Министерство образования и науки Российской Федерации

Сибирский федеральный университет

АЛГЕБРА

Часть I

Электронное издание

Красноярск
СФУ
2014

УДК 512 (07)
ББК 22.14я73
А 456

Составители: Осипов Николай Николаевич, Медведева Мария Ивановна

А 456 Алгебра. Часть I: учебно-методическое пособие [Электронный ресурс] / сост. Н. Н. Осипов, М. И. Медведева. — Электрон. дан. — Красноярск: Сиб. федер. ун-т, 2014. — Систем. требования: PC не ниже класса Pentium I; 128 Mb RAM; Windows 98/XP/7; Adobe Reader V8.0 и выше. — Загл. с экрана.

Настоящее пособие составлено в соответствии с рабочими программами дисциплин «Алгебра», «Высшая алгебра» и включает в себя следующие разделы: «Системы линейных уравнений. Арифметические векторные пространства», «Матричная алгебра. Теория определителей», «Основные алгебраические структуры».

Предназначено для студентов специальностей 090301.65 «Компьютерная безопасность», 090900.62 «Информационная безопасность» и 231300.62 «Прикладная математика».

УДК 512 (07)
ББК 22.14я73

Электронное учебное издание

Подготовлено к публикации Издательским центром БИК СФУ

Подписано в свет 25.03.2014 г. Заказ 0451.
Тиражируется на машиночитаемых носителях.

Издательский центр Библиотечно-издательского комплекса
Сибирского федерального университета
660041, г. Красноярск, пр. Свободный, 79
Тел/факс (391) 206-21-49. e-mail: rio.bik@mail.ru
http://rio.sfu-kras.ru

Содержание

Предисловие

Учебно-методическое пособие представляет собой конспект лекций, составленный в соответствии с рабочими программами дисциплин «Алгебра», «Высшая алгебра» для специальностей 090301.65 «Компьютерная безопасность», 090900.62 «Информационная безопасность» и 231300.62 «Прикладная математика».

Конспект состоит из 3-х глав: «Системы линейных уравнений. Арифметические векторные пространства», «Матричная алгебра. Теория определителей» и «Основные алгебраические структуры». Главы разделены на параграфы, каждый из которых по объёму материала соответствует примерно одной реальной лекции.

По традиции, а также из соображений преемственности между школьной математикой и математикой в университете первая глава посвящена решению и исследованию общих систем линейных уравнений. Во второй главе излагается необходимая для этого и важная сама по себе техника матриц и определителей. На этом пути естественным образом возникают основные структуры алгебры, первоначальное знакомство с которыми составляет содержание третьей главы.

Каждый параграф имеет собственную нумерацию «теоремоподобных» конструкций (определений, лемм, теорем и т. п.), это же относится и к нумерации формул.

Важная роль отводится теоретическим упражнениям: авторы настоятельно рекомендуют их регулярно прорешивать, что будет способствовать более основательному пониманию идей и методов доказательства теоретических фактов. Следует подчеркнуть, что чтение одного лишь конспекта лекций не может заменить собой чтения полноценных учебников, к которым также рекомендуется периодически обращаться за получением более полного представления о предмете (см. список литературы).

Глава 1
Системы линейных уравнений. Арифметические векторные пространства

§ 1. Системы линейных уравнений. Метод Гаусса. Однородные системы линейных уравнений

Система линейных уравнений (СЛУ). Классификация СЛУ по количеству решений. Равносильность СЛУ. Элементарные преобразования СЛУ и их свойства. Исследование СЛУ методом исключения неизвестных (метод Гаусса). Однородная система линейных уравнений (ОСЛУ). Теорема о ненулевых решениях ОСЛУ. Связь между решениями СЛУ и решениями ассоциированной ОСЛУ.

Простейшие типы систем линейных уравнений возникают ещё в школьном курсе алгебры. В качестве примера рассмотрим систему из двух уравнений с двумя неизвестными:

$$\begin{cases} ax + by = c, \\ dx + ey = f. \end{cases}$$

Здесь a, b, …, f — фиксированные числа, x, y — неизвестные, которые подлежат определению. Задача состоит в том, чтобы найти все возможные наборы значений неизвестных, удовлетворяющие данной системе уравнений.

Далее мы сформулируем эту задачу в общем виде и укажем основной способ её решения.

I. Определения и примеры. Начнём с основных определений.

Определение 1. Уравнение вида

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

называется *линейным уравнением* с неизвестными x_1, …, x_n и коэффициентами a_1, …, a_n, b. Коэффициенты являются фиксированными вещественными числами, значения неизвестных также предполагаются вещественными.

Замечание. Под числом в дальнейшем мы будем понимать, как правило, вещественное (действительное) число. Множество всех вещественных чисел обычно обозначают через $\mathbb{R}$. Общепринятые обозначения для других числовых множеств: $\mathbb{N}$, $\mathbb{Z}$ и $\mathbb{Q}$ — множества натуральных, целых и рациональных чисел соответственно.

Произвольная *система линейных уравнений* (далее коротко СЛУ) с неизвестными x_1, …, x_n может быть записана в виде

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

Число a_{ij} есть коэффициент при j-м неизвестном x_j в i-м уравнении системы. Число b_i называется свободным коэффициентом i-го уравнения системы. Количество уравнений в СЛУ (1) равно m и оно, вообще говоря, не совпадает с числом неизвестных n. Те СЛУ (1), для которых $m = n$, принято называть *квадратными*.

Определение 2. *Решением* СЛУ (1) называют любой такой упорядоченный набор

$$x^* = (x_1^*, \ldots, x_n^*)$$

чисел, что при подстановке $x_j = x_j^*\,(j = 1, \ldots, n)$ все уравнения системы превращаются в верные числовые равенства.

Например, решениями СЛУ

$$\begin{cases} x_1 + 2x_2 - 3x_3 = 0, \\ 2x_1 + 3x_2 = 5 \end{cases}$$

будут наборы чисел $(1, 1, 1)$ и $(-2, 3, \frac{4}{3})$, но есть и другие решения. А вот СЛУ

$$\begin{cases} x_1 - 2x_2 = 0, \\ x_1 - 2x_2 = 1, \end{cases}$$

как очевидно, не имеет ни одного решения.

Определение 3. *Решить* СЛУ (1) — это значит найти все её решения или доказать, что решений не существует.

Мы будем использовать следующую терминологию: *совместная* СЛУ или *разрешимая* — та, у которой есть хотя бы одно решение; *несовместная* СЛУ или *неразрешимая* — не имеющая никаких решений; *совместная определённая* СЛУ или *однозначно разрешимая* — такая, которая имеет единственное решение; *совместная неопределённая* СЛУ имеет более одного решения.

Основную задачу теории СЛУ можно сформулировать так: выяснить, совместна ли данная СЛУ; если она совместна, то установить количество её решений, а также указать способ, позволяющий найти все эти решения.

Далее мы рассмотрим

II. Основной метод решения СЛУ. Этим методом является *метод последовательного исключения неизвестных* или *метод Гаусса*[1)].

Прежде чем переходить к изложению метода Гаусса, дадим ещё несколько определений и докажем один вспомогательный факт.

Определение 4. Две СЛУ называются *равносильными*, если они имеют одно и то же множество решений (быть может, пустое).

