}$. Множество $\{i_1, i_2, \dots, i_s\}$ называется *нетривиальной орбитой* подстановки π длины s (*тривиальная орбита* состоит из неподвижного элемента). Каждая нетривиальная орбита имеет циклическое строение: все символы, входящие в орбиту, могут быть получены из произвольного символа орбиты путём последовательного действия подстановкой π. Следовательно, две орбиты подстановки либо не пересекаются, либо совпадают, и каждый символ из M принадлежит некоторой орбите (тривиальной или нетривиальной). Таким образом, множество M относительно подстановки π распадается в объединение непересекающихся орбит, а носитель $\operatorname{supp}(\pi)$ — объединение непересекающихся нетривиальных орбит.

Пример. Пусть

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

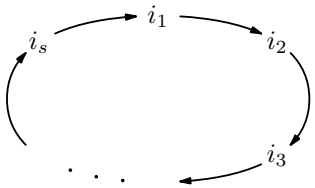
Тогда $\{1,6,4\}$, $\{2,3\}$, $\{5\}$ — орбиты подстановки π на множестве M, первые две из них нетривиальны. Имеем $M = \{1,6,4\} \cup \{2,3\} \cup \{5\}$ и $\operatorname{supp}(\pi) = \{1,6,4\} \cup \{2,3\}$.

В соответствие с разбиением множества $\operatorname{supp}(\pi)$ в объединение непересекающихся орбит существует удобная форма представления подстановки в виде произведения независимых циклов, которую мы сейчас и рассмотрим.

Определение 2.2.3. Подстановка $\pi \in S_n$ вида

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{s-1} & i_s & k_1 & \dots & k_t \\ i_2 & i_3 & \dots & i_s & i_1 & k_1 & \dots & k_t \end{pmatrix},$$

где $\{i_1, i_2, \dots, i_s, k_1, \dots, k_t\} = \{1, 2, \dots, n\}$ и $s \geqslant 2$, называется *циклом длины* s и обозначается $(i_1, i_2, \dots, i_s)$.



Иными словами, подстановка является циклом тогда и только тогда, когда её носитель состоит ровно из одной нетривиальной орбиты.

Примеры. 1. Подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1,2,4) = (2,4,1) = (4,1,2) —$$

цикл длины 3.

2. Подстановка $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ циклом не является.

Предложение 2.2.2. *Порядок $|\alpha|$ цикла α длины s (как элемента группы S_n) равен s.*

Доказательство. Пусть $\alpha = (i_1, i_2, \dots, i_s)$. Наименьшее натуральное число k такое, что $i_1\pi^k = i_1$, равно s. Но тогда $i_l\pi^s = i_l$ для любого $l = 1, 2, \dots, s$. □

Определение 2.2.4. Циклы α и β из S_n называются независимыми, если $\operatorname{supp}(\alpha) \cap \operatorname{supp}(\beta) = \varnothing$.

Предложение 2.2.3. *Если циклы α и β независимы, то $\alpha\beta = \beta\alpha$.*

Доказательство. Пусть i — произвольный символ из M. Разберём последовательно три возможных случая.

1. $i \notin \operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$. Тогда $i\alpha\beta = i = i\beta\alpha$.
2. $i \in \operatorname{supp}(\alpha)$. Тогда $i\alpha\beta = i\alpha = i\beta\alpha$.
3. $i \in \operatorname{supp}(\beta)$. Тогда $i\alpha\beta = i\beta = i\beta\alpha$. □

Следствие. *Если $\alpha_1, \alpha_2 \ldots, \alpha_k$ — попарно независимые циклы, то порядок подстановки $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_k$ равен наименьшему общему кратному длин циклов $\alpha_1, \alpha_2 \ldots, \alpha_k$.*

Упражнение 2.2.3. *Доказать следствие из предложения* 2.2.3.

Теорема 2.2.2. *Пусть π — нетождественная подстановка из S_n. Тогда $\pi = \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_k$ есть произведение попарно независимых циклов $\sigma_1, \sigma_2, \ldots, \sigma_k$. Это разложение единственно с точностью до порядка сомножителей.*

Доказательство. Проведём доказательство индукцией по числу нетривиальных орбит, на которые множество $M = \{1, 2, \ldots, n\}$ распадается под действием подстановки π. Поскольку π не тождественна, по крайней мере одна такая орбита $\{i_1, i_2, \ldots, i_s\}$ существует. Пусть $\sigma_1 = (i_1, i_2, \ldots, i_s)$ — соответствующий этой орбите цикл. Если других нетривиальных орбит нет, то $\pi = \sigma_1$ — цикл, и теорема доказана. Предположим, что $\operatorname{supp}(\sigma_1) \subset \operatorname{supp}(\pi)$, и рассмотрим подстановку $\pi_1 = \sigma_1^{-1}\pi$. Если $i \in \operatorname{supp}(\sigma_1)$, т. е. $i = i_l$ для некоторого $l \in \{1, 2, \ldots, s\}$, то $i\pi_1 = i_l\pi_1 = i_l(\sigma_1^{-1}\pi) = (i_l\sigma_1^{-1})\pi = i_{l-1}\pi = i_l = i$. Поэтому все символы из $\operatorname{supp}(\sigma_1)$ неподвижны относительно действия подстановки π_1. С другой стороны, если $i \notin \operatorname{supp}(\sigma_1)$, то $i\pi_1 = i(\sigma_1^{-1}\pi) = (i\sigma_1^{-1})\pi = i\pi$. Иными словами, на всех остальных символах действие подстановки π_1 совпадает с действием подстановки π. Таким образом, подстановка π_1 имеет носитель $\operatorname{supp}(\pi_1) = \operatorname{supp}(\pi) \setminus \operatorname{supp}(\sigma_1)$, и он распадается на единицу меньшее число нетривиальных орбит, чем носитель $\operatorname{supp}(\pi)$ исходной подстановки. Следовательно, по предположению индукции $\pi_1 = \sigma_2 \cdot \ldots \cdot \sigma_k$ есть произведение независимых циклов $\sigma_2, \ldots, \sigma_k$, причём это разложение единственно с точностью до порядка сомножителей. Поскольку $\pi = \sigma_1\pi_1$ и $\operatorname{supp}(\sigma_1) \cap \operatorname{supp}(\pi_1) = \varnothing$, разложение $\pi = \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_k$ является искомым.

Предположим, что $\pi = \tau_1\tau_2 \cdot \ldots \cdot \tau_m$ — другое разложение π в произведение независимых циклов. Поскольку $i_1 \in \operatorname{supp}(\pi)$, найдётся цикл τ_l из этого разложения такой, что $i_1 \in \operatorname{supp}(\tau_l)$. Так как циклы $\tau_1, \tau_2, \ldots, \tau_m$ независимы, то они перестановочны, и можно считать, что $i_1 \in \operatorname{supp}(\tau_1)$.

Тогда $i_1\tau_1 = i_1\pi = i_1\sigma_1 = i_2$, $i_2\tau_1 = i_2\pi = i\sigma_1 = i_3, \ldots, i_s\tau_1 = i_s\pi = i_s\sigma_1 = i_1$. Отсюда $\tau_1 = \sigma_1$ и $\pi = \tau_1\pi_1 = \sigma_1\pi_1$, а однозначность разложения π_1 вытекает из предположения индукции. □

Замечание. Иногда удобно считать, что неподвижный символ i относительно подстановки π образует цикл единичной длины, и записывать этот цикл как (i).

Пример. Для подстановки

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

имеет место разложение $\pi = (1, 6, 4)(2, 3)$ или, если необходимо упомянуть неподвижные символы, $\pi = (1, 6, 4)(2, 3)(5)$.

Таким образом, имеется взаимно однозначное соответствие между орбитами, на которые разбивается множество M относительно подстановки π, и циклами, в произведение которых π раскладывается. Причём это верно как в случае, когда мы учитываем только нетривиальные орбиты и неединичные циклы, так и в общем случае.

Имеется ещё один существенный для нас способ разложить подстановку в произведение циклов специального вида, так называемых *транспозиций*.

Определение 2.2.5. Цикл длины 2 называется *транспозицией*.

Предложение 2.2.4. *Каждая подстановка $\pi \in S_n$ раскладывается в произведение транспозиций.*

Доказательство. В силу теоремы 2.2.2 достаточно представить в виде произведения транспозиций произвольный цикл. Пусть $\sigma = (i_1, i_2, \ldots, i_s)$ — цикл длины s. Непосредственно проверяется, что $\sigma = (i_1, i_2)(i_1, i_3) \cdot \ldots \cdot (i_1, i_s)$ — искомое разложение. □

Представление произвольной подстановки в виде произведения транспозиций в отличие от её представления в виде произведения независимых циклов уже не является однозначным. В частности, число транспозиций в различных разложениях одной и той же подстановки может быть различным.

Пример. $(1, 2)(1, 3)(1, 2) = (2, 3)$.

Тем не менее чётность этого числа не зависит от способа разложения. Доказательству этого важного факта мы и посвятим остаток параграфа.

Определение 2.2.6. Пусть подстановка $\pi \in S_n$, множество $\mathrm{supp}(\pi)$ перемещаемых символов которой состоит из m элементов, раскладывается в произведение k независимых циклов. *Декрементом* $d(\pi)$ подстановки π называется разность $m - k$. *Знаком* подстановки π называется число $\mathrm{sgn}(\pi) = (-1)^{d(\pi)}$. Подстановка называется *чётной*, если $\mathrm{sgn}(\pi) = 1$, и нечётной, если $\mathrm{sgn}(\pi) = -1$.

Пример. Для подстановки π из предыдущего примера имеем $d(\pi) = 5 - 2 = 3$, $\mathrm{sgn}(\pi) = (-1)^3 = -1$, т. е. подстановка π нечётна.

Замечание. Декремент подстановки π множества M можно также определить как разность между общим числом символов в M и общим числом циклов (включая единичные).

Теорема 2.2.3. *Умножение на транспозицию меняет знак подстановки на противоположный.*

Доказательство. Пусть π — подстановка, а $\tau = (i, j)$ — транспозиция из S_n. На самом деле, мы докажем более сильное утверждение, чем в формулировке теоремы. А именно, покажем, что $d(\pi\tau) = d(\pi) \pm 1$. Пусть $\pi = \sigma_1\sigma_2 \cdot \ldots \sigma_k$ — разложение подстановки в произведение циклов (в том числе и единичных). Для удобства договоримся считать, что $\mathrm{supp}(\sigma) = \{i\}$ в случае единичного цикла $\sigma = (i)$. Символы i и j, перемещаемые транспозицией τ, либо лежат в одной орбите относительно действия π, либо в двух разных орбитах. Разберём обе эти возможности.

Пусть сначала i, j лежат в одной орбите $\{k_1, k_2, \ldots, k_s\}$, т. е. найдётся цикл $\sigma = (k_1, k_2, \ldots, k_s)$ в разложении π на независимые циклы такой, что $i, j \in \mathrm{supp}(\sigma)$. Пусть для определённости $i = k_1, j = k_m$ (напомним, что цикл можно начинать с любого символа). Тогда непосредственно проверяется, что $(k_1, \ldots, k_m, \ldots, k_s)(i, j) = (k_1, \ldots, k_{m-1})(k_m, \ldots, k_s)$. Таким образом, в разложении подстановки вместо одного из независимых циклов появляются два новых независимых цикла (циклы, носитель которых не содержит i, j, очевидно, не изменятся). Следовательно, в этом случае $d(\pi\tau) = d(\pi) - 1$.

Пусть теперь i лежит в орбите $\{i_1, i_2, \ldots, i_s\}$ и $i = i_1$, а j лежит в орбите $\{j_1, j_2, \ldots, j_t\}$ и $j = j_1$ (подчеркнём, что орбиты могут в этом случае быть и тривиальными). Этим орбитам в разложении π соответствуют независимые циклы $(i_1, i_2, \ldots, i_s)$ и $(j_1, j_2, \ldots, j_t)$. Равенство $(i_1, i_2, \ldots, i_s)(j_1, j_2, \ldots, j_t)(i, j) = (i_1, i_2, \ldots, i_s, j_1, \ldots, j_t)$ показывает, что в рассматриваемом нами случае два независимых цикла в разложении π превращаются в один цикл в разложении $\pi\tau$. Таким образом, $d(\pi\tau) = d(\pi) + 1$. □

Замечание. При доказательстве теоремы мы умножали подстановку на транспозицию справа. Несложно понять, что аналогичные рассуждения проходят при умножении на транспозицию слева.

Следствие 1. *Чётность числа транспозиций, в произведение которых раскладывается подстановка π, не зависит от способа разложения и совпадает с чётностью декремента $d(\pi)$.*

Доказательство. Начнём с того, что декремент тождественной подстановки ε равен нулю, а значит, $\operatorname{sgn}(\varepsilon) = 1$. Пусть $\pi = \tau_1\tau_2\cdot\ldots\cdot\tau_k$ — произвольное разложение подстановки π в произведение транспозиций. По теореме 2.2.3 имеем $\operatorname{sgn}(\tau_1) = \operatorname{sgn}(\varepsilon\tau_1) = (-1)^1$. Аналогично, $\operatorname{sgn}(\tau_1\tau_2) = (-1)^2$ и т. д. Таким образом, $\operatorname{sgn}(\pi) = (-1)^{d(\pi)} = (-1)^k$. □

Упражнение 2.2.4. *Доказать, что наименьшее возможное число транспозиций, в произведение которых можно разложить произвольную подстановку π, равно её декременту $d(\pi)$.*

Отметим ещё одно полезное следствие из только что доказанной теоремы.

Следствие 2. *Пусть π, σ — произвольные подстановки из S_n. Тогда* $\operatorname{sgn}(\pi\tau) = \operatorname{sgn}(\pi)\operatorname{sgn}(\tau)$.

Упражнение 2.2.5. *Доказать следствие* 2 *из теоремы* 2.2.3.

Упражнение 2.2.6. *Докажите, что число чётных подстановок множества M равно числу нечётных подстановок того же множества. Докажите, что подмножество всех чётных подстановок A_n из группы S_n является подгруппой в S_n. Группа A_n называется знакопеременной группой подстановок. Докажите, что при $n \geqslant 3$ каждый элемент из группы A_n раскладывается в произведение циклов длины* 3.

Упражнение 2.2.7.* *Докажите, что каждый элемент из S_n представим в виде произведения двух элементов порядка* 2.

§ 2.3. Кольцо квадратных матриц

Определение 2.3.1. Пусть задано непустое множество S. *Матрицей* над S размера m на n (или $(m \times n)$-матрицей) называется прямо-

угольная таблица вида

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

где $a_{ij} \in S$, $i \in \{1, 2, \dots, m\}$ — номер строки, $j \in \{1, 2, \dots, n\}$ — номер столбца таблицы. В случае, когда число строк матрицы совпадает с числом столбцов, т. е. $m = n$, будем называть матрицу *квадратной*, а число n *размерностью* матрицы. Множество всех матриц размера m на n над S обозначается через $M_{m\times n}(S)$, а множество всех квадратных $(n \times n)$-матриц — через $M_n(S)$.

Мы будем обозначать матрицу заглавной буквой и использовать ту же строчную букву для обозначения её элементов. Например, будем писать $A = (a_{ij})$ или $A = (a_{ij})_{m\times n}$, если хотим подчеркнуть её размер. Две матрицы A и B *равны*, если они имеют один и тот же размер и их элементы, стоящие на одних и тех же местах, равны: если $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$, то $A = B \Leftrightarrow a_{ij} = b_{ij}\ \forall i = 1 \dots m, \forall j = 1 \dots n$.

Примеры.

1. $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ — матрица размера 2×3 над множеством $\{1\}$.
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ — матрица размера 1×5 над множеством $\mathbb{N}$.
3. $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$ — матрица размера 4×1 над множеством $\mathbb{N}$.

Иногда мы будем называть матрицы размера $1 \times n$ *строками* длины n, а матрицы размера $m\times 1$ *столбцами* высоты m. В этой терминологии матрица из примера 2 — строка длины 5, а матрица из примера 3 — столбец высоты 4.

Замечание. Назвав матрицу прямоугольной таблицей, мы, конечно, пожертвовали математической строгостью в угоду интуитивной ясности. Недостаток строгости в определении матрицы можно исправить следующим образом. Очевидно, что множество всех строк длины n над множеством S может быть отождествлено с множеством всех упорядоченных n-ок элементов из S, т. е. с декартовой n-ой степенью S^n множества S. Тогда множество $M_{m\times n}(S)$ всех матриц размера m на n над S

можно рассматривать как множество всех упорядоченных m-ок, элементами которых являются упорядоченные n-ки элементов из S, или, иными словами, как декартову m-ую степень $(S^n)^m$ множества S^n. Ещё один вариант состоит в том, чтобы дать определение матрицы на языке отображений. Пусть $I = \{(i,j) \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$. Произвольная матрица $A = (a_{ij})$ из множества $M_{m\times n}(S)$ может быть определена как отображение из множества I в множество S, сопоставляющее каждой паре индексов (i,j) элемент $a_{ij} \in S$, а само множество $M_{m\times n}(S)$ — как множество всех таких отображений.

Пусть на множестве S задана операция сложения $+$. Тогда матрицы одного и того же размера будем складывать по следующему правилу:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ \dots & \dots & \dots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & \dots & a_{2n}+b_{2n} \\ \dots & \dots & \dots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}.$$

Точнее,

Определение 2.3.2. Пусть $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$ — матрицы одного и того же размера над множеством S с операцией сложения. *Суммой* матриц A и B называется матрица $C = (c_{ij})_{m\times n} = A + B$ над S того же размера, для которой $c_{ij} = a_{ij} + b_{ij}$.

Если на S помимо ассоциативной и коммутативной операции сложения задана операция умножения, то на матрицах согласованных размеров можно определить операцию умножения следующим образом.

Определение 2.3.3. Пусть $A = (a_{ik})_{m\times s}$ и $B = (b_{kj})_{s\times n}$ — две матрицы над S такие, что число столбцов первой матрицы равно числу строк второй матрицы. Пусть на S заданы операции сложения и умножения. *Произведением* матриц A и B называется матрица $C = (c_{ij})_{m\times n} = AB$ над S размера m на n, для которой

$$c_{ij} = \sum_{k=1}^{s} a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{is}b_{sj}.$$

Иными словами, чтобы получить элемент, стоящий в i-ой строке и j-ом столбце произведения двух матриц, нужно элементы i-ой строки первой матрицы умножить на соответствующие элементы j-ого столбца второй матрицы и полученные произведения сложить.

Пример. Пусть $S = \mathbb{Z}$ — кольцо целых чисел.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 1\cdot 0 + 2\cdot 2 + 3\cdot 4 & 1\cdot 1 + 2\cdot 3 + 3\cdot 5 \\ 4\cdot 0 + 5\cdot 2 + 0\cdot 4 & 4\cdot 1 + 5\cdot 3 + 0\cdot 5 \end{pmatrix} = \begin{pmatrix} 16 & 22 \\ 10 & 19 \end{pmatrix}.$$

Заметим, что если A и B — квадратные матрицы одной и той же размерности, то их можно и складывать, и умножать.

Теорема 2.3.1. *Пусть $\langle R, +, \cdot\rangle$ — кольцо, n — произвольное натуральное число. Тогда $M_n(R)$ — кольцо относительно операций сложения и умножения матриц.*

Доказательство. Мы разобьём доказательство теоремы на ряд последовательных лемм, в каждой из которых будет рассматриваться ситуация несколько более общая, чем в формулировке самой теоремы.

Лемма 1. *Если $\langle R, +\rangle$ — абелева группа, то $\langle M_{m\times n}(R), +\rangle$ — абелева группа.*

Доказательство. Пусть $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij}) \in M_{m\times n}(R)$. Поскольку R — кольцо, для всех i, j имеют место равенства $a_{ij} + b_{ij} = b_{ij} + a_{ij}$ и $(a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij})$. Следовательно, $A + B = B + A$ и $(A + B) + C = A + (B + C)$. Нейтральным по сложению элементом, очевидно, является матрица, каждый элемент которой — нуль кольца R. Кроме того, матрица $-A = (-a_{ij})$ является противоположным элементом к матрице $A = (a_{ij})$. Таким образом, $M_{m\times n}(R)$ — абелева группа относительно операции сложения. □

Лемма 2. *Пусть $A = (a_{ij})$, $B = (b_{ij}) \in M_{m\times s}(R)$ и $C = (c_{ij}) \in M_{s\times n}(R)$. Тогда $(A + B)C = AC + BC$.*

Доказательство. Пусть $D = (d_{ij}) = (A + B)C$, а $F = (f_{ij}) = AC + BC$. Для любых i, j имеем

$$d_{ij} = \sum_{k=1}^{n} (a_{ik} + b_{ik})c_{kj} = \sum_{k=1}^{n} (a_{ik}c_{kj} + b_{ik}c_{kj}) = \sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj} = f_{kj}.$$

Следовательно, $D = F$ и правая дистрибутивность доказана. □

Закон левой дистрибутивности $A(B + C) = AB + AC$ для матриц соответствующих размеров, в том числе квадратных, проверяется аналогично.

Нам осталось проверить аксиому ассоциативности умножения матриц. Сформулируем сначала некоторое вспомогательное утверждение о перемене порядка суммирования, так называемую *лемму бухгалтера*.

Предложение 2.3.1 (лемма бухгалтера)**.** *Пусть* $\langle S, + \rangle$ *— коммутативная полугруппа и* $X = (x_{ij})_{m \times n}$ *— матрица над* S*. Тогда*

$$\sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} = \sum_{j=1}^{n} \sum_{i=1}^{m} x_{ij}.$$

Доказательство. Поскольку операция сложения на S коммутативна и ассоциативна, элементы матрицы можно складывать в любом порядке. Осталось заметить, что в левой и правой части доказываемого равенства стоит сумма всех элементов матрицы X. □

Лемма 3. *Если* $A = (a_{ij}) \in M_{m \times s}(R)$*,* $B = (b_{ij}) \in M_{s \times t}(R)$ *и* $C = (c_{ij}) \in M_{t \times n}(R)$*, то* $(AB)C = A(BC)$*.*

Доказательство. Пусть $D = AB$, $F = BC$ и $G = (AB)C = DC$, $H = A(BC) = AF$. Нам надо доказать, что $G = H$. Заметим, во-первых, что G и H — матрицы одного и того же размера m на n. Кроме того, $\forall i \in \{1 \dots m\}, \forall j \in \{1 \dots n\}$ выполняется

$$g_{ij} = \sum_{k=1}^{t} d_{ik} c_{kj} = \sum_{k=1}^{t} \left(\sum_{l=1}^{s} a_{il} b_{lk} \right) c_{kj} = \sum_{k=1}^{t} \sum_{l=1}^{s} (a_{il} b_{lk}) c_{kj} =$$

$$= \sum_{l=1}^{s} \sum_{k=1}^{t} a_{il} (b_{lk} c_{kj}) = \sum_{l=1}^{s} a_{il} \left(\sum_{k=1}^{t} (b_{lk} c_{kj}) \right) = \sum_{l=1}^{s} a_{il} f_{lj} = h_{ij}.$$

□

Поскольку утверждения лемм 1–3 верны, в частности, для квадратных матриц, алгебраическая система $M_n(R)$ — кольцо. Теорема доказана. □

Рассмотрим теперь вопрос о том, переносятся ли остальные свойства умножения с кольца R (если R ими обладает) на кольцо $M_n(R)$. Во-первых, если $n = 1$, то отображение $\varphi : R \to M_1(R)$, действующее по правилу $a\varphi = (a)_{1 \times 1}$, очевидно, является изоморфизмом. Поэтому любое алгебраическое свойство кольца R выполняется и для $M_1(R)$. В частности, если R — поле, то $M_1(R)$ тоже является полем.

Во-вторых, если R — кольцо с единицей, то $M_n(R)$ — кольцо с единицей для любого $n \in \mathbb{N}$. Действительно, матрица

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

у которой $e_{ij} = 1$ при $i = j$ и $e_{ij} = 0$ в остальных случаях, является, как несложно проверить непосредственно, единицей кольца $M_n(R)$. Мы будем называть E *единичной матрицей*.

С другой стороны, если $n > 1$, то свойства коммутативности умножения и существования обратного элемента не переносятся с R на $M_n(R)$. Пусть, например, F — произвольное поле, 0 и 1 – его нейтральные элементы по сложению и умножению соответственно. Рассмотрим матрицы из $M_2(F)$

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ и } B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Имеем

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = BA.$$

Следовательно, кольцо $M_2(F)$ некоммутативно. Кроме того, поскольку

$$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0,$$

матрица A не имеет обратной. Действительно, если бы существовала матрица A^{-1} такая, что $A^{-1}A = E$, то, умножая равенство $A^2 = 0$ слева на A^{-1}, мы бы получили неверное равенство $A = 0$.

В дальнейшем предполагается, что множество F, над которым задана матрица, является полем относительно операций сложения и умножения. Мы будем называть поле F *полем определения* матрицы, а его элементы *скалярами*.

Как и в случае с подстановками, мы научимся представлять каждую квадратную матрицу в виде произведения матриц специального (и достаточно простого) вида.

Определение 2.3.4. *Диагональная матрица* $D(\alpha_1, \alpha_2, \ldots, \alpha_n)$ — это квадратная матрица вида

$$D = (d_{ij})_{n\times n} = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix},$$

где $d_{ii} = \alpha_i$ и $d_{ij} = 0$ при $i \neq j$. Диагональная матрица $D(\alpha_1, \alpha_2, \ldots, \alpha_n)$ называется *скалярной*, если $\alpha_1 = \alpha_2 = \ldots = \alpha_n = \alpha$.

В частности, единичная и нулевая матрицы являются диагональными и даже скалярными: $E = D(1, 1, \ldots, 1)$, $0 = D(0, 0, \ldots, 0)$.

Совокупность элементов $\{a_{ii} \mid i = 1, \dots, n\}$ квадратной матрицы $A = (a_{ij})_{n\times n}$, стоящих на пересечении строк и столбцов с одинаковыми номерами, принято называть *главной диагональю* матрицы A. Используя этот термин, можно определить диагональную матрицу как квадратную матрицу, все элементы которой вне главной диагонали равны 0.

Посмотрим, что произойдёт с произвольной матрицей $A = (a_{ij}) \in M_{m\times n}(F)$ при умножении её слева (а потом справа) на некоторую диагональную матрицу D.

$$D(\alpha_1, \alpha_2, \dots, \alpha_m)\cdot A = \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_m \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1 a_{11} & \alpha_1 a_{12} & \dots & \alpha_1 a_{1n} \\ \alpha_2 a_{21} & \alpha_2 a_{22} & \dots & \alpha_2 a_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_n a_{m1} & \alpha_n a_{m2} & \dots & \alpha_n a_{mn} \end{pmatrix} = (\alpha_i a_{ij})_{m\times n}.$$

Таким образом, *при умножении матрицы $A = (a_{ij})_{m\times n}$ слева на диагональную матрицу $D(\alpha_1, \alpha_2, \dots, \alpha_m)$ все элементы i-ой строки матрицы A умножаются на α_i для каждого $i = 1, \dots, m$.*

С другой стороны,

$$A \cdot D(\alpha_1, \alpha_2, \dots, \alpha_n) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_n \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1 a_{11} & \alpha_2 a_{12} & \dots & \alpha_n a_{1n} \\ \alpha_1 a_{21} & \alpha_2 a_{22} & \dots & \alpha_n a_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_1 a_{m1} & \alpha_2 a_{m2} & \dots & \alpha_n a_{mn} \end{pmatrix} = (\alpha_j a_{ij})_{m\times n},$$

т. е. *при умножении матрицы $A = (a_{ij})_{m\times n}$ справа на диагональную матрицу $D(\alpha_1, \alpha_2, \dots, \alpha_n)$ все элементы j-ого столбца матрицы A умножаются на α_j для каждого $j = 1, \dots, n$.*

Упражнение 2.3.1. *Докажите, что для любых двух диагональных матриц $D_1, D_2 \in M_n(F)$ матрица D_1D_2 является диагональной и имеет место равенство $D_1D_2 = D_2D_1$.*

Если диагональная матрица является скалярной $D = D(\alpha, \alpha, \ldots, \alpha)$, то для любой квадратной матрицы $A = (a_{ij})$ имеет место равенство $DA = AD = (\alpha a_{ij})$. Иными словами, при умножении на скалярную матрицу (с любой стороны) все элементы матрицы A умножаются на скаляр α. Мы будем записывать матрицу, которая получилась в результате, как αA. В частности, саму скалярную матрицу $D(\alpha, \alpha, \ldots, \alpha)$ можно записать как αE, где E — единичная матрица соответствующего размера.

Упражнение 2.3.2. *Докажите, что множество всех скалярных матриц из $M_n(F)$ является полем относительно сложения и умножения матриц, а отображение φ из F на множество всех скалярных матриц из $M_n(F)$, действующее по правилу $\alpha\varphi = \alpha E$, является изоморфизмом полей.*

Упражнение 2.3.3. *Докажите, что матрица $A \in M_n(F)$ перестановочна (коммутирует) по умножению со всеми матрицами из $M_n(F)$ тогда и только тогда, когда A — скалярная матрица.*

Определение 2.3.5. *Клеточно диагональная матрица A* — это квадратная матрица размера $n \times n$ вида

$$\begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix},$$

где для каждого $i = 1, \ldots, s$ матрица A_i — квадратная матрица размера $n_i \times n_i$, $\sum_{i=1}^{s} n_i = n$, объединение главных диагоналей матриц A_i является главной диагональю матрицы A и все элементы матрицы A, не попавшие ни в одну матрицу A_i, равны 0.

Предложение 2.3.2. *Пусть*

$$A = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix} \text{ и } B = \begin{pmatrix} B_1 & & & 0 \\ & B_2 & & \\ & & \ddots & \\ 0 & & & B_s \end{pmatrix} —$$

две клеточно диагональные матрицы, причём размеры клеток A_i и B_i

совпадают для каждого $i = 1, \dots, s$. *Тогда их произведение*

$$AB = \begin{pmatrix} A_1B_1 & & & 0 \\ & A_2B_2 & & \\ & & \ddots & \\ 0 & & & A_sB_s \end{pmatrix}.$$

Упражнение 2.3.4. *Докажите предложение* 2.3.2.

Определение 2.3.6. Пусть $\alpha \in F$, r и s — два числа из множества $\{1, 2, \dots, n\}$, причём $r \neq s$. *Элементарная матрица* $E_{rs}(\alpha)$ — это квадратная матрица вида

$$E_{rs}(\alpha) = (t_{ij})_{n\times n} = \begin{array}{c} \\ \\ r - \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & & s & & \\ & & & & | & & \end{array} \\ \begin{pmatrix} 1 & & & & \vdots & & \\ & \ddots & & & \vdots & & \\ \cdots\cdots & 1 & \cdots & \alpha & \cdots\cdots & & \\ & & \ddots & \vdots & & & \\ & & & 1 & & & \\ & & & \vdots & \ddots & & \\ & & & \vdots & & 1 & \end{pmatrix} \end{array},$$

где $t_{rs} = \alpha$, $t_{ii} = 1$ и $t_{ij} = 0$ в остальных случаях. Элементарные матрицы называют также *трансвекциями*.

Заметим, что единичную матрицу можно считать элементарной, поскольку $E = E_{rs}(0)$.

Посмотрим теперь, что происходит с произвольной матрицей A при

её умножении на элементарную матрицу. Имеем

$$E_{rs}(\alpha)A = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & \alpha & & & \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & \dots & \dots & \\ a_{r1} & a_{r2} & \dots & a_{rn} \\ & \dots & \dots & \\ a_{s1} & a_{s2} & \dots & a_{sn} \\ & \dots & \dots & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ & \dots & \dots & \\ a_{r1} + \alpha a_{s1} & a_{r2} + \alpha a_{s2} & \dots & a_{rn} + \alpha a_{sn} \\ & \dots & \dots & \\ a_{s1} & a_{s2} & \dots & a_{sn} \\ & \dots & \dots & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Таким образом, *при умножении матрицы A слева на элементарную матрицу $E_{rs}(\alpha)$ к r-ой строке матрицы A прибавляется s-ая строка, умноженная на α.*

С другой стороны,

$$AE_{rs}(\alpha) = \begin{pmatrix} a_{11} & \dots & a_{1r} & \dots & a_{1s} & \dots & a_{1n} \\ a_{21} & \dots & a_{2r} & \dots & a_{2s} & \dots & a_{2n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1} & \dots & a_{mr} & \dots & a_{ms} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} 1 & & & & & \\ & \ddots & \alpha & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & \dots & a_{1r} & \dots & a_{1s} + \alpha a_{1r} & \dots & a_{1n} \\ a_{21} & \dots & a_{2r} & \dots & a_{2s} + \alpha a_{2r} & \dots & a_{2n} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1} & \dots & a_{mr} & \dots & a_{ms} + \alpha a_{mr} & \dots & a_{mn} \end{pmatrix}.$$

Иными словами, *при умножении матрицы A справа на элементарную матрицу $E_{rs}(\alpha)$ к s-ому столбцу матрицы A прибавляется r-й столбец, умноженный на α.*

Предложение 2.3.3. *Матрица $E_{rs}(-\alpha)$ является обратным элементом по умножению к матрице $E_{rs}(\alpha)$, т. е. $E_{rs}(\alpha) \cdot E_{rs}(-\alpha) = E$.*

Упражнение 2.3.5. *Докажите предложение* 2.3.3.