Говоря о равносильных СЛУ, мы, естественно, подразумеваем, они имеют одинаковый набор неизвестных (в частности, число неизвестных одно и то же). Один из способов решения любой системы уравнений состоит в её замене равносильной системой, которая в некотором смысле проще исходной. Переход к равносильной системе обычно осуществляется при помощи преобразований уравнений системы.

[1)] К. Ф. Гаусс (1777 — 1855) — немецкий математик, астроном и геодезист.

Применительно к СЛУ (1) мы будем говорить о следующих четырёх типах *элементарных преобразований* над уравнениями.

1. Перестановка местами двух каких-нибудь уравнений.

2. Умножение какого-нибудь уравнения на любое число $\lambda \neq 0$.

3. Прибавление к некоторому уравнению другого уравнения, предварительно умноженного на какое-нибудь число λ. При этом изменяется только то уравнение, к которому мы прибавляем.

4. Удаление *тривиального уравнения* $0x_1 + \ldots + 0x_n = 0$.

Можно отказаться от элементарных преобразований первого типа, поскольку каждое такое преобразование можно представить как композицию нескольких преобразований второго и третьего типов. Однако это неудобно практически, и этого не делают.

Упражнение 1. Найдите эту композицию.

Основной факт об элементарных преобразованиях описан в следующей теореме.

Теорема 1. Элементарные преобразования приводят СЛУ к равносильной ей СЛУ.

Доказательство. Пусть дана СЛУ (1). Предположим, что мы совершили какое-нибудь элементарное преобразование третьего типа, например ко второму уравнению прибавили первое уравнение, умноженное на число λ. Получилась СЛУ

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ (a_{21} + \lambda a_{11})x_1 + \ldots + (a_{2n} + \lambda a_{1n})x_n = b_2 + \lambda b_1, \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m, \end{cases} \tag{2}$$

которая отличается от СЛУ (1) только вторым уравнением. Нетрудно видеть, что СЛУ (2) равносильна СЛУ (1).

Действительно, всякое решение $x^* = (x_1^*, \ldots, x_n^*)$ СЛУ (1) очевидно будет и решением СЛУ (2), поскольку единственное вызывающее вопросы равенство

$$(a_{21} + \lambda a_{11})x_1^* + \ldots + (a_{2n} + \lambda a_{1n})x_n^* = b_2 + \lambda b_1$$

является следствием пары верных числовых равенств

$$a_{11}x_1^* + \ldots + a_{1n}x_n^* = b_1, \quad a_{21}x_1^* + \ldots + a_{2n}x_n^* = b_2$$

(первое из них умножим на λ и почленно сложим со вторым).

Обратное утверждение также верно, так как СЛУ (1), в свою очередь, может быть получена из СЛУ (2) элементарным преобразованием третьего типа, а именно: ко второму уравнению прибавим первое уравнение, умноженное на число $-\lambda$.

Итак, утверждение теоремы доказано для элементарных преобразований третьего типа. Для остальных типов элементарных преобразований оно очевидно. □

Таким образом, если к СЛУ применить одно или несколько элементарных преобразований, то полученная в результате СЛУ будет равносильна исходной.

Определение 5. Уравнение вида $0x_1 + \ldots + 0x_n = b$, где $b \neq 0$, называется *противоречивым уравнением*.

В отличие от тривиального уравнения, которое удовлетворяется любым набором значений неизвестных, противоречивое уравнение нельзя удовлетворить никаким набором значений неизвестных. Таким образом, наличие в СЛУ противоречивого уравнения сразу свидетельствует о её несовместности.

Идея метода Гаусса состоит в последовательном исключении неизвестных из уравнений данной СЛУ при помощи серий соответствующим образом подобранных элементарных преобразований. В итоге либо будет сделан вывод о несовместности исходной СЛУ, либо будет получена равносильная СЛУ специального вида, множество решений которой сравнительно легко найти.

Пусть $j_1 \geqslant 1$ — такой минимальный индекс, что среди коэффициентов $a_{1j_1}, \ldots, a_{mj_1}$ при неизвестном x_{j_1} есть ненулевые (мы предполагаем, что не все коэффициенты a_{ij} при неизвестных равны нулю). Не ограничивая общности рассуждений, будем считать, что $a_{1j_1} \neq 0$. Теперь исключим неизвестное x_{j_1} из всех уравнений СЛУ (1), начиная со второго, сделав серию элементарных преобразований третьего типа: для $i = 2, \ldots, m$ умножим первое уравнение на

$$\lambda_i = -\frac{a_{ij_1}}{a_{1j_1}}$$

и прибавим к i-му уравнению. Если при этом возникнут тривиальные уравнения, удалим их. Считая, что противоречивого уравнения не появилось (иначе СЛУ (1) несовместна), получим СЛУ следующего вида:

$$\begin{cases} a_{1j_1}x_{j_1} + \ldots + a_{1j_2}x_{j_2} + \ldots + a_{1n}x_n = b_1, \\ a'_{2j_2}x_{j_2} + \ldots + a'_{2n}x_n = b'_2, \\ \ldots \\ a'_{sj_2}x_{j_2} + \ldots + a'_{sn}x_n = b'_s. \end{cases} \tag{3}$$

Здесь $j_2 \geqslant 2$ — индекс первого неисключившегося неизвестного, поэтому среди коэффициентов $a'_{2j_2}, \ldots, a'_{sj_2}$ есть ненулевые (исключая x_{j_1}, мы могли исключить и несколько следующих неизвестных), $s \leqslant m$ — число оставшихся уравнений. Предполагая теперь, что $a'_{2j_2} \neq 0$, применим к подсистеме СЛУ (3), состоящей из всех уравнений, кроме первого, аналогичную серию элементарных преобразований с целью исключить неизвестное x_{j_2} из всех уравнений, начиная с третьего. И так далее.

В результате, если противоречивое уравнения так и не возникнет, мы придём к *ступенчатой* СЛУ из $r \leqslant n$ уравнений:

$$\begin{cases} a_{1j_1}x_{j_1} + \ldots + a_{1j_2}x_{j_2} + \ldots + a_{1j_r}x_{j_r} + \ldots + a_{1n}x_n = b_1, \\ a'_{2j_2}x_{j_2} + \ldots + a'_{2j_r}x_{j_r} + \ldots + a'_{2n}x_n = b'_2, \\ \ldots \\ \widetilde{a}_{rj_r}x_{j_r} + \ldots + \widetilde{a}_{rn}x_n = \widetilde{b}_r, \end{cases} \tag{4}$$

где $1 \leqslant j_1 < j_2 < \ldots < j_r \leqslant n$ и все коэффициенты $a_{1j_1}, a'_{2j_2}, \ldots, \widetilde{a}_{rj_r}$ отличны от нуля. Переход от СЛУ (1) к СЛУ (4) называют *прямым ходом* метода Гаусса. Множество решений ступенчатой СЛУ (4) можно найти при помощи *обратного хода* метода Гаусса. Опишем его, рассматривая отдельно случаи $r = n$ и $r < n$.

При $r = n$ ступенчатая СЛУ (4) называется *треугольной*: последнее уравнение содержит одно неизвестное, предпоследнее — два неизвестных и т. д. Такая система име-

ет единственное решение $(x_1^*, \ldots, x_n^*)$: сначала из последнего уравнения находим единственное возможное значение неизвестного $x_n = x_n^*$, затем из предпоследнего уравнения находим единственное возможное значение $x_{n-1} = x_{n-1}^*$ и т. д.

В случае $r < n$ неизвестные x_{j_k} $(k = 1, \ldots, r)$ будем называть *главными*, а остальные неизвестные — *свободными*. Двигаясь по уравнениям СЛУ (4) снизу вверх, мы последовательно, начиная с главного неизвестного x_{j_r}, выразим все главные неизвестные только через свободные неизвестные (можно сказать, что при фиксированных значениях свободных неизвестных СЛУ (4) представляет собой треугольную СЛУ относительно главных неизвестных). Придавая теперь свободным неизвестным произвольные значения и вычисляя по найденным формулам соответствующие значения главных неизвестных, мы получим всё множество искомых решений.

Итак, при $r = n$ исходная СЛУ (1) оказывается совместной определённой, а в случае $r < n$ — совместной неопределённой, при этом множество её решений будет бесконечным.

Подведём итог в виде следующей теоремы.

Теорема 2. СЛУ (1) несовместна, если в процессе приведения её к ступенчатому виду получено противоречивое уравнение. Иначе она совместна и равносильна некоторой ступенчатой СЛУ (4) с $r \leqslant n$ уравнениями. Если $r = n$, то СЛУ (1) является определённой, а если $r < n$, то неопределённой и имеющей бесконечное множество решений.

Следствие. Совместная СЛУ (1) с $m < n$ является неопределённой.

Доказательство. Поскольку при исключении неизвестных число уравнений может только уменьшиться, а противоречивого уравнения заведомо не возникнет, получим $r \leqslant m$. Значит, $r < n$ и по теореме СЛУ (1) будет неопределённой. □

Замечание. Набор главных неизвестных x_{j_k} $(k = 1, \ldots, r)$ не зависит от той последовательности элементарных преобразований, которая приводит СЛУ (1) к ступенчатой СЛУ (4). В частности, инвариантом является число r всех главных неизвестных.

Примеры решения конкретных СЛУ методом Гаусса будут даны на практических занятиях.

III. Однородные системы линейных уравнений. Здесь мы рассмотрим один важный класс СЛУ, имеющий специфические особенности.

Определение 6. СЛУ (1) называется *однородной*, если $b_i = 0$ $(i = 1, \ldots, m)$.

Произвольная однородная СЛУ (далее ОСЛУ) имеет вид

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + \ldots + a_{2n}x_n = 0, \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0. \end{cases} \tag{5}$$

Очевидно, любая ОСЛУ совместна, поскольку она имеет *нулевое* решение $(0, \ldots, 0)$. Представляет интерес критерий, позволяющий определить, есть ли ненулевые решения у данной ОСЛУ. Следующая теорема даёт лишь достаточное условие существования ненулевых решений, а критерий будет дан в § 6.

Теорема 3. ОСЛУ (5), в которой $m < n$, всегда имеет ненулевые решения.

Доказательство. Это частный случай следствия теоремы 2. □

Важным свойством ОСЛУ является замкнутость множества решений относительно естественных операций над решениями. Речь идёт о *сумме* решений, а также о *произведении* решения на число, которые определяются следующим образом.

Если $x^{(1)} = (x_1^{(1)}, \ldots, x_n^{(1)})$ и $x^{(2)} = (x_1^{(2)}, \ldots, x_n^{(2)})$ — упорядоченные наборы чисел, то их сумма (разность) определяется как

$$x^{(1)} \pm x^{(2)} = (x_1^{(1)} \pm x_1^{(2)}, \ldots, x_n^{(1)} \pm x_n^{(2)}),$$

а произведение $x^{(1)} = (x_1^{(1)}, \ldots, x_n^{(1)})$ на число λ есть по определению

$$\lambda x^{(1)} = (\lambda x_1^{(1)}, \ldots, \lambda x_n^{(1)}).$$

Упражнение 2. Докажите, что если $x^{(1)}$, $x^{(2)}$ — решения некоторой ОСЛУ и λ — произвольное число, то $x^{(1)} + x^{(2)}$ и $\lambda x^{(1)}$ также являются решениями этой ОСЛУ. Верно ли аналогичное утверждение для неоднородных СЛУ?

Иногда имеет смысл рассматривать СЛУ (1) вместе с *ассоциированной* с ней (т. е. имеющей те же коэффициенты a_{ij} при неизвестных) ОСЛУ (5). В этом случае между решениями этих двух систем возникает естественная связь, которая позволяет по-другому взглянуть на множество решений СЛУ (1). А именно, справедливы следующие утверждения.

1. Сумма любого решения СЛУ (1) с любым решением ассоциированной ОСЛУ (5) является решением СЛУ (1).

2. Разность любых двух решений СЛУ (1) есть решение ассоциированной ОСЛУ (5).

Несложные доказательства этих утверждений предоставим читателю как

Упражнение 3.

Теперь множество всех решений совместной СЛУ (1) можно описать следующим образом. Пусть $x^{(\text{част})}$ — какое-нибудь фиксированное *частное решение* этой системы. Тогда любое решение представляются в виде суммы

$$x^{(\text{част})} + x^{(\text{одн})}, \tag{6}$$

где $x^{(\text{одн})}$ — произвольное решение ассоциированной ОСЛУ (5). Как говорят, формула (6) предоставляет *общее решение* СЛУ (1).

Упражнение 4. Дана квадратная СЛУ. Предположим, что ассоциированная с ней ОСЛУ имеет только нулевое решение. Докажите, что исходная СЛУ однозначно разрешима. Верно ли это для произвольных СЛУ?

Указание. Покажите, что данная СЛУ не может оказаться несовместной.

Результат упражнения 4 можно с успехом приложить к решению *задачи о нагретой пластинке* (см. [4], стр. 18) — хороший пример того, как простые соображения позволяют установить довольно нетривиальный факт.

§ 2. Арифметическое n-мерное векторное пространство $\mathbb{R}^n$. Основная теорема о линейной зависимости

Арифметическое n-мерное векторное пространство $\mathbb{R}^n$. Линейно зависимые и линейно независимые системы векторов в $\mathbb{R}^n$. Критерий и признаки линейной зависимости. Основная теорема о линейной зависимости и её следствия.

I. Определения. Фиксируем натуральное число n и скажем, что мы будем понимать под n-мерным арифметическим вектором. Это понятие по существу нам уже встречалось (см. определение 2 из § 1).

Определение 1. *Арифметическим n-мерным вектором*

$$a = (a_1, \ldots, a_n)$$

называется упорядоченный набор из n вещественных чисел a_i $(i = 1, \ldots, n)$ — его *компонент*.

Отметим, что два n-мерных арифметических вектора $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ считаются *равными*, если равны их соответствующие компоненты:

$$a_i = b_i, \quad i = 1, \ldots, n.$$

Арифметические n-мерные векторы можно складывать (вычитать) и умножать на числа λ. Эти операции определяются покомпонентно:

$$a \pm b = (a_1 \pm b_1, \ldots, a_n \pm b_n), \quad \lambda a = (\lambda a_1, \ldots, \lambda a_n).$$

При $n \leqslant 3$ это похоже на аналогичные действия с обычными геометрическими векторами, заданными своими координатами в некоторой системе координат. Далее, употребляя слово «вектор», мы будем иметь в виду «n-мерный арифметический вектор».