Преобразования строк и столбцов матрицы, описанные выше, при которых к одной из строк (одному из столбцов) матрицы прибавляется другая строка (другой столбец), умноженная на некоторый скаляр из поля определения, принято называть *элементарными преобразованиями*. Таким образом, элементарным преобразованиям строк соответствует умножение слева на элементарную матрицу, а элементарным преобразованиям столбцов — умножение справа на элементарную матрицу.

Теорема 2.3.2. *Пусть $A \in M_n(F)$ — квадратная матрица над полем F. Тогда найдутся элементарные матрицы $E_1, \dots, E_k$, $E_{k+1}, \dots, E_s \in M_n(F)$ и диагональная матрица $D \in M_n(F)$ такие, что $A = E_1 \dots E_k D E_{k+1} \dots E_s$.*

Доказательство. Проведём доказательство индукцией по размерности n матрицы A.

При $n = 1$ имеем $A = (a_{11}) = D(a_{11})$ и утверждение доказано.

Предположим, что утверждение теоремы верно для любой матрицы $\widetilde{A} \in M_{n-1}(F)$, и докажем его для матрицы $A \in M_n(F)$. Разобьём доказательство на три этапа.

Этап 1.

$$A = \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1,n-1} & 0 \\ \dots & \dots & \dots & \vdots \\ a_{n-1,1} & \dots & a_{n-1,n-1} & 0 \\ \hline 0 & \dots & 0 & a_{nn} \end{array}\right) = \left(\begin{array}{ccc|c} & & & 0 \\ & \widetilde{A} & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & a_{nn} \end{array}\right).$$

Заметим, что матрица

$$\widetilde{A} = \begin{pmatrix} a_{11} & \dots & a_{1,n-1} \\ \dots & \dots & \dots \\ a_{n-1,1} & \dots & a_{n-1,n-1} \end{pmatrix}$$

лежит в $M_{n-1}(F)$. Следовательно, по предположению индукции найдутся элементарные матрицы $\widetilde{E}_1, \dots, \widetilde{E}_k, \widetilde{E}_{k+1}, \dots, \widetilde{E}_s \in M_{n-1}(F)$ и диагональная матрица $\widetilde{D} \in M_{n-1}(F)$ такие, что $\widetilde{A} = \widetilde{E}_1 \dots \widetilde{E}_k \widetilde{D} \widetilde{E}_{k+1} \dots \widetilde{E}_s$.

Пусть для каждого $i = 1, \dots, s$

$$E_i = \left(\begin{array}{ccc|c} & \widetilde{E}_i & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & 1 \end{array}\right) \text{ и } D = \left(\begin{array}{ccc|c} & \widetilde{D} & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & a_{nn} \end{array}\right).$$

Тогда матрицы E_i — элементарные матрицы, а D — диагональная матрица из $M_n(F)$. В силу предложения 2.3.2 имеем $E_1 \dots E_k D E_{k+1} \dots E_s =$

$$= \left(\begin{array}{ccc|c} & \widetilde{E}_1 \dots \widetilde{E}_k \widetilde{D} \widetilde{E}_{k+1} \dots \widetilde{E}_s & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & a_{nn} \end{array}\right) = \left(\begin{array}{ccc|c} & \widetilde{A} & & \begin{matrix}0\\ \vdots \\ 0\end{matrix} \\ \hline 0 & \dots & 0 & a_{nn} \end{array}\right) = A.$$

Первый этап доказательства завершен. Отметим, что на этом этапе мы не делали никаких предположений относительно элемента a_{nn} матрицы A, в частности, могло оказаться, что $a_{nn} = 0$.

Этап 2. На этом этапе A — произвольная матрица из $M_n(F)$ с единственным условием $a_{nn} \neq 0$. Пусть матрица $\widetilde{A} \in M_{n-1}(F)$ такова, что

$$A = \left(\begin{array}{ccc|c} & & & a_{1n} \\ & \widetilde{A} & & \vdots \\ & & & a_{n-1,n} \\ \hline a_{n1} & \dots & a_{n,n-1} & a_{nn} \end{array}\right).$$

Совершим элементарное преобразование матрицы A, прибавив к её первой строке последнюю, умноженную на $\alpha = -a_{1n}a_{nn}^{-1}$ (обратный элемент к a_{nn} существует, поскольку по нашему предположению $a_{nn} \neq 0$). Обозначим полученную в результате этого преобразования матрицу через A_1. Тогда $A_1 = E_{1n}(\alpha)A =$

$$= \left(\begin{array}{ccc|c} & & & 0 \\ & & & a_{2n} \\ & \widetilde{A}_1 & & \vdots \\ & & & a_{n-1,n} \\ \hline a_{n1} & \dots & a_{n,n-1} & a_{nn} \end{array}\right),$$

где $\widetilde{A}_1$ — некоторая матрица из $M_{n-1}(F)$. Отметим, что в матрице A_1 на месте $(1, n)$ стоит 0. В силу предложения 2.3.3 матрица

$A = E_{1n}(a_{1n}/a_{nn})A_1$, где $a_{1n}/a_{nn} = -\alpha = -(-a_{1n}a_{nn}^{-1})$. Если мы умножим матрицу A_1 слева на элементарную матрицу $E_{2n}(-a_{2n}/a_{nn})$, то в получившейся матрице A_2 на пересечении 2-ой строки и n-го столбца появится 0. Кроме того, $A = E_{1n}(a_{1n}/a_{nn})E_{2n}(a_{2n}/a_{nn})A_2$. Продолжая этот процесс, занулим все элементы последнего столбца матрицы A, кроме элемента a_{nn}. Проведя аналогичные преобразования со столбцами матрицы A, занулим все элементы последней строки матрицы A (за исключением a_{nn}). В результате получим, что $A = E_{1n}(a_{1n}/a_{nn})\dots$ $\dots E_{n-1,n}(a_{n-1,n}/a_{nn})BE_{n,n-1}(a_{n,n-1}/a_{nn})\dots E_{n1}(a_{n1}/a_{nn})$, где B — матрица вида, для которого мы уже провели доказательство на первом этапе. Заменив в нашем равенстве B на соответствующее ей разложение, получим искомое разложение для матрицы A. Этап 2 завершен.

Этап 3. Пусть теперь матрица $A \in M_n(F)$ произвольна. Если $a_{nn} \neq 0$, то мы действуем, как на втором этапе. Следовательно, можно полагать, что $a_{nn} = 0$. Если все элементы последней строки и последнего столбца матрицы A равны 0, то мы действуем, как на первом этапе доказательства. Значит, можно считать, что либо в последней строке, либо в последнем столбце найдётся элемент, отличный от нуля. Не теряя общности, можно считать, что $a_{1n} \neq 0$. Прибавим к последней строке матрицы A её первую строку, умножив A слева на элементарную матрицу $E_{n1}(1)$. В получившейся матрице $B = E_{n1}(1)A$ элемент, стоящий на месте (n, n), не равен 0. Поэтому для B существует разложение $B = E_1 \dots E_l D E_{l+1} \dots E_t$ в произведение элементарных и диагональной матрицы. Тогда $A = E_{n1}(-1)E_1 \dots E_l D E_{l+1} \dots E_t$ — искомое разложение для матрицы A, и теорема доказана. □

Упражнение 2.3.6. *Пользуясь методом, изложенным при доказательстве теоремы, разложите в произведение элементарных и диагональной матриц матрицу*

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & -1 \\ -2 & 1 & 0 \end{pmatrix}.$$

§ 2.4. Определитель

В этом параграфе мы продолжим заниматься квадратными матрицами, заданными над некоторым полем. Мы определим и изучим очень важную скалярную характеристику матрицы, которую называют *определителем* или *детерминантом* матрицы.

Определение 2.4.1. Пусть n — натуральное число, S_n — симметрическая группа подстановок множества $\{1, \ldots, n\}$, F — поле, $A = (a_{ij})_{n\times n}$ — квадратная матрица из $M_n(F)$. *Определителем* (или *детерминантом*) матрицы A называется элемент поля F, который обозначается $\det(A)$ или $|A|$ и определяется следующим образом:

$$\det(A) = \sum_{\sigma\in S_n} \operatorname{sgn}\sigma \cdot a_{11\sigma}a_{22\sigma}\ldots a_{nn\sigma}.$$

Замечание. В формуле определителя сумма берётся по всем подстановкам σ из S_n, а под $a_{ii\sigma}$ понимается элемент матрицы A, стоящий на пересечении i-ой строки и $(i\sigma)$-ого столбца, где $i\sigma$ — образ i под действием подстановки σ.

Примеры. 1. Пусть $n = 1$. Тогда $S_1 = \{\varepsilon\}$, $A = (a_{11})$ и $\det(A) = a_{11}$.

2. Пусть $n = 2$. Имеем $S_2 = \{\varepsilon, (1,2)\}$, где $\operatorname{sgn}\varepsilon = 1$ и $\operatorname{sgn}(1,2) = -1$. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Тогда

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Определитель (2×2)-матрицы возникает естественным образом в следующих ситуациях.

Пусть дана система

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1, \\ a_{21}x_1 + a_{22}x_2 = b_2 \end{cases}$$

из двух линейных уравнений с двумя неизвестными. Тогда она имеет единственное решение

$$x_1 = \frac{b_1a_{22} - b_2a_{12}}{a_{11}a_{22} - a_{12}a_{21}},\ x_2 = \frac{b_2a_{11} - b_1a_{21}}{a_{11}a_{22} - a_{12}a_{21}}$$

в том и только том случае, когда $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$. Заметим, что в случае, когда определитель равен 0, система может либо не иметь решения, либо иметь бесконечно много решений.

Геометрический пример. Пусть на плоскости задана прямоугольная система координат и векторы x и y имеют в этой системе координаты

(x_1, x_2) и (y_1, y_2) соответственно. Тогда площадь S параллелограмма, натянутого на векторы x и y, равна модулю определителя $\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}$. В частности, векторы x и y коллинеарны тогда и только тогда, когда этот определитель равен 0.

Упражнение 2.4.1. *Докажите утверждение о площади параллелограмма, сформулированное в предыдущем абзаце.*

3. Пусть $n = 3$. Тогда $S_n = \{\varepsilon, (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\}$, а $A_n = \{\varepsilon, (1,2,3), (1,3,2)\}$. Следовательно,

$$\text{если } A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \text{ то } \det(A) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} =$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}.$$

Оказывается, что выписанная выше формула вновь позволяет ответить на вопросы о существовании единственного решения системы линейных уравнений (трёх уравнений от трёх неизвестных), а также вычислить объём параллелепипеда и сформулировать критерий компланарности векторов в пространстве. Более того, и для системы из n линейных уравнений от n неизвестных критерий существования единственного решения выглядит, как в случаях $n = 1, 2, 3$, — решение единственно в том и только том случае, когда определитель так называемой матрицы коэффициентов системы не равен 0 (подробнее об этом в главе 4). И в пространствах размерности $n > 3$ имеет место формула *объёма* фигуры, натянутой на n векторов, а также критерий линейной зависимости n векторов. Мы вернёмся к вопросу о приложениях определителя позднее, а пока изучим его основные свойства.

Предложение 2.4.1. *Пусть $A = (a_{ij})$, $B = (b_{ij}) \in M_n(F)$, $\alpha \in F$, r — некоторое натуральное число из множества $\{1, 2, \ldots, n\}$. Пусть для каждого $j = 1, \ldots, n$ имеют место равенства $b_{rj} = \alpha a_{rj}$ и $b_{ij} = a_{ij}$ при $i \neq r$. Тогда $\det(B) = \alpha \det(A)$.*

Иными словами, *при умножении некоторой строки матрицы на скаляр α определитель полученной матрицы равен произведению определителя исходной матрицы на скаляр α.*

Доказательство. Требуемое вытекает из равенств $\det(B) = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma b_{11\sigma} \ldots b_{rr\sigma} \ldots b_{nn\sigma} = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma a_{11\sigma} \ldots (\alpha a_{rr\sigma}) \ldots a_{nn\sigma} = \alpha \sum_{\sigma \in S_n} \operatorname{sgn}\sigma a_{11\sigma} \ldots a_{rr\sigma} \ldots a_{nn\sigma} = \alpha \det(A)$. □

Следствие. *Если одна из строк матрицы A нулевая (все элементы этой строки равны 0), то* $\det(A) = 0$.

Упражнение 2.4.2. *Пусть $A \in M_n(F)$, $\alpha \in F$. Выразите* $\det(\alpha A)$ *через* $\det(A)$.

Предложение 2.4.2. *Пусть $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij}) \in M_n(F)$, r — некоторое натуральное число из множества $\{1, 2, \ldots, n\}$. Пусть для каждого $j = 1, \ldots, n$ имеют место равенства $c_{rj} = a_{rj} + b_{rj}$ и $c_{ij} = a_{ij} = b_{ij}$ при $i \neq r$. Тогда* $\det(C) = \det(A) + \det(B)$.

Иными словами, *если две матрицы различаются лишь по r-ой строке, то матрица, составленная из тех же строк, а также r-ой строки, равной сумме r-ых строк исходных матриц, имеет определитель, равный сумме определителей исходных матриц.*

Доказательство. Требуемое вытекает из равенств $\det(C) =$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}\sigma c_{11\sigma} \ldots c_{rr\sigma} \ldots c_{nn\sigma} = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma c_{11\sigma} \ldots (a_{rr\sigma} + b_{rr\sigma}) \ldots c_{nn\sigma} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}\sigma c_{11\sigma} \ldots a_{rr\sigma} \ldots c_{nn\sigma} + \sum_{\sigma \in S_n} \operatorname{sgn}\sigma c_{11\sigma} \ldots b_{rr\sigma} \ldots c_{nn\sigma} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}\sigma a_{11\sigma} \ldots a_{rr\sigma} \ldots a_{nn\sigma} + \sum_{\sigma \in S_n} \operatorname{sgn}\sigma b_{11\sigma} \ldots b_{rr\sigma} \ldots b_{nn\sigma} =$$

$$= \det(A) + \det(B). \qquad \square$$

Предложение 2.4.3. *Пусть $A = (a_{ij}) \in M_n(F)$, r, s — два различных натуральных числа из множества $\{1, 2, \ldots, n\}$. Если для каждого $j = 1, \ldots, n$ выполняются равенства $a_{rj} = a_{sj}$, то* $\det(A) = 0$.

Иными словами, *если в матрице две строки совпадают, то её определитель равен 0.*

Доказательство. Обозначим через τ транспозицию $(r, s) \in S_n$. В силу утверждения упражнения 2.1.1 отображение $\varphi_\tau : \sigma \mapsto \tau\sigma$ является биекцией множества S_n на себя. Поэтому если σ пробегает всё множество S_n, то и $\pi = \tau\sigma$ тоже пробегает всё S_n. С другой стороны, поскольку $\operatorname{sgn}\pi = \operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}\sigma$, когда σ пробегает множество всех чётных подстановок A_n, подстановка π пробегает множество всех нечётных подстановок $S_n \setminus A_n$. Поэтому

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma a_{11\sigma} \ldots a_{rr\sigma} \ldots a_{ss\sigma} \ldots a_{nn\sigma} =$$

$$= \sum_{\sigma \in A_n} a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - \sum_{\pi \in S_n \setminus A_n} a_{11\pi} \dots a_{rr\pi} \dots a_{ss\pi} \dots a_{nn\pi} =$$

$$= \sum_{\sigma \in A_n} a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - \sum_{\sigma \in A_n} a_{11\tau\sigma} \dots a_{rr\tau\sigma} \dots a_{ss\tau\sigma} \dots a_{nn\tau\sigma} =$$

$$= \sum_{\sigma \in A_n} (a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma} - a_{11\sigma} \dots a_{rr\sigma} \dots a_{ss\sigma} \dots a_{nn\sigma}) = 0.$$

□

Следствие. *Пусть* $A = (a_{ij})$, $B = (b_{ij}) \in M_n(F)$, r, s — *некоторые натуральные числа из множества* $\{1, 2, \dots, n\}$. *Пусть для каждого* $j = 1, \dots, n$ *имеют место равенства* $a_{rj} = b_{sj}$, $a_{sj} = b_{rj}$ *и* $a_{ij} = b_{ij}$ *при* $r \neq i \neq s$. *Тогда* $\det(A) + \det(B) = 0$.

Иными словами, *при перестановке местами двух строк матрицы её определитель меняет знак на противоположный.*

Доказательство. Используя предложения 2.4.2 и 2.4.3, получаем следующую цепочку равенств:

$$\begin{vmatrix} \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \end{vmatrix} + \begin{vmatrix} \vdots \\ \cdots\ b_{rj}\ \cdots \\ \vdots \\ \cdots\ b_{sj}\ \cdots \\ \vdots \end{vmatrix} = \begin{vmatrix} \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \end{vmatrix} + \begin{vmatrix} \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \end{vmatrix} =$$

$$= \begin{vmatrix} \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \end{vmatrix} + \begin{vmatrix} \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \end{vmatrix} + \begin{vmatrix} \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \end{vmatrix} + \begin{vmatrix} \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \end{vmatrix} =$$

$$= \begin{vmatrix} \vdots \\ \cdots\ a_{rj}\ \cdots \\ \vdots \\ \cdots\ a_{rj} + a_{sj}\ \cdots \\ \vdots \end{vmatrix} + \begin{vmatrix} \vdots \\ \cdots\ a_{sj}\ \cdots \\ \vdots \\ \cdots\ a_{rj} + a_{sj}\ \cdots \\ \vdots \end{vmatrix} = \begin{vmatrix} \vdots \\ \cdots\ a_{rj} + a_{sj}\ \cdots \\ \vdots \\ \cdots\ a_{rj} + a_{sj}\ \cdots \\ \vdots \end{vmatrix} = 0.$$

Предложение 2.4.4. *Пусть* $A = (a_{ij})$, $B = (b_{ij}) \in M_n(F)$, $\alpha \in F$, r, s — *некоторые натуральные числа из множества* $\{1, 2, \ldots, n\}$. *Пусть для каждого* $j = 1, \ldots, n$ *имеет место* $b_{rj} = a_{rj} + \alpha a_{sj}$, *и* $a_{ij} = b_{ij}$ *при* $i \neq r$. *Тогда* $\det(B) = \det(A)$.

Иными словами, *при элементарных преобразованиях строк матрицы её определитель не меняется.*

Доказательство. Обозначим через $C = (c_{ij})$ и $D = (d_{ij})$ матрицы из $M_n(F)$ такие, что для каждого $j = 1, \ldots n$ имеют место равенства $c_{rj} = \alpha a_{sj}$, $d_{rj} = a_{sj}$ и $c_{ij} = d_{ij} = a_{ij}$ при $i \neq r$. Тогда по предложению 2.4.3 определитель матрицы D равен нулю (её r-ая и s-ая строки совпадают). В силу предложения 2.4.1 имеет место равенство $\det(C) = \alpha \det(D) = 0$. Наконец, из предложения 2.4.2 следует, что $\det(B) = \det(A) + \det(C) = \det(A)$. □

Определение 2.4.2. *Верхнетреугольная* матрица $A = (a_{ij})$ — это квадратная $(n \times n)$-матрица, в которой для любых $i, j \in \{1, \ldots, n\}$ таких, что $i > j$, имеет место равенство $a_{ij} = 0$. Иными словами, все элементы матрицы, расположенные под главной диагональю, равны 0. Квадратная матрица называется *нижнетреугольной*, если все её элементы, расположенные над главной диагональю, равны 0. Квадратная матрица называется *треугольной*, если она либо верхнетреугольная, либо нижнетреугольная.

Предложение 2.4.5. *Пусть* $A = (a_{ij}) \in M_n(F)$ — *треугольная матрица. Тогда её определитель равен произведению элементов, стоящих на главной диагонали, т. е.* $\det(A) = a_{11}a_{22}\ldots a_{nn}$.

Доказательство. Мы проведём доказательство, предполагая, что A — верхнетреугольная матрица. Случай нижнетреугольных матриц разбирается аналогично.

Предположим, что подстановка $\sigma \in S_n$ обладает свойством: для каждого $i = 1, \ldots, n$ выполняется $i \leqslant i\sigma$. Тогда $n\sigma = n$, поскольку иначе требуемое неравенство не имеет места. Далее, $(n-1)\sigma = n-1$, так как n уже является образом элемента n. Продолжая рассуждение, получаем, что $(n-2)\sigma = n-2$, …, $2\sigma = 2$, $1\sigma = 1$. Следовательно, σ — тождественная подстановка. Таким образом, для каждой нетождественной подстановки $\sigma \in S_n$ найдётся $i \in \{1, \ldots, n\}$ такой, что $i > i\sigma$.

Пусть A — верхнетреугольная матрица. Тогда для каждой нетождественной подстановки σ произведение $a_{11\sigma}a_{22\sigma}\ldots a_{nn\sigma}$ равно 0. Поэтому $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}\sigma a_{11\sigma}a_{22\sigma}\ldots a_{nn\sigma} = a_{11}a_{12}\ldots a_{1n}$. □

Следствие. *Пусть* $D = D(\alpha_1, \ldots, \alpha_n)$ — *диагональная матрица,* $T = E_{rs}(\alpha)$ — *элементарная матрица. Тогда* $\det(D) = \alpha_1 \ldots \alpha_n$, $\det(T) = 1$. *В частности, определитель единичной матрицы равен единице.*

Теорема 2.4.1. *Пусть* $A, B \in M_n(F)$. *Тогда* $|AB| = |A| \cdot |B|$.

Доказательство. Предположим сначала, что $A = D(\alpha_1, \ldots, \alpha_n)$ — диагональная матрица. При умножении матрицы B слева на A для каждого $i \in \{1, 2, \ldots, n\}$ i-ая строка матрицы B умножается на α_i. Следовательно, по предложению 2.4.1 имеет место равенство $|AB| = \alpha_1 \ldots \alpha_n |B| = |A||B|$.

Если $A = E_{rs}(\alpha)$ — элементарная матрица, то её определитель равен 1. С другой стороны, при умножении на элементарную матрицу слева происходит элементарное преобразование строк. По предложению 2.4.4 и в этом случае имеем $|AB| = |B| = 1|B| = |A||B|$.

Пусть теперь A — произвольная квадратная матрица. По теореме 2.3.2 найдутся элементарные матрицы $E_1, \ldots, E_k, E_{k+1}, \ldots, E_s$ и диагональная матрица D из $M_n(F)$ такие, что $A = E_1 \ldots E_k D E_{k+1} \ldots E_s$. Тогда $|A| = |E_1(E_2 \ldots E_k D E_{k+1} \ldots E_s)| = |E_2 \ldots E_k D E_{k+1} \ldots E_s| = \ldots = |D(E_{k+1} \ldots E_s)| = |D||E_{k+1} \ldots E_s| = |D|$. Наконец, $|AB| = |E_1 \ldots E_k D E_{k+1} \ldots E_s B| = |D(E_{k+1} \ldots E_s B)| = |D||E_{k+1} \ldots E_s B| = |D||B| = |A||B|$. □

Упражнение 2.4.3. *Пусть*

$$A = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_s \end{pmatrix} —$$

клеточно диагональная матрица. Тогда $|A| = |A_1||A_2| \ldots |A_s|$.

Определение 2.4.3. Пусть $A = (a_{ij})$ — $(m \times n)$-матрица над множеством S. Матрица $B = (b_{ij})$ размера n на m над S называется *транспонированной* к матрице A, если $b_{ij} = a_{ji}$ для каждого $i = 1, \ldots, n$ и каждого $j = 1, \ldots, m$. Мы будем обозначать матрицу, транспонированную к матрице A, через A' или $A^\top$.

Сформулируем в виде упражнения свойства транспонирования матриц.

Упражнение 2.4.4. *Для прямоугольных матриц A и B согласованных размеров докажите следующие утверждения:*
1) $A'' = (A')' = A$;
2) $(A + B)' = A' + B'$;
3) $(AB)' = B'A'$.

Замечание. Несложно заметить также, что если D — диагональная матрица, а $E_{rs}(\alpha)$ — элементарная матрица, то $D' = D$ и $E_{rs}(\alpha)' = E_{sr}(\alpha)$.

Предложение 2.4.6. *Пусть $A \in M_n(F)$. Тогда* $\det(A') = \det(A)$.

Доказательство. Заметим, во-первых, что из утверждения 3) упражнения 2.4.4 несложно вывести по индукции следующее правило транспонирования произведения нескольких матриц: $(A_1A_2 \dots A_s)' = A'_s \dots A'_2A'_1$. Как мы знаем, $A = E_1 \dots E_kDE_{k+1} \dots E_s$, где $E_1, \dots, E_k$, $E_{k+1}, \dots, E_s$ — элементарные матрицы, а D — диагональная матрица, причём $|A| = |D|$. Поэтому $A' = E'_s \dots E'_{k+1}D'E'_k \dots E'_1$ и $|A'| = |D'| = |D| = |A|$. □

Следствие. *Если в каждом доказанном нами утверждении о свойствах определителя заменить слово «строка» на слово «столбец», то утверждение останется верным.*

Упражнение 2.4.5. *Сформулируйте и обоснуйте указанные утверждения для столбцов матрицы.*

Следующая наша задача — доказать утверждение, которое позволит вычислять определитель матрицы размера n через определители матриц меньшего размера.

Определение 2.4.4. Пусть $A = (a_{ij}) \in M_n(F)$. *Минором*, дополнительным к элементу a_{rs} матрицы A, называется матрица $M_{rs}(A)$ из $M_{n-1}(F)$, полученная из матрицы A вычеркиванием r-ой строки и s-го столбца.

Пример.

$$\text{Для } A = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 4 & 6 \\ 7 & 8 & 9 \end{pmatrix} \text{ минор } M_{23}(A) = \begin{pmatrix} 1 & 2 \\ 7 & 8 \end{pmatrix}.$$

Определение 2.4.5. Пусть $A = (a_{ij}) \in M_n(F)$. *Алгебраическое дополнение* в A к элементу a_{rs} — это скаляр $A_{rs} = (-1)^{r+s}|M_{rs}(A)|$.

Иными словами, *алгебраическое дополнение к элементу матрицы с номером (r, s) — это определитель минора, дополнительного к данному*

элементу, взятый со знаком плюс, если сумма $r+s$ чётна, и знаком минус, если эта сумма нечётна.

Пример. Для элемента a_{23} матрицы A из предыдущего примера выполняется

$$A_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix} = (-1) \cdot (1 \cdot 8 - 2 \cdot 7) = 6.$$

Теорема 2.4.2 (о разложении определителя по строке)**.** *Пусть $A = (a_{ij}) \in M_n(F)$. Тогда для любых $i, k \in \{1, \ldots, n\}$ имеет место равенство*

$$\sum_{j=1}^{n} a_{ij} A_{kj} = \begin{cases} |A|, & \text{если } k = i \\ 0, & \text{если } k \neq i. \end{cases}$$

Замечание. *Формула разложения определителя* по i-ой строке:

$$|A| = \sum_{j=1}^{n} a_{ij} A_{ij},$$

выполняющаяся для каждого $i = 1, \ldots, n$, очевидно, является частным случаем теоремы при $k = i$.

Доказательство. Сначала мы докажем теорему в случае, когда $i = k$, т. е. докажем, что $|A| = \sum_{j=1}^{n} a_{ij} A_{ij}$ для каждого $i = 1, \ldots, n$. Разобьём это доказательство на четыре этапа.

Этап 1. Пусть $i = n$, $a_{n1} = a_{n2} = \ldots = a_{n,n-1} = 0$. Матрица A имеет вид

$$\left(\begin{array}{ccc|c} & & & * \\ & M_{nn} & & \vdots \\ & & & * \\ \hline 0 & \ldots & 0 & a_{nn} \end{array} \right),$$

где $M_{nn} = M_{nn}(A)$ — минор, дополнительный к элементу a_{nn} в матрице A, а $*$ обозначает произвольный скаляр.

Для подстановки $\sigma = \begin{pmatrix} 1 & \ldots & n-1 & n \\ i_1 & \ldots & i_{n-1} & n \end{pmatrix} \in S_n$ положим $\sigma' = \begin{pmatrix} 1 & \ldots & n-1 \\ i_1 & \ldots & i_{n-1} \end{pmatrix} \in S_{n-1}$. Имеем $|A| =$

$$= \sum_{\sigma \in S_n} \operatorname{sgn} \sigma a_{11\sigma} \ldots a_{n-1,(n-1)\sigma} a_{nn\sigma} = \sum_{\substack{\sigma \in S_n \\ n\sigma = n}} \operatorname{sgn} \sigma a_{11\sigma} \ldots a_{n-1,(n-1)\sigma} a_{nn} =$$

$$= a_{nn} \cdot \sum_{\sigma' \in S_{n-1}} \operatorname{sgn} \sigma' a_{11\sigma'} \dots a_{n-1,(n-1)\sigma'} = a_{nn}|M_{nn}| = a_{nn}(-1)^{n+n}|M_{nn}| =$$

$$= a_{nn}A_{nn} = 0 \cdot A_{n1} + \ldots + 0 \cdot A_{n,n-1} + a_{nn}A_{nn} = \sum_{j=1}^{n} a_{nj}A_{nj}.$$

Этап 2. Пусть $i = n$, $a_{nj} = 0$, кроме, быть может, одного элемента a_{ns}.

Если $s = n$, то мы получаем матрицу из первого этапа доказательства. Пусть $s < n$. Пусть матрица A_1 получена из матрицы A перестановкой s-го и $(s+1)$-го столбца. Тогда в силу следствия из предложения 2.4.3 и следствия из предложения 2.4.6 имеет место равенство $|A| = -|A_1|$. Если $s = n-1$, то полученная матрица имеет вид, как у матрицы на первом этапе доказательства, а минор $M_{nn}(A_1) = M_{n,n-1}(A)$. Следовательно, $|A| = -|A_1| = -a_{n,n-1}|M_{n,n-1}| = a_{n,n-1}A_{n,n-1}$, что и требовалось. Если $s < n-1$, то мы продолжаем указанный процесс, меняя $(s+1)$-ый столбец матрицы A_1 (т. е. s-ый столбец матрицы A) с $(s+2)$-ым столбцом и так далее, пока не поставим s-ый столбец матрицы A на место n-го столбца. Всего нам потребуется $n - s$ перестановок. Получившаяся в результате матрица B имеет вид

$$\left(\begin{array}{ccc|c} & & & * \\ & M_{ns}(A) & & \vdots \\ & & & * \\ \hline 0 & \dots & 0 & a_{ns} \end{array}\right).$$

Поэтому $|A| = (-1)^{n-s}|B| = (-1)^{n-s+2s}a_{ns}|M_{ns}(A)| = a_{ns}A_{ns} = \sum_{j=1}^{n} a_{nj}A_{nj}$, что и требовалось. Отметим, что наше рассуждение существенно использует последовательную перестановку соседних столбцов матрицы A. Если мы, к примеру, сразу поменяем между собой s-ый и n-ый столбцы, то в левом верхнем углу получившейся матрицы не будет минора $M_{ns}(A)$ и предложенное рассуждение будет неверным.

Этап 3. Пусть $i = n$. Обозначим через A_j матрицу того же размера n, что и A, у которой первые $n-1$ строк совпадают с соответствующими строками матрицы A, в последней строке на месте (n, j) стоит элемент a_{nj} матрицы A, а остальные элементы последней строки равны нулю. По предложению 2.4.2 имеем $|A| = |A_1| + |A_2| + \ldots + |A_n| = \sum_{j=1}^{n} a_{nj}A_{nj}$.

Этап 4. Пусть номер строки произволен. Если $i = n$, то утверждение доказано. Пусть $i < n$. Поменяем местами i-ую и $(i+1)$-ую строки матрицы A так же, как на втором этапе мы меняли местами соседние столбцы. Затем $(i+1)$-ую и $(i+2)$-ую строки получившейся матрицы

и так далее, продолжая процесс до тех пор, пока i-ая строка матрицы A не переместится на место n-ой строки. Обозначим полученную в результате всех этих перестановок матрицу через B. В силу следствия из предложения 2.4.3 имеем $|A| = (-1)^{n-i}|B|$.