Нулевым вектором будем называть вектор с нулевыми компонентами: $0 = (0, \ldots, 0)$. Нулевой вектор обладает следующим свойством: $a + 0 = a$ для любого вектора a.

Вектором, *противоположным* вектору $a = (a_1, \ldots, a_n)$, называется вектор

$$-a = (-a_1, \ldots, -a_n).$$

Очевидно, $a + (-a) = 0$ для любого вектора a.

Перечислим основные свойства операций над векторами (далее a, b, c — произвольные векторы, λ, μ — произвольные числа).

1. *Коммутативность сложения*: $a + b = b + a$.

2. *Ассоциативность сложения*: $a + (b + c) = (a + b) + c$.

3. *Смешанная ассоциативность*: $\lambda(\mu a) = (\lambda\mu)a$.

4. $1a = a$.

5. *Дистрибутивность*: $\lambda(a + b) = \lambda a + \lambda b$ и $(\lambda + \mu)a = \lambda a + \mu a$.

Доказательство этих свойств непосредственно вытекает из определений и соответствующих свойств арифметических операций над числами.

Замечание. Свойство ассоциативности сложения векторов делает осмысленными выражения типа $a + b + c + d$, ибо здесь результат уже не зависит от конкретного способа расстановки скобок. Свойства дистрибутивности позволяют привычным образом раскрывать скобки и приводить подобные.

Определение 2. Множество всех n-мерных арифметических векторов, рассматриваемое вместе с операциями сложения векторов и умножения вектора на число, называется *арифметическим n-мерным векторным пространством* и обозначается $\mathbb{R}^n$.

II. Линейно зависимые системы векторов в $\mathbb{R}^n$. Как известно, вектор b называют *пропорциональным* вектору a, если $b = \lambda a$ для некоторого числа λ. Это понятие можно обобщить.

Определение 3. Пусть дана конечная система векторов $a_1, \ldots, a_m$. *Линейной комбинацией* этих векторов с коэффициентами $\lambda_1, \ldots, \lambda_m$ называется сумма

$$\lambda_1 a_1 + \ldots + \lambda_m a_m.$$

Линейная комбинация называется *тривиальной*, если все её коэффициенты равны нулю:

$$\lambda_1 = \ldots = \lambda_m = 0.$$

Очевидно, тривиальная линейная комбинация любой системы векторов равна нулевому вектору 0. Говорят, что вектор a *линейно выражается* через векторы $a_1, \ldots, a_m$, если он равен некоторой линейной комбинации этих векторов:

$$a = \lambda_1 a_1 + \ldots + \lambda_m a_m.$$

Следующее определение является центральным во всей главе.

Определение 4. Система векторов $a_1, \ldots, a_m$ называется *линейно зависимой*, если существует нетривиальная линейная комбинация этих векторов, равная нулевому вектору:

$$\lambda_1 a_1 + \ldots + \lambda_m a_m = 0,$$

при этом среди коэффициентов λ_i $(i = 1, \ldots, m)$ есть отличные от нуля.

Если же такой линейной комбинации не существует (т. е. только тривиальная линейная комбинация векторов этой системы может быть равна нулевому вектору), то система векторов $a_1, \ldots, a_m$ называется *линейно независимой*.

Пример 1. В пространстве $\mathbb{R}^3$ рассмотрим систему векторов

$$a_1 = (1, 0, -1), \quad a_2 = (2, -1, 0), \quad a_3 = (5, -2, -1).$$

Эта система векторов линейно зависима, поскольку справедливо равенство

$$a_1 + 2a_2 - a_3 = 0.$$

В самом деле, имеем

$$a_1 + 2a_2 - a_3 = (1, 0, -1) + 2(2, -1, 0) - (5, -2, -1) = (0, 0, 0).$$

Разумеется, нужно ещё объяснить, откуда взялось это равенство (см. следующий пример, где всё будет по-честному). □

Типичная задача состоит в том, чтобы для данной системы векторов пространства $\mathbb{R}^n$ выяснить, является ли она линейно зависимой, и если да, то предъявить нетривиальную линейную комбинацию векторов системы, равную нулевому вектору.

Пример 2. Решим эту задачу для системы векторов

$$a_1 = (1, 2, 3), \quad a_2 = (2, 1, 0), \quad a_3 = (1, 0, 0)$$

пространства $\mathbb{R}^3$. Для этого исследуем векторное уравнение

$$\lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 a_3 = 0,$$

считая неизвестными коэффициенты λ_1, λ_2, λ_3. Это уравнение равносильно ОСЛУ

$$\begin{cases} \lambda_1 + 2\lambda_2 + \lambda_3 = 0, \\ 2\lambda_1 + \lambda_2 = 0, \\ 3\lambda_1 = 0, \end{cases}$$

которая, очевидно, имеет только нулевое решение. Следовательно, нетривиальной линейной комбинации системы векторов a_1, a_2, a_3, равной нулевому вектору, нет, т. е. данная система векторов линейно независима. □

В общем случае вопрос о линейной зависимости системы векторов $a_1, \ldots, a_m$ сводится к исследованию соответствующей ОСЛУ, равносильной векторному уравнению

$$\lambda_1 a_1 + \ldots + \lambda_m a_m = 0,$$

на предмет наличия у неё ненулевых решений (в роли неизвестных выступают коэффициенты $\lambda_1, \ldots, \lambda_m$). Для получения ответа можно применить метод Гаусса, разобранный в § 1. Полезно также иметь в виду следующие простые *признаки* (достаточные условия) линейной зависимости.

1. Если система векторов содержит нулевой вектор, то она линейно зависима.

2. Если система векторов включает в себя некоторую линейно зависимую подсистему, то она сама также линейно зависима.

Эти утверждения непосредственно следуют из определения 4, причём первое из них является частным случаем второго.

Упражнение 1. Напишите подробное доказательство.

Следующий *критерий* (необходимые и достаточные условия) линейной зависимости системы векторов для практики мало полезен, однако удобен в теории как иной взгляд на понятие линейной зависимости.

Теорема 1. Система векторов $a_1, \ldots, a_m$ является линейно зависимой тогда и только тогда, когда один из векторов линейно выражается через остальные.

Здесь $m > 1$. Очевидно, что система, состоящая из одного вектора, линейно зависима только если этот вектор — нулевой.

ДОКАЗАТЕЛЬСТВО. Пусть векторы $a_1, \ldots, a_m$ линейно зависимы, т. е.

$$\lambda_1 a_1 + \ldots + \lambda_m a_m = 0 \tag{1}$$

для некоторых коэффициентов $\lambda_1, \ldots, \lambda_m$, не все из которых равны нулю. Пусть, к примеру, $\lambda_1 \neq 0$. Тогда из равенства (1) следует равенство

$$a_1 = \mu_2 a_2 + \ldots + \mu_m a_m, \tag{2}$$

где $\mu_i = -\lambda_i/\lambda_1$ $(i = 2, \ldots, m)$. Это значит, что вектор a_1 можно выразить через векторы $a_2, \ldots, a_m$.

Обратно, предположим, что один из векторов системы (скажем, a_1) линейно выражается через остальные, т. е. имеет место равенство (2) с некоторыми коэффициентами $\mu_2, \ldots, \mu_m$. Тогда

$$a_1 + (-\mu_2)a_2 + \ldots + (-\mu_m)a_m = 0,$$

и мы имеем нетривиальную линейную комбинацию векторов $a_1, \ldots, a_m$, равную нулевому вектору. □

III. Основная теорема о линейной зависимости. Здесь мы докажем основной факт о линейно зависимых системах векторов пространства $\mathbb{R}^n$ и затем выведем из него ряд важных следствий. В частности, в обозначении $\mathbb{R}^n$ индекс n приобретёт новый содержательный смысл.

Пусть A: $a_1, \ldots, a_m$ и B: $b_1, \ldots, b_s$ — две системы векторов в $\mathbb{R}^n$. Будем говорить, что система B *линейно выражается* через систему A, если каждый вектор системы B линейно выражается через систему A:

$$b_i = \mu_{i1} a_1 + \ldots + \mu_{im} a_m, \quad i = 1, \ldots, s, \tag{3}$$

где μ_{ij} — некоторые числа. В этих обозначениях справедлива

Теорема 2. Если система векторов B линейно выражается через систему векторов A, при этом $s > m$, то B линейно зависима.

ДОКАЗАТЕЛЬСТВО. Будем искать нетривиальную линейную комбинацию векторов системы B, которая равна нулевому вектору:

$$\lambda_1 b_1 + \ldots + \lambda_s b_s = 0.$$

Учитывая (3), последнее равенство можно записать в виде

$$(\lambda_1\mu_{11} + \ldots + \lambda_s\mu_{s1})a_1 + \ldots + (\lambda_1\mu_{1m} + \ldots + \lambda_s\mu_{sm})a_m = 0.$$

Ясно, что это равенство заведомо будет выполнено, если все выражения в скобках будут равны нулю:

$$\begin{cases} \lambda_1\mu_{11} + \ldots + \lambda_s\mu_{s1} = 0, \\ \ldots \\ \lambda_1\mu_{1m} + \ldots + \lambda_s\mu_{sm} = 0. \end{cases} \tag{4}$$

Таким образом, мы можем подбирать коэффициенты $\lambda_1, \ldots, \lambda_s$, исходя из ОСЛУ (4). Но $s > m$, поэтому по теореме 3 из § 1 эта ОСЛУ обязательно имеет ненулевые решения. Взяв одно из них, мы и получим искомый набор коэффициентов для нетривиальной линейной комбинации векторов $b_1, \ldots, b_s$, равной нулевому вектору. □

Можно дать и другое доказательство, не опирающееся на теорию СЛУ из § 1. Оно использует так называемый *принцип математической индукции* (см., например, [4], стр. 46).

Будем доказывать утверждение теоремы индукцией по числу m векторов системы A. При $m = 1$ (*база индукции*) утверждение верно, так как два вектора b_1, b_2, пропорциональных вектору a_1, линейно зависимы. Сделаем *индукционный шаг* от m к $m + 1$. Пусть

$$b_i = \mu_{i1}a_1 + \ldots + \mu_{im}a_m + \mu_{i,m+1}a_{m+1}, \quad i = 1, \ldots, s,$$

при этом $s > m+1$. Если $\mu_{i,m+1} = 0$ при любом $i = 1, \ldots, s$, то можно сослаться на *индукционное предположение*. Допустим, что один из коэффициентов $\mu_{i,m+1}$ не равен нулю: $\mu_{s,m+1} \neq 0$. Положим $\alpha_i = -\mu_{i,m+1}/\mu_{s,m+1}$ и рассмотрим новую систему векторов B': $b'_1, \ldots, b'_{s-1}$, где

$$b'_i = b_i + \alpha_i b_s, \quad i = 1, \ldots, s-1. \tag{5}$$

Эта система B' линейно выражается через систему A': $a_1, \ldots, a_m$ (для этого подбирались соответствующие коэффициенты α_i) и, так как $s - 1 > m$, по предположению индукции система B' линейно зависима. Следовательно, существует нетривиальная линейная комбинация векторов системы B', равная нулевому вектору:

$$\lambda_1 b'_1 + \ldots + \lambda_{s-1} b'_{s-1} = 0.$$

После замены по формулам (5) и приведения подобных это равенство пример вид

$$\lambda_1 b_1 + \ldots + \lambda_{s-1} b_{s-1} + \lambda_s b_s = 0,$$

где $\lambda_s = \lambda_1\alpha_1 + \ldots + \lambda_{s-1}\alpha_{s-1}$. Поскольку уже среди коэффициентов $\lambda_1, \ldots, \lambda_{s-1}$ есть ненулевые, мы получили нетривиальную линейную комбинацию векторов системы B: $b_1, \ldots, b_s$, равную нулевому вектору. Значит, B линейно зависима, и индукционный шаг сделан.

Это доказательство, разумеется, нельзя считать принципиально иным, поскольку связь с методом Гаусса очевидна: преобразование системы векторов по формулам (5) вполне аналогично серии элементарных преобразований третьего типа.

Сформулируем два следствия теоремы 2.

Следствие 1. Если система B линейно независима и линейно выражается через систему A, то $s \leqslant m$.

Доказательство. Рассуждая от противного, получим противоречие с утверждением теоремы. □

Следствие 2. В пространстве $\mathbb{R}^n$ любая система, состоящая более чем из n векторов, является линейно зависимой.

Доказательство. Рассмотрим в качестве системы A систему *единичных* векторов:

$$e_i = (0, \ldots, 1, \ldots, 0), \quad i = 1, \ldots, n$$

(i-я компонента равна единице, а остальные — нулю). Каждый вектор $a = (a_1, \ldots, a_n)$ линейно выражается через систему единичных векторов:

$$a = a_1 e_1 + \ldots + a_n e_n.$$

Пусть B — произвольная система, содержащая $s > n$ векторов. Тогда она линейно выражается через A и по теореме должна быть линейно зависимой. □

Очевидно, сама система $e_1, \ldots, e_n$ единичных векторов линейно независима. Таким образом, число n есть максимально возможное число векторов в любой линейно независимой системе векторов пространства $\mathbb{R}^n$.

Особый интерес представляют максимальные, т. е. состоящие из n векторов, линейно независимые системы, одним из примеров (далеко не единственным) которых является система единичных векторов. Свойства таких систем мы будем обсуждать в следующем параграфе.

§ 3. Базис системы векторов. Базис пространства $\mathbb{R}^n$

Базис системы векторов в пространстве $\mathbb{R}^n$. Теорема о существовании базиса системы векторов. Ранг системы векторов. Базис пространства $\mathbb{R}^n$. Теорема о числе векторов в произвольном базисе пространства $\mathbb{R}^n$. Теорема о замене вектора в базисе.

I. Базис системы векторов. Понятие базиса столь же фундаментально, как и само понятие линейной зависимости. Начнём с определения базиса системы векторов.

Определение 1. Пусть дана конечная система векторов S пространства $\mathbb{R}^n$. Её *базисом* называется любая подсистема B, удовлетворяющая следующим условиям:

а) B линейно независима;

б) S линейно выражается через B.