Если для краткости обозначить k-ые строки матриц A и B через a_k и b_k соответственно, то для них будут иметь места равенства: $b_k = a_k$ при $1 \leqslant k < i$, $b_k = a_{k+1}$ при $i \leqslant k < n$ и $b_n = a_i$. В частности, $M_{nj}(B) = M_{ij}(A)$ для каждого $j = 1, \ldots, n$. Поэтому $|A| =$

$$= (-1)^{n-i}|B| = (-1)^{n-i}\sum_{j=1}^{n} b_{nj}B_{nj} = (-1)^{n-i}\sum_{j=1}^{n} b_{nj}(-1)^{n+j}|M_{nj}(B)| =$$

$$\sum_{j=1}^{n} a_{ij}(-1)^{n+j+n-i}|M_{ij}(A)| = \sum_{j=1}^{n} a_{ij}(-1)^{i+j+2(n-i)}|M_{ij}(A)| = \sum_{j=1}^{n} a_{ij}A_{ij}.$$

Таким образом, формула разложения определителя по строке доказана.

Докажем оставшуюся часть теоремы. А именно, покажем, что при $i \neq k$ имеет место равенство $\sum_{j=1}^{n} a_{ij}A_{kj} = 0$. Определим матрицу B той же размерности n, что и матрица A, следующим образом: все строки матрицы B, кроме k-ой строки, совпадают с соответствующими строками матрицы A, а на месте k-ой строки стоит i-я строка матрицы A. Поскольку i-ая и k-ая строки матрицы B равны между собой (обе равны i-ой строке матрицы A), по предложению 2.4.3 определитель матрицы B равен нулю. С другой стороны, раскладывая определитель матрицы B по k-ой строке, получаем

$$|B| = \sum_{j=1}^{n} b_{kj}B_{kj} = \sum_{j=1}^{n} a_{ij}A_{kj},$$

так как миноры M_{kj} матриц A и B совпадают (единственная строка, различная в матрицах A и B, строка под номером k, вычеркивается при вычислении этих миноров). Теорема доказана. □

Следствие (о разложении определителя по столбцу)**.** *Пусть* $A = (a_{ij}) \in M_n(F)$. *Тогда для любых* $j, k \in \{1, \ldots, n\}$ *имеет место равенство*

$$\sum_{i=1}^{n} a_{ij}A_{ik} = \begin{cases} |A|, & \text{если } j = k \\ 0, & \text{если } j \neq k. \end{cases}$$

Доказательство. Доказательство дословно повторяет доказательство теоремы с заменой слова «строка» на слово «столбец» и обратно. Кроме того, следствие можно доказать, применив теорему о разложении по строке к транспонированной матрице A'. □

Упражнение 2.4.6. *Вычислите определитель матрицы A из примера после определения дополнительного минора двумя способами: разложив его сначала по второй строке, а затем по третьему столбцу.*

Имеется одна полезная переформулировка только что доказанной нами теоремы, так называемая *матричная форма* теоремы о разложении по строке, для которой нам понадобится следующее определение.

Определение 2.4.6. Пусть $A = (a_{ij}) \in M_n(F)$. Матрица $\widehat{A} = (\widehat{a}_{ij}) \in M_n(F)$, для которой $\widehat{a}_{ij} = A_{ji}$ при всех $i, j \in \{1, \ldots, n\}$, называется *присоединённой* к матрице A.

Иными словами, *присоединённая матрица — это транспонированная матрица алгебраических дополнений.*

Теперь теорема 2.4.2 может быть сформулирована следующим образом.

Теорема 2.4.2′ (матричная форма теоремы о разложении по строке). *Пусть A — квадратная матрица из $M_n(F)$, а $\widehat{A}$ — присоединённая к ней матрица. Тогда*

$$A\widehat{A} = \widehat{A}A = |A|E = \begin{pmatrix} |A| & 0 & \ldots & 0 \\ 0 & |A| & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & |A| \end{pmatrix}.$$

Доказательство. Обозначив через B матрицу $A\widehat{A}$, имеем

$$b_{ij} = \sum_{k=1}^{n} a_{ik}\widehat{a}_{kj} = \sum_{k=1}^{n} a_{ik}A_{jk} = \begin{cases} |A|, & \text{если } i = j \\ 0, & \text{если } i \neq j. \end{cases}$$

Для матрицы $\widehat{A}A$ результат получается аналогично. □

Используя матричную форму теоремы, несложно доказать критерий обратимости матрицы.

Определение 2.4.7. Квадратная матрица A называется *вырожденной*, если $\det(A) = 0$, и *невырожденной* в противном случае.

Определение 2.4.8. Пусть A — квадратная матрица из $M_n(F)$. Матрица A^{-1} называется *обратной* к матрице A, если $AA^{-1} = A^{-1}A = E$.

Теорема 2.4.3 (об обратной матрице)**.** *Пусть $A \in M_n(F)$ и $\widehat{A}$ — присоединённая к ней матрица. Матрица A обратима (имеет обратную матрицу) тогда и только тогда, когда она невырождена. Обратная матрица*

$$A^{-1} = \frac{1}{|A|}\widehat{A} = \frac{1}{|A|}\begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots\dots\dots\dots\dots & & & \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix}.$$

Доказательство. Пусть сначала $|A| = 0$. Предположим, что для матрицы A существует обратная матрица A^{-1}. Тогда по теореме об определителе произведения матриц $1 = |E| = |AA^{-1}| = |A||A^{-1}| = 0$; противоречие.

Если же матрица A невырождена, то матрица $\frac{1}{|A|}\widehat{A}$ всегда существует. Напомним, что для скаляра α и матрицы $A = (a_{ij})$ матрица αA — это матрица (αa_{ij}). Кроме того, αE — это скалярная матрица с элементом α по главной диагонали. В частности, в силу упражнения 2.3.3 выполняется $\alpha A = \alpha EA = A(\alpha E)$.

По теореме 2.4.2′ имеют место равенства

$$A(\frac{1}{|A|}\widehat{A}) = A(\frac{1}{|A|}E\widehat{A}) = \frac{1}{|A|}E(A\widehat{A}) = \frac{1}{|A|}E|A|E = E$$

$$\text{и } (\frac{1}{|A|}\widehat{A})A = \frac{1}{|A|}|A|E = E.$$

□

Упражнение 2.4.7. *Для матрицы A из примера после определения дополнительного минора вычислите присоединённую матрицу. Проверьте, что полученная из неё делением на определитель матрица удовлетворяет определению обратной матрицы.*

Упражнение 2.4.8. *Пусть $GL_n(F) = \{A \in M_n(F) \mid \det(A) \neq 0\}$. Докажите, что $GL_n(F)$ — группа относительно операции умножения матриц.*

Определение 2.4.9. Группа $GL_n(F)$, определённая в упражнении 2.4.8, называется *общей линейной группой матриц над полем* F, а любая её подгруппа –*линейной группой матриц над полем* F.

Заметим, что теорема об обратной матрице влечёт, что линейные матричные уравнения: $AX = B$ и $YA = B$ имеют единственное решение в том и только том случае, когда матрица A невырождена (предполагается, что матрицы A, B, X, Y — квадратные матрицы одной размерности). Решениями уравнений будут матрицы $X = A^{-1}B$ и $Y = BA^{-1}$ соответственно.

Рассмотрим теперь ещё один способ вычисления обратной матрицы, а также решения линейных матричных уравнений, основанный на разложении квадратной матрицы в произведение элементарной и диагональной матриц. Мы изложим его в виде серии упражнений.

Упражнение 2.4.9. *Докажите, что если матрица A невырождена, то её можно разложить в произведение диагональной и элементарных матриц так, чтобы диагональная матрица оказалась в произведении последней справа (слева). Иными словами, требуется доказать, что невырожденную матрицу можно привести к диагональному виду, пользуясь только элементарными преобразованиями строк (или только столбцов).*

Упражнение 2.4.10. *Пусть $A, B \in M_n(F)$ и $|A| \neq 0$. Преобразование строки (столбца) прямоугольной матрицы, при котором все элементы строки (столбца) умножаются на ненулевой скаляр α, будем так же, как и прибавление к строке (столбцу) другой строки (другого столбца), умноженной на скаляр, называть элементарным преобразованием строки (столбца). Докажите, что прямоугольную $(n \times 2n)$-матрицу $(A \mid B)$, составленную из матриц A и B, можно элементарными преобразованиями строк привести к виду $(E \mid X)$, где E — единичная матрица, а X — матрица $A^{-1}B$, т. е. решение матричного уравнения $AX = B$. В частности, если положить $B = E$, то $X = A^{-1}$. Доказать, что элементарными преобразованиями столбцов $(2n \times n)$-матрицу $\left(\frac{A}{B}\right)$ можно привести к виду $\left(\frac{E}{Y}\right)$, где Y — решение уравнения $YA = B$.*

Замечание. Существуют ещё два способа ввести понятие определителя: аксиоматический и индуктивный. В первом случае мы определяем det как функцию из $M_n(F)$ в F, удовлетворяющую свойствам, указанным в предложениях 2.4.1–2.4.3, и принимающую значение 1 на единичной матрице. Во втором случае мы полагаем, что для матрицы $A = (a) \in M_1(F)$ её определитель равен a, а для матрицы $A \in M_n(F)$ определяем $\det(A)$ по индукции через определители матриц размерно-

сти $n-1$, используя формулу разложения по строке (см. теорему 2.4.2).

Упражнение 2.4.11.* *Покажите, что три предложенных определения определителя (включая данное нами в этом курсе) эквивалентны.*

§ 2.5. Поле комплексных чисел

Определение 2.5.1. *Полем комплексных чисел* называется поле $\mathbb{C}$, удовлетворяющее следующим условиям.

1. Поле $\mathbb{C}$ содержит в качестве подполя поле R, изоморфное полю $\mathbb{R}$ действительных чисел.

2. Поле $\mathbb{C}$ содержит элемент i такой, что $i^2 = -1$, где -1 — это элемент, противоположный к единице поля $\mathbb{C}$, а значит, и его подполя R.

3. Каждый элемент z поля $\mathbb{C}$ однозначно представляется в виде $a+bi$, где $a, b \in R$, подполе R определено в п. 1, а i — в п. 2.

Теорема 2.5.1. *Поле $\mathbb{C}$ комплексных чисел существует и единственно с точностью до изоморфизма.*

Доказательство. Обозначим через $\mathbb{C}$ множество квадратных матриц вида

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \text{ где } a, b \in \mathbb{R}.$$

В силу равенств:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix}, \tag{1}$$

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \tag{2}$$

множество $\mathbb{C}$ замкнуто относительно операций сложения и умножения матриц.

Докажем, что $\mathbb{C}$ является полем относительно этих операций. Поскольку нулевая и единичная матрицы из $M_2(\mathbb{R})$ лежат в $\mathbb{C}$, а само $M_2(\mathbb{R})$ является кольцом с единицей, нам остаётся проверить лишь коммутативность умножения матриц из $\mathbb{C}$, а также существование противоположного и обратного элемента для произвольного

$$z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C}.$$

Выполнив умножение матриц из равенства (2) в обратном порядке, получим

$$\begin{pmatrix} c & -d \\ d & c \end{pmatrix} \cdot \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix}.$$

Следовательно, умножение элементов из $\mathbb{C}$ коммутативно. Поскольку матрица

$$\begin{pmatrix} -a & -(-b) \\ -b & -a \end{pmatrix}$$

лежит в $\mathbb{C}$, имеет место и аксиома существования противоположного элемента.

Нам осталось показать, что любой ненулевой элемент $z \in \mathbb{C}$ имеет обратный в $\mathbb{C}$. Воспользуемся теоремой 2.4.3 об обратной матрице. Во-первых,

$$\begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0,$$

кроме случая $a = b = 0$, в котором элемент z есть нулевая матрица. Во-вторых,

$$z^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{C}.$$

Таким образом, $\mathbb{C}$ — поле. Покажем, что $\mathbb{C}$ удовлетворяет условиям 1–3 из определения 2.5.1 и, следовательно, является полем комплексных чисел.

Пусть

$$R = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in \mathbb{R} \right\}.$$

Очевидно, что R — подмножество множества $\mathbb{C}$. С другой стороны, в силу утверждения упражнения 2.3.2 множество R как множество всех скалярных матриц из $M_2(R)$ есть поле, изоморфное полю $\mathbb{R}$ действительных чисел. В качестве изоморфизма здесь выступает отображение φ, действующее по правилу $(aE)\varphi = a \in \mathbb{R}$.

Обозначим через i элемент поля $\mathbb{C}$, равный

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Несложно проверить, что

$$i^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Элемент, полученный в результате этого умножения, является противоположным к единичной матрице и переходит в -1 при отображении φ из R в $\mathbb{R}$.

Для произвольного элемента $z \in \mathbb{C}$, записываемого в виде матрицы

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

положим

$$a = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \text{ и } b = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}.$$

Тогда

$$z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = a + bi.$$

Предположим, что элемент z имеет два представления $z = a + bi = c + di$. Тогда $a - c = (d - b)i$. Возводя последнее равенство в квадрат, получаем $(a - c)^2 = -(d - b)^2$. Поскольку a, b, c, d можно считать действительными числами, имеем $a - c = d - b = 0$. Отсюда $a = c$ и $b = d$, а значит, представление $z = a + bi$ единственно. Таким образом, $\mathbb{C}$ — поле комплексных чисел.

Пусть C — ещё одно поле, удовлетворяющее определению комплексных чисел. Обозначим через i' элемент этого поля со свойством $(i')^2 = -1$. Тогда в силу свойства 3 любой элемент поля C однозначно представим в виде $a + bi'$, где элементы a и b в силу свойства 1 можно считать действительными числами. Поэтому отображение $\psi : \mathbb{C} \to C$, действующее по правилу $(a + bi)\psi = a + bi'$, является биекцией. Кроме того, равенства $(a + bi') + (c + di') = (a + c) + (b + d)i'$ и $(a + bi')(c + di') = (ac - bd) + (ad + bc)i'$ вместе с равенствами (1) и (2) показывают, что ψ есть изоморфизм. □

Замечание. В дальнейшем мы будем называть элементы поля $\mathbb{C}$ *комплексными числами* и, как правило, обозначать через $a + bi$. Кроме того, если договориться, что элементы вида $a+0i = a$ — это действительные числа, то можно считать, что $\mathbb{R}$ есть подполе поля $\mathbb{C}$. Поскольку поле $\mathbb{Q}$ рациональных чисел является подполем поля $\mathbb{R}$, его также можно рассматривать как подполе поля $\mathbb{C}$. Мы будем называть *числовым полем* любое подполе поля комплексных чисел.

Определение 2.5.2. Действительные числа a и b называются *действительной и мнимой частью* комплексного числа $z = a + bi$ и обозначаются $a = \operatorname{Re} z$ и $b = \operatorname{Im} z$ соответственно. Число i со свойством

$i^2 = -1$ из определения поля комплексных чисел называется *мнимой единицей*.

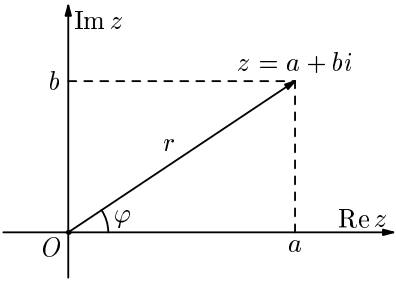
В поле $\mathbb{C}$ имеется два элемента, которые в квадрате дают -1. Если один из них обозначен через i, то второй равен $-i$. Как легко проверить, решая уравнение $(a + bi)^2 = -1 + 0i$, других элементов с таким свойством в $\mathbb{C}$ нет. Если в доказательстве единственности поля комплексных чисел положить $i' = -i$, то мы получим, что отображение $z = a + bi \to \overline{z} = a - bi$ есть изоморфизм поля комплексных чисел на себя. Этот изоморфизм называется *комплексным сопряжением*, а числа z и $\overline{z}$ *комплексно сопряжёнными*. Поскольку комплексное сопряжение — изоморфизм, для любых комплексных чисел z и u выполняются следующие равенства: $\overline{z + u} = \overline{z} + \overline{u}$ и $\overline{zu} = \overline{z} \cdot \overline{u}$. Кроме того, очевидно, что $\overline{\overline{z}} = z$.

Упражнение 2.5.1.* *Доказать, что любой изоморфизм поля действительных чисел на себя является тождественным, а изоморфизмов поля комплексных чисел на себя ровно два: тождественный и комплексное сопряжение.*

Указание. Используя упражнение 2.1.10, *докажите, что любой изоморфизм поля рациональных чисел на себя является тождественным. Затем используйте определение действительных чисел, а также следующее соображение: для действительного числа a выполняется $a \geqslant 0 \Leftrightarrow$ $\Leftrightarrow \exists b \in \mathbb{R} : b^2 = a$.*

В силу определения поля $\mathbb{C}$ два комплексных числа z и u равны тогда и только тогда, когда $\operatorname{Re} z = \operatorname{Re} u$ и $\operatorname{Im} z = \operatorname{Im} u$. Поэтому существует биекция множества $\mathbb{C}$ на множество пар действительных чисел $\mathbb{R}^2$, которое в свою очередь можно отождествить с множеством всех точек плоскости (или множеством всех векторов плоскости). Таким образом, комплексное число $z = a+bi$ изображается точкой с координатами (a, b). Координатную плоскость в этом случае называют *комплексной плоскостью*, ось абсцисс — *действительной осью*, а ось ординат — *мнимой осью*.

При векторном представлении комплексному числу $z = a + bi$ ставится в соответствие вектор $\overrightarrow{z}$ с координатами (a, b). При таком представлении сложению комплексных чисел соответствует сложение соответствующих векторов по правилу параллелограмма. Для того чтобы естественным образом указать вектор, соответствующий произведению двух комплексных чисел, удобнее перейти к терминологии, связанной с полярными координатами.



Определение 2.5.3. Пусть $z = a + bi \in \mathbb{C}$. *Модулем* комплексного числа $z = a + bi$ называется неотрицательное действительное число $r = \sqrt{a^2 + b^2}$, равное длине вектора $\overrightarrow{z}$ с координатами (a, b). Модуль комплексного числа z обозначается через $|z|$.

Замечание. При таком определении модуль произвольного действительного числа $z = a+0i$, понимаего как комплексное число с нулевой мнимой частью, равен $\sqrt{a^2 + 0^2}$ и совпадает обычным определением модуля действительного числа.

Определение 2.5.4. *Аргументом* ненулевого комплексного числа $z = a + bi$ называется величина угла, образуемого соответствующим вектором $\overrightarrow{z}(a, b)$ с положительным направлением действительной оси комплексной плоскости. Аргумент определяется с точностью до прибавления целого кратного числа 2π. Аргумент числа 0 не определён. Аргумент числа z обозначается через $\arg z$.

Замечание. Хотя для числа 0 аргумент не определён, проблем не возникает, поскольку число 0 однозначно определяется свои модулем.

Пусть r и φ — модуль и аргумент комплексного числа $z = a + bi$. Несложно понять, что $a = r\cos\varphi$ и $b = r\sin\varphi$. Поэтому

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

Это представление комплексного числа называется его *тригонометрической формой*.

Из данных нами определений следует, что два комплексных числа $z = r(\cos\varphi + i\sin\varphi)$ и $u = s(\cos\psi + i\sin\psi)$, записанных в тригонометрической форме, равны тогда и только тогда, когда $r = s$ и $\varphi = \psi + 2k\pi$, $k \in \mathbb{Z}$.

Предложение 2.5.1. *Пусть заданы два комплексных числа* $z = r(\cos\varphi + i\sin\varphi)$ *и* $u = s(\cos\psi + i\sin\psi)$. *Тогда их произведение* $zu = rs(\cos(\varphi + \psi) + i\sin(\varphi + \psi))$.

Иными словами, *при умножении двух комплексных чисел их модули перемножаются, а аргументы складываются.*

Доказательство. Формула умножения комплексных чисел легко выводится с использованием тригонометрических формул косинуса и синуса суммы двух углов. □

Следствие (формула Муавра)**.** *Пусть* $z = r(\cos\varphi + i\sin\varphi)$. *Тогда* $z^n = r^n(\cos n\varphi + i\sin n\varphi)$.

Корнем n*-ой степени* из комплексного числа z мы назовём комплексное число u такое, что $u^n = z$. Используя формулу Муавра, мы докажем следующую теорему о корнях n-ой степени из комплексного числа.

Теорема 2.5.2. *Пусть* $z = r(\cos\varphi + i\sin\varphi)$ — *ненулевое комплексное число. Тогда уравнение* $x^n = z$ *имеет ровно* n *различных решений* $x_0, x_1 \ldots, x_{n-1}$ *в поле комплексных чисел. Причём для* $k = 0, 1, \ldots, n-1$

$$x_k = \sqrt[n]{r}(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}).$$

Доказательство. Пусть комплексное число $u = s(\cos\psi + i\sin\psi)$ — решение уравнения $x^n = z$. По формуле Муавра $s^n = r$ и $n\psi = \varphi + 2k\pi$ ($k \in \mathbb{Z}$). Следовательно, $s = \sqrt[n]{r}$ (арифметический корень) и $\psi = \frac{\varphi+2k\pi}{n}$. Заметим, что для $k, m \in \{0, 1, \ldots, n-1\}$ значения косинуса и синуса от чисел $\frac{\varphi+2k\pi}{n}$ и $\frac{\varphi+2m\pi}{n}$ совпадают только в том случае, когда $k = m$. С другой стороны, при $m = k + nj$ ($j \in \mathbb{Z}$) аргументы $\frac{\varphi+2k\pi}{n}$ и $\frac{\varphi+2m\pi}{n} = \frac{\varphi+2k\pi}{n} + 2j\pi$ различаются лишь на целое кратное 2π. Следовательно, множество различных решений данного уравнения есть

$$\left\{ \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right) \;\middle|\; k = 0, 1, \ldots, n-1 \right\}.$$

□

Отметим в качестве упражнения некоторые полезные свойства корней n-ой степени из единицы.

Упражнение 2.5.2.

1. *Множество* $\mathbb{C}_n = \{\varepsilon_k \mid k = 0, 1, \ldots, n-1\}$, *где* $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, *есть множество всех решений уравнения* $x^n = 1$.

2. *Если* x_0 — *некоторое решение уравнения* $x^n = z$, *то множество* $\{x_k = x_0\varepsilon_k \mid k = 0, 1, \ldots, n-1\}$ *есть множество всех решений уравнения* $x^n = z$.

3. *Множество* $\mathbb{C}_n$ *относительно операции умножения комплексных чисел образует абелеву группу. Причём* $< \mathbb{C}_n, \cdot > \simeq < \mathbb{Z}_n, + >$ (*см. упражнение* 2.1.8).

Глава 3

Векторные пространства

§ 3.1. Определение векторного пространства

Использование алгебраических методов в геометрии неразрывно связано с понятием вектора. В этой главе мы изучим класс алгебраических систем, возникающих как обобщение геометрических векторов и связанных с ними операций. Напомним, что в элементарной геометрии рассматриваются следующие операции с векторами: сложение двух векторов и умножение вектора на число. Отметим, что умножение вектора на число нельзя рассматривать в качестве бинарной операции, так как множители берутся из разных множеств. Однако для каждого числа $\alpha \in \mathbb{R}$ умножение на α можно рассматривать как унарную операцию f_α, сопоставляющую вектору v вектор αv.

Определение 3.1.1. Пусть F — поле. *Векторное* (или *линейное*) *пространство* над полем F — это множество V (его элементы называются *векторами*), на котором определена бинарная операция $+$ (*сложение векторов*) и по одной унарной операции $v \mapsto \alpha v$ (*умножение вектора на скаляр*) для каждого скаляра α из поля F, обладающие следующими свойствами.

1. $< V, + >$ — абелева группа.
2. Для любых $\alpha \in F$ и $u, v \in V$ выполняется $\alpha(u + v) = \alpha u + \alpha v$.
3. Для любых $\alpha, \beta \in F$ и $v \in V$ выполняется $(\alpha + \beta)v = \alpha v + \beta v$.
4. Для любых $\alpha, \beta \in F$ и $v \in V$ выполняется $(\alpha\beta)v = \alpha(\beta v)$.
5. Для любого $v \in V$ и единицы 1 поля F выполняется $1v = v$.

Укажем в качестве упражнения некоторые элементарные свойства операций, заданных на векторном пространстве.

Упражнение 3.1.1. *Пусть V — векторное пространство над полем F; $\alpha, \beta \in F$; $u, v \in V$; 0 — ноль поля F, 1 — единица поля F, а $\overline{0}$ — нейтральный по сложению вектор из V. Тогда*

1) $\alpha\overline{0} = \overline{0}$;
2) $\alpha(-v) = -\alpha v$;
3) $\alpha(u - v) = \alpha u - \alpha v$;
4) $0v = \overline{0}$;

5) $(-1)v = -v$;

6) $(\alpha - \beta)v = \alpha v - \beta v$.

Замечание. В дальнейшем, если не возникает путаницы с нулём поля F, мы будем обозначать нулевой вектор просто через 0.

Примеры. 1. Пусть F — некоторое поле. Зададим на множестве $F^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid \alpha_i \in F\}$ всех упорядоченных n-ок из элементов поля F операции сложения и умножения на скаляр $\alpha \in F$ по правилам:

1) $(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$;

2) $\alpha(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n)$.

Тогда F^n относительно указанных операций образует векторное пространство над полем F. Это пространство называется *арифметическим векторным пространством*.

Заметим, что если ввести на плоскости (или в пространстве) систему координат и отождествить геометрические векторы плоскости (пространства) с их координатами в этой системе, то мы получим арифметическое векторное пространство $\mathbb{R}^2$ ($\mathbb{R}^3$).

2. Пусть F — подполе поля K. Тогда K можно рассматривать как векторное пространство над полем F относительно операции сложения элементов поля K и умножения элемента поля K на скаляр из F, понимаего как обычное умножение элементов поля K (напомним, что $F \subseteq K$). Так, поле $\mathbb{R}$ действительных чисел можно рассматривать как векторное пространство над полем $\mathbb{Q}$ рациональных чисел, а поле $\mathbb{C}$ комплексных чисел — как векторное пространство над полем $\mathbb{R}$.

3. Множество $F(X, K)$ всех функций из множества X в поле K является векторным пространством относительно обычных операций: сложения функций $(f+g)(x) = f(x)+g(x)$ и умножения функции на скаляр $(\alpha f)(x) = \alpha f(x)$.

4. Векторным пространством является множество $F[x]$ всех многочленов от переменной x над полем F относительно тех же операций, что и в предыдущем примере.

5. Множество M всех матриц размера $m \times n$ над полем F является векторным пространством относительно операций сложения матриц и умножения матрицы на скаляр $\alpha \in F$ по правилу $A \mapsto \alpha A$, где через αA, как обычно, обозначена матрица, полученная из матрицы A умножением каждого её элемента на α.

В частности, векторным пространством над полем F будет множество $M_n(F)$ квадратных матриц. Напомним, что $M_n(F)$ является также кольцом относительно операций сложения и умножения матриц. Ал-

гебраические системы, которые являются одновременно и кольцом, и векторным пространством, принято называть *алгебрами*.

Определение 3.1.2. *Алгеброй* над полем F называется множество A с двумя бинарными операциями: сложением и умножением, а также унарными операциями умножения на скаляр для каждого скаляра из поля F, если выполняется:

1) A — кольцо относительно операций сложения и умножения;

2) A — векторное пространство относительно сложения и умножения на скаляр;

3) для любых $\alpha \in F$ и $a, b \in A$ выполняется $\alpha(ab) = (\alpha a)b = a(\alpha b)$.

Упражнение 3.1.2.

1. *Проверьте, что $M_n(F)$ является алгеброй над F.*

2. *Используя приведённые примеры векторных пространств, приведите примеры алгебр.*

Определение 3.1.3. Пусть V — векторное пространство над полем F. Непустое подмножество U множества V называется *подпространством* пространства V, если оно замкнуто относительно операций, заданных на V, т. е. для любых $u, v \in U$ и $\alpha \in F$ выполняется $u + v \in U$ и $\alpha u \in U$.

Замечание. Заметим, что подпространство U пространства V над полем F само является векторным пространством над F. Действительно, ассоциативность и коммутативность сложения, а также все свойства, связывающие между собой операции сложения и умножения на скаляр, имеют место для векторов из U, поскольку векторы из U одновременно являются векторами из V. С другой стороны, в силу утверждения 5 упражнения 3.1.1 для любого элемента $u \in U$ противоположный к нему элемент $-u = (-1)u$ снова лежит в U, а значит, там лежит и нуль-вектор как их сумма.

Определение 3.1.4. Пусть A — алгебра над полем F. Непустое подмножество B множества A называется *подалгеброй* алгебры A, если оно замкнуто относительно операций, заданных на A, т. е. для любых $a, b \in B$ и $\alpha \in F$ выполняется $a + b \in B$, $ab \in B$ и $\alpha a \in B$.

Примеры. 1. Любое пространство V всегда содержит два подпространства: *нулевое подпространство* $0 = \{0\}$ и само пространство V. Всякое подпространство, отличное от нулевого, мы будем называть *нетривиальным*, а всякое подпространство, отличное от самого пространства, — *собственным*. Аналогичные понятия можно определить и

для произвольной алгебры A.

2. Множество $\mathbb{R}$ действительных чисел можно рассматривать как подпространство (подалгебру) пространства (алгебры) $\mathbb{C}$ над полем $\mathbb{R}$.

Упражнение 3.1.3. *Докажите следующие утверждения:*

1. *Подмножество* $\{(\alpha_1, \ldots, \alpha_n) \mid \alpha_1 + \ldots + \alpha_n = 0\}$ *векторов арифметического пространства* F^n *над полем* F *является подпространством.*

2. *Подмножество* $F_n[x]$ *многочленов от переменной* x*, степень которых не превосходит* n*, является подпространством пространства* $F[x]$ *всех многочленов от переменной* x *над полем* F*. Однако если рассматривать* $F[x]$ *как алгебру над* F *то* $F_n[x]$ *уже не является её подалгеброй.*

3. *Множество всех симметрических матриц из* $M_n(F)$*, т. е. матриц* $A \in M_n(F)$*, для которых* $A' = A$*, является подпространством пространства* $M_n(F)$ *над полем* F*. Является ли это множество подалгеброй в алгебре* $M_n(F)$?

§ 3.2. Базис и размерность векторного пространства

Пусть V — векторное пространство над полем F. Под *набором* векторов $a_1, a_2, \ldots, a_s$ (не обязательно различных между собой!) мы будем понимать их упорядоченную совокупность.

Определение 3.2.1. *Линейной комбинацией* векторов (набора векторов) $a_1, a_2, \ldots, a_s$ векторного пространства V над полем F с коэффициентами $\alpha_1, \alpha_2, \ldots, \alpha_s$ из поля F называется выражение вида $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s$, а также вектор, получающийся в результате выполнения операций в этом выражении. Линейная комбинация называется *тривиальной*, если $\alpha_1 = \alpha_2 = \ldots = \alpha_s = 0$, и *нетривиальной* в противном случае.

Замечание. Из свойств операций, заданных на V, следует, что тривиальная линейная комбинация любого набора векторов всегда равна 0.

Определение 3.2.2. Набор векторов $a_1, a_2, \ldots, a_s$ называется *линейно зависимым*, если существует нетривиальная линейная комбинация векторов этого набора, равная 0. В противном случае набор называется *линейно независимым*.

Иными словами, набор векторов $a_1, a_2, \ldots, a_s$ называется *линейно независимым*, если из равенства $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$ следует, что $\alpha_1 = \alpha_2 = \ldots = \alpha_s = 0$.

Определение 3.2.3. Вектор a *линейно выражается* через набор

векторов $a_1, a_2, \ldots, a_s$, если существует линейная комбинация векторов этого набора, равная вектору a.

Примеры. 1. Набор векторов

$$\begin{gathered} a_1 = (1, 0, \ldots, 0) \\ a_2 = (0, 1, \ldots, 0) \\ \ldots \\ a_n = (0, 0, \ldots, 1) \end{gathered}$$

из $\mathbb{R}^n$, векторы которого составляют строки единичной матрицы, является линейно независимым, поскольку из равенства $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n = (\alpha_1, \alpha_2, \ldots, \alpha_n) = (0, 0, \ldots, 0) = 0$ очевидно следует, что $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.

2. Напротив, набор векторов $a_1 = (1, 1, 1)$, $a_2 = (0, 1, 2)$, $a_3 = (1, 2, 3)$ из $\mathbb{R}^3$ является линейно зависимым, так как $1a_1 + 1a_2 + (-1)a_3 = 0$. Заметим, что в этом случае вектор a_3 линейно выражается через векторы a_1 и a_2: $a_3 = 1a_1 + 1a_2$.

Последнее замечание обобщается следующим образом.

Предложение 3.2.1 (критерий линейной зависимости)**.** *Набор векторов $a_1, a_2, \ldots, a_s$ линейно зависим тогда и только тогда, когда один из этих векторов линейно выражается через предыдущие, т. е. найдётся $i \in \{1, \ldots, s\}$ такое, что $a_i = \beta_1 a_1 + \ldots + \beta_{i-1} a_{i-1}$.*

Замечание. Для удобства мы будем считать, что нулевой вектор и только он один линейно выражается через пустой набор векторов.

Доказательство. Из указанной договорённости следует, что наше утверждение верно для набора, состоящего из одного вектора. Поэтому в дальнейшем мы полагаем, что в нашем наборе есть по крайней мере два вектора.

Докажем необходимость. Пусть имеется нетривиальная комбинация $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s = 0$. Тогда существует $i \in \{1, \ldots, s\}$ такое, что $\alpha_i \neq 0$ и $\alpha_{i+1} = \ldots = \alpha_s = 0$ (возможно, что $i = s$). Отсюда $\alpha_1 a_1 + \ldots + \alpha_{i-1} a_{i-1} + \alpha_i a_i = 0$. Тогда

$$a_i = -\alpha_i^{-1}(\alpha_1 a_1 + \ldots + \alpha_{i-1} a_{i-1}) = (-\frac{\alpha_1}{\alpha_i})a_1 + \ldots + (-\frac{\alpha_{i-1}}{\alpha_i})a_{i-1}$$

и необходимость доказана.

Пусть теперь существует такое i, что $a_i = \beta_1 a_1 + \ldots + \beta_{i-1} a_{i-1}$. Тогда линейная комбинация $\beta_1 a_1 + \ldots + \beta_{i-1} a_{i-1} + (-1)a_i + 0a_{i+1} + \ldots + 0a_s$ равна 0 и нетривиальна, поскольку коэффициент при $a_i = -1$ не равен 0. □

Определение 3.2.4. Пусть A и B — наборы векторов. Набор A *линейно выражается* через набор B, если каждый вектор набора A линейно выражается через векторы набора B. Наборы A и B *эквивалентны*, если A линейно выражается через B, а B линейно выражается через A.

Определение 3.2.5. *Линейной оболочкой* набора A векторов $a_1, a_2, \ldots, a_s$ называется множество векторов, являющихся линейными комбинациями векторов набора A. Линейная оболочка набора A обозначается через $L(A)$ или $\langle A \rangle$.

Таким образом,

$$L(A) = \langle a_1, a_2, \ldots, a_s \rangle = \{\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_s a_s \mid \alpha_i \in F, i = 1, 2, \ldots, s\}.$$

Договоримся считать, что линейной оболочкой пустого набора векторов является нулевое подпространство, т. е. множество векторов, состоящее только из нуль-вектора.

Упражнение 3.2.1.

1. *Линейная оболочка $L(A)$ произвольного набора векторов A векторного пространства V является его подпространством.*

2. *Набор A линейно выражается через набор B тогда и только тогда, когда $L(A) \subseteq L(B)$. В частности, наборы A и B эквивалентны тогда и только тогда, когда $L(A) = L(B)$.*

3. *Если набор B получен из набора A перестановкой векторов, то $L(A) = L(B)$.*

Теперь мы готовы сформулировать и доказать основное техническое утверждение этого параграфа, так называемую *теорему о замене.*

Теорема 3.2.1 (о замене)**.** *Пусть A и B — наборы векторов $a_1, a_2 \ldots, a_r$ и $b_1, b_2, \ldots, b_s$ соответственно, причём набор A линейно независим и линейно выражается через набор B. Тогда $r \leqslant s$ и существует перенумерация набора векторов B такая, что после неё набор B эквивалентен набору векторов $a_1, \ldots, a_r, b_{r+1}, \ldots, b_s$.*

Иными словами, если условия теоремы выполнены, то найдётся r векторов набора B при *замене* которых на векторы набора A получится набор, эквивалентный исходному набору B.

Доказательство. Утверждение теоремы очевидно при $r = 0$. Предположим, что мы доказали теорему в случае, когда A состоит из $r - 1$ вектора, и докажем её для r векторов. Обозначим через A' поднабор набора A, состоящий из векторов $a_1, a_2, \ldots, a_{r-1}$. Очевидно, что A' ли-

нейно выражается через B. Кроме того, из определения линейной независимости несложно вывести, что A' линейно независим как поднабор линейно независимого набора A. Таким образом, наборы A' и B удовлетворяют условиям теоремы, а значит, по нашему предположению, $r-1 \leqslant s$ и существует перенумерация векторов набора B такая, что набор B', состоящий из векторов $a_1, \ldots, a_{r-1}, b_r, \ldots, b_s$, эквивалентен набору B, т. е. $L(B') = L(B)$.

По условию теоремы $a_r \in L(B) = L(B')$. Следовательно, вектор a_r линейно выражается через векторы набора B':

$$a_r = \alpha_1 a_1 + \ldots + \alpha_{r-1} a_{r-1} + \beta_r b_r + \ldots + \beta_s b_s. \tag{1}$$

Если $r-1 = s$ или $\beta_r = \ldots = \beta_s = 0$, то $a_r = \alpha_1 a_1 + \ldots + \alpha_{r-1} a_{r-1}$ и a_r линейно выражается через предыдущие векторы набора A, что в силу предложения 3.2.1 противоречит линейной независимости набора A. Таким образом, $r \leqslant s$ и среди коэффициентов $\beta_r, \ldots, \beta_s$ есть хотя бы один ненулевой. Перенумеруем векторы $b_r, \ldots, b_s$ так, чтобы $\beta_r \neq 0$. Обозначим через B'' набор $a_1, \ldots, a_r, b_{r+1}, \ldots, b_s$. Если мы докажем, что B'' эквивалентен набору B', то из равенств $L(B'') = L(B') = L(B)$ будет следовать утверждение теоремы.

Поскольку векторы $a_1, \ldots, a_{r-1}, b_{r+1}, \ldots, b_s$ принадлежат как набору B'', так и набору B', нам нужно лишь показать, что $a_r \in L(B')$ и $b_r \in L(B'')$. Первое сразу следует из равенства (1). С другой стороны, поскольку $\beta_r \neq 0$, из (1) следует, что вектор b_r равен

$$\left(-\frac{\alpha_1}{\beta_r}\right) a_1 + \ldots + \left(-\frac{\alpha_{r-1}}{\beta_r}\right) a_{r-1} + \frac{1}{\beta_r}\, a_r + \left(-\frac{\beta_{r+1}}{\beta_r}\right) b_{r+1} + \ldots + \left(-\frac{\beta_s}{\beta_r}\right) b_s.$$

Таким образом, $b_r \in L(B'')$. Поэтому наборы B' и B'', а значит, и наборы B и B'' эквивалентны. □

Следствие. *Если два линейно независимых набора эквивалентны, то они состоят из одного и того же числа векторов.*

Определение 3.2.6. Векторное пространство V над полем F называется *конечномерным*, если в V существует конечный набор векторов $v_1, v_2 \ldots, v_s$, линейная оболочка которого совпадает со всем пространством, т. е. $\langle v_1, v_2 \ldots, v_s \rangle = V$.

Определение 3.2.7. *Базисом* (или *базой*) векторного пространства V над полем F называется линейно независимый набор векторов пространства V, линейная оболочка которого совпадает с V.

Теорема 3.2.2 (о базисе)**.** *Пусть V — конечномерное векторное пространство над полем F. Тогда верны следующие утверждения.*

1. *V обладает базисом.*

2. *Два базиса пространства V состоят из одного и того же числа векторов.*

3. *Если выбран базис пространства V, то каждый вектор пространства однозначно представляется в виде линейной комбинации векторов этого базиса.*

4. *Если A — линейно независимый набор векторов $a_1, a_2, \ldots, a_r$ пространства V, то существует базис пространства V, содержащий A в качестве поднабора.*

Доказательство. 1. Пусть $v_1, v_2, \ldots, v_s$ — набор векторов пространства V, линейная оболочка которого совпадает с V. Исключим последовательно (начиная с первого) из него все векторы, которые выражаются через предыдущие. Заметим, что первый вектор требуется исключить только в том случае, если он нулевой. Обозначим получившийся в результате набор векторов через B. В силу предложения 3.2.1 набор B линейно независим. С другой стороны, поскольку любой вектор исходного набора линейно выражается через векторы из B, любой вектор пространства V также линейно выражается через векторы из B. Следовательно, $L(B) = V$, что и требовалось.

2. Пусть B и B' — два базиса пространства V. Поскольку $L(B) = L(B') = V$, наборы B и B' эквивалентны. По следствию из теоремы о замене получаем, что число векторов в этих наборах одно и то же.

3. Пусть B — базис пространства V, состоящий из векторов $b_1, b_2, \ldots, b_n$. Предположим, что некоторый вектор $v \in V$ имеет два представления через векторы базиса: $v = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n = \beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_n b_n$. Тогда линейная комбинация $(\alpha_1 - \beta_1)b_1 + (\alpha_2 - -\beta_2)b_2 + \ldots + (\alpha_n - \beta_n)b_n$ равна 0. Поскольку векторы из B линейно независимы, эта комбинация должна быть тривиальной. Следовательно, $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$ и представление вектора v однозначно.

4. Пусть B — базис пространства V, состоящий из векторов $b_1, b_2, \ldots, b_n$. Набор A линейно независим и линейно выражается через набор B. Следовательно, по теореме о замене существует эквивалентный набору B набор B', состоящий из n векторов и содержащий набор A в качестве поднабора. Поскольку B' эквивалентен B, выполняется $L(B') = L(B) = V$. С другой стороны, если B' линейно зависим, то, исключая из него лишние векторы, как при доказательстве п. 1, мы получим его поднабор из меньшего числа векторов, который являет-

ся базисом пространства, что противоречит п. 2. Таким образом, B' — базис пространства V, содержащий A в качестве поднабора. □

Определение 3.2.8. Число векторов в базисе векторного пространства V называется размерностью пространства и обозначается через $\dim V$.

Замечание. В силу п. 2 теоремы о базисе определение размерности пространства корректно, поскольку любые два базиса состоят из одного и того же числа векторов.

Следствие. *Пусть V — векторное пространство размерности n над полем F. Имеют место следующие утверждения:*

1. *При $m > n$ любые m векторов из V линейно зависимы. Любые n линейно независимых векторов образуют базис пространства V.*

2. *При $m < n$ линейная оболочка любого набора A из m векторов не совпадает с V. Любой набор B из n векторов, для которого $L(B) = V$, образует базис пространства V.*

Упражнение 3.2.2. *Доказать следствие из теоремы о базисе.*

Примеры. 1. Пусть $V = F^n$ — арифметическое векторное пространство над полем F. Тогда V конечномерно, $\dim V = n$, а в качестве базиса можно взять, например, набор:

$$\begin{gathered} a_1 = (1, 0, \ldots, 0), \\ a_2 = (0, 1, \ldots, 0), \\ \ldots \\ a_n = (0, 0, \ldots, 1) \end{gathered}$$

из F^n, векторы которого составляют строки единичной матрицы из $M_n(F)$.

2. Если мы обозначим через E^2 (E^3) пространство геометрических векторов плоскости (пространства), то любые два неколлинеарных (три некомпланарных) вектора этого пространства образуют базис. В частности, $\dim E^2 = 2$ и $\dim E^3 = 3$.

3. Поле $\mathbb{C}$ комплексных чисел, рассматриваемое как векторное пространство над полем $\mathbb{R}$ действительных чисел, имеет размерность 2. Базисом этого пространства является, в частности, набор, состоящий из 1 и i, поскольку любое комплексное число однозначно представимо в виде $a + bi$, где $a, b \in \mathbb{R}$.

4. Векторное пространство $V = \mathbb{R}[x]$ многочленов от одной переменной над полем $\mathbb{R}$ действительных чисел не является конечномерным.

Докажем это. Предположим, что V имеет конечный базис, состоящий из многочленов $f_1, \ldots, f_n$. Обозначим через m наибольшую степень многочленов из этого базиса (степенью многочлена называется максимальная степень входящего в него одночлена с ненулевым коэффициентом). Тогда степень любого многочлена, являющегося линейной комбинацией многочленов $f_1, f_2, \ldots, f_n$, не превосходит m. В частности, многочлен x^{m+1} не выражается через $f_1, f_2, \ldots, f_n$. Полученное противоречие показывает, что V не конечномерно.

Упражнение 3.2.3. *Докажите, что набор векторов $b_1, b_2, \ldots, b_n$ арифметического пространства F^n является базисом этого пространства тогда и только тогда, когда матрица, строками которой являются упорядоченные n-ки $b_1, b_2, \ldots, b_n$, невырождена.*

Упражнение 3.2.4. *Докажите, что пространство $M_{m\times n}(F)$ матриц конечномерно. Найдите базис и размерность этого пространства.*

Упражнение 3.2.5. *Докажите, что пространство $F(X, K)$ всех функций из множества X в поле K конечномерно тогда и только тогда, когда множество X конечно. Найдите размерность этого пространства в случае, когда $|X| = n$.*

Указание. Рассмотрите набор функций φ_a (здесь a пробегает всё множество X), каждая из которых действует по правилу:

$$\varphi_a(x) = \begin{cases} 1, & \text{если } x = a, \\ 0, & \text{если } x \neq a. \end{cases}$$

Мы определили базис векторного пространства как набор векторов, который с одной стороны линейно независим, а с другой обладает тем свойством, что каждый вектор пространства линейно выражается через векторы этого набора. Следующее утверждение показывает, что базис можно определить, используя каждое из этих свойств по отдельности.

Предложение 3.2.2. *Пусть B — набор векторов конечномерного векторного пространства V. Следующие утверждения эквивалентны.*

1. *B — базис пространства V.*

2. *B — максимальный линейно независимый набор векторов пространства V.*

3. *B — минимальный набор векторов пространства, линейная оболочка которого совпадает со всем пространством V.*

Замечание. Максимальность (минимальность) набора с заданным свойством означает, что если мы добавим к набору (исключим из на-

бора) произвольный вектор, то набор перестанет обладать указанным свойством.

Доказательство. (1 ⇒ 2). Поскольку каждый вектор v пространства V выражается через векторы базиса B, добавление v к B приведёт к тому, что полученный набор перестанет быть линейно независимым.

(2 ⇒ 1). Из максимальности B следует, что любой вектор, не входящий в B, линейно выражается через векторы из B. Следовательно, $L(B) = V$ и B — базис.

(1 ⇒ 3). Пусть базис B не является минимальным набором с условием $L(B) = V$. Тогда в B найдётся вектор v, который линейно выражается через остальные векторы из B. Это противоречит линейной независимости набора B.

(3 ⇒ 1). Из минимальности B следует, что ни один из векторов набора B не выражается через остальные. Следовательно, набор B линейно независим. □

Определение 3.2.9. Пусть V — векторное пространство над полем F и $\dim V = n$. Зафиксируем некоторый базис B пространства V, состоящий из векторов $b_1, b_2, \ldots, b_n$. Каждый вектор $v \in V$ единственным образом записывается в виде линейной комбинации $v = \beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_n b_n$ векторов базиса. Упорядоченная n-ка $[v]_B = (\beta_1, \beta_2, \ldots, \beta_n)$ называется *строкой координат* вектора v в базисе B.

Теорема 3.2.3. *Векторное пространство V размерности n над полем F изоморфно арифметическому векторному пространству F^n. Изоморфизмом является отображение $\varphi : V \to F^n$, действующее по правилу $v\varphi = [v]_B$ для некоторого фиксированного базиса B пространства V.*

Доказательство. Поскольку базис B предполагается фиксированным, обозначим строку координат $[v]_B$ вектора v через $[v]$. Тогда $v\varphi = [v]$. Каждый вектор пространства V единственным образом представляется в виде линейной комбинации векторов базиса, а значит, равенство $[u] = [v]$ влечёт равенство $u = v$. Следовательно, отображение φ взаимно однозначно. Поскольку для любой упорядоченной n-ки $(\beta_1, \beta_2, \ldots, \beta_n)$ из F^n вектор $v = \beta_1 b_1 + \beta_2 b_2 + \ldots + \beta_n b_n$ лежит в V, отображение φ — сюръекция. Таким образом, φ — биекция.

Пусть $[u] = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $[v] = (\beta_1, \beta_2, \ldots, \beta_n)$. Тогда $u\varphi + v\varphi = [u] + [v] = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n) = [u + v] = (u + v)\varphi$. Аналогично, для каждого скаляра α имеем $\alpha(v\varphi) = \alpha[v] = [\alpha v] = (\alpha v)\varphi$. Таким обра-

зом, φ сохраняет операции, заданные на V, и, следовательно, является изоморфизмом. □

Следствие. *Два конечномерных векторных пространства одной и той же размерности над одним и тем же полем изоморфны.*

Доказательство. Пусть V и U — векторные пространства над полем F и $\dim V = \dim U = n$. Пространства V и U изоморфны F^n, а значит, изоморфны между собой. □

Рассмотрим теперь вопрос о том, как изменится запись вектора в виде строки координат при переходе от одного базиса пространства к другому.

Пусть V — векторное пространство размерности n над полем F. Пусть A и B — два базиса пространства V, состоящие из векторов $a_1, \ldots, a_n$ и $b_1, \ldots, b_n$ соответственно. Поскольку A — базис, для каждого $i = 1, \ldots, n$ вектор b_i из B линейно выражается через векторы A:

$$b_i = t_{i1}a_1 + \ldots + t_{in}a_n. \tag{2}$$

Обозначим через a и b столбцы высоты n, элементами которых являются векторы базисов A и B. Иными словами,

$$a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \text{ и } b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Тогда равенства (2) можно записать в матричном виде:

$$b = Ta, \text{ где } T = \begin{pmatrix} t_{11} & \ldots & t_{1n} \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \\ t_{n1} & \ldots & t_{nn} \end{pmatrix}.$$

Матрица T называется *матрицей перехода* от базиса A к базису B.

Докажем небольшое вспомогательное утверждение.

Предложение 3.2.3. *Пусть $X = (x_{ij})$, $Y = (y_{ij})$ — $(m \times n)$-матрицы. Пусть a — столбец высоты n, элементы которого — линейно независимые векторы $a_1, \ldots, a_n$. Тогда из равенства $Xa = Ya$ следует равенство $X = Y$.*

Доказательство. Из равенства $Xa = Ya$ следует, что для каждого $i = 1, \ldots, m$ имеет место равенство $x_{i1}a_1 + \ldots + x_{in}a_n = y_{i1}a_1 + \ldots + y_{in}a_n$.

Отсюда $(x_{i1}-y_{i1})a_1+\ldots+(x_{in}-y_{in})a_n=0$. Из линейной независимости векторов $a_1,\ldots,a_n$ следует, что для каждого $i=1,\ldots,m$ и каждого $j=1,\ldots,n$ имеет место равенство $x_{ij}=y_{ij}$, т. е. $X=Y$. □

Пусть v — произвольный вектор пространства V и $[v]_A$, $[v]_B$ — строки координат вектора v в базисах A и B соответственно. Используя матричную форму записи, вектор v можно записать так: $v=[v]_Aa=[v]_Bb$. С другой стороны, $[v]_Bb=[v]_B(Ta)=([v]_BT)a$ (последнее равенство следует из ассоциативности умножения матриц согласованных размеров). В силу предложения 3.2.3 из равенства $[v]_Aa=([v]_BT)a$ получаем равенство $[v]_A=[v]_BT$. Полученный нами результат можно сформулировать следующим образом:

Если T — матрица перехода от базиса A к базису B, то строка координат вектора v в базисе A получается в результате умножения строки координат вектора v в базисе B на матрицу перехода T.

Пусть A, B, C — базисы пространства V, а a, b, c — столбцы, составленные из векторов этих базисов. Пусть T — матрица перехода от базиса A к базису B, S — матрица перехода от базиса B к базису C, а P — матрица перехода от базиса A к базису C. Из равенств $c=Sb=S(Ta)=(ST)a$ и предложения 3.2.3 следует, что матрица перехода P от базиса A к базису C равна ST. В частности, $[v]_A=[v]_CP=[v]_C(ST)$.

Упражнение 3.2.6. *Пусть T — матрица перехода от базиса A к базису B. Тогда матрица T обратима, обратная к ней матрица T^{-1} есть матрица перехода от базиса B к базису A и для любого вектора v имеет место равенство $[v]_B=[v]_AT^{-1}$.*

Указание. В предшествующем рассуждении положите $A=C$ и заметьте, что матрица перехода от базиса A к базису A является единичной.

Упражнение 3.2.7.* *Установите биекцию между всеми базисами пространства V размерности n над полем F и множеством $GL_n(F)$ всех невырожденных квадратных $(n\times n)$-матриц над полем F. В случае, когда поле F имеет конечный порядок q, найдите порядок группы $GL_n(F)$.*

Замечание. Принятый нами способ записи вектора в виде строки координат называется *система вектор-строка*. В некоторых случаях удобнее использовать запись вектора v в некотором базисе B в виде столбца координат (*система вектор-столбец*). Используя принятые нами обозначения и операцию транспонирования матриц, эту запись можно отобразить следующим образом: $v=b'[v]'_B$. Если A — ещё один базис

пространства и $v = a'[a]'_A$, то матрица перехода $\widetilde{T}$ от базиса A к базису B в системе вектор-столбец есть транспонированная матрица перехода в принятой нами системе вектор-строка. Действительно, из равенства $b = Ta$ после транспонирования получим $b' = a'T' = a'\widetilde{T}$. Аналогично, в системе вектор-столбец столбец координат вектора v в базе A выражается следующим образом: $[v]'_A = \widetilde{T}[v]'_B$.

§ 3.3. Взаимное расположение подпространств

Начнём этот параграф с ещё одного определения понятия подпространства.

Определение 3.3.1. Пусть V — векторное пространство над полем F. Подмножество U множества V называется подпространством, если каждая линейная комбинация векторов из U снова лежит в U.

Замечание. В этом определении, которое, очевидно, эквивалентно определению, данному в § 3.1, нам уже не нужно заранее предполагать, что множество U не пусто, поскольку нуль-вектор, как линейная комбинация пустого набора векторов, лежит в U.

Теорема 3.3.1. *Пусть U — подпространство векторного пространства V размерности n над полем F. Тогда выполняются следующие утверждения.*

1. *U — конечномерное векторное пространство, и $\dim U \leqslant n$.*

2. *Каждая база пространства U может быть дополнена до базы пространства V.*

3. *Если $\dim U = n$, то $U = V$.*

Доказательство. 1. Если $U = 0 = \{\overline{0}\}$, то U конечномерно (его база — пустой набор векторов, а размерность равна 0).

Если $U \neq 0$, то найдётся ненулевой вектор $u_1 \in U$. Если $L(u_1) = U$, то $\dim U = 1$ и утверждение доказано (заметим, что $u_1 \in V$, а значит, $\dim V \geqslant \dim U = 1$).

Пусть $U \neq L(u_1)$. Тогда найдётся вектор $u_2 \in U$ такой, что набор u_1, u_2 линейно независим. Если $L(u_1, u_2) = U$, то снова утверждение доказано. Если же $L(u_1, u_2) \neq U$, то снова выбираем вектор $u_3 \in U \setminus L(u_1, u_2)$. Поскольку u_3 нельзя линейно выразить через u_1, u_2, набор векторов u_1, u_2, u_3 линейно независим. Продолжаем этот процесс, получая на каждом шаге линейно независимый набор векторов из U. Поскольку пространство V имеет размерность n, число векторов в этом наборе не может превосходить n (см. утверждение 1 из следствия теоре-

мы о базисе). Значит, наш процесс оборвётся через конечное число шагов. Следовательно, для некоторого неотрицательного целого числа k, не превосходящего n, выполняется $L(u_1, \ldots, u_k) = U$. Откуда $\dim U = k$.

2. Поскольку любой базис U является линейно независимым набором векторов из V, утверждение сразу следует из п. 4 теоремы о базисе.

3. Если $\dim U = n$, то базис B пространства U состоит из n линейно независимых векторов пространства V. В силу п. 1 следствия из теоремы о базисе B является базисом пространства V. □

Определение 3.3.2. Базис пространства V, который содержит некоторый базис пространства U в качестве поднабора, называется *согласованным* с подпространством U.

В силу п. 2 теоремы 3.3.1 для каждого подпространства пространства V найдётся базис, согласованный с этим подпространством. Далее мы докажем, что даже для двух произвольных подпространств всегда найдётся базис пространства, одновременно согласованный с каждым из них.

Определение 3.3.3. Пусть $U_1, U_2, \ldots, U_s$ — подпространства векторного пространства V над полем F. *Суммой* подпространств $U_1, U_2, \ldots, U_s$ называется множество

$$U_1 + U_2 + \ldots + U_s = \sum_{i=1}^{s} U_i = \{u_1 + u_2 + \ldots + u_s \mid u_i \in U_i, i = 1, 2, \ldots, s\}.$$

Упражнение 3.3.1. *Пусть U, W — подпространства пространства V. Докажите следующие утверждения.*

1. *$U \cap W$, $U + W$ — подпространства пространства V.*

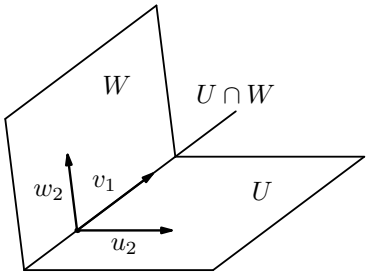
2. *$U + W$ есть пересечение всех подпространств, содержащих и U, и W.*

3. *$U \cup W$ — подпространство тогда и только тогда, когда $U \subseteq W$ или $W \subseteq U$.*

Замечание. В утверждениях упражнения пересечение и объединение понимаются в теоретико-множественном смысле. Используя индукцию по s, несложно проверить, что сумма и пересечение подпространств $U_1, U_2, \ldots, U_s$ являются подпространствами пространства V.

Теорема 3.3.2. *Пусть U, W — подпространства конечномерного пространства V над полем F. Найдётся базис пространства V, согласованный с каждым из подпространств.*

Доказательство. Пусть $v_1, \ldots, v_r$ — базис пересечения $U \cap W$ (возможно, пустой). Пусть $v_1, \ldots, v_r, u_{r+1}, \ldots, u_s$ — базис пространства U, а $v_1, \ldots, v_r$, $w_{r+1}, \ldots, w_t$ — базис пространства W. Заметим, что оба эти базиса согласованы с $U \cap W$.



Если мы докажем, что набор векторов $v_1, \ldots, v_r$, $u_{r+1}, \ldots, u_s$, $w_{r+1}, \ldots, w_t$ линейно независим, то, дополнив его до базиса всего пространства, получим требуемое. Предположим, что линейная комбинация векторов данного набора равна нулю:

$$\alpha_1 v_1 + \ldots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \ldots + \alpha_s u_s + \beta_{r+1} w_{r+1} + \ldots + \beta_t w_t = 0.$$

Откуда

$$\alpha_1 v_1 + \ldots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \ldots + \alpha_s u_s = -(\beta_{r+1} w_{r+1} + \ldots + \beta_t w_t).$$

Вектор, стоящий в левой части последнего равенства, лежит в U, а вектор, стоящий в его правой части, лежит в W. Поскольку левая и правая части равны, вектор z, равный левой (или правой) части равенства, лежит в $U \cap W$. Поскольку $v_1, \ldots, v_r$ — базис $U \cap W$, выполняется

$$z = \gamma_1 v_1 + \ldots + \gamma_r v_r = -(\beta_{r+1} w_{r+1} + \ldots + \beta_t w_t).$$

Следовательно,

$$\gamma_1 v_1 + \ldots + \gamma_r v_r + \beta_{r+1} w_{r+1} + \ldots + \beta_t w_t = 0.$$

В силу того, что $v_1, \ldots, v_r, w_{r+1}, \ldots, w_t$ — базис пространства W, имеем $\gamma_1 = \ldots = \gamma_r = \beta_{r+1} = \ldots = \beta_t = 0$. Отсюда $z = 0$. Следовательно, $\alpha_1 v_1 + \ldots + \alpha_r v_r + \alpha_{r+1} u_{r+1} + \ldots + \alpha_s u_s = 0$. Поскольку $v_1, \ldots, v_r, u_{r+1}, \ldots, u_s$ — базис пространства U, выполняется $\alpha_1 = \ldots = \alpha_s = 0$, что и требовалось доказать. □

Следствие. *Если U, W — подпространства конечномерного пространства V, то* $\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$.

Доказательство. Из определения суммы следует, что U и W — подпространства пространства $U+W$. Сохраняя обозначения теоремы, докажем, что $U+W = \langle v_1, \ldots, v_r, u_{r+1}, \ldots, u_s, w_{r+1}, \ldots, w_t\rangle$. Для любого $v \in U+W$ имеем $v = u + w = (\alpha_1 v_1 + \ldots + \alpha_r v_r + \alpha_{r+1}u_{r+1} + \ldots + \alpha_s u_s) + (\beta_1 v_1 + \ldots + \beta_r v_r + \beta_{r+1}w_{r+1} + \ldots + \beta_t w_t) = (\alpha_1 + \beta_1)v_1 + \ldots + (\alpha_r + \beta_r)v_r + \alpha_{r+1}u_{r+1} + \ldots + \alpha_s u_s + \beta_{r+1}w_{r+1} + \ldots + \beta_t w_t$. Таким образом, $v_1, \ldots, v_r, u_{r+1}, \ldots, u_s, w_{r+1}, \ldots, w_t$ — базис пространства $U+W$. Поэтому $\dim(U+W) = s + (t-r) = \dim U + \dim W - \dim(U \cap W)$. □

Упражнение 3.3.2. *Пусть $U_1, U_2, \ldots, U_s$ — подпространства векторного пространства V и S — сумма этих подпространств. Тогда* $\dim S \leqslant \sum_{i=1}^{s} \dim U_i$.

Указание. Используя следствие из теоремы 3.3.2, *провести рассуждение индукцией по s.*

Определение 3.3.4. Пусть $U_1, U_2, \ldots, U_s$ — подпространства векторного пространства V над полем F. Сумма $U_1 + U_2 + \ldots + U_s$ этих подпространств называется *прямой суммой*, если из равенства $u_1 + u_2 + \ldots + u_s = 0$, где $u_i \in U_i$, $i = 1, 2, \ldots, s$, следует $u_1 = u_2 = \ldots = u_s = 0$. Прямая сумма подпространств $U_1, U_2, \ldots, U_s$ обозначается

$$U_1 \oplus U_2 \oplus \ldots \oplus U_s \text{ или } \bigoplus_{i=1}^{s} U_i.$$

Теорема 3.3.3. *Пусть $U_1, U_2, \ldots, U_s$ — подпространства конечномерного векторного пространства V над полем F и $S = U_1 + U_2 + \ldots + U_s$ — сумма этих подпространств. Следующие утверждения эквивалентны.*

1. *S — прямая сумма.*

2. *Каждый вектор $v \in S$ единственным образом записывается в виде суммы $v = u_1 + u_2 + \ldots + u_s$, где $u_i \in U_i$, $i = 1, 2, \ldots, s$.*

3. *Набор векторов, составленный из баз подпространств U_1, U_2, $\ldots$, U_s, есть база пространства S.*

4. $\dim S = \sum_{i=1}^{s} \dim U_i$.

5. *Пусть $S_j = U_1 + \ldots + U_{j-1} + U_{j+1} + \ldots + U_s$. Для каждого $j \in \{1, 2, \ldots, s\}$ имеет место $U_j \cap S_j = 0$.*

Доказательство. $(1 \Rightarrow 2)$. Пусть для некоторого $v \in S$ выполняется $v = u_1 + u_2 + \ldots + u_s = w_1 + w_2 + \ldots + w_s$, где $u_i, w_i \in U_i$. Тогда

$(u_1 - w_1) + (u_2 - w_2) + \ldots + (u_s - w_s) = 0$, а значит, $u_1 = w_1$, $u_2 = w_2$, $\ldots$, $u_s = w_s$.

$(2 \Rightarrow 3)$. Пусть для каждого $i = 1, 2, \ldots, s$ набор B_i векторов $b_{i1}, \ldots, b_{it_i}$ — базис пространства U_i. Нам нужно показать, что набор B, составленный из наборов $B_1, B_2, \ldots, B_s$, является базой пространства S. Поскольку $S = \sum_{i=1}^{s} U_i$, выполняется $L(B) = S$. Остаётся показать, что набор B линейно независим. Предположим, что

$$\sum_{i=1}^{s} \sum_{j=1}^{t_i} \alpha_{ij} b_{ij} = 0. \tag{1}$$

Для $i = 1, 2, \ldots, s$ положим $u_i = \sum_{j=1}^{t_i} \alpha_{ij} b_{ij}$. Тогда $\sum_{i=1}^{s} u_i = 0$. Поскольку нуль-вектор единственным образом записывается в сумму u_i, для каждого $i = 1, 2, \ldots, s$ имеем $u_i = 0$. Из линейной независимости наборов B_i следует, что все коэффициенты α_{ij} в равенстве (1) равны 0.