Условие б) фактически означает, что всякий вектор из S, не принадлежащий B, линейно выражается через векторы B. Более того, такое выражение возможно единственным способом. Действительно, пусть B: $b_1, \ldots, b_r$ и a — некоторый вектор из S, допускающий два представления:

$$a = \lambda_1 b_1 + \ldots + \lambda_r b_r = \mu_1 b_1 + \ldots + \mu_r b_r.$$

Тогда $(\lambda_1 - \mu_1)b_1 + \ldots + (\lambda_r - \mu_r)b_r = 0$, откуда, так как B линейно независима, получим $\lambda_i = \mu_i$ для всех $i = 1, \ldots, r$. Равенство вида

$$a = \lambda_1 b_1 + \ldots + \lambda_r b_r \tag{1}$$

называют *разложением* вектора $a \in S$ по базису B: $b_1, \ldots, b_r$ системы S.

Рассмотрим следующий

Пример 1. В пространстве $\mathbb{R}^3$ дана система S векторов

$$a_1 = (1, 2, -1), \quad a_2 = (0, -1, 3), \quad a_3 = (2, 3, 1).$$

Покажем что подсистема B, состоящая из векторов a_1, a_2, является базисом S.

В самом деле, вектор a_1 не пропорционален вектору a_2 и наоборот, поэтому они линейно независимы. Кроме того, можно заметить, что $a_3 = 2a_1 + a_2$. □

Прежде чем обсуждать вопрос о том, как найти какой-нибудь базис данной системы векторов, покажем, что базисы всегда существуют.

Теорема 1. Любая система векторов S пространства $\mathbb{R}^n$, содержащая хотя бы один ненулевой вектор, имеет базис.

Доказательство. Поскольку S содержит ненулевые векторы, они имеет линейно независимые подсистемы. Пусть B — одна из максимальных (по количеству векторов) линейно независимых подсистем системы S. Докажем, что она является базисом S.

Подсистема B линейно независима по определению, поэтому достаточно проверить, что S линейно выражается через B. Пусть B: $b_1, \ldots, b_r$ и a — произвольный вектор из S, не принадлежащий B. Рассмотрим подсистему B': $b_1, \ldots, b_r, a$. Эта подсистема не

может оказаться линейно независимой, поэтому найдутся такие числа $\lambda_1, \ldots, \lambda_r, \lambda$, не все равные нулю и такие, что

$$\lambda_1 b_1 + \ldots + \lambda_r b_r + \lambda a = 0.$$

Здесь $\lambda \neq 0$, так как иначе подсистема B была бы линейно зависимой. Но тогда

$$a = (-\lambda_1/\lambda)b_1 + \ldots + (-\lambda_r/\lambda)b_r,$$

т. е. вектор a линейно выражается через подсистему B. □

Укажем теперь удобный практический способ отыскать какой-нибудь базис данной системы векторов. Пусть S: $a_1, \ldots, a_m$, где

$$a_i = (a_{1i}, \ldots, a_{ni}) \in \mathbb{R}^n, \quad i = 1, \ldots, m.$$

Рассмотрим векторное уравнение

$$\lambda_1 a_1 + \ldots + \lambda_m a_m = 0$$

с неизвестными коэффициентами $\lambda_1, \ldots, \lambda_m$. Оно равносильно следующей ОСЛУ:

$$\begin{cases} a_{11}\lambda_1 + \ldots + a_{1m}\lambda_m = 0, \\ \ldots \\ a_{n1}\lambda_1 + \ldots + a_{nm}\lambda_m = 0. \end{cases} \tag{2}$$

Будем решать эту ОСЛУ с неизвестным $\lambda_1, \ldots, \lambda_m$ методом Гаусса. Пусть в полученной ступенчатой ОСЛУ главные неизвестные имеют индексы $1 \leqslant j_1 < \ldots < j_r \leqslant m$. В этих обозначениях справедлива

Теорема 2. Базис системы S образуют векторы $a_{j_1}, \ldots, a_{j_r}$.

Доказательство. Чтобы избежать громоздких обозначений, будем считать главными неизвестными первые r неизвестных $\lambda_1, \ldots, \lambda_r$. Пусть они выражаются через свободные неизвестные $\lambda_{r+1}, \ldots, \lambda_m$ следующим образом:

$$\lambda_i = c_{i,r+1}\lambda_{r+1} + \ldots + c_{im}\lambda_m, \quad i = 1, \ldots, r, \tag{3}$$

где c_{ij} — некоторые числа. По формулам (3) можно найти любое решение ОСЛУ (2).

а) Докажем, что векторы $a_1, \ldots, a_r$ линейно независимы. Пусть

$$\mu_1 a_1 + \ldots + \mu_r a_r = \mu_1 a_1 + \ldots + \mu_r a_r + 0a_{r+1} + \ldots + 0a_m = 0.$$

Это значит, что набор чисел $(\mu_1, \ldots, \mu_r, 0, \ldots, 0)$ является решением ОСЛУ (2). Но тогда он должен получаться по формулам (3) при $\lambda_{r+1} = \ldots = \lambda_m = 0$. Подставив, мы получим $\mu_1 = \ldots = \mu_r = 0$.

б) Покажем, что каждый из оставшихся векторов $a_{r+1}, \ldots, a_m$ можно линейно выразить через векторы $a_1, \ldots, a_r$. Сделаем это на примере вектора a_m. Положим

$$\lambda_{r+1} = \ldots = \lambda_{m-1} = 0, \quad \lambda_m = 1$$

и по формулам (3) получим $\lambda_1 = c_{1m}, \ldots, \lambda_r = c_{rm}$. Следовательно, имеем

$$c_{1m}a_1 + \ldots + c_{rm}a_r + a_m = 0,$$

откуда $a_m = (-c_{1m})a_1 + \ldots + (-c_{rm})a_r$, что и требовалось. □

Для иллюстрации этого способа рассмотрим

Пример 2. Пусть дана системы S векторов

$$a_1 = (1, -2, 1), \quad a_2 = (-2, 4, -2), \quad a_3 = (1, -3, 0), \quad a_4 = (1, 0, 3)$$

пространства $\mathbb{R}^3$. Найдём некоторый её базис и разложим векторы, не вошедшие в базис, по этому базису.

Уравнение

$$\lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 a_3 + \lambda_4 a_4 = 0$$

равносильно ОСЛУ

$$\begin{cases} \lambda_1 - 2\lambda_2 + \lambda_3 + \lambda_4 = 0, \\ -2\lambda_1 + 4\lambda_2 - 3\lambda_3 = 0, \\ \lambda_1 - 2\lambda_2 + 3\lambda_4 = 0. \end{cases}$$

После приведения к ступенчатому виду получим

$$\begin{cases} \lambda_1 - 2\lambda_2 + \lambda_3 + \lambda_4 = 0, \\ \lambda_3 - 2\lambda_4 = 0. \end{cases}$$

Здесь λ_1, λ_3 — главные неизвестные, а λ_2, λ_4 — свободные, при этом

$$\lambda_1 = 2\lambda_2 - 3\lambda_4, \quad \lambda_3 = 2\lambda_4.$$

Таким образом, базис системы S образуют векторы a_1, a_3. Чтобы найти, например, разложение вектора a_4 по этому базису, положим $\lambda_2 = 0$, $\lambda_4 = 1$. Тогда $\lambda_1 = -3$, $\lambda_3 = 2$, так что мы имеем

$$-3a_1 + 2a_3 + a_4 = 0,$$

откуда $a_4 = 3a_1 - 2a_3$. Аналогично находим $a_2 = -2a_1$. □

Заметим, что у одной и той же системы векторов может быть несколько разных базисов. Так, в примере 1 ещё одним базисом системы S будет подсистема a_1, a_3. В следующей теореме описывается то, что объединяет все базисы данной системы векторов.