$(3 \Rightarrow 4)$. Очевидно.

$(4 \Rightarrow 5)$. Заметим, что для каждого $j \in \{1, 2, \ldots, s\}$ выполняется $S = U_j + S_j$. По условию $\dim S = \sum_{i=1}^{s} \dim U_i$. С другой стороны, в силу следствия из теоремы 3.3.2 имеем $\dim S = \dim U_j + \dim S_j - \dim(U_j \cap S_j)$. Отсюда $\sum_{i=1, i\neq j}^{s} \dim U_i = \dim S_j - \dim(U_j \cap S_j)$. Поскольку из утверждения упражнения 3.3.2 следует, что $\dim S_j \leqslant \sum_{i=1, i\neq j}^{s} \dim U_i$, имеем $\dim(U_j \cap S_j) = 0$. Следовательно, $U_j \cap S_j = 0$.

$(5 \Rightarrow 1)$. Пусть $\sum_{i=1}^{s} u_i = 0$ и существует $j \in \{1, 2, \ldots, s\}$ такое, что $u_j \neq 0$. Тогда из равенства $u_j = -u_1 + \ldots + (-u_{j-1}) + (-u_{j+1}) + \ldots + (-u_s)$ следует, что $u_j \in U_j \cap S_j$; противоречие. □

Замечание. Из п. 5 теоремы следует, что сумма $U + W$ двух подпространств U и W является прямой тогда и только тогда, когда $U \cap W = 0$.

Упражнение 3.3.3. *Приведите пример трёх подпространств, все попарные пересечения которых равны нулю, а их сумма не является прямой.*

Определение 3.3.5. Пусть $V = U \oplus W$. Тогда каждый вектор $v \in V$ однозначно представляется в виде $v = u + w$, где $u \in U$, $w \in W$. Вектор u называется *проекцией* вектора v на пространство U параллельно пространству W.

Замечание. Определение проекции u вектора v зависит как от выбора подпространства U, так и выбора подпространства W (поскольку такой выбор не определяется однозначно выбором U).

Определение проекции несложно перенести на случай прямой суммы

нескольких подпространств. В этом случае проектирование на одно из них происходит параллельно прямой сумме остальных.

Примеры. 1. Пусть набор B векторов $b_1, b_2, \ldots, b_n$ — базис пространства V над полем F. Тогда $V = \langle b_1\rangle \oplus \langle b_2\rangle \oplus \ldots \oplus \langle b_n\rangle$ есть прямая сумма n одномерных подпространств. Проекция вектора $v \in V$ на $\langle b_i\rangle$ есть вектор $\alpha_i b_i$, где α_i — это i-я координата вектора v в базисе B.

2. Рассмотрим пространство $V = F[\mathbb{R}, \mathbb{R}]$ всех функций на вещественной прямой. Обозначим через V_+, V_- подмножества множества V всех чётных и всех нечётных функций соответственно. Несложно проверить, что V_+ и V_- — подпространства пространства V. Пусть $f \in F[\mathbb{R}, \mathbb{R}]$. Зададим функции f_+ и f_- следующим образом: $f_+(x) = \frac{1}{2}(f(x)+f(-x))$ и $f_-(x) = \frac{1}{2}(f(x)-f(-x))$. Тогда f_+ — чётная функция, f_- — нечётная функция и $f = f_+ + f_-$. Следовательно, $V = V_+ + V_-$. С другой стороны, $V_+ \cap V_- = 0$. Поэтому $V = V_+ \oplus V_-$. Отметим, что в этом примере и само пространство, и два подпространства, в прямую сумму которых оно разлагается, бесконечномерны.

Напомним, что квадратная матрица A называется *симметрической*, если $A' = A$. Квадратная матрица A называется *кососимметрической*, если $A' = -A$. В силу утверждения (3) упражнения 3.1.3 подмножество всех симметрических матриц пространства $M_n(F)$ является подпространством.

Упражнение 3.3.4. *Проверьте, что подмножество всех кососимметрических матриц пространства $M_n(F)$ квадратных матриц является подпространством. Докажите, что векторное пространство $M_n(F)$ есть прямая сумма подпространств симметрических и кососимметрических матриц.*

Глава 4

Системы линейных уравнений

§ 4.1. Ранг матрицы

Эта глава посвящена системам линейных уравнений. Однако в первом параграфе мы введём и обсудим понятие ранга матрицы. Используя это понятие, в следующем параграфе мы сформулируем критерий совместности системы линейных уравнений.

Определение 4.1.1. Пусть A — набор векторов $a_1, a_2, \ldots, a_s$ векторного пространства V над полем F. *Рангом набора* A называется размерность его линейной оболочки $L(A)$. Ранг набора A обозначается через $r(A)$.

Пусть ранг набора A равен r. Отметим, что, рассуждая, как при доказательстве п. 1 теоремы о базисе, несложно выбрать r векторов набора A, составляющих базис $L(A)$. Иногда, допуская некоторую вольность речи, мы будем называть выбранные таким образом векторы *базисом набора*.

Определение 4.1.2. Пусть A — $(m \times n)$-матрица над полем F. Обозначим через $a_1, \ldots, a_m$ строки, а через $\widetilde{a}_1, \ldots, \widetilde{a}_n$ столбцы матрицы A. Строки матрицы A можно рассматривать как векторы пространства F^n, а её столбцы — как векторы пространства F^m. *Строчный ранг* матрицы A — это ранг набора $a_1, \ldots, a_m$. *Столбцевой ранг* матрицы A — это ранг набора $\widetilde{a}_1, \ldots, \widetilde{a}_n$.

Оказывается, для любой матрицы её строчный и столбцевой ранги совпадают. Мы докажем это утверждение, называемое теоремой о ранге матрицы, показав, что оба указанных числа равны третьему, так называемому *минорному рангу*. В § 2.3 было введено понятие минора, дополнительного к элементу матрицы. Теперь нам потребуется более общий термин.

Определение 4.1.3. Пусть $A = (a_{ij})$ — $(m \times n)$-матрица над полем F и r — некоторое натуральное число такое, что $r \leqslant \min\{m, n\}$. Пусть выбраны некоторые r строк и r столбцов матрицы A. Квадратная матрица M, составленная из элементов матрицы A, стоящих на

пересечении данных r строк и r столбцов, взятых в соответствующем расположении, называется *минором* размерности r матрицы A. Более точно, если выбраны строки с номерами $i_1, \ldots, i_r$ и столбцы с номерами $j_1, \ldots, j_r$, то элемент m_{kl} минора M равен a_{i_k, j_l}.

Замечание. Следуя традиции, было бы точнее назвать минором определитель матрицы, которую мы назвали минором. Тем не менее мы фиксируем определение минора как матрицы, а не как её определителя, считая его более удобным.

Пример. Пусть

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 2 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \text{ Тогда } M = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \text{ — минор размерности 2,}$$

составленный из элементов матрицы A, стоящих на пересечении первой, второй строки и первого, третьего столбцов.

Упражнение 4.1.1. *Если $C_k^r = \frac{k!}{r!(k-r)!}$ — число сочетаний из k предметов по r, то число миноров размерности r в $(m \times n)$-матрице равно $C_m^r \cdot C_n^r$.*

Определение 4.1.4. *Минорным рангом* матрицы A называется наибольшая размерность её невырожденного минора. Иными словами, минорный ранг матрицы равен r, если в ней есть хотя бы один невырожденный минор размерности r и нет невырожденных миноров размерности $r+1$.

Пример. В предыдущем примере ранг матрицы A равен 2. Невырожденным минором размерности 2 является минор M.

Теорема 4.1.1 (о ранге матрицы)**.** *Пусть $A = (a_{ij})$ — $(m \times n)$-матрица над полем F. Строчный, столбцевой и минорный ранги матрицы A совпадают.*

Доказательство. Мы докажем, что строчный ранг равен минорному. Доказательство того факта, что столбцевой ранг совпадает с минорным, а значит, и со строчным, проводится аналогично с одновременной заменой слова *строка* на слово *столбец* и наоборот.

Пусть минорный ранг матрицы A равен r. Это означает, что можно выбрать r строк и r столбцов матрицы A так, что на их пересечении стоит минор M размерности r, определитель которого не равен 0. Кроме того, все миноры размерности $r+1$ матрицы A, если такие миноры вообще существуют, вырождены. Не теряя общности, мы можем считать,

что невырожденный минор M стоит на пересечении первых r строк и первых r столбцов. Действительно, это предположение просто позволяет нам вместо номеров $i_1, i_2, \ldots, i_r$ использовать номера $1, 2, \ldots, r$ для обозначения соответствующих строк. То же верно и для обозначений столбцов. Итак, пусть $M = (a_{ij})$, где $i, j \in \{1, 2, \ldots, r\}$.

Обозначим через a_i i-ю строку матрицы A, а через $\overline{a}_i$ i-ю строку минора M. Тогда для $i \in \{1, 2, \ldots, r\}$ строка $\overline{a}_i$ — подстрока строки a_i, состоящая из первых её r элементов. Предположим, что строки $a_1, a_2, \ldots, a_r$ линейно зависимы как векторы арифметического пространства F^n, т. е. найдётся нетривиальная линейная комбинация этих строк, равная нулю. Тогда линейная комбинация с теми же самыми коэффициентами строк $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_r$ как векторов пространства F^r тоже, очевидно, равна нулю. Следовательно, они линейно зависимы. Но тогда в силу утверждения упражнения 3.2.3 имеем $\det M = 0$; противоречие. Итак, строки $a_1, a_2, \ldots, a_r$ матрицы A линейно независимы, т. е. её строчный ранг больше либо равен r.

Если $m = r$, то теорема доказана. Поэтому мы можем считать, что $m > r$. Докажем, что строки матрицы A с номером, большим r, линейно выражаются через первые r строк. Очевидно, что достаточно доказать это для какой-то одной строки. Например, для $(r+1)$-ой. Пусть $\overline{a}_{r+1} = (a_{r+1,1}, a_{r+1,2}, \ldots, a_{r+1,r})$. Поскольку r строк $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_r$ пространства F^r линейно независимы, они образуют базис в этом пространстве. Следовательно, строка $\overline{a}_{r+1}$ является их линейной комбинацией: $\overline{a}_{r+1} = \alpha_1\overline{a}_1 + \alpha_2\overline{a}_2 + \ldots + \alpha_r\overline{a}_r$. Обозначим через b строку пространства F^n, равную $a_{r+1} - (\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_r a_r)$. Если мы докажем, что $b = (\beta_1, \beta_2, \ldots, \beta_n) = \overline{0}$, то получим требуемое. Отметим, что в силу выбора коэффициентов $\alpha_1, \alpha_2, \ldots, \alpha_r$ первые r элементов строки b уже равны нулю. Пусть найдётся элемент β_i $(i > r)$ такой, что $\beta_i \neq 0$. Опять не теряя общности можно считать, что $i = r+1$. Рассмотрим минор M^* размерности $r+1$ матрицы A, составленный из первых $r+1$ строк и первых $r+1$ столбцов.

$$\left(\begin{array}{|ccc|c} a_{11} & \ldots & a_{1r} & a_{1,r+1} \\ \vdots & M & \vdots & \vdots \\ a_{r1} & \ldots & a_{rr} & a_{r,r+1} \\ \hline a_{r+1,1} & \ldots & a_{r+1,r} & a_{r+1,r+1} \end{array}\right) \longrightarrow \left(\begin{array}{|ccc|c} a_{11} & \ldots & a_{1r} & a_{1,r+1} \\ \vdots & M & \vdots & \vdots \\ a_{r1} & \ldots & a_{rr} & a_{r,r+1} \\ \hline 0 & \ldots & 0 & \beta_{r+1} \end{array}\right)$$

По условию $\det M^* = 0$. Вычтем из последней строки минора M^*

последовательно первую строку, умноженную на α_1, вторую строку, умноженную на α_2, ..., r-ю строку, умноженную на α_r. Полученная в результате матрица M^{**} будет иметь определитель, равный определителю матрицы M^*. С другой стороны, все элементы её $r+1$-ой строки, а это $\beta_1, \beta_2, \ldots, \beta_{r+1}$, кроме, быть может, последнего, равны нулю. Разложив определитель матрицы M^{**} по последней строке, получим $0 = \det M^* = \det M^{**} = \beta_{r+1} \det M$. Поскольку $\det M \neq 0$, выполняется равенство $\beta_{r+1} = 0$, что противоречит выбору β_{r+1}. Таким образом, $b = 0$ и $a_{r+1} = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_r a_r$. □

Определение 4.1.5. Строчный (столбцевой, минорный) ранг матрицы A называется её *рангом* и обозначается через $r(A)$.

Следствие. *Ранг квадратной $(n \times n)$-матрицы A равен n тогда и только тогда, когда* $\det A \neq 0$.

Замечание. Минор M^* размерности $r+1$, полученный из минора M размерности r в результате добавления некоторой строки и некоторого столбца, принято называть минором, *окаймляющим* минор M. Изучив доказательство теоремы о ранге, обоснуйте следующее утверждение.

Упражнение 4.1.2. *Если все окаймляющие миноры невырожденного минора размерности r матрицы A равны нулю или их вообще нет, то ранг матрицы A равен r.*

Утверждение, сформулированное в упражнении, указывает способ вычисления ранга (в данном случае минорного ранга) матрицы. Однако на практике проще найти строчный ранг матрицы, используя её приведение к так называемому ступенчатому виду. Ступенчатая матрица — это матрица вида

$$\begin{pmatrix} a_{1j_1} & \ldots & \ldots & \ldots & \ldots \\ & a_{2j_2} & \ldots & \ldots & \ldots \\ & & \ldots & \ldots & \ldots \\ & & & \ldots & \ldots \\ & & & & a_{rj_r} \quad \ldots \\ & & 0 & & \end{pmatrix} \tag{1}$$

Точнее,

Определение 4.1.6. Назовём *ведущим* элементом ненулевой строки матрицы её первый слева ненулевой элемент. Матрица называется *ступенчатой*, если выполнены следующие условия:

1) номера столбцов ведущих элементов ненулевых строк матрицы образуют строго возрастающую последовательность;

2) нулевые строки, если они есть, стоят в конце.

Несложно заметить, что ранг ступенчатой матрицы равен числу ненулевых строк. В частности, у представленной матрицы невырожденным является минор, стоящий на пересечении первых r строк и столбцов с номерами $j_1, j_2, \ldots, j_r$, а невырожденных миноров размерности $(r+1)$, очевидно, не имеется.

Напомним, что мы назвали *элементарными* следующие преобразования строк (столбцов) матрицы:

1) прибавление к строке (столбцу) другой строки (другого столбца), умноженной на скаляр;

2) умножение строки (столбца) на ненулевой скаляр.

Добавим к этим преобразованиям ещё один тип преобразований:

3) перестановка двух строк (столбцов) местами.

Отметим, что любое преобразование третьего типа можно представить в виде цепочки последовательных преобразований первого и второго типов, и в этом смысле его введение является *избыточным*. Причина его добавления — удобство при применении.

Практическое разыскание ранга матрицы основано на двух следующих утверждениях.

Предложение 4.1.1. *При элементарных преобразованиях строк (столбцов) матрицы A её ранг не меняется.*

Доказательство. Достаточно заметить, что строки a_i, a_j линейно выражаются через строки $a_i + \alpha a_j$ и a_j, а строка a_i — через строку αa_i, если $\alpha \neq 0$. □

Предложение 4.1.2. *Каждая матрица приводится элементарными преобразованиями строк к ступенчатому виду.*

Доказательство. Утверждение доказывается индукцией по числу m строк матрицы $A = (a_{ij})_{m\times n}$. Пусть j_1 — наименьший номер столбца матрицы A, содержащего ненулевой элемент. Переставив при необходимости строки местами, получим матрицу, в которой элемент, стоящий на месте $(1, j_1)$, не равен нулю. Используя элементарные преобразования первого типа, занулим с помощью этого элемента все остальные

элементы j_1-го столбца. В результате получится матрица вида

$$\left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & a_{1j_1} & * & \dots & * \\ \hline & & & 0 & & & \\ & 0 & & \vdots & & \mathbf{A_1} & \\ & & & 0 & & & \end{array}\right).$$

В силу предположения индукции матрицу A_1 можно привести элементарными преобразованиями к ступенчатому виду. В результате вся матрица A будет приведена к виду (1). □

Мы завершаем этот параграф утверждением о ранге суммы и произведения матриц.

Предложение 4.1.3.

1. *Пусть* $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{m\times n}$ — *матрицы над полем* F. *Тогда* $r(A+B) \leqslant r(A) + r(B)$.

2. *Пусть* $A = (a_{ij})_{m\times s}$, $B = (b_{ij})_{s\times n}$ — *матрицы над полем* F. *Тогда* $r(AB) \leqslant r(A)$ *и* $r(AB) \leqslant r(B)$.

Доказательство. 1. Пусть $C = (c_{ij})_{m\times n} = A+B$. Рассмотрим матрицы A, B, C как наборы векторов арифметического пространства F^n, состоящие из строк этих матриц. Поскольку для каждого $i = 1, 2, \dots, m$ выполняется $c_i = a_i + b_i$, имеем $L(C) \subseteq L(A) + L(B)$. Следовательно, $r(C) = \dim L(C) \leqslant \dim(L(A) + L(B)) \leqslant \dim L(A) + \dim L(B) = r(A) + r(B)$.

2. Пусть $C = (c_{ij})_{m\times n} = AB$. Докажем сначала, что $r(C) \leqslant r(B)$. Рассмотрим матрицы B, C как наборы векторов арифметического пространства F^n, состоящие из строк этих матриц. Поскольку для каждого $i = 1, 2, \dots, m$ выполняется $c_i = (c_{i1}, \dots, c_{in}) =$

$$= \left(\sum_{k=1}^{s} a_{ik}b_{k1}, \dots, \sum_{k=1}^{s} a_{ik}b_{kn}\right) = \sum_{k=1}^{s} a_{ik}(b_{k1}, \dots, b_{kn}) = \sum_{k=1}^{s} a_{ik}b_k,$$

набор C линейно выражается через набор B. Отсюда $L(C) \subseteq L(B)$ и $r(C) \leqslant r(B)$.

Доказательство неравенства $r(C) \leqslant r(A)$ проводится аналогично. Нужно лишь рассмотреть наборы столбцов матриц A и C. □

§ 4.2. Совместность системы линейных уравнений

Определение 4.2.1. *Системой линейных уравнений над полем* F *от* (или *относительно*) *неизвестных* $x_1, x_2, \ldots, x_n$ называется упорядоченный набор

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} \tag{1}$$

выражений вида $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = b_i$ $(i = 1, 2, \ldots, m)$, где $a_{ij}, b_i \in F$. Каждое из этих выражений называется *уравнением системы* (1). Элементы a_{ij} называются *коэффициентами при неизвестных*, а элементы b_i — *свободными коэффициентами системы*.

Определение 4.2.2. Строка $x^0 = (x_1^0, x_2^0, \ldots, x_n^0) \in F^n$ называется *решением системы* (1), если для каждого $i = 1, 2, \ldots, m$ имеет место равенство $a_{i1}x_1^0 + a_{i2}x_2^0 + \ldots + a_{in}x_n^0 = b_i$. Система называется *совместной*, если она имеет хотя бы одно решение. Две системы линейных уравнений над одним и тем же полем и от одних и тех же переменных называются *эквивалентными* (или *равносильными*), если множества их решений совпадают.

Обозначим через a_j столбец $(a_{1j}, a_{2j}, \ldots, a_{mj})'$ коэффициентов системы (1) при неизвестной x_j для каждого $j = 1, 2, \ldots, n$, а через b — столбец $(b_1, b_2, \ldots, b_m)'$ свободных коэффициентов системы (1). Тогда систему (1) можно записать в виде

$$x_1a_1 + x_2a_2 + \ldots + x_na_n = b. \tag{2}$$

Этот вид называется *векторной формой* системы (1).

Составим из коэффициентов системы (1) матрицу $A = (a_{ij})_{m\times n}$. Она называется *матрицей коэффициентов* или просто *матрицей системы* (1). Запишем систему (1) в виде

$$Ax' = b. \tag{3}$$

Этот вид называется *матричной формой* системы (1).

Назовём $(m \times (n+1))$-матрицу $\widetilde{A} = (A \mid b)$, полученную из матрицы A добавлением к ней справа столбца b свободных коэффициентов, *расширенной матрицей* системы (1).

Теорема 4.2.1 (критерий совместности системы линейных уравнений)**.** *Система* (1) *совместна тогда и только тогда, когда ранг матрицы A системы* (1) *равен рангу расширенной матрицы этой системы, т. е.* $r(A) = r(\widetilde{A})$.

Доказательство. Воспользуемся векторной формой (2) записи системы (1). Заметим, что строка $x^0 = (x_1^0, x_2^0, \ldots, x_n^0)$ есть решение системы (1) тогда и только тогда, когда $b = x_1^0 a_1 + x_2^0 a_2 + \ldots + x_n^0 a_n$, т. е. вектор b — линейная комбинация векторов $a_1, a_2, \ldots, a_n$ с коэффициентами $x_1^0, x_2^0, \ldots, x_n^0$. Следовательно, совместность системы (1) равносильна равенству линейных оболочек $\langle a_1, a_2, \ldots, a_n\rangle = \langle a_1, a_2, \ldots, a_n, b\rangle$, а значит, и равенству $r(A) = r(\widetilde{A})$. □

Замечание. Этот критерий также называют теоремой Кронекера–Капелли.

На практике проверить, совместна ли система линейных уравнений, можно следующим образом. Приведём элементарными преобразованиями строк расширенную матрицу $\widetilde{A}$ к ступенчатому виду. При этом к ступенчатому виду будет приведена и матрица A как подматрица матрицы $\widetilde{A}$. Если в полученной ступенчатой матрице есть строка с ведущим элементом, стоящим в последнем столбце, то система несовместна. В противном случае $r(A) = r(\widetilde{A})$ и система совместна.

Для решения совместной системы уравнений вида (1) можно использовать метод, который называется *методом Гаусса*, основанный на справедливости следующего утверждения.

Предложение 4.2.1. *При элементарных преобразованиях уравнений системы* (1)*, соответствующих элементарным преобразованиям строк расширенной матрицы её коэффициентов, множество решений системы не изменяется.*

Доказательство. Прямая проверка, как в доказательстве предложения 4.1.1. □

Изложению метода Гаусса мы и посвятим остаток параграфа.

Определение 4.2.3. Ступенчатая матрица A называется *унифицированной*, если выполнены следующие условия:

1) ведущие элементы её ненулевых строк равны 1;

2) все элементы любого столбца, содержащего ведущий элемент, кроме самого ведущего элемента, равны 0.

Упражнение 4.2.1. *Каждая матрица приводится элементарными преобразованиями строк к унифицированному ступенчатому виду.*

Пусть система линейных уравнений (1) совместна. Приведём расширенную матрицу $\widetilde{A} = (A \mid b)$ её коэффициентов элементарными преобразованиями строк к унифицированному ступенчатому виду. Обозначим получившуюся матрицу, из которой мы убрали все нулевые строки, через $\widetilde{C} = (C \mid d)$. Тогда система

$$Cx' = d \tag{4}$$

равносильна исходной системе $Ax' = b$. Предположим, что $r(\widetilde{A}) = r(A) = r$. Тогда $\widetilde{C}$ — $(r \times (n+1))$-матрица, строки которой линейно независимы. Пусть подстановка

$$\begin{pmatrix} 1 & \dots & r & \dots & n \\ j_1 & \dots & j_r & \dots & j_n \end{pmatrix}$$

выбрана так, что $c_{1j_1} = c_{2j_2} = \ldots = c_{rj_r} = 1$ — ведущие элементы строк матрицы $\widetilde{C}$. Назовём неизвестные $x_{j_1}, \ldots, x_{j_r}$ *связанными*, а неизвестные $x_{j_{r+1}}, \ldots, x_{j_n}$ *свободными*. Перенесём все свободные неизвестные системы (4) вместе со стоящими перед ними коэффициентами в правую часть каждого из уравнений системы. В результате получится система вида

$$\begin{cases} x_{j_1} = -c_{1j_{r+1}}x_{j_{r+1}} - \ldots - c_{1j_n}x_{j_n} + d_1, \\ x_{j_2} = -c_{2j_{r+1}}x_{j_{r+1}} - \ldots - c_{2j_n}x_{j_n} + d_2, \\ \qquad\qquad \ldots \\ x_{j_r} = -c_{rj_{r+1}}x_{j_{r+1}} - \ldots - c_{rj_n}x_{j_n} + d_r, \end{cases} \tag{5}$$

равносильная системе (4), а значит, и системе (1).

Пусть $t_1, t_2, \ldots, t_{n-r}$ — произвольный упорядоченный набор из $n-r$ элементов поля F. Определим элементы строки x^0 пространства F^n следующим образом: $x_i^0 = f_i(t_1, t_2 \ldots, t_{n-r})$ для $i = 1, \ldots, n$, где $f_{j_i}(t_1, t_2, \ldots, t_{n-r}) = -c_{ij_{r+1}}t_1 - \ldots - c_{ij_n}t_{n-r} + d_i$ при $i = 1, \ldots, r$ и $f_{j_i}(t_1, t_2, \ldots, t_{n-r}) = t_{i-r}$ при $i = r+1, \ldots, n$. Тогда x^0 — решение системы (5). С другой стороны, если $x^0 = (x_1^0, x_2^0, \ldots, x_n^0)$ — произвольное решение системы (5), то, положив $t_1 = x_{j_{r+1}}^0, \ldots, t_{n-r} = x_{j_n}^0$, получим, что любое решение системы (5) может быть записано в виде $x^0 = (f_1(t_1, \ldots, t_{n-r}), \ldots, f_n(t_1, \ldots, t_{n-r}))$. Поскольку системы (1) и (5) эквивалентны, мы получили общее решение системы (1). Уточним полученный результат следующим образом.

Определение 4.2.4. Пусть F — поле. Упорядоченная n-ка функций $(f_1(t_1, \ldots, t_s), \ldots, f_n(t_1, \ldots, t_s))$, где $f_i : F^s \to F$, называется *общим ре-*

шением системы (1), если множество решений системы (1) равно множеству

$$\{(f_1(t_1,\dots,t_s),\dots,f_n(t_1,\dots,t_s)) \mid (t_1,\dots,t_s)\in F^s\}.$$

Выше мы фактически доказали следующее утверждение.

Теорема 4.2.2. *Пусть система* (1) *совместна и ранг её матрицы коэффициентов равен* r. *Тогда существуют* n *функций* $f_i : F^{n-r} \to F$ *вида* $f_i(t_1,\dots,t_{n-r}) = \alpha_{i1}t_1 + \dots + \alpha_{i,n-r}t_{n-r} + \beta_i$, *где* $i = 1,2,\dots,n$, *от* $n-r$ *переменных, упорядоченная* n*-ка которых является общим решением системы* (1).

Как следует из утверждения теоремы, каждое частное решение системы получается из общего решения подстановкой на место переменных некоторого набора из $n-r$ элементов поля F. Подчеркнём, что из нашего анализа следует, что, хотя общее решение системы может быть записано различными способами, число переменных, от которых зависят функции, составляющие общее решение системы, является инвариантом системы (1). Это число равно разности между числом неизвестных и рангом матрицы коэффициентов системы.

Иногда общим решением системы (1) называют просто систему (5).

Упражнение 4.2.2. *Для системы*

$$\begin{cases} x_1 + 2x_2 + x_3 = 2, \\ x_1 + 3x_2 + 2x_3 - x_4 = 4, \\ 2x_1 + x_2 - x_3 + 3x_4 = -2, \\ 2x_1 - 2x_3 + 4x_4 = -4 \end{cases} \tag{6}$$

запишите её векторную и матричную формы. Приведите расширенную матрицу системы к ступенчатому виду и проверьте, что система совместна. Приведите полученную матрицу к унифицированному ступенчатому виду и найдите общее решение системы.

Для решения систем уравнений, в которых количество независимых уравнений (ранг матрицы коэффициентов системы) равно количеству неизвестных, применяют также *метод Крамера*, основанный на вычислении определителей специального вида. И хотя для практического разыскания решения системы метод Гаусса удобнее, мы докажем в заключение этого параграфа утверждение, на котором основан метод Крамера, поскольку он имеет существенное теоретическое значение.

Теорема 4.2.3. *Пусть система* (1) *имеет квадратную* ($m = n$) *матрицу* A *коэффициентов и* $\det A \neq 0$. *Тогда система совместна и*

имеет единственное решение $x^0 = (x_1^0, \ldots, x_n^0)$. *Это решение находится по формулам:*

$$x_i^0 = \frac{d_i}{d}, \qquad i = 1, 2, \ldots, n, \tag{7}$$

где $d = |A|$, *а* d_i — *определитель матрицы, полученной из матрицы* A *заменой* i*-го столбца на столбец свободных коэффициентов.*

Доказательство. Запишем данную систему в матричном виде $Ax' = b$. Заметим, что строка $(A^{-1}b)'$ — решение системы. Действительно, $A((A^{-1}b)')' = A(A^{-1}b) = b$. Поэтому система совместна. С другой стороны, если x^0 — решение системы, то $A(x^0)' = b$. Следовательно, $(x^0)' = A^{-1}b$ и, окончательно, $x^0 = (A^{-1}b)' = b'(A^{-1})'$. Таким образом, решение единственно.

Нам осталось доказать, что $b'(A^{-1})' = (\frac{d_1}{d}, \ldots, \frac{d_n}{d})$. По теореме об обратной матрице $(A^{-1})' = (\frac{A_{ij}}{d})$. Перемножая b' и i-ый столбец матрицы $(A^{-1})'$, в силу теоремы о разложении определителя по строке (в данном случае по столбцу) получаем требуемое. □

Замечание. Формулы (7) называют формулами Крамера.

§ 4.3. Однородные системы линейных уравнений

Определение 4.3.1. Система линейных уравнений от n неизвестных над полем F

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0, \end{cases} \tag{1}$$

у которой столбец свободных коэффициентов нулевой, называется *однородной.*

Замечание. Однородная система всегда совместна, поскольку обладает *тривиальным решением* $x^0 = (0, \ldots, 0)$.

Теорема 4.3.1. *Множество* X *решений однородной системы* (1) *является подпространством пространства* F^n. *Размерность пространства* X *равна* $n - r$, *где* r — *ранг матрицы коэффициентов системы.*

Доказательство. Запишем однородную систему (1) в матричном виде $Ax' = 0$. Пусть x^1, x^2 — два решения этой системы (не обязательно различные). Тогда $A((x^1)' + (x^2)') = A(x^1)' + A(x^2)' = 0 + 0 = 0$.

Следовательно, строка $x^0 = x^1 + x^2$ — снова решение системы. Аналогично доказывается, что строка αx^0 является решением системы, если строка x^0 — решение, а α — произвольный скаляр.

Пусть упорядоченная n-ка функций $f_i(t_1, \ldots, t_{n-r})$, где $i = 1, \ldots, n$, есть общее решение системы (1), существующее в силу теоремы 4.2.2. Для $k = 1, \ldots, n-r$ и $i = 1, \ldots, n$ положим $x_i^k = f_i(0, \ldots, 0, 1, 0, \ldots, 0)$, где 1 стоит на k-ом месте. Рассмотрим набор из $n-r$ строк $x^k = (x_1^k, \ldots, x_n^k) \in F^n$. Во-первых, для каждого $k = 1, \ldots, n-r$ строка x^k — решение системы (1). Во-вторых, эти строки линейно независимы, поскольку составленная из них матрица содержит минор размерности $n-r$, равный единичной матрице. В-третьих, любое решение системы можно выразить в виде линейной комбинации строк этого набора. Действительно, произвольное решение можно записать в виде $x^0 = (f_1(\alpha_1, \ldots, \alpha_{n-r}), \ldots, f_n(\alpha_1, \ldots, \alpha_{n-r})) = \alpha_1 x^1 + \ldots + \alpha_{n-r} x^{n-r}$. Таким образом, набор $x^1, \ldots, x^{n-r}$ — базис пространства X. □

Определение 4.3.2. Базис пространства решений однородной системы линейных уравнений называется *фундаментальным набором решений* системы.