Теорема 3. Любые два базиса системы S состоят из одинакового числа векторов.

Доказательство. Пусть B_1 и B_2 — два базиса системы S. Тогда B_2 линейно выражается через B_1, поскольку B_1 является базисом. При этом, тоже будучи базисом, подсистема B_2 линейно независима. Тогда по следствию 1 из § 1 в B_2 содержится не более векторов, чем в B_1. Ввиду симметрии в B_1 должно быть не более векторов, чем в B_2. Значит, B_1 и B_2 состоят из одинакового числа векторов. □

Теорема 3 делает корректным следующее

Определение 2. *Рангом* системы векторов S называется число векторов в любом её базисе. Обозначение: $\operatorname{rank}(S)$.

Практически вопрос о ранге произвольной системы векторов решается той же теоремой 2, ибо $\operatorname{rank}(S) = r$.

II. Базис пространства $\mathbb{R}^n$. Базис всего пространства определяется аналогично базису системы векторов.

Определение 3. *Базисом* пространства $\mathbb{R}^n$ называется любая система векторов B, удовлетворяющая следующим условиям:

а) B линейно независима;

б) любой вектор пространства $\mathbb{R}^n$ линейно выражается через B.

Очевидно, базисы пространства $\mathbb{R}^n$ существуют: например, система E: $e_1, \ldots, e_n$ единичных векторов будет базисом. Прежде чем объяснить, как устроен произвольный базис, установим следующий принципиальный факт.

Теорема 4. Любой базис пространства $\mathbb{R}^n$ состоит из n векторов.

Доказательство. См. доказательство теоремы 3, где следует взять $B_1 = E$. □

Напомним, что n — это максимально возможное число векторов в любой линейно независимой системе векторов пространства $\mathbb{R}^n$. Таким образом, базисы пространства $\mathbb{R}^n$ являются примерами таких систем. Оказывается, верно и обратное.

Теорема 5. Всякая линейно независимая система из n векторов пространства $\mathbb{R}^n$ является его базисом.

Доказательство. Пусть B: $b_1, \ldots, b_n$ — произвольная линейно независимая система векторов. Нам нужно показать, что всякий вектор $a \in \mathbb{R}^n$ допускает представление в виде

$$a = \lambda_1 b_1 + \ldots + \lambda_n b_n, \tag{4}$$

где $\lambda_1, \ldots, \lambda_n$ — некоторые числа. □

Упражнение 1. Завершите доказательство теоремы 5, используя идею доказательства теоремы 1.

Замечание. Можно также воспользоваться результатом упражнения 4 из § 1.

Аналогично равенству (1), равенство (3) называют *разложением* вектора $a \in \mathbb{R}^n$ по базису B: $b_1, \ldots, b_n$. Очевидно, такое разложение единственно.

Упражнение 2. Всё-таки объясните, почему.

Итак, в качестве базиса пространства $\mathbb{R}^n$ можно взять произвольную линейно независимую систему из n векторов. Если же нужен базис с какими-то специальными свойствами, то можно несколько раз применить следующую теорему о замене вектора в базисе.

Теорема 6. Пусть B: $b_1, b_2, \ldots, b_n$ — некоторый базис пространства $\mathbb{R}^n$. Предположим, что в разложении

$$b = \lambda_1 b_1 + \lambda_2 b_2 + \ldots + \lambda_n b_n$$

вектора $b \in \mathbb{R}^n$ по этому базису $\lambda_1 \neq 0$. Тогда B': $b, b_2, \ldots, b_n$ — также базис $\mathbb{R}^n$.

Доказательство. Достаточно убедиться в линейной независимости системы B'. Равенство

$$\mu b + \mu_2 b_2 + \ldots + \mu_n b_n = 0,$$

равносильно равенству

$$\mu\lambda_1 b_1 + (\mu_2 + \mu\lambda_2) b_2 + \ldots + (\mu_n + \mu\lambda_n) b_n = 0,$$

откуда, поскольку B — базис, получим

$$\mu\lambda_1 = \mu_2 + \mu\lambda_2 = \ldots = \mu_n + \mu\lambda_n = 0.$$

Так как $\lambda_1 \neq 0$, то $\mu = 0$ и, далее, $\mu_2 = \ldots = \mu_n = 0$. Значит, система B' действительно линейно независима. $\square$

§ 4. Подпространства пространства $\mathbb{R}^n$. Подпространство решений однородной системы линейных уравнений

Понятие подпространств $\mathbb{R}^n$. Базис и размерность подпространства. Подпространство решений ОСЛУ. Фундаментальная система решений ОСЛУ и способ её построения.

I. Определения, примеры и основные факты. Некоторые подмножества векторов пространства $\mathbb{R}^n$ по своим свойствам, связанным с операциями над векторами, ничем не отличаются от всего пространства $\mathbb{R}^n$. Такие подмножества принято называть подпространствами. Более точно это сформулировано в следующем определении.

Определение 1. Непустое подмножество L пространства $\mathbb{R}^n$ называется *подпространством*, если выполняются следующие условия:

а) если $x \in L$ и $y \in L$, то $x + y \in L$;

б) если $x \in L$ и $\lambda \in \mathbb{R}$, то $\lambda x \in L$.

Условия а) и б) означают, что подмножество L *замкнуто* относительно векторных операций, т. е. результат выполнения этих операций над векторами из L не должен оказаться вне L. Тривиальными подпространствами называются *нулевое* подпространство $\{0\}$ и само пространство $\mathbb{R}^n$.

Пример 1. Рассмотрим подмножества

$$L_1 = \{x = (x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\},$$
$$L_2 = \{x = (x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}$$

пространства $\mathbb{R}^3$. Первое из них является подпространством, а второе — нет. □

Упражнение 1. Докажите эти утверждения.

Упражнение 2. Пусть L — подпространство и S — произвольная система векторов из L. Докажите, что любая линейная комбинация векторов системы S принадлежит L.

Чтобы сконструировать подпространство, достаточно взять произвольную систему векторов S: $a_1, \ldots, a_m$ пространства $\mathbb{R}^n$ и образовать подмножество

$$L = \langle S \rangle = \{\lambda_1 a_1 + \ldots + \lambda_m a_m : \lambda_i \in \mathbb{R}, i = 1, \ldots, m\}, \qquad (1)$$

называемое *линейной оболочкой* системы S (говорят также, что L *порождается* системой S).

Упражнение 3. Докажите, что $L = \langle S \rangle$ — подпространство $\mathbb{R}^n$.

Как будет показано далее, эта конструкция носит общий характер, т. е. любое подпространство можно представить в виде линейной оболочки некоторых векторов.

Определение 2. *Базисом* подпространства L называется любая система B векторов из L, удовлетворяющая условиям:

а) B линейно независима;

б) любой вектор подпространства L линейно выражается через B.