Следствие. *Пусть $V = F^n$ — арифметическое векторное пространство размерности n над полем F, а U — подпространство размерности k пространства V. Тогда существует однородная система линейных уравнений от n неизвестных над полем F, пространство решений которой совпадает с U.*

Доказательство. Пусть набор векторов $u_i = (\beta_{i1}, \ldots, \beta_{in})$, где $i = 1, \ldots, k$, является базисом подпространства U. Рассмотрим однородную систему $By' = 0$, матрица коэффициентов которой $B = (\beta_{ij})_{k \times n}$ состоит из записанных построчно коэффициентов этого базиса. Поскольку ранг матрицы B равен k, по теореме 4.3.1 пространство решений системы $By' = 0$ имеет размерность $n-k$. Выберем некоторый фундаментальный набор решений этой системы: $a_i = (\alpha_{i1}, \ldots, \alpha_{in})$, где $i = 1, \ldots, n-k$. Пусть $A = (\alpha_{ij})_{(n-k) \times n}$ — матрица, строки которой являются элементами этого фундаментального набора. Поскольку $\alpha_{i1}\beta_{j1} + \ldots + \alpha_{in}\beta_{jn} = 0$ для каждого $i = 1, \ldots, n-k$ и $j = 1, \ldots, k$, строка u_j является решением однородной системы $Ax' = 0$ для каждого $j = 1, \ldots, k$. Поэтому U лежит в пространстве X решений системы $Ax' = 0$. С другой стороны, ранг матрицы A равен $n-k$, а значит, размерность пространства X равна $n - (n-k) = k$. Следовательно, $U = X$ и следствие доказано. □

Теорема 4.3.2. *Пусть совместная система линейных уравнений $Ax' = b$ имеет матрицу коэффициентов A и $Ax' = 0$ — однородная система с той же матрицей коэффициентов. Пусть x^0 — одно из решений системы $Ax' = b$, X — множество всех решений системы $Ax' = b$, а Z — множество всех решений системы $Ax' = 0$. Тогда $X = x^0 + Z = \{x^0 + z \mid z \in Z\}$.*

Доказательство. Пусть z^0 — решение однородной системы. Тогда $A(x^0 + z^0)' = A(x^0)' + A(z^0)' = b + 0 = b$. Следовательно, $x^0 + Z \subseteq X$. С другой стороны, если x — произвольное решение исходной неоднородной системы, то $A(x - x^0)' = Ax' - A(x^0)' = b - b = 0$. Следовательно, $z = x - x^0$ — решение однородной системы. Поэтому $X \subseteq x^0 + Z$. □

Следствие. *Если система $Ax' = b$ совместна, то она имеет единственное решение тогда и только тогда, когда система $Ax' = 0$ имеет только тривиальное решение.*

Ещё одно утверждение о связи между однородной и неоднородной системами уравнений называют *теоремой Фредгольма.*

Теорема 4.3.3 (Фредгольм)**.** *Пусть даны система линейных уравнений $Ax' = b$ и однородная система $A'y' = 0$, матрица коэффициентов которой есть транспонированная матрица коэффициентов неоднородной системы. Система $Ax' = b$ совместна тогда и только тогда, когда для любого решения y системы $A'y' = 0$ выполняется равенство $yb = 0$.*

Доказательство. Предположим, что система $Ax' = b$ совместна и строка x^0 — некоторое её решение. Тогда выполняется матричное равенство $A(x^0)' = b$. Заметим, что равенство $A'y' = 0$ равносильно равенству $yA = 0$ (одно получается из другого с помощью транспонирования). Следовательно, для каждого y такого, что $A'y' = 0$, выполняется $yb = y(A(x^0)') = (yA)(x^0) = 0$.

Пусть для каждого y такого, что $A'y' = 0$, выполняется $yb = 0$, а значит, и $b'y' = 0$. Тогда пространство решений системы

$$\left(\frac{A'}{b'}\right) y' = 0$$

совпадает с пространством решений системы $A'y' = 0$. Следовательно, имеет место равенство рангов

$$r(A') = r\left(\frac{A'}{b'}\right),$$

которое после транспонирования матриц превращается в равенство $r(A) = r(A \mid b)$. Отсюда в силу теоремы Кронекера–Капелли вытекает совместность системы $Ax' = b$. □

Упражнение 4.3.1. *Рассмотрите однородную систему линейных уравнений с той же матрицей коэффициентов, что и неоднородная система из упражнения* 4.2.2. *Найдите общее решение этой системы и её фундаментальный набор решений. Проверьте справедливость утверждений теорем* 4.3.2 *и* 4.3.3 *на этом примере.*

Отметим, что мы строили теорию систем линейных уравнений над произвольным полем (в том числе и произвольным конечным полем).

Упражнение 4.3.2. *Пусть* $F = \mathbb{Z}_2$ — *поле вычетов по модулю* 2 *и система*

$$\begin{cases} x_2 + x_3 + x_5 = 1, \\ x_1 + x_2 = 1, \\ x_2 + x_3 + x_4 + x_5 = 0, \\ x_1 + x_2 + x_4 = 0 \end{cases}$$

задана над этим полем. Найти все решения данной системы и соответствующей ей однородной системы.

Глава 5

Кольцо многочленов

§ 5.1. Кольцо многочленов от одной переменной

Эта глава посвящена многочленам. Под многочленом (от одной переменной) с действительными коэффициентами обычно понимается функция $f : \mathbb{R} \to \mathbb{R}$ вида $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, где $a_i \in \mathbb{R}$. Однако если рассматривать многочлены над произвольным полем (или даже кольцом), то в случае конечного поля (кольца) определение многочлена как отображения не слишком удачно. Действительно, многочлены x и x^2 над полем $F = \mathbb{Z}_2$ порядка 2, очевидно, совпадают как отображения, так как $0^2 = 0$ и $1^2 = 1$. Поскольку удобнее считать их различными, мы дадим более абстрактное определение многочлена, а потом покажем, что в случае бесконечного поля данное нами определение не отличается от определения многочлена как функции. Для краткости обозначим через $\mathbb{N}_0$ множество $\mathbb{N} \cup \{0\}$ целых неотрицательных чисел.

Определение 5.1.1. Пусть $k \in \mathbb{N}_0$. *Многочленом* (или *полиномом*) f от переменной x над кольцом R называется выражение

$$f(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 x^0 + a_1 x^1 + \ldots + a_k x^k + \ldots,$$

где коэффициенты a_k лежат в кольце R и лишь конечное их число отлично от 0. Ненулевой коэффициент многочлена f с наибольшим индексом называется *старшим коэффициентом* многочлена, а сам этот индекс называется *степенью* многочлена f и обозначается через $\deg f$. Коэффициент многочлена с индексом нуль называется *свободным* коэффициентом. Множество всех многочленов от переменной x над кольцом R обозначается через $R[x]$.

Замечание. Если договориться, что одночлены, т. е. выражения вида $a_k x^k$, с нулевыми коэффициентами при записи многочлена могут быть опущены, то многочлен степени n можно записать в виде $f(x) = a_0 x^0 + a_1 x^1 + \ldots + a_n x^n$. Кроме того, многочлены нулевой степени естественным образом отождествляются с элементами кольца R ($a_0 x^0 = a_0$). Используя это отождествление, мы приходим к привычной

форме записи многочлена $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Отметим также, что нулевой многочлен $0 = \sum_{k=0}^{\infty} 0x^k$ не является многочленом степени 0. Его степень считается неопределённой. Иногда для удобства (об этом ниже) полагают, что $\deg 0 = -\infty$.

Определение 5.1.2. Многочлены $f(x) = \sum_{k=0}^{\infty} a_k x^k$ и $g(x) = \sum_{k=0}^{\infty} b_k x^k$ *равны*, если для любого $k \in \mathbb{N}_0$ имеет место равенство $a_k = b_k$.

Замечание. В силу данного определения многочлены x и x^2 над полем $\mathbb{Z}_2$ должны рассматриваться как различные.

Определение 5.1.3. Пусть R — кольцо и многочлены

$$f(x) = \sum_{k=0}^{\infty} a_k x^k,\ g(x) = \sum_{k=0}^{\infty} b_k x^k \in R[x].$$

Многочлены

$$h(x) = \sum_{k=0}^{\infty} c_k x^k \text{ и } p(x) = \sum_{k=0}^{\infty} d_k x^k \in R[x]$$

называются соответственно *суммой* и *произведением* многочленов f и g, если для любого $k \in \mathbb{N}_0$ выполняется $c_k = a_k + b_k$ и $d_k = \sum_{i+j=k} a_i b_j$. Обозначения: $h = f + g$ и $p = fg$.

Замечание. Данное определение корректно, поскольку $h = f + g$ и $p = fg$ имеют лишь конечное число отличных от нуля коэффициентов, а значит, являются многочленами.

Теорема 5.1.1. *Пусть R — кольцо. Тогда имеют место следующие утверждения.*

1. *$R[x]$ — кольцо относительно операций сложения и умножения многочленов.*

2. *Если R — коммутативное кольцо, то $R[x]$ — коммутативное кольцо.*

3. *Если R — кольцо с единицей, то $R[x]$ — кольцо с единицей.*

Доказательство. Доказательство теоремы представляет собой последовательную проверку аксиом кольца, а также свойств коммутативности и существования единицы. Например, если $f(x) = \sum_{k=0}^{\infty} a_k x^k$, $g(x) = \sum_{k=0}^{\infty} b_k x^k$, $h(x) = \sum_{k=0}^{\infty} c_k x^k$, то закон правой дистрибутивности $fh + gh = (f + g)h$ следует из равенств

$$\sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j = \sum_{i+j=k} (a_i + b_i) c_j \text{ для } k \in \mathbb{N}_0,$$

которые, в свою очередь, легко выводятся из соответствующих аксиом кольца R. □

Замечание. Отождествление элементов кольца R с многочленами нулевой степени в $R[x]$ (и нуля с нулевым многочленом) позволяет считать, что R — подкольцо кольца $R[x]$.

Упражнение 5.1.1. *Докажите теорему* 5.1.1 *полностью.*

Предложение 5.1.1. *Пусть R — кольцо и $f, g \in R[x]$, $f, g \neq 0$. Тогда имеют место следующие утверждения.*

1. $\deg(f+g) \leqslant \max\{\deg f, \deg g\}$.

2. $\deg fg \leqslant \deg f + \deg g$, *причём если R — кольцо без делителей нуля, то* $\deg fg = \deg f + \deg g$ *и $R[x]$ — кольцо без делителей нуля.*

Замечание. Отметим, что если один из многочленов в формулировке предложения нулевой, то утверждение п. 2 предложения остаётся в силе, если считать, что $\deg 0 = -\infty$.

Следствие. *Если R — поле, то множество $R[x]^*$ всех обратимых элементов кольца $R[x]$ — это множество всех многочленов нулевой степени.*

Упражнение 5.1.2. *Докажите предложение* 5.1.1 *и следствие из него. Приведите пример кольца R, для многочленов над которым формула* $\deg fg = \deg f + \deg g$ *неверна.*

В дальнейшем мы будем рассматривать многочлены над некоторым полем F. Как уже отмечалось, множество многочленов $F[x]$ относительно операций сложения и умножения на скаляр образует векторное пространство. Следовательно, $F[x]$ — алгебра над полем F. Отметим, что эта алгебра всегда бесконечномерна.

§ 5.2. Делимость в кольце многочленов

В силу следствия из предложения 5.1.1 многочлен ненулевой степени не имеет обратного по умножению в кольце $F[x]$. Поэтому деление в привычном смысле в кольце многочленов невозможно. Однако, как и в кольце целых чисел, в кольце многочленов можно естественным образом определить деление с остатком.

Теорема 5.2.1 (о делении с остатком)**.** *Пусть F — поле, f, g — многочлены из $F[x]$ и $g \neq 0$. Тогда существуют многочлены $q, r \in F[x]$ такие, что $f = qg + r$ и либо $r = 0$, либо* $\deg r < \deg g$. *Многочлены q и r, удовлетворяющие этим условиям, определены однозначно.*

Доказательство. Начнём с доказательства существования. Если $\deg f < \deg g$, то, полагая $q = 0$, $r = f$, получим требуемое. Таким образом, мы можем считать, что $\deg f = n \geqslant \deg g = m$. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0$ и $b(x) = b_m x^m + \ldots + b_1 x + b_0$. Используем индукцию по n. Поскольку для $n = 0$ утверждение очевидно (речь идет о делении в поле F), база индукции установлена. Следовательно, мы можем полагать, что $n > 0$ и для всех многочленов степени, меньшей n, утверждение уже доказано. Рассмотрим многочлен $f_1 = f - \frac{a_n}{b_m} x^{n-m} g$. Его степень меньше n, следовательно, существуют такие многочлены q_1 и r, что $f_1 = q_1 g + r$ и либо $r = 0$, либо $\deg r < \deg g$. Тогда $f = \frac{a_n}{b_m} x^{n-m} g + f_1 = (\frac{a_n}{b_m} x^{n-m} + q_1) g + r$, и многочлены $q = \frac{a_n}{b_m} x^{n-m} + q_1$ и r — искомые.

Пусть $f = qg + r = q'g + r'$. Тогда $r - r' = (q' - q)g$. Если $q' - q$ — ненулевой многочлен, то в силу п. 2 предложения 5.1.1 степень многочлена, стоящего в правой части равенства, больше или равна $\deg g$. С другой стороны, степень многочлена, стоящего в левой части, в силу п. 1 того же предложения и условия на степени многочленов r, r' меньше $\deg g$. Полученное противоречие показывает, что $q' = q$, а значит, и $r = r'$. □

Определение 5.2.1. Многочлены q и r, определённые в теореме, называются соответственно (*неполным*) *частным* и *остатком* при делении f на g.

Определение 5.2.2. Многочлен $g \neq 0$ *делит* многочлен f, если найдётся многочлен q такой, что $f = qg$. В этом случае g называется *делителем* многочлена f, а f — *кратным* многочлена g. Запись $g \mid f$ означает, что g *делит* f, а запись $f \vdots g$ означает, что f *делится на* g.

Замечание. Тот факт, что g не делит f, будем кратко обозначать так: $g \nmid f$.

Предложение 5.2.1 (свойства делимости многочленов)**.** *В кольце $F[x]$ выполняются следующие утверждения.*

1. *Если $g \mid f$ и $g \mid h$, то $g \mid (f + h)$.*
2. *Если $g \mid f$, то для каждого $h \in F[x]$ выполняется $g \mid (fh)$.*
3. *Если $\deg g = 0$, то для каждого $h \in F[x]$ выполняется $g \mid h$.*
4. *Если $\deg h = 0$ и $g \mid f$, то $(hg) \mid f$.*

Упражнение 5.2.1. *Доказать предложение* 5.2.1, *используя определение делимости.*

Определение 5.2.3. Пусть $f, g \in F[x]$. *Наибольшим общим дели-*

телем многочленов f и g называется многочлен $d \in F[x]$, удовлетворяющий следующим условиям:

1) $d \mid f$ и $d \mid g$;

2) если $d' \in F[x]$ таков, что $d' \mid f$ и $d' \mid g$, то $d' \mid d$.

Обозначение: $d = (f, g)$.

Замечание. Из свойств 2 и 4 делимости многочленов следует, что если d — наибольший общий делитель многочленов f и g, то многочлен w также является наибольшим общим делителем многочленов f и g тогда и только тогда, когда $w = ud$, где u — многочлен нулевой степени. Иными словами, наибольший общий делитель определяется с точностью до скаляра из поля F. Поэтому запись вида $(f, g) = (u, v)$ ниже означает, что наибольшие делители соответствующих многочленов равны с точностью до ненулевого скаляра.

Теорема 5.2.2 (алгоритм Евклида)**.** *Пусть $f, g \in F[x]$ и $g \neq 0$. Тогда существует наибольший общий делитель этих многочленов $d = (f, g)$ и он может быть представлен в виде $d = fu + gv$, где $u, v \in F[x]$. Более того, если степени f и g больше 0, то многочлены u и v можно выбрать так, что $\deg u < \deg g$ и $\deg v < \deg f$.*

Доказательство. Доказательство теоремы основано на следующем несложном утверждении.

Лемма. *Пусть r — остаток от деления f на g. Тогда множество общих делителей многочленов f и g совпадает с множеством общих делителей многочленов g и r. В частности, $(f, g) = (g, r)$.*

Доказательство. Если $h \mid g$ и $h \mid r$, то в силу свойств 1 и 2 делимости многочленов h делит $f = qg + r$. Обратно, если $h \mid f$ и $h \mid g$, то $h \mid r$, так как $r = f - qg$. Таким образом, множества общих делителей совпадают, а значит, совпадают и наибольшие по делимости элементы этих множеств. □

Вернёмся к доказательству теоремы. Если f делится на g, то $d = g = f \cdot 0 + g \cdot 1$ и теорема доказана. В противном случае разделим с остатком f на g, затем g на полученный остаток, затем первый остаток на второй и т. д. Поскольку степени остатков убывают, на некотором шаге произойдёт деление без остатка. Получим цепочку равенств:

$$f = q_1 g + r_1,$$

$$\begin{aligned} g &= q_2 r_1 + r_2, \\ &\dots\dots\dots\dots\dots \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n, \end{aligned} \tag{1}$$

где $r_i \neq 0$ для каждого $i = 1, \dots, n$.

Имеем $r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \dots = (r_1, r_2) = (g, r_1) = (f, g)$. Таким образом, наибольшим общим делителем многочленов f и g оказывается многочлен r_n — последний ненулевой остаток в этой цепочке.

Проходя по цепочке сверху вниз, мы последовательно получаем, что

$$\begin{aligned} r_1 &= fu_1 + gv_1, \\ r_2 &= fu_2 + gv_2, \\ &\dots\dots\dots\dots\dots \\ r_{n-1} &= fu_{n-1} + gv_{n-1} \\ r_n &= fu_n + gv_n, \end{aligned} \tag{2}$$

где u_i, v_i $(i = 1, \dots, n)$ — некоторые многочлены из $F[x]$ (например, $u_1 = 1$, $v_1 = -q_1$). Таким образом, $d = r_n$ можно представить в виде суммы $fu + gv$.

Пусть в представлении $d = fu + gv$ степень u больше или равна степени g. Поделим с остатком u на g: $u = qg + r$. Подставляя в исходное равенство, имеем $d = f(qg + r) + gv = fr + gv'$. В получившемся новом представлении $\deg r < \deg g$. Если $\deg f \leqslant \deg v'$, то $\deg fr < \deg gv'$. Кроме того, поскольку в случае, когда g делит f, теорема уже доказана, мы можем полагать, что $\deg d < \deg g \leqslant \deg gv'$. С другой стороны, $gv' = d - fr$, следовательно, $\deg gv' = \deg(d - fr) \leqslant \max\{\deg d, \deg fr\}$; противоречие. Таким образом, $\deg v' < \deg f$. □

Замечание. Практический метод поиска наибольшего общего делителя основан на цепочке равенств (1). Его принято называть *алгоритмом Евклида*. Мы договоримся считать, что старший коэффициент наибольшего общего делителя (f, g) многочленов f и g равен единице. Тогда (f, g) уже единственным образом определяется по f и g.

Определение 5.2.4. Многочлены $f, g \in F[x]$ называются *взаимно простыми*, если $(f, g) = 1$.

Теорема 5.2.3 (критерий взаимной простоты многочленов)**.** *Многочлены $f, g \in F[x]$ взаимно просты тогда и только тогда, когда существуют многочлены $u, v \in F[x]$ такие, что $1 = fu + gv$.*

Доказательство. Если $(f, g) = 1$, то u, v, удовлетворяющие условию, существуют по теореме 5.2.2. Обратно, если существуют многочлены u, v такие, что $1 = fu + gv$, то любой общий делитель d многочленов f, g делит $fu + gv = 1$. Следовательно, d — многочлен нулевой степени. □

Предложение 5.2.2 (свойства взаимно простых многочленов)**.** *Пусть $f, g, h \in F[x]$. Тогда выполняются следующие утверждения.*

1. *Если $(f, g) = (f, h) = 1$, то $(f, gh) = 1$.*
2. *Если $(f, g) = 1$ и $f \mid (gh)$, то $f \mid h$.*
3. *Если $(f, g) = 1$, $f \mid h$ и $g \mid h$, то $(fg) \mid h$.*

Доказательство. Докажем первое утверждение. Поскольку $(f, g) = 1$, существуют $a, b \in F[x]$ такие, что $fa + gb = 1$. Тогда $h = h(fa) + h(gb)$. Кроме того, существуют $c, d \in F[x]$ такие, что $fc + hd = 1$. Подставим в последнее равенство выражение для h. Получим $fc + (hfa + hgb)d = f(c + had) + (gh)cd = 1$. Полагая $u = c + ha$ и $v = cd$, имеем $fu + (gh)v = 1$. Следовательно, по теореме 5.2.3 многочлены f и gh взаимно просты.

Второй и третий пункт предложения доказываются схожим образом с использованием критерия взаимной простоты. □

Упражнение 5.2.2. *Докажите* пп. 2 *и* 3 *предложения* 5.2.2.

Аналогия между кольцом многочленов и кольцом целых чисел, которую мы имеем в виду на протяжении этого параграфа, приводит к понятию *неразложимого* многочлена, соответствующего понятию простого числа.

Определение 5.2.5. Многочлен $f \in F[x]$ степени, большей нуля, называется *неразложимым*, если из равенства $f = uv$, где $u, v \in F[x]$, следует, что либо $\deg u = 0$, либо $\deg v = 0$. В противном случае многочлен f *разложим*.

Замечание. К многочленам нулевой степени понятие разложимости не применяется, так же как в случае кольца целых чисел единица не считается ни простым, ни составным числом. Кроме того, очевидно, что многочлен первой степени всегда неразложим.

Пример. Многочлен $x^2 + 1$ неразложим в $\mathbb{Q}[x]$ и $\mathbb{R}[x]$, но разложим в $\mathbb{C}[x]$: $x^2 + 1 = (x + i)(x - i)$. Многочлен $x^2 - 2$ неразложим в $\mathbb{Q}[x]$, но разложим в $\mathbb{R}[x]$: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. Таким образом, ответ на вопрос о разложимости многочлена зависит от того, над каким полем задан многочлен.

Предложение 5.2.3. *Пусть $f \in F[x]$ неразложим. Тогда выполняются следующие утверждения.*

1. *Многочлен af неразложим тогда и только тогда, когда a — многочлен нулевой степени.*
2. *Для каждого $g \in F[x]$ либо $f \mid g$, либо $(f, g) = 1$.*
3. *Если $g \in F[x]$ таков, что $g \neq 0$ и $\deg g < \deg f$, то $(f, g) = 1$.*

Упражнение 5.2.3. *Доказать предложение* 5.2.3.

Теорема 5.2.4. *Пусть $f \in F[x]$, $f \neq 0$. Тогда существуют $a \in F$ и неразложимые многочлены $p_1, p_2, \ldots, p_r$ со старшими коэффициентами, равными 1, такие, что*

$$f = ap_1p_2 \ldots p_r. \tag{3}$$

Разложение (3) *единственно с точностью до перестановки сомножителей.*

Доказательство. Пусть a — старший коэффициент многочлена f. Если $\deg f = 0$, то $f = a$, $r = 0$, и теорема доказана. Поэтому в дальнейшем мы полагаем, что $\deg f > 0$.

Докажем сначала существование разложения (3). Если f неразложим, то многочлен $p_1 = \frac{1}{a}f$ тоже неразложим и его старший коэффициент равен 1. Тогда $f = ap_1$ — искомое разложение. Воспользуемся теперь индукцией по степени многочлена f. Поскольку f разложим, существуют многочлены $u, v \in F[x]$ такие, что $f = uv$ и $\deg u < \deg f$, $\deg v < \deg f$. По предположению индукции $u = bp_1 \ldots p_s$, $v = cp_{s+1} \ldots p_r$. Тогда $f = (bc)p_1 \ldots p_r$.

Нам осталось доказать единственность разложения (3). Пусть $f = ap_1p_2 \ldots p_r = bq_1q_2 \ldots q_s$ — два разложения для f. Очевидно, что $a = b$, поскольку оба числа равны старшему коэффициенту многочлена f. Поскольку кольцо $F[x]$ не имеет делителей нуля, из равенства $a(p_1 \ldots p_r - q_1 \ldots q_s) = 0$ следует равенство $p_1 \ldots p_r = q_1 \ldots q_s$. Пусть для определённости $r \leqslant s$. Мы уже доказали теорему при $r = 0$. Поэтому предположим, что $r > 0$, и докажем единственность разложения индукцией по r.

Поскольку $p_r \mid q_1 \ldots q_s$, найдётся $j \in \{1, \ldots, s\}$ такое, что $p_r \mid q_j$. Переставив при необходимости сомножители, можем считать, что $p_r \mid q_s$, т. е. $q_s = up_r$. Многочлен q_s неразложим, а значит, степень u равна 0. С другой стороны, старшие коэффициенты многочленов p_r и q_s равны единице, откуда $u = 1$ и $p_r = q_s$. Следовательно, $p_r(p_1 \ldots p_{r-1} -$

$-q_1 \dots q_{s-1}) = 0$, откуда $p_1 \dots p_{r-1} = q_1 \dots q_{s-1}$, так как $p_r \neq 0$. Использование индукционного предположения завершает доказательство теоремы. □

Замечание. Доказанная нами теорема — очевидный аналог *основной теоремы арифметики* о разложении целого числа в произведение простых множителей.

§ 5.3. Значения и корни многочленов

Определение 5.3.1. Пусть $f = a_n x^n + \dots + a_1 x + a_0 \in F[x]$, $\alpha \in F$. *Значение* многочлена f в точке α — это элемент $f(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0$ поля F.

Упражнение 5.3.1. *Пусть $f, g \in F[x]$, $\alpha \in F$. Тогда*

1. $(f + g)(\alpha) = f(\alpha) + g(\alpha)$.
2. $(fg)(\alpha) = f(\alpha)g(\alpha)$.

Определение 5.3.2. Элемент α поля F называется *корнем* многочлена $f \in F[x]$, если $f(\alpha) = 0$.

Теорема 5.3.1 (Безу)**.** *Пусть $f \in F[x]$, $\alpha \in F$. Значение многочлена f в точке α равно остатку от деления f на $x - \alpha$. В частности, элемент α — корень многочлена f тогда и только тогда, когда $(x - \alpha) \mid f$.*

Доказательство. Разделим многочлен f с остатком на $x-\alpha$. Имеем $f = q(x - \alpha) + r$, где $r = 0$ или $\deg r = 0$. Поскольку стоящие в левой и правой части равенства многочлены равны, равны и их значения в точке α. Поэтому $f(\alpha) = r$. Отсюда следует утверждение теоремы. □

Теорема 5.3.2.

1. *Ненулевой многочлен $f \in F[x]$ степени n имеет не более n корней.*

2. *Пусть для $i = 1, \dots, n$ элементы $\alpha_i \in F$, причём $\alpha_i \neq \alpha_j$, если $i \neq j$. Пусть $f, g \in F[x]$, степени многочленов f, g меньше n и $f(\alpha_i) = g(\alpha_i)$ для каждого $i = 1, \dots, n$. Тогда $f = g$.*

3. *Пусть для $i = 1, \dots, n$ элементы $\alpha_i, \beta_i \in F$, причём $\alpha_i \neq \alpha_j$, если $i \neq j$. Тогда существует и единствен многочлен f степени меньше n такой, что для каждого $i = 1, \dots, n$ выполняется $f(\alpha_i) = \beta_i$. Много-*

член f определяется формулой

$$f(x) = \sum_{i=1}^{n} \beta_i \frac{(x-\alpha_1)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_n)}{(\alpha_i-\alpha_1)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)}. \quad (1)$$

Замечание. Многочлен, определённый формулой (1), называется *интерполяционным многочленом Лагранжа*.

Доказательство. 1. Пусть $\alpha_1, \dots, \alpha_s$ — различные корни многочлена f. Заметим, что при $i \neq j$ выполняется $(x-\alpha_i, x-\alpha_j) = 1$. Действительно, оба многочлена неразложимы, поскольку они первой степени. Если бы их наибольший общий делитель имел ненулевую степень, то он равнялся бы каждому из этих многочленов. Следовательно, они были бы равны между собой, что невозможно. Из предложения о свойствах взаимно простых многочленов вытекает, что $g = (x-\alpha_1)\dots(x-\alpha_s) \mid f$. А значит, число $s = \deg g$ различных корней многочлена f не превосходит $n = \deg f$.

2. Положим $h = f - g$. Тогда $\deg h \leqslant \max\{\deg f, \deg g\} < n$ и $h(\alpha_i) = f(\alpha_i) - g(\alpha_i) = 0$ для каждого $i = 1, \dots, n$. Если $h \neq 0$, то получаем противоречие с п. 1 теоремы.

3. Подставляя элементы α_i в формулу (1), получаем $f(\alpha_i) = \beta_i$ для $i = 1, \dots, n$. Единственность многочлена f следует из п. 2 теоремы. □

Замечание. Если поле F бесконечно, то, как показывает утверждение п. 2 теоремы, абстрактное определение многочлена f над полем F (определение 5.1.1) совпадает с определением f как отображения. Иными словами, многочлены $f, g \in F[x]$ равны тогда и только тогда, когда для любого $\alpha \in F$ выполняется $f(\alpha) = g(\alpha)$.

Упражнение 5.3.2. *Используя формулу* (1), *найдите многочлен, принимающий в точках* 1, 2, 3 *значения* 1, 4, 9 *соответственно.*

Если α — корень многочлена f, то f может делиться не только на $x - \alpha$, но и на некоторую большую степень $x - \alpha$. В этом случае α принято называть *кратным корнем*. Уточним.

Определение 5.3.3. Пусть $f \in F[x]$, $r \in \mathbb{N}_0$. Элемент α поля F называется корнем многочлена f *кратности* r, если $(x-\alpha)^r \mid f$ и $(x-\alpha)^{r+1} \nmid f$. Корень кратности 1 будем называть *простым* корнем, а корень, кратность которого больше 1, — *кратным* корнем многочлена f.

Замечание. Корень кратности 0, очевидно, корнем многочлена не является.

В ситуации, когда α — корень кратности r, полезно бывает считать, что многочлен f имеет r корней, равных α. В этом случае мы будем говорить, что рассматриваем корни многочлена *с учётом их кратности.*

Теорема 5.3.3. *Ненулевой многочлен $f \in F[x]$ степени n имеет не более n корней с учётом их кратности. Кроме того, f имеет ровно n корней тогда и только тогда, когда он раскладывается над F на линейные множители, т. е. $f = a(x-\alpha_1)^{r_1}\dots(x-\alpha_s)^{r_s}$, где $a, \alpha_i \in F$ и $\sum_{i=1}^{s} r_i = n$.*

Доказательство. Доказательство практически аналогично доказательству п. 1 теоремы 5.3.2. Пусть $\alpha_1, \dots, \alpha_s$ — различные корни многочлена f и их кратности равны $r_1, \dots, r_s$ соответственно. Покажем, что $((x-\alpha_i)^{r_i}, (x-\alpha_j)^{r_j}) = 1$ при $i \neq j$. Действительно, из единственности разложения многочлена в произведение неразложимых (теорема 5.2.4) следует, что если многочлен d делит многочлен $(x-\alpha)^m$, то $d = c(x-\alpha)^k$, где $c \in F$ и $0 \leqslant k \leqslant m$. Поэтому наибольший общий делитель многочленов $(x-\alpha_i)^{r_i}$ и $(x-\alpha_j)^{r_j}$ должен одновременно иметь вид $(x-\alpha_i)^{k_i}$ и $(x-\alpha_j)^{k_j}$, что по той же теореме о разложении в произведение неразложимых возможно, только если d — многочлен нулевой степени.

Таким образом, многочлен $g = (x-\alpha_1)^{r_1}\dots(x-\alpha_s)^{r_s}$ делит многочлен f. Поэтому $\deg g \leqslant \deg f$. Последнее утверждение теоремы следует из того, что в данном случае равносильны равенства $\deg g = \deg f$ и $f = ag$, где a — многочлен нулевой степени, т. е. ненулевой скаляр. □

Кратность корня многочлена можно интерпретировать также с помощью понятия производной. Ясно, что аналитическое определение производной может не иметь смысла в случае произвольного поля. Поэтому мы дадим следующее абстрактное определение.

Определение 5.3.4. Пусть $f(x) = \sum_{k=0}^{n} a_k x^k$ — многочлен степени n над полем F. Многочлен f', определённый по правилу

$$f'(x) = \sum_{k=1}^{n} k a_k x^{k-1},$$

называется *производной* многочлена f.

Замечание. В определении производной предполагается, что ka, где $k \in \mathbb{N}$ и $a \in F$, — это элемент поля F, равный сумме k элементов a поля F.

Упражнение 5.3.3. *Пусть $f, g \in F[x]$, $\alpha, \beta \in F$, $k \in \mathbb{N}$. По определению производной докажите следующие утверждения.*

1. $(\alpha f + \beta g)' = \alpha f' + \beta g'$.
2. $(fg)' = f'g + fg'$.
3. $(\alpha(x-\beta)^k)' = k\alpha(x-\beta)^{k-1}$.

Определение 5.3.5. Пусть $f \in F[x]$. Если k — натуральное число и $f^{(0)} = f$, то k-я производная многочлена f определяется по индукции: $f^{(k)} = (f^{(k-1)})'$.

Отметим, что над произвольным полем некоторые очевидные с аналитической точки зрения свойства производной могут не выполняться. Например, если мы рассмотрим полином $f(x) = x^2$ над полем $F = \mathbb{Z}_2$, то обнаружим, что его производная $f'(x) = 2x = 0x = 0$. Ниже мы ограничимся рассмотрением только тех полей, в которых $ka \neq 0$ для любого натурального числа k и ненулевого скаляра $a \in F$. Иными словами, полями *нулевой характеристики*. Приведём точное определение характеристики поля.

Определение 5.3.6. Пусть F — поле. Наименьшее натуральное число p такое, что $p1 = 0$ (сумма p единиц поля равна 0), если оно существует, называется *характеристикой* поля F. Если такого числа нет, то *характеристика* поля F по определению равна 0. Характеристика поля обозначается $\operatorname{char} F$.

Пример. Поле $\mathbb{Z}_2$ имеет характеристику 2. Числовые поля $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ имеют нулевую характеристику.

Упражнение 5.3.4. *Если p — ненулевая характеристика некоторого поля, то p — простое число.*

Указание. Использовать тот факт, что в поле нет делителей нуля.

Упражнение 5.3.5. *Если $\operatorname{char} F = 0$, $a \in F$ и $k \in \mathbb{N}$, то $ka = 0$ тогда и только тогда, когда $a = 0$. В частности, для любого $b \in F$ и $k \in \mathbb{N}$ определён элемент $b/k = b \cdot (k1)^{-1}$ поля F.*

Сделав в многочлене $f(x) = a_0 + a_1x + \ldots + a_nx^n$ замену $x = y + \alpha$, мы получим новый многочлен (той же степени) от переменной $y = x - \alpha$. Фактически, мы получим представление

$$f(x) = b_0 + b_1(x-\alpha) + \ldots + b_n(x-\alpha)^n, \tag{2}$$

которое называется *разложением f по степеням $x - \alpha$*.

Теорема 5.3.4 (формула Тейлора)**.** *Пусть $\operatorname{char} F = 0$, $\alpha \in F$, $f \in F[x]$ и $\deg f = n$. Разложение многочлена f по степеням $x - \alpha$*

определяется формулой

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(\alpha)}{k!}(x-\alpha)^k. \tag{3}$$

Эта формула называется формулой Тейлора для многочленов.

Доказательство. Продифференцируем равенство (2) k раз и подставим $x = \alpha$. Тогда $f^{(k)}(\alpha) = k!b_k$. Откуда и следует формула (3). □

Следствие (о кратных корнях многочлена)**.** *Пусть* $\operatorname{char} F = 0$, $f \in F[x]$ *и* $r \in \mathbb{N}$. *Тогда выполняются следующие утверждения.*

1. *Элемент* α *поля* F *— корень кратности* r *многочлена* f *тогда и только тогда, когда* $f^{(k)}(\alpha) = 0$ *для всех* $k = 0, \dots, r-1$ *и* $f^{(r)}(\alpha) \neq 0$. *В частности,* α *— корень кратности* $r-1$ *производной* f' *многочлена* f.

2. *Множество корней многочлена* f *совпадает с множеством корней многочлена* $g = \frac{f}{(f,f')}$, *и все корни многочлена* g *— простые. В частности, многочлен* f *не имеет кратных корней тогда и только тогда, когда* $(f, f') = 1$.

Замечание. В п. 1 подразумевается, что если α — простой корень многочлена f ($r = 1$), то α не является корнем его производной f' (α — корень нулевой кратности для f').

Доказательство. 1. Кратность корня α многочлена f, очевидно, равна номеру первого отличного от нуля коэффициента в разложении (2). Поэтому утверждение следует из формулы Тейлора.

2. Если α — корень f кратности r, то $(x-\alpha)^{r-1} \mid (f, f')$ и $(x-\alpha)^r \nmid (f, f')$. Следовательно, α — простой корень многочлена g. С другой стороны, поскольку $f = g(f, f')$, то любой корень многочлена g будет и корнем многочлена f. □

Упражнение 5.3.6. *Для многочлена* $f(x) = x^5 - 3x^4 - 6x^3 + 10x^2 + 21x + 9$ *найдите многочлен* $g = \frac{f}{(f,f')}$ *и решите уравнение* $f(x) = 0$.

В случае, когда поле имеет ненулевую характеристику, утверждение следствия о кратных корнях может не выполняться. Тем не менее, можно доказать его ослабленную версию.

Упражнение 5.3.7. *Докажите следующее утверждение. Если* F *— произвольное поле,* f *— многочлен из* $F[x]$ *и* α *— его корень кратности* r, *то для каждого* $i \in \{0, 1, \dots, r-1\}$ *выполняется* $f^{(i)}(\alpha) = 0$. *В частности, если* $(f, f') = 1$, *то* f *не имеет кратных корней.*

Последнее утверждение в этом параграфе — теорема о существовании так называемого *многочлена Лагранжа–Сильвестра.* Этот много-

член не только имеет фиксированные значения в данных точках, но и фиксированные значения своих последовательных производных в тех же точках. Он понадобится нам в шестой главе.

Теорема 5.3.5. *Пусть* $\operatorname{char} F = 0$, $s \in \mathbb{N}$ *и для каждого* $i = 1, \ldots, s$ *числа* $r_i \in \mathbb{N}_0$, *элементы* $\alpha_i, \beta_{i0}, \ldots, \beta_{ir_i} \in F$, *причём* $\alpha_m \neq \alpha_k$ *при* $m \neq k$. *Тогда существует единственный многочлен* f *степени меньше, чем* $\sum_{i=1}^{s}(r_i+1)$, *такой, что для каждого* $i = 1, \ldots, s$ *и каждого* $j = 0, \ldots, r_i$ *выполняется* $f^{(j)}(\alpha_i) = \beta_{ij}$.

Доказательство. Будем искать многочлен f в виде $f = \sum_{i=1}^{s} f_i$, где $f_i = d_i g_i$ и $d_i, g_i \in F[x]$ для каждого $i = 1, \ldots, s$. Причём $d_i(x) = \prod_{k \neq i}(x - \alpha_j)^{r_k+1}$, а g_i подбираются исходя из следующей леммы.

Лемма. *Пусть даны* $\alpha, \beta_0, \ldots, \beta_r \in F$ *и* $d \in F[x]$ *такие, что* $d(\alpha) \neq 0$. *Тогда существует многочлен* g *степени, не превосходящей* r, *такой, что* $(dg)^{(j)}(\alpha) = \beta_j$ *для всех* $j = 0, \ldots, r$.

Доказательство леммы. Сначала докажем, что для любого многочлена $u \in F[x]$ и каждого $t = 1, \ldots, n$, где $n \in \mathbb{N}$, найдётся многочлен $v \in F[x]$ такой, что

$$(u(x-\alpha)^n)^{(t)} = \frac{n!}{(n-t)!}u(x-\alpha)^{n-t} + v(x-\alpha)^{n-t+1}. \tag{4}$$

Доказательство формулы (4) проводится индукцией по t. При $t = 1$ имеем

$$(u(x-\alpha)^n)' = n(x-\alpha)^{n-1}u + u'(x-\alpha)^n$$

и, полагая $v = u'$, получаем требуемое.

По предположению индукции существует многочлен v_1 такой, что

$$(u(x-\alpha)^n)^{(t-1)} = \frac{n!}{(n-t+1)!}u(x-\alpha)^{n-t+1} + v_1(x-\alpha)^{n-t+2}.$$

Следовательно,

$$(u(x-\alpha)^n)^{(t)} = \left(\frac{n!}{(n-t+1)!}u(x-\alpha)^{n-t+1}\right)' + \left(v_1(x-\alpha)^{n-t+2}\right)' =$$

$$= \frac{n!}{(n-t)!}u(x-\alpha)^{n-t} + v(x-\alpha)^{n-t+1},$$

что и требовалось.

Утверждение леммы мы докажем индукцией по r. При $r = 0$ искомый скаляр g (в данном случае степень g не должна превосходить 0) находится из равенства $(dg)(\alpha) = \beta_0$. Действительно, если $g = \frac{\beta_0}{d(\alpha)}$, то $gd(\alpha) = g(\alpha)d(\alpha) = (dg)(\alpha) = \beta_0$.

Пусть $r > 0$ и для чисел, меньших r, утверждение леммы доказано. Иными словами, существует многочлен h степени, меньшей r, такой, что для каждого $j = 0, \ldots, r-1$ выполняется $(dh)^{(j)}(\alpha) = \beta_j$. Тогда для любого $\gamma \in F$ многочлен $g = h + \gamma(x-\alpha)^r$ удовлетворяет условию $(dg)^{(j)}(\alpha) = \beta_j$ при $j = 0, \ldots, r-1$. Действительно,

$$(dg)^{(j)} = (dh)^{(j)} + (d\gamma(x-\alpha)^r)^{(j)} = (dh)^{(j)} + (x-\alpha)w \quad \text{(см. формулу (4))}.$$

Поэтому $(dg)^{(j)}(\alpha) = (dh)^{(j)}(\alpha) + 0 = \beta_j$ при $j < r$. Осталось подобрать γ так, чтобы $(dg)^{(r)} = \beta_r$. Имеем

$$(dg)^{(r)} = (dh)^{(r)} + (d\gamma(x-\alpha)^r)^{(r)} = (dh)^{(r)} + d\gamma r!(x-\alpha)^0 + v(x-\alpha).$$

Выражая γ из равенства

$$(dg)^{(r)}(\alpha) = (dh)^{(r)}(\alpha) + d(\alpha)\gamma r! = \beta_r,$$

получаем, что при

$$\gamma = \frac{\beta_r - (dh)^{(r)}(\alpha)}{d(\alpha)r!}$$

выполняется последнее необходимое равенство $(dg)^{(r)}(\alpha) = \beta_r$. Отметим, что γ находится всегда, поскольку $r! \neq 0$ в силу того, что $\operatorname{char} F = 0$, а $d(\alpha) \neq 0$ по условию. □

Вернёмся к доказательству теоремы. Введённые нами многочлены d_i обладают тем свойством, что $d_i(\alpha_i) \neq 0$ для каждого $i = 1, \ldots, s$. Следовательно, для каждого из них в силу утверждения леммы найдётся многочлен g_i степени, не превосходящей r_i, такой, что $f_i^{(j)}(\alpha_i) = (d_i g_i)^{(j)}(\alpha_i) = \beta_{ij}$, где $i = 1, \ldots, s$, а $j = 0, \ldots, r_i$.

Поскольку $(x-\alpha_i)^{r_i+1} \mid d_k$ при $k \neq i$, имеем $f_k^{(j)}(\alpha_i) = 0$ для всех $k \neq i$ и всех $j = 0, \ldots, r_i$. Таким образом, для всех $i = 1, \ldots, s$ и всех $j = 0, \ldots, r_i$ выполняется

$$f^{(j)}(\alpha_i) = \sum_{k=1}^{s} f_k^{(j)}(\alpha_i) = f_i^{(j)}(\alpha_i) = \beta_{ij}.$$

Далее,

$$\deg f \leqslant \max_{i=1,\dots,s}\{\deg f_i\} < \sum_{i=1}^{s}(r_i+1).$$

Пусть g — многочлен, удовлетворяющий условию теоремы, и $g \neq f$. Положим $h = f - g$. Тогда $h^{(j)}(\alpha_i) = 0$ для $i = 1, \dots, s$ и $j = 0, \dots, r_i$. По следствию теоремы 5.3.4 о кратных корнях имеем $\prod_{i=1}^{s}(x-\alpha_i)^{r_i+1} \mid h$. Следовательно, $\deg h \geqslant \sum_{i=1}^{s}(r_i+1)$; противоречие. □

Упражнение 5.3.8. *Используя в качестве руководства доказательство теоремы, постройте интерполяционный многочлен Лагранжа–Сильвестра f, удовлетворяющий следующим условиям: $f(1) = 1$, $f'(1) = 2$, $f(2) = 4$.*

§ 5.4. Симметрические многочлены

В этом параграфе речь пойдёт о многочленах от нескольких переменных. Хотя для них, также как и в случае многочленов от одной переменной, существует содержательная теория, мы затронем в этих лекциях лишь один важный факт, относящийся к многочленам специального вида, так называемым *симметрическим многочленам*. Начнём с того, что дадим общее определение многочленов от нескольких переменных, используя доказанные нами свойства кольца многочленов от одной переменной и индукцию, базисом которой является определение кольца многочленов от одной переменной.

Определение 5.4.1. Пусть n — натуральное число, большее 1, R — кольцо и уже определено кольцо $R[x_1, \dots, x_{n-1}]$ многочленов над R от $n-1$ переменной. *Кольцом многочленов над R от n переменных* называется кольцо $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$, т. е. кольцо многочленов от переменной x_n над кольцом $R[x_1, \dots, x_{n-1}]$.

Замечание. Корректность определения множества $R[x_1, \dots, x_n]$ как кольца следует из теоремы 5.1.1. Кроме того, из той же теоремы сразу следует, что свойства коммутативности или существования единицы в кольце R влекут те же свойства кольца $R[x_1, \dots, x_n]$.

Определение 5.4.2. Многочлен вида $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$, где $a \in R$, называется *одночленом* (или *мономом*). Элемент a будем называть *коэффициентом* одночлена, n-ку $(k_1, k_2, \dots, k_n)$ — *степенью* одночлена, число k_i — *степенью* одночлена *по переменной* x_i, а сумму $k_1+k_2+\dots+k_n$ — его *степенью по совокупности переменных*.

В дальнейшем мы будем рассматривать многочлены над полем F.

Анализ определения показывает, что многочлен $f \in F[x_1, \ldots, x_n]$ имеет вид:

$$f(x_1, x_2, \ldots, x_n) = \sum_{k_1, k_2, \ldots, k_n} a_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \ldots x^{k_n}, \qquad (1)$$

где суммирование происходит по упорядоченным наборам $k_1, k_2 \ldots, k_n$ неотрицательных целых чисел, элементы $a_{k_1 k_2 \ldots k_n} \in F$ и лишь конечное их число отлично от нуля. Два многочлена равны, если для каждого набора индексов $(k_1, k_2 \ldots, k_n)$ их коэффициенты совпадают. Таким образом, каждый многочлен от n переменных можно считать суммой конечного числа одночленов. Мы будем упорядочивать одночлены с ненулевыми коэффициентами, составляющие многочлен, *лексикографически* упорядочивая их степени. Степень $(k_1, k_2, \ldots, k_n)$ и соответствующий ей одночлен *старше*, чем степень $(l_1, l_2, \ldots, l_n)$ и соответствующий ей одночлен, если найдётся $i \in \{1, 2, \ldots, n\}$ такое, что $k_1 = l_1, \ldots, k_{i-1} = l_{i-1}$ и $k_i > l_i$. Если u, v — одночлены, мы будем обозначать через $u \succ v$ тот факт, что u старше v. *Степенью многочлена* мы будем называть старшую степень его одночленов.

Пример. Следующий многочлен упорядочен по убыванию степеней его одночленов:

$$x_1^2 x_2 - 2x_1 x_2 x_3 + 3x_1 x_3^3 - 2x_2^2 x_3 + 1.$$

Отметим, что одночлен $3x_1 x_3^3$ младше, чем старший одночлен $x_1^2 x_2$, а также одночлен $-2x_1 x_2 x_3$, хотя его степень по совокупности переменных больше соответствующих степеней двух последних одночленов.

Несложно проверить следующие свойства лексикографического упорядочения одночленов над полем F.

Предложение 5.4.1. *Пусть F — поле, u, v, w, z — одночлены из $F[x_1, \ldots, x_n]$. Тогда выполняются следующие утверждения.*

1. *Если $u \succ v$, $v \succ w$, то $u \succ v$.*
2. *Если $u \succ v$ и $w \neq 0$, то $uw \succ vw$.*
3. *Если $u \succ v$, $w \succ z$, то $uw \succ vz$.*

Упражнение 5.4.1. *Докажите предложение* 5.4.1.

Следствие. *Старший одночлен произведения многочленов из кольца $F[x_1, \ldots, x_n]$ равен произведению старших одночленов сомножителей. В частности, кольцо $F[x_1, \ldots, x_n]$ не имеет делителей нуля.*

Определение 5.4.3. Многочлен $f \in F[x_1, x_2, \ldots, x_n]$ называется *симметрическим*, если для любой подстановки $\sigma \in S_n$ выполняется равенство $f(x_1, x_2, \ldots, x_n) = f(x_{1\sigma}, x_{2\sigma}, \ldots, x_{n\sigma})$, т. е. многочлен f не меняется при любой перестановке переменных.

Примеры. 1. Многочлены

$$s_k = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_k}, \tag{2}$$

где $k = 1, 2, \ldots, n$, являются симметрическими. Они называются *элементарными симметрическими многочленами.*

2. Многочлен $x_1^m + x_2^m + \ldots + x_n^m$ является симметрическим при любом натуральном m.

3. Всякий многочлен нулевой степени по совокупности переменных является симметрическим.

4. Многочлен $3x_1x_2 + 3x_1x_3$ не является симметрическим, поскольку подстановка переменных $\sigma = (1, 2) \in S_3$ переводит его в многочлен $3x_1x_2 + 3x_2x_3$.

Предложение 5.4.2. *Сумма и произведение двух симметрических многочленов — симметрические многочлены. Множество всех симметрических многочленов от n переменных образует подкольцо кольца $F[x_1, \ldots, x_n]$. Если $g \in F[y_1, \ldots, y_m]$ и $p_1, \ldots, p_m$ — симметрические многочлены от переменных $x_1, \ldots, x_n$, то $g(p_1, \ldots, p_m)$ — симметрический многочлен от переменных $x_1, \ldots, x_n$.*

Упражнение 5.4.2. *Доказать предложение* 5.4.2.

Мы готовы сформулировать основной результат этого параграфа.

Теорема 5.4.1 (основная теорема о симметрических многочленах)**.** *Пусть $f \in F[x_1, \ldots, x_n]$ — симметрический многочлен. Тогда существует многочлен $g \in F[y_1, \ldots, y_n]$ такой, что $f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n)$, где s_k — элементарные симметрические многочлены от переменных $x_1, \ldots, x_n$ над полем F.*

Доказательство. Пусть $u = ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ — старший одночлен многочлена f. Сначала мы докажем, что для его степени выполняются неравенства $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n$. Иначе рассмотрим наименьшее число i такое, что $k_i < k_{i+1}$. Транспозиция $\sigma = (i, i+1)$ переводит одночлен $u = ax_1^{k_1} \ldots x_i^{k_i}x_{i+1}^{k_{i+1}} \ldots x_n^{k_n}$ в одночлен $v = ax_1^{k_1} \ldots x_i^{k_{i+1}}x_{i+1}^{k_i} \ldots x_n^{k_n}$, степень которого по нашему предположению старше степени v. С дру-

гой стороны, поскольку f симметрический, он должен содержать одночлен v, что противоречит выбору u в качестве старшего одночлена.

Если f — многочлен нулевой степени, т. е. многочлен степени $(0,\dots,0)$, то утверждение теоремы очевидно. Поскольку существует только конечное число степеней $(l_1,\dots,l_n)$, удовлетворяющих неравенству $l_1 \geqslant l_2 \geqslant \dots \geqslant l_n$ и младших, чем старшая степень $(k_1,\dots,k_n)$ многочлена f, можно использовать индукцию по степени f. Таким образом, мы можем считать, что для всех многочленов, младших многочлена f, утверждение теоремы уже доказано.

Рассмотрим многочлен $h = as_1^{k_1-k_2}\dots s_{n-1}^{k_{n-1}-k_n}s_n^{k_n}$. Поскольку многочлены s_k симметрические, в силу предложения 5.4.2 сам h — симметрический многочлен от переменных $x_1,\dots,x_n$. Пусть v — старший одночлен многочлена h. Для каждого $i \in \{1,2,\dots,n\}$ степень v по переменной x_i равна k_i, так как x_i входит в старшие одночлены элементарных симметрических многочленов $s_i,\dots,s_n$ по одному разу и не входит в старшие одночлены многочленов $s_1,\dots,s_{i-1}$. Следовательно, старший одночлен v многочлена h совпадает с u, старшим одночленом многочлена f. Поэтому многочлен $f_1 = f - h$ является симметрическим многочленом, степень которого младше степени f. По предположению индукции существует многочлен g_1 из $F[y_1,\dots,y_n]$ такой, что $f_1(x_1,\dots,x_n) = g_1(s_1,\dots,s_n)$. Значит, многочлен $g = ay_1^{k_1-k_2}\dots y_{n-1}^{k_{n-1}-k_n}y_n^{k_n} + g_1(y_1,\dots,y_n)$ является искомым. □

Замечание. Доказательство теоремы можно использовать для выражения любого симметрического многочлена через элементарные симметрические многочлены.

Упражнение 5.4.3. *Докажите, что* $x_1^2+\dots+x_n^2 = s_1^2 - 2s_2$ *и* $x_1^3+\dots+x_n^3 = s_1^3 - 3s_1s_2 + 3s_3$.

§ 5.5. Алгебраическая замкнутость поля комплексных чисел

Результаты предыдущих параграфов ничего не говорят о существовании у многочлена хотя бы одного корня. Более того, как показывают несложные примеры, существуют многочлены, не имеющие корней в поле, над которым они заданы. Так, многочлен $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ не имеет рациональных корней, а многочлен $g = x^2 + 1$ не имеет корней даже в $\mathbb{R}$. Тем не менее f имеет корни в $\mathbb{R}$, а g — в $\mathbb{C}$, т. е. в полях, которые содержат поля коэффициентов многочлена в качестве подполя. Иными словами, в *расширениях* полей коэффициентов.

Определение 5.5.1. Поле K называется *расширением* поля F, если F — подполе поля K, т. е. F — подмножество в K и операции, заданные на F, являются сужениями на F соответствующих операций, заданных на K.

Оказывается, что отмеченное нами свойство многочленов $x^2 - 2$ и $x^2 + 1$, которые имеют корни в расширении поля своих коэффициентов, носит универсальный характер.

Теорема 5.5.1. *Пусть F — поле, многочлен $f \in F[x]$ и $\deg f > 0$. Тогда существует расширение K поля F такое, что для некоторого элемента $\alpha \in K$ выполняется $f(\alpha) = 0$.*

Замечание. Выражение $f(\alpha)$ в формулировке теоремы имеет смысл, поскольку коэффициенты многочлена f, лежащие в F, лежат и в расширении K этого поля. Кроме того, операции сложения и умножения на скаляр (коэффициент) можно рассматривать как операции в поле K. Иными словами, если K — расширение поля F и $f \in F[x]$, то всегда можно считать, что f задан и над K. Таким образом, $f(\alpha)$ — это значение многочлена f в точке α, где $f \in K[x]$.

Доказательство. По теореме 5.2.4 многочлен f раскладывается над F в произведение неразложимых многочленов со старшими коэффициентами, равными единице: $f = ap_1p_2 \dots p_s$. Если α — корень многочлена p_1 в расширении K поля F, то $f(\alpha) = ap_1(\alpha) \dots p_s(\alpha) = 0$ и поле K и его элемент α — искомые. Таким образом, можно считать, что многочлен f неразложим над F и его старший коэффициент равен 1. Пусть $\deg f = n$ и

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n. \tag{1}$$

Заметим, что можно считать, что $\deg f > 1$. Иначе $f = a_0 + x$, $-a_0$ — корень многочлена f в поле F, и мы полагаем, что $K = F$.

Теперь мы явным образом построим поле, которое удовлетворяет условиям теоремы. Обозначим через K множество многочленов над F от переменной t, степень которых строго меньше n. Иными словами,

$$K = \{g(t) \in F[t] \mid \deg g < \deg f\}.$$

Определим на K операции сложения и умножения, которые мы обозначим через $+$ и $\circ$, следующим образом. Сложение $+$ — это обычное сложение многочленов. А результат умножения $\circ$ для многочленов $g, h \in K$ — это остаток от деления обычного произведения многочленов

$g(t)h(t)$ на многочлен $f(t)$, т. е. $g \circ h = r$, где r удовлетворяет условиям $gh = fq + r$ и $\deg r < \deg f$. Отметим, что K замкнуто относительно определённых нами операций. Действительно, $\deg(g + h) \leqslant \max\{\deg g, \deg h\} < \deg f$ и $\deg r < \deg f$ по теореме о делении с остатком. Кроме того, по той же теореме остаток r определяется однозначно, поэтому предложенная нами операция умножения корректно определена на K.

Проверим, что K — поле относительно введённых нами операций.

Тот факт, что $\langle K, + \rangle$ — абелева группа, очевиден, поскольку сложение многочленов обладает всеми необходимыми свойствами.

Проверим аксиому правой дистрибутивности. Пусть $g, h, u \in K$ и $gu = fq_1 + r_1$, $hu = fq_2 + r_2$ и $(g+h)u = fq + r$. Тогда $g \circ u + h \circ u = r_1 + r_2$, а $(g + h) \circ u = r$. С другой стороны, $F[t]$ — кольцо. Следовательно, для многочленов $g, h, u \in F[t]$ выполняется $gu + hu = (g+h)u$. Поэтому, если мы обозначим многочлен $(g+h)u$ через w, то $w = f(q_1 + q_2) + (r_1 + r_2) = = fq + r$. В силу теоремы о делении с остатком имеем $r_1 + r_2 = r$, а значит, $g \circ u + h \circ u = (g + h) \circ u$. Закон левой дистрибутивности проверяется аналогично.

Доказательство ассоциативности умножения в K проводится схожим образом и основано на ассоциативности умножения многочленов в кольце $F[t]$. Коммутативность умножения следует из определения операции $\circ$. Единицей в K, как и в кольце $F[t]$, является многочлен нулевой степени, равный единице поля F. Таким образом, нам осталось для каждого ненулевого элемента из K указать обратный к нему элемент.

Пусть $g(t) \in K$ и $g(t) \neq 0$. Поскольку $f(t)$ неразложим над F и $\deg g < \deg f$, по п. 3 предложения 5.2.3 имеем $(g, f) = 1$. Следовательно, существуют многочлены $u, v \in F[t]$ такие, что $gu + fv = 1$ и $\deg u < \deg f$. Поэтому $u \in K$ и $g \circ u = 1$, так как $gu = f(-v) + 1$. Следовательно, многочлен $u \in K$ является обратным по умножению элементом к многочлену g. Таким образом, K — поле.

Пусть $a, b \in F$. Рассмотрим их как многочлены нулевой степени из K. Тогда их сумма в поле F — это многочлен нулевой степени из K, равный $a + b$. Остаток от деления ab на f равен, очевидно, ab. Поэтому $a \circ b = ab \in F$. Таким образом, F — подполе поля K, а значит, K — расширение поля F.

Рассмотрим теперь элемент $\alpha \in K$, равный многочлену $t = 0 + 1 \cdot t + +0 \cdot t^2 \ldots + 0 \cdot t^{n-1} \in F[t]$. Отметим, что $\alpha = t$ действительно лежит в K, поскольку мы считаем, что $\deg f > 1$. Найдём теперь $f(\alpha)$ в поле K. Подставляя t в равенство (1), имеем

$$f(\alpha) = a_0 + a_1 \circ t + a_2 \circ t^2 + \ldots + a_{n-1} \circ t^{n-1} + t^n,$$

причём для $k = 1, \ldots n$ под t^k понимается произведение k элементов t в поле K, т. е.

$$t^k = \underbrace{t \circ \ldots \circ t}_{k \text{ раз}}.$$

Остатки от деления многочлена $a_k t^k$, рассматриваемого в обычном смысле, на f при $k < n$ очевидно равны $a_k t^k$, поскольку $\deg a_k t^k < \deg f$. Это неверно для многочлена t^n ($\deg t^n = n = \deg f$). Разделим с остатком t^n на f:

$$t^n = f(t) \cdot 1 - (a_0 + a_1 t + \ldots + a_{n-1} t^{n-1}).$$

Поэтому в поле K произведение из n элементов, равных t, равно $-(a_0 + a_1 t + \ldots + a_{n-1} t^{n-1})$. Следовательно,

$$f(\alpha) = a_0 + a_1 t + \ldots + a_{n-1} t^{n-1} - (a_0 + a_1 t + \ldots + a_{n-1} t^{n-1}) = 0.$$

Теорема доказана. □

Пример. Рассмотрим многочлен $g(x) = x^2 + 1 \in \mathbb{R}[x]$. Он неразложим над $\mathbb{R}$. Построим, пользуясь способом, указанным при доказательстве теоремы, расширение поля $\mathbb{R}$, в котором g имеет корень. Имеем $K = \{a + bt \mid a, b \in \mathbb{R}\}$. Остаток от деления t^2 на $t^2 + 1$ равен, очевидно, -1. Следовательно, $(t \circ t) + 1 = -1 + 1 = 0$, а значит, многочлен $t \in K$ является корнем многочлена $g(x) \in K[x]$. Несложно заметить, что построенное нами поле K изоморфно полю $\mathbb{C}$ комплексных чисел. Достаточно положить $t = i$.

Упражнение 5.5.1. *Проверьте, что многочлен $g(x) = x^2 + 1$ имеет корень в поле $F = \mathbb{Z}_2$ вычетов по модулю 2, а многочлен $f(x) = x^2 + x + 1$ неразложим над тем же полем. Постройте расширение K поля F, в котором f будет иметь корень. Чему равен порядок поля K?*

Следствие 1 (о разложении многочлена на линейные множители)**.** *Пусть $f \in F[x]$ и $\deg f = n$. Тогда существуют расширение K поля F и элементы $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ (не обязательно различные) такие, что*

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n), \tag{2}$$

т. е. f раскладывается над K на линейные множители.

Доказательство. Индукция по степени f. Если $\deg f = 0$, то $F = K$ и $f = a \in F$ — искомое разложение. Если $\deg f > 0$, то по теореме существуют расширение K_1 поля F и элемент $\alpha_1 \in K_1$ такие, что $f(\alpha_1) = 0$. Поэтому над полем K_1 многочлен f разложим в произведение $f = (x-\alpha_1)f_1$. Степень многочлена f_1 равна $n-1$. Следовательно, по предположению индукции найдутся расширение K поля K_1 и элементы $\alpha_2, \ldots, \alpha_n \in K$ такие, что $f_1 = a(x-\alpha_2)\ldots(x-\alpha_n) \in K[x]$. Поэтому имеет место разложение (2) многочлена f над K. Осталось заметить, что расширение K поля K_1 является и расширением поля F. □

Пример. Многочлен $x^2+1 \in \mathbb{R}[x]$ не только имеет корень в $\mathbb{C}$, но и раскладывается над ним на линейные множители.

Упражнение 5.5.2. *Покажите, что многочлен $f(x) = x^4 - 5x^2 + 6$ из $\mathbb{Q}[x]$ имеет корень в поле $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, но не раскладывается над ним на линейные множители. Постройте расширение поля $\mathbb{Q}$, над которым f раскладывается на линейные множители.*

Ещё одно следствие доказанной нами теоремы связано с так называемыми *формулами Виета* для коэффициентов многочлена.

Следствие 2 (формулы Виета)**.** *Предположим, что многочлен $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in F[x]$ имеет разложение $f(x) = a_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ в расширении K поля F. Тогда для каждого $k = 1, \ldots, n$*

$$s_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \tag{3}$$

где s_k — k-ый элементарный симметрический многочлен от n переменных. В частности, если g — произвольный симметрический многочлен от n переменных с коэффициентами из поля F, то $g(\alpha_1, \ldots, \alpha_n)$ лежит в F.

Доказательство. Формулы (3) проверяются непосредственно. Последнее же утверждение вытекает из теоремы 5.4.1 о представлении произвольного симметрического многочлена в виде многочлена от элементарных симметрических многочленов. □

Замечание. Последнее утверждение следствия достаточно любопытно. Несмотря на то, что сами корни $\alpha_1, \ldots, \alpha_n$ не обязаны лежать в поле F, значение любого симметрического многочлена с коэффициентами из F от этих корней лежит в F.

Пример. Корни i и $-i$ многочлена x^2+1 не лежат в $\mathbb{R}$, но сумма их квадратов $i^2+(-i)^2 = -2$ лежит в $\mathbb{R}$. Более того, для вычисления суммы

квадратов корней многочлена $x^2 + 1$ нам совершенно не обязательно знать, чему они равны. Действительно, если обозначить эти корни через α_1, α_2, то в силу утверждения упражнения 5.4.3 выполняются равенства $\alpha_1^2 + \alpha_2^2 = s_1^2(\alpha_1, \alpha_2) - 2s_2(\alpha_1, \alpha_2)$. С другой стороны, по формулам Виета $s_1(\alpha_1, \alpha_2) = 0/1 = 0$, $s_2(\alpha_1, \alpha_2) = 1/1 = 1$, и мы получаем тот же результат.

В каком-то смысле историю развития алгебры как теории алгебраических уравнений можно рассматривать в контексте доказанной нами теоремы. Действительно, невозможность решения уравнений вида $x^2 - 2 = 0$ в поле рациональных чисел приводит к необходимости его расширения до поля действительных чисел, а желание найти корни многочлена $x^2 + 1$ — к построению поля комплексных чисел. Возникает естественный вопрос, имеет ли каждый многочлен с комплексными коэффициентами корень в поле комплексных чисел, или требуется новое расширение уже этого поля? Оказывается, поле комплексных чисел в отличие от полей рациональных и действительных чисел обладает тем замечательным свойством, что любой многочлен, заданный над ним, имеет в $\mathbb{C}$ корень, иными словами, поле комплексных чисел *алгебраически замкнуто*.

Определение 5.5.2. Поле F называется *алгебраически замкнутым*, если каждый многочлен из $F[x]$ ненулевой степени имеет в F корень.

Теорема об алгебраической замкнутости поля комплексных чисел, впервые доказанная Гауссом в конце XVIII века, является одним из самых замечательных достижений всей математики. Поэтому её иногда называют *основной теоремой алгебры*. Любопытно отметить, что несмотря на название теоремы любое её доказательство, а таких доказательств существует множество, по необходимости использует в той или иной мере аппарат математического анализа, а точнее, те свойства действительных и комплексных чисел, которые связаны с непрерывностью. Приведённое далее доказательство почти целиком алгебраическое. Единственный факт из анализа, который мы будем использовать, интуитивно очевиден. А именно, непрерывность многочлена с действительными коэффициентами как вещественной функции позволяет утверждать, что любой такой многочлен нечётной степени имеет хотя бы один корень в $\mathbb{R}$.

Замечание. Восходящее к Гауссу доказательство теоремы, использующее так называемую лемму Даламбера, напротив, почти целиком аналитично. Его можно прочесть в [2] или [5].

Теорема 5.5.2 (основная теорема алгебры)**.** *Пусть f — многочлен из $\mathbb{C}[x]$ и $\deg f > 0$. Тогда существует элемент α из $\mathbb{C}$ такой, что $f(\alpha) = 0$.*

Доказательство. Поскольку при умножении на ненулевой скаляр корни многочлена не изменятся, можно полагать, что старший коэффициент многочлена f равен 1, т. е.

$$f = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n. \tag{4}$$

Мы начнём с уже упомянутого нами утверждения о существовании действительного корня у многочлена нечётной степени с действительными коэффициентами.

Лемма 1. *Пусть $f \in \mathbb{R}[x]$ и $\deg f$ — нечётное число. Тогда существует $\alpha \in \mathbb{R}$ такое, что $f(\alpha) = 0$.*

Доказательство леммы. Положим $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$. Пусть $\beta \in \mathbb{R}$ удовлетворяет условию $|\beta| > 1 + A$. Тогда

$$\begin{gathered} |a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1}| \leqslant A(1 + |\beta| + \ldots + |\beta|^{n-1}) = \\ = A\frac{|\beta|^n - 1}{|\beta| - 1} < \frac{A}{|\beta| - 1}|\beta|^n < |\beta|^n. \end{gathered} \tag{5}$$

Поскольку степень n многочлена f нечётна, из неравенства (5) следует, что если $\beta > 0$, то $f(\beta) > 0$, а $f(-\beta) < 0$. Поскольку $f(x)$ — непрерывная действительная функция действительного аргумента, по теореме Коши–Больцано она имеет действительный корень α на отрезке $[-\beta, \beta]$, и лемма доказана. □

Замечание. Отметим, что цепочка неравенств (5) выполняется и в том случае, когда $a_i, \beta \in \mathbb{C}$. Фактически, она позволяет оценить значение модуля корня произвольного многочлена с числовыми коэффициентами. Мы сформулируем этот результат вместе с необходимым утверждением о свойствах модуля комплексного числа в качестве упражнения.

Упражнение 5.5.3.

1. *Если $\alpha, \beta \in \mathbb{C}$, то $|\alpha + \beta| \leqslant |\alpha| + |\beta|$ и $|\alpha\beta| = |\alpha||\beta|$.*

2. *Если $f \in \mathbb{C}[x]$ имеет вид (4), $\alpha \in \mathbb{C}$ и $f(\alpha) = 0$, то $|\alpha| \leqslant 1 + A$, где $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|\}$. Иными словами, любой корень многочлена f лежит на комплексной плоскости в круге радиуса $1 + A$ с центром в начале координат.*

Вернёмся к доказательству теоремы. Следующая ключевая лемма показывает, что произвольный многочлен с действительными коэффициентами имеет хотя бы один комплексный корень.

Лемма 2. *Пусть* $f \in \mathbb{R}[x]$ *и* $\deg f > 0$. *Тогда существует* $\alpha \in \mathbb{C}$ *такое, что* $f(\alpha) = 0$.

Доказательство леммы. Пусть f многочлен вида (4) и $n = 2^k m$, где $k \in \mathbb{N}_0$ и m — нечётное натуральное число. Будем вести индукцию по k, воспользовавшись тем, что база индукции нами уже установлена в предыдущей лемме. Таким образом, предположение индукции состоит в том, что любой многочлен из $\mathbb{R}[x]$, степень которого не делится на 2^k, имеет комплексный корень.

Поскольку $\mathbb{R} \subseteq \mathbb{C}$, можно считать, что $f \in \mathbb{C}[x]$. В силу следствия о разложении многочлена на линейные множители в расширении поля из теоремы 5.5.1 существует расширение K поля $\mathbb{C}$ такое, что $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$, где $\alpha_i \in K$ для любого $i = 1, \dots, n$. Пусть γ — произвольное действительное число. Для $i, j \in \{1, \dots, n\}$ таких, что $i < j$, положим

$$\beta_{ij} = \alpha_i \alpha_j + \gamma(\alpha_i + \alpha_j). \tag{6}$$

Элементы β_{ij} лежат в поле K и общее их число равно

$$\frac{n(n-1)}{2} = \frac{2^k m(2^k m - 1)}{2} = 2^{k-1} l,$$

где число l нечётно. Кроме того, несложно заметить, что любая перестановка в наборе α_i приводит лишь к перестановке в наборе β_{ij}.

Пусть многочлен $g(x) \in K[x]$ имеет в качестве корней в точности все элементы β_{ij}, т. е

$$g(x) = \prod_{i<j} (x - \beta_{ij}). \tag{7}$$

Докажем, что многочлен g имеет действительные коэффициенты. В силу формул Виета коэффициенты многочлена g являются элементарными симметрическими многочленами от β_{ij}. Следовательно, ввиду (6) они являются многочленами от $\alpha_1, \dots, \alpha_n$ с действительными коэффициентами (число γ действительное). Более того, поскольку любая перестановка в наборе $\alpha_1, \dots, \alpha_n$ влечёт лишь перестановку в наборе β_{ij}, коэффициенты g — симметрические многочлены с действительными коэффициентами от $\alpha_1, \dots, \alpha_n$. В силу основной теоремы о симметрических многочленах коэффициенты g — многочлены с действительными коэффициентами от элементарных симметрических многочленов от

$\alpha_1, \ldots, \alpha_n$, т. е от коэффициентов многочлена f, которые лежат по условию в $\mathbb{R}$. Таким образом, $g \in \mathbb{R}[x]$.

С другой стороны, степень многочлена g равна $2^{k-1}l$ и не делится на 2^k, (хотя, возможно, и больше степени многочлена f). Значит, по предположению индукции g имеет хотя бы один комплексный корень. Поскольку действительное число γ мы выбирали произвольно, для каждого $\gamma \in \mathbb{R}$ найдутся такие $i, j \in \{1, \ldots, n\}$, где $i < j$, что $\beta_{ij} \in \mathbb{C}$. Кроме того, имеется лишь конечное число пар (i, j), а множество $\mathbb{R}$ бесконечно. Поэтому найдётся два различных действительных числа γ_1 и γ_2 таких, что для одной и той же пары индексов (i, j) числа a и b, удовлетворяющие равенствам

$$\begin{cases} a = \alpha_i\alpha_j + \gamma_1(\alpha_i + \alpha_j), \\ b = \alpha_i\alpha_j + \gamma_2(\alpha_i + \alpha_j), \end{cases} \tag{8}$$

одновременно лежат в поле комплексных чисел. Из системы равенств (8) вытекает, что $(\gamma_1 - \gamma_2)(\alpha_i + \alpha_j) = a - b$. Следовательно, сумма

$$\alpha_i + \alpha_j = \frac{a - b}{\gamma_1 - \gamma_2}$$

является комплексным числом. Но тогда и произведение $\alpha_i\alpha_j$ — комплексное число. Следовательно, α_i, α_j — корни квадратного уравнения с комплексными коэффициентами, а значит, сами лежат в поле $\mathbb{C}$. Лемма доказана. □

Завершим доказательство теоремы. Пусть $f \in \mathbb{C}[x]$. Положим

$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_{n-1}x^{n-1} + x^n,$$

где черта над коэффициентами означает комплексное сопряжение, и рассмотрим многочлен

$$h(x) = f(x)\overline{f}(x) = b_0 + b_1 x + \ldots + b_{2n-1}x^{2n-1} + b_{2n}x^{2n}.$$

Коэффициенты многочлена h удовлетворяют равенствам

$$b_k = \sum_{i+j=k} a_i\overline{a}_j.$$

Поэтому

$$\overline{b}_k = \sum_{i+j=k} \overline{a}_i a_j = b_k,$$

откуда $b_k \in \mathbb{R}$ для любого $k = 0, \ldots, 2n$. Следовательно, $h \in \mathbb{R}[x]$ и по лемме 2 существует $\alpha \in \mathbb{C}$ такой, что $h(\alpha) = f(\alpha)\overline{f}(\alpha) = 0$. Если

$f(\alpha) \neq 0$, то $\overline{f}(\alpha) = 0$. Отсюда $f(\overline{\alpha}) = \overline{\overline{f}(\alpha)} = \overline{0} = 0$. В любом случае, либо α, либо $\overline{\alpha}$ — корень многочлена f. Теорема доказана. □

Следствие (о разложимости многочленов над полями действительных и комплексных чисел)**.** 1. *Каждый многочлен $f \in \mathbb{C}[x]$ степени, большей 0, раскладывается над $\mathbb{C}$ на линейные множители.*

2. *Каждый многочлен $f \in \mathbb{R}[x]$ степени, большей 0, раскладывается над $\mathbb{R}$ в произведение многочленов степени не выше 2.*

Доказательство. 1. Индукция по степени многочлена. Поскольку в силу доказанной нами теоремы f имеет корень α в $\mathbb{C}$, для некоторого многочлена $f_1 \in \mathbb{C}$ выполняется $f = (x-\alpha)f_1$. Степень f_1 меньше степени f, значит, для него по предположению индукции искомое разложение существует. Следовательно, оно существует и для f.

2. Снова индукция по степени f. Если f имеет хотя бы один действительный корень, то, рассуждая, как при доказательстве п. 1, приходим к многочлену $f_1 \in \mathbb{R}$, имеющему степень меньше степени f. Таким образом, можно считать, что действительных корней у f нет. Тем не менее, по основной теореме алгебры хотя бы один комплексный корень у f имеется. Заметим, что в нашем случае $\overline{f}(x) = f(x)$. Следовательно, если α — комплексный корень многочлена f, то $f(\overline{\alpha}) = \overline{\overline{f}(\alpha)} = \overline{f(\alpha)} = \overline{0} = 0$. Поэтому $\overline{\alpha}$ — ещё один корень многочлена f. Поскольку $(x-\alpha, x-\overline{\alpha}) = 1$, многочлен f делится на многочлен $g(x) = (x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$, коэффициенты которого, как несложно проверить, лежат в $\mathbb{R}$. Таким образом, $f = gf_1$, где степень f_1 меньше степени f. □

§ 5.6. Разложимость над полем рациональных чисел

В этом параграфе мы рассмотрим вопрос о разложимости многочленов с рациональными коэффициентами. В отличие от многочленов с действительными и комплексными коэффициентами в этом случае явного описания неразложимых многочленов получить не удаётся. В частности, как мы покажем ниже, существуют неразложимые над $\mathbb{Q}$ многочлены сколь угодно большой степени.

Пусть

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Q}[x], a_i = \frac{p_i}{q_i}, p_i \in \mathbb{Z}, q_i \in \mathbb{N}. \qquad (1)$$

Если обозначить через a наименьшее общее кратное чисел q_i, $i = 1, \ldots, n$, то многочлен $af(x)$ имеет уже целые коэффициенты. С

другой стороны, вопрос о разложимости f равносилен вопросу о разложимости af (см. предложение 5.2.3). Поэтому в дальнейшем мы будем предполагать, что $f \in \mathbb{Z}[x]$, т. е. его коэффициенты a_i — целые числа.

Определение 5.6.1. Многочлен $f \in \mathbb{Z}[x]$ называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1.

Если $f \in \mathbb{Z}[x]$, то $f(x) = dp(x)$, где d — наибольший общий делитель a_i, а $p(x)$ — примитивный многочлен. Таким образом, решая вопрос о разложимости многочлена f с рациональными коэффициентами над $\mathbb{Q}$, мы можем полагать, что f — примитивный многочлен с целыми коэффициентами. Оказывается, что вопрос о разложимости многочлена с целыми коэффициентами над $\mathbb{Q}$ равносилен вопросу о его разложимости над $\mathbb{Z}$.

Теорема 5.6.1. *Если многочлен $f \in \mathbb{Z}[x]$ неразложим над $\mathbb{Z}$, то f неразложим и над $\mathbb{Q}$.*

Доказательство. Ключевую роль в доказательстве играет следующая

Лемма (Гаусс)**.** *Произведение примитивных многочленов есть примитивный многочлен.*

Доказательство леммы. Пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n$ и $g(x) = b_0 + b_1x + \ldots + b_mx^m$ — примитивные многочлены и $h = fg = \sum_{k=0}^{n+m} c_kx^k$. Предположим, что найдётся простое число p, которое делит c_k для каждого $k = 0, 1, \ldots, n+m$. Из примитивности многочленов f и g следует, что p не может делить все коэффициенты этих многочленов. Пусть a_r — коэффициент с наименьшим индексом в f, который не делится на p, а b_s — коэффициент с наименьшим индексом в g, который не делится на p. Коэффициент c_{r+s} многочлена h равен

$$\sum_{i+j=r+s} a_ib_j = \underbrace{(a_0b_{r+s} + \ldots + a_{r-1}b_{s+1})}_{\vdots p} + \underbrace{a_rb_s}_{\not\vdots p} + \underbrace{(a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0)}_{\vdots p}.$$

Таким образом, c_{r+s} не делится на p; противоречие. □

Вернёмся к доказательству теоремы. Пусть f — многочлен с целыми коэффициентами. Предположим, что f раскладывается в произведение многочленов $g, h \in \mathbb{Q}[x]$ и $\deg g < \deg f$, $\deg h < \deg f$. Многочлены g и h можно представить в виде

$$g(x) = \frac{a}{b}u(x), h = \frac{c}{d}v(x),$$

где $a, b, c, d \in \mathbb{N}$, u, v — примитивные многочлены над $\mathbb{Z}$. Тогда

$$f = \frac{ac}{bd}uv = \frac{p}{q}uv, \text{ где } (p, q) = 1.$$

Отсюда вытекает равенство

$$qf = puv. \tag{2}$$

В силу леммы Гаусса произведение uv — снова примитивный многочлен. Поэтому наибольший общий делитель коэффициентов многочлена, стоящего в правой части равенства (2), равен p. С другой стороны, все коэффициенты многочлена, стоящего в левой части равенства (2), делятся на q. Следовательно, q делит p. Поскольку $(p, q) = 1$, имеем $q = 1$. Таким образом, $f = puv = (pu)v$ раскладывается в произведение многочленов (pu) и v с целыми коэффициентами, степень которых меньше степени f. □

Теперь мы укажем признак неразложимости многочлена над $\mathbb{Q}$.

Теорема 5.6.2 (признак Эйзенштейна). *Пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$. Если существует простое число p, удовлетворяющее следующим условиям:*

1) $p \mid a_k$ *для каждого* $k = 0, 1, \ldots, n-1$,

2) $p \nmid a_n$,

3) $p^2 \nmid a_0$,

то многочлен f неразложим над $\mathbb{Q}$.

Доказательство. Пусть $f = gh$, $g, h \in \mathbb{Q}[x]$, $\deg g < n$, $\deg h < n$ и $g = \sum_{i=0}^{m} b_ix^i$, $h = \sum_{j=0}^{s} c_jx^j$. В силу теоремы 5.6.1 можно считать, что коэффициенты b_i, c_j многочленов g и h — целые числа.

Поскольку p делит $a_0 = b_0c_0$, оно делит либо b_0, либо c_0. Пусть для определённости $p \mid b_0$. С другой стороны, p^2 не делит a_0, следовательно, p не делит c_0. Рассмотрим следующий коэффициент $a_1 = b_0c_1 + b_1c_0$. Число p делит a_1 и b_0, следовательно, p делит $b_1c_0 = a_1 - b_0c_1$. Поскольку p — простое число и p не делит c_0, оно делит b_1. Действуя аналогичным образом, можно показать, что p делит b_i для любого $i = 0, 1, \ldots, m$. Действительно, пусть для $i < k$ это уже доказано. В силу того, что p делит $a_k = b_0c_1 + \ldots + b_{k-1}c_1 + b_kc_0$, оно делит b_kc_0. Отсюда p делит b_k. В частности, отсюда следует, что p делит старший коэффициент b_m многочлена g. Но тогда p делит и старший коэффициент $a_n = b_mc_s$ многочлена f, что противоречит условию теоремы. □

Следствие. *Для любого натурального числа n существует многочлен $f \in \mathbb{Z}[x]$, неразложимый над $\mathbb{Q}$. В частности, над $\mathbb{Q}$ неразложим многочлен $x^n - 2$.*

Доказательство. Достаточно применить признак Эйзенштейна к многочлену $x^n - 2$. □

Таким образом, как уже говорилось в начале этого параграфа, явного описания многочленов, неразложимых над $\mathbb{Q}$, получить нельзя. Однако для каждого конкретного многочлена $f \in \mathbb{Q}[x]$ за конечное число шагов можно определить, разложим ли он над $\mathbb{Q}$ или нет. Иными словами, проблема разложимости многочлена в $\mathbb{Q}[x]$ *алгоритмически разрешима.*

Теорема 5.6.3. *Проблема разложимости многочлена из $\mathbb{Q}[x]$ алгоритмически разрешима: если $f \in \mathbb{Q}[x]$, то за конечное число шагов можно определить, разложим ли f в $\mathbb{Q}[x]$, и, если f разложим, найти представление $f = uv$, где $u, v \in \mathbb{Q}[x]$ и $\deg u < \deg f$, $\deg v < \deg f$.*

Доказательство. Можно считать, что $f \in \mathbb{Z}[x]$ и $\deg f > 1$. По теореме 5.6.1 многочлен f разложим над $\mathbb{Q}$ тогда и только тогда, когда он разложим над $\mathbb{Z}$. Поэтому, если f разложим, то найдутся многочлены $u, v \in \mathbb{Z}[x]$ такие, что $f = uv$. Поскольку для степеней многочленов u и v выполняется $\deg u + \deg v = n$, меньшая из этих степеней не превосходит числа $m = \left[\frac{n}{2}\right]$. Пусть для определённости $\deg u \leqslant m$. Рассмотрим некоторый набор $\alpha_0, \alpha_1, \ldots, \alpha_m$ из $m+1$ целого числа такой, что все числа, входящие в набор, попарно различны. Для каждого $k = 0, 1, \ldots, m$ выполняется $f(\alpha_k) = u(\alpha_k)v(\alpha_k)$. Поэтому целое число $u(\alpha_k)$ делит целое число $f(\alpha_k)$. Заметим, что мы можем считать, что $f(\alpha_k) \neq 0$, иначе $f = (x - \alpha_k)f_1$, многочлен f разложим и искомое разложение найдено. Поэтому для каждого $k = 0, 1, \ldots, m$ множество $M_k = \{\beta \in \mathbb{Z} \mid \beta \text{ делит } f(\alpha_k)\}$ состоит из конечного числа элементов. Конечным будет и множество $M = \{(\beta_0, \beta_1, \ldots, \beta_m) \mid \beta_k \in M_k\}$. Зафиксируем некоторый элемент $c = (\beta_0, \beta_1, \ldots, \beta_m) \in M$. Построим интерполяционный многочлен Лагранжа u_c, для которого $u_c(\alpha_k) = \beta_k$ для всех $k = 0, 1, \ldots, m$. Поскольку многочлен степени, не превосходящей m, однозначно определяется своими значениями в $m+1$ точке, если многочлен f разложим, то многочлен u должен совпасть с одним из многочленов u_c для некоторого $c \in M$. Следовательно, деля последовательно многочлен f на интерполяционные многочлены u_c, где $c \in M$, мы либо найдём подходящие многочлены u и v, либо, исключив все возможности, придём к выводу, что f неразложим. В любом случае, потребуется лишь конечное число шагов, так как множество M конечно. □

Следствие. *Многочлен $f \in \mathbb{Q}[x]$ за конечное число шагов можно разложить в произведение неразложимых многочленов из $\mathbb{Q}[x]$. В частности, за конечное число шагов можно определить все рациональные корни многочлена f.*

Доказательство. Индукция по степени f. Если f неразложим, то в силу доказанной нами теоремы мы определим это за конечное число шагов. Если он разложим, то за конечное число шагов мы найдём представление f в виде произведения двух многочленов из $\mathbb{Q}[x]$, для каждого из которых утверждение следствия выполняется по предположению индукции. Следовательно, и разложение для f будет получено за конечное число шагов. Далее, если $\alpha_1, \ldots, \alpha_s$ — все рациональные корни многочлена f, то в полученном нами за конечное число шагов разложении f на неразложимые множители, которое единственно в силу теоремы 5.2.4, встретятся делители $(x - \alpha_1), \ldots, (x - \alpha_s)$. □

Заметим, что вопрос о рациональных корнях многочлена с целыми (рациональными) коэффициентами можно решить и не прибегая к методу, развитому в доказательстве теоремы 5.6.3. В частности, для решения этого вопроса достаточно следующих утверждений, которые мы сформулируем в качестве упражнения.

Упражнение 5.6.1. *Пусть $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$, $\alpha = \frac{p}{q}$, где $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $(p, q) = 1$ и $f(\alpha) = 0$. Тогда выполняются следующие утверждения:*

1) $p \mid a_0$;

2) $q \mid a_n$;

3) $(p - mq) \mid f(m)$ *для каждого* $m \in \mathbb{Z}$.

Замечание. На самом деле, уже первых двух пунктов достаточно, чтобы свести вопрос о рациональных корнях многочлена f к перебору конечного числа вариантов. Применение же п. 3 позволяет зачастую свести такой перебор к минимуму.

Упражнение 5.6.2. *Для многочлена* $f(x) = 2x^6 + 5x^5 - 3x^4 + 2x^3 + 7x^2 + 2x - 3$

1) *используя предыдущее упражнение, найдите его рациональные корни;*

2) *используя метод, изложенный при доказательстве теоремы, а также результаты предыдущего пункта, разложите f в произведение неразложимых многочленов из $\mathbb{Q}[x]$.*

В заключение отметим, что задача разложения произвольного многочлена f в произведение неразложимых многочленов над полями $\mathbb{R}$

и $\mathbb{C}$, даже если предположить, что коэффициенты f — целые числа, не разрешима за конечное число шагов. Так, для многочлена $f(x) = x^5 - 10x + 10$ не существует алгоритма разложения его на линейные множители над полем $\mathbb{C}$. Это утверждение, как и общий вопрос о разрешимости уравнений степени, большей 4, составляет содержание теории Галуа, изложение которой лежит за рамками этого курса.

Предметный указатель

Указатель обозначений

Приложение

Программа курса высшей алгебры

2010–11 учебный год

1 семестр

1. Введение

Алгебраическая операция, алгебраическая система, сужение операции на подмножество, подсистема, изоморфизм [4, гл. 4, § 1]; [1, § 9].

2. Группы, кольца, поля

Группа, кольцо, поле: аксиомы, примеры, элементарные свойства, кольцо вычетов [1, § 6, 11, 12]; [5, § 63, 64, 43–45]; [2, гл. 1, § 3, 6]. Группа подстановок: проверка аксиом, разложение подстановки в произведение циклов, декремент, чётность, разложение в произведение транспозиций, чётность произведения, знакопеременная группа [4, гл. 4, § 2]. Кольцо квадратных матриц: проверка аксиом [6, § 1], разложение матрицы в произведение элементарных и диагональной матриц. Определитель, его поведение при простейших преобразованиях. Определитель произведения матриц. Разложение определителя по строке (столбцу) [5, § 4–6]. Обратная матрица: существование, вычисление, решение линейных матричных уравнений [6, § 2]. Поле комплексных чисел: существование, единственность. Геометрическая интерпретация комплексных чисел: модуль, аргумент, тригонометрическая форма записи, формула Муавра, извлечение корня n-ой степени из комплексного числа [4, гл. 5, § 1]; [5, § 46]; [2, гл. 1,§ 5].

3. Векторные пространства

Векторное пространство над полем: аксиомы, примеры, понятие подпространства. Алгебра и подалгебра над полем: примеры [5, § 9, 29]; [6, § 4]; [2, гл. 1, § 7, 8]. Базис и размерность векторного пространства: линейные комбинации, линейная зависимость, эквивалентные наборы

векторов, теорема о замене и её следствия, базис пространства, размерность, координаты, изоморфизм пространств. Матрица перехода, её невырожденность, связь между координатами в разных базах [5, § 9, 29, 30]; [6, § 4, 5]; [2, гл. 1, § 7, гл. 2, § 2]. Подпространство, базис, согласованный с подпространством, взаимное расположение подпространств, сумма и пересечение подпространств, связь между их размерностями, прямая сумма [6, § 6]; [2, гл. 5, § 1].

4. Системы линейных уравнений

Ранг матрицы: ранг набора векторов, строчный и столбцевой ранги матрицы, минор, минорный ранг, теорема о совпадении трёх рангов, вычисление ранга приведением матрицы к ступенчатому виду, ранг суммы и произведения матриц [5, § 10]; [6, § 5]; [2, гл. 2, § 1]. Система линейных уравнений: векторная и матричная формы, критерий совместности системы линейных уравнений (теорема Кронекера–Капелли), общее решение и метод Гаусса его поиска, системы линейных уравнений с ненулевым определителем, формулы Крамера [5, § 1, 7]; [6, § 5]; [2, гл. 2, § 1]. Однородные системы: пространство решений, фундаментальный набор решений, связь между однородными и неоднородными системами, теорема Фредгольма [5, § 11, 12]; [6, § 5].

5. Кольца многочленов

Многочлены от одной переменной: определение, кольцо многочленов над кольцом и полем, степень суммы и произведения многочленов [5, § 20]; [2, гл. 3, § 1]. Делимость в кольце многочленов: деление с остатком, наибольший общий делитель, алгоритм Евклида, взаимно простые многочлены, неразложимые многочлены, разложение на линейные множители [5, § 21, 48]; [2, гл. 3, § 5]. Значения и корни многочленов: теорема Безу, теорема о числе корней, интерполяционный многочлен Лагранжа, кратные корни, характеристика поля, производная и её приложения к многочленам над полем характеристики 0, формула Тейлора, интерполяционный многочлен Лагранжа–Сильвестра [5, § 22], [6, § 16.3]; [2, гл. 3, § 2]. Кольцо многочленов от нескольких переменных: определение, элементарные свойства, лексикографическое упорядочение одночленов, старшая степень, симметрические многочлены, основная теорема о симметрических многочленах [5, § 51–52]; [2, гл. 3, § 7, 8]. Теорема о существовании корня многочлена в расширении поля и её следствия: разложение на линейные множители в расширении

поля, формулы Виета [5, § 49]. Алгебраическая замкнутость поля комплексных чисел и разложение многочленов на множители над полями комплексных и вещественных чисел [5, § 55]. Разложимость многочлена над полем рациональных чисел: сведение к многочленам с целочисленными коэффициентами, признак неразложимости над кольцом целых чисел и существование неразложимого многочлена произвольной степени, алгоритмическая разрешимость проблемы разложения многочлена над полем рациональных чисел [5, § 56-57]; [2, гл. 3, § 6]. Оценка числа действительных корней: границы корней, ряд Штурма и теорема Штурма [5, § 39, 40].

2 семестр

6. Линейные преобразования векторных пространств

Линейное преобразование (ЛП) и его матрица. Координаты образа, связь между матрицами ЛП в разных базах, подобные матрицы. Операции над ЛП, изоморфизм алгебраической системы ЛП и алгебры матриц [6, § 8,9]. Ядро и образ ЛП, невырожденные ЛП [6, § 10]; [7]. Инвариантное пространство, ограничение на нём ЛП. Собственные векторы и собственные значения, характеристический многочлен [6, § 11]; [7]. Корневые подпространства, разложение в прямую сумму корневых подпространств. Нильпотентное ЛП, разложение в прямую сумму циклических подпространств. Жорданова база пространства. Жорданова форма матрицы [7]; [4, Дополнение]; [2, гл. 6, § 4]. Многочлены от матриц и линейных преобразований. Минимальный аннулирующий многочлен, теорема Гамильтона–Кэли, теорема о ядерном разложении. Функции от матриц и линейных преобразований, представления их значений значениями многочленов [6, § 16]; [7].

7. Евклидовы и унитарные пространства и их линейные преобразования

Евклидовы и унитарные пространства: аксиомы, примеры. Процесс ортогонализации, ортонормированные базы, ортогональное дополнение к подпространству. Сопряжённые преобразования: связь между матрицами. Нормальные преобразования, свойство их собственных векторов, канонический вид матрицы нормального преобразования в унитарном и евклидовом пространстве. Унитарные, ортогональные и самосопряжённые преобразования, их матрицы, канонический вид унитарного, ортогонального и самосопряжённого преобразований. Неотрицательные

самосопряжённые преобразования, сингулярные числа, полярное и сингулярное разложение матрицы [6, § 17–20].

8. Квадратичные формы

Матрица квадратичной формы, её изменение при линейной замене. Алгоритм Лагранжа приведения к диагональному виду. Нормальная форма вещественной квадратичной формы, закон инерции квадратичных форм. Приведение к главным осям. Положительно определённые квадратичные формы и одновременная диагонализация двух форм [6, § 22–23]; [5, §26–28].

9. Элементы теории групп

Группы и их подгруппы: примеры. Порождающее множество и циклическая подгруппа. Смежные классы по подгруппе, индекс подгруппы и теорема Лагранжа. Сопряжённые элементы, коммутаторы, нормальные подгруппы и фактор-группы. Теоремы о гомоморфизмах. Прямые произведения групп, связь между двумя определениями. Разложение циклической группы конечного порядка в прямое произведение примарных подгрупп. Действие группы на множестве. Стабилизатор и орбита, связь между их порядками. Теорема Бернсайда о количестве орбит и её применение к задаче о раскраске тетраэдра [5, гл. 14]; [2, гл. 4 и гл. 10 § 1,3]; [3, § 1–2, 4, 11]; [1, гл. 2].

Список литературы

1. *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1976.
2. *Винберг Э. Б.* Курс алгебры. М.: Факториал Пресс, 2002.
3. *Каргополов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1982.
4. *Кострикин А. И.* Введение в алгебру. М.: Наука, 1977.
5. *Курош А. Г.* Курс высшей алгебры. М.: Наука, 1968.
6. *Мальцев А. И.* Основы линейной алгебры. М.: Наука, 1970.
7. *Чуркин В. А.* Жорданова классификация конечномерных линейных операторов. Новосибирск: НГУ, 1991.

Учебное издание

Васильев Андрей Викторович,
Мазуров Виктор Данилович

ВЫСШАЯ АЛГЕБРА

Конспект лекций

Часть I

Редактор Е.В. Дубовцева

Подписано в печать 03.12.2010
Формат 60 × 84 1/16. Офсетная печать
Уч.-изд. л. 8,9. Усл. печ. л. 8,3. Тираж 130 экз.
Заказ №

Редакционно-издательский центр НГУ
630090, Новосибирск-90, ул. Пирогова, 2