Это определение обобщает определение базиса пространства $\mathbb{R}^n$ (см. определение 3 из § 3). Основные свойства базиса при этом сохраняются.

Теорема 1. Всякое подпространство $L \neq \{0\}$ пространства $\mathbb{R}^n$ имеет базис. Любые два базиса L содержат одно и то же число векторов, не превосходящее n.

Доказательство. Существование базиса подпространства можно доказать точно так же, как и существование базиса системы векторов (см. теорему 1 из § 3). Единственное отличие — необходимо сослаться на следствие 2 из § 2, чтобы обосновать существование максимальных линейно независимых систем векторов из L.

Можно дать более конструктивное доказательство. Пусть b_1 — некоторый ненулевой вектор подпространства L. Если все остальные векторы L пропорциональны b_1, то базис построен. Если же некоторый вектор b_2 из L не пропорционален b_1, то система векторов b_1, b_2 будет линейно независимой, и к ней можно применить аналогичные рассуждения. Процесс добавления новых векторов оборвётся в силу следствия 2 из § 2, и на некотором шаге $r \leqslant n$ мы получим базис $b_1, b_2, \ldots, b_r$.

Что касается равномощности любых двух базисов подпространства L, то и здесь годится рассуждение, доказывающее аналогичный факт для системы векторов (см. теорему 3 из § 3). □

Упражнение 4. Напишите подробное доказательство теоремы 1.

Следующее определение вполне аналогично определению 2 из § 3.

Определение 3. *Размерностью* подпространства $L \neq \{0\}$ пространства $\mathbb{R}^n$ называется число векторов в любом базисе этого подпространства. Обозначение: $\dim(L)$.

Как мы уже видели, $\dim(L) \leqslant n$ для любого подпространства L, при этом

$$\dim(\mathbb{R}^n) = n.$$

Размерность нулевого подпространства удобно считать равной нулю.

Если B — некоторый базис подпространства L, то, очевидно, $L = \langle B \rangle$. Таким образом, способ задания подпространства в виде линейной оболочки действительно является общим. Рассмотрим вопрос о том, как найти какой-нибудь базис линейной оболочки (1). Следующее утверждение довольно очевидно и предлагается читателю как

Упражнение 5. В качестве базиса линейной оболочки (1) можно взять любой базис порождающей системы векторов S.

Таким образом, вопрос сводится к отысканию базиса порождающей системы векторов S, а значит, решается теоремой 2 из § 3. В частности, $\dim(\langle S \rangle) = \operatorname{rank}(S)$.

II. Подпространство решений ОСЛУ. Рассмотрим произвольную ОСЛУ с n неизвестными:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + \ldots + a_{2n}x_n = 0, \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0. \end{cases} \tag{2}$$

Каждое её решение $x^* = (x_1^*, \ldots, x_n^*)$ можно интерпретировать как вектор пространства $\mathbb{R}^n$, а всё множество решений — как некоторое подмножество L пространства $\mathbb{R}^n$.

Упражнение 6. Докажите, что L является подпространством пространства $\mathbb{R}^n$.

Так, например, подпространство L_1 из примера 1 является подпространством решений ОСЛУ, состоящей из одного уравнения $x_1 + x_2 + x_3 = 0$.

Далее мы обсудим вопрос о том, как найти какой-нибудь базис подпространства решений L ОСЛУ (2), который по традиции называют *фундаментальной системой решений* (ФСР). Опишем стандартный способ отыскания ФСР.

Будем решать ОСЛУ (2) методом Гаусса. Предположим, что в получившейся ступенчатой ОСЛУ оказалось s свободных неизвестных. Выразим главные неизвестные через свободные, после чего придадим свободным неизвестным следующие значения: одну из них положим равной 1, а остальные пусть будут равны 0 (очевидно, число таких специальных наборов значений равно s). Вычислив затем соответствующие значения главных неизвестных, мы в итоге получим s решений $b_1, \ldots, b_s$. Как следует из метода Гаусса, все решения ОСЛУ (2) можно представить в виде линейной комбинации

$$\lambda_1 b_1 + \ldots + \lambda_s b_s,$$

где $\lambda_1, \ldots, \lambda_s$ — произвольные числа (а именно, значения свободных неизвестных). Более того, система B: $b_1, \ldots, b_s$ линейно независима, т. е. является искомой ФСР. В частности, $\dim(L) = s$.

Упражнение 7. Убедитесь в линейной независимости так построенной системы векторов B.

Замечание. Можно показать, что любое подпространство L пространства $\mathbb{R}^n$ может быть задано как подпространство решений некоторой ОСЛУ (2).

В заключение рассмотрим один типичный пример.

Пример 2. Найдём ФСР для ОСЛУ

$$\begin{cases} x_1 + 2x_2 + 4x_3 - 3x_4 = 0, \\ 3x_1 + 5x_2 + 6x_3 - 4x_4 = 0, \\ 4x_1 + 5x_2 - 2x_3 + 3x_4 = 0, \\ 3x_1 + 8x_2 + 24x_3 - 19x_4 = 0. \end{cases}$$

Здесь множество решений есть подпространство пространства $\mathbb{R}^4$ и требуется найти базис этого подпространства. Метод Гаусса приводит к формулам

$$x_1 = 8x_3 - 7x_4, \quad x_2 = -6x_3 + 5x_4$$

(x_1, x_2 — главные неизвестные, а x_3, x_4 — свободные). Положив $x_3 = 1, x_4 = 0$, получим решение $b_1 = (8, -6, 1, 0)$, а при $x_3 = 0, x_4 = 1$ — решение $b_2 = (-7, 5, 0, 1)$. Произвольное решение теперь можно записать в виде

$$\lambda_1(8, -6, 1, 0) + \lambda_2(-7, 5, 0, 1),$$

где λ_1, λ_2 — любые числа. Таким образом, ФСР данной ОСЛУ образуют векторы b_1, b_2, а размерность подпространства решений равна 2 — числу свободных неизвестных. □

Глава 2
Матричная алгебра. Теория определителей

§ 5. Матрицы. Ранг матрицы

Понятие матрицы. Строчечный ранг матрицы и его инвариантность при элементарных преобразованиях строк. Строчечный ранг ступенчатой матрицы. Столбцовый ранг матрицы. Теорема о равенстве строчечного и столбцового рангов матрицы. Ранг матрицы.

I. Матрицы. Решая СЛУ методом Гаусса, мы совершаем элементарные преобразования над уравнениями системы, но при этом фактически работаем со строками коэффициентов (при неизвестных и в правых частях уравнений). Удобно эти строки объединить в таблицу и заниматься соответствующими преобразованиями этой таблицы.

Определение 1. Прямоугольная таблица чисел вида

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots\dots\dots\dots & & \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \tag{1}$$

называется *матрицей* размера $m \times n$. При $m = n$ эта матрица называется *квадратной* матрицей n-го порядка.

Матрица (1) состоит из m *строк* и n *столбцов*. Её строки и столбцы можно интерпретировать как n-мерные и m-мерные арифметические векторы соответственно. На пересечении i-й строки и j-го столбца находится число a_{ij}. Числа, которыми заполнена матрица, называют её *элементами* (в принципе, в роли элементов матрицы может быть что угодно, но мы в основном будем иметь дело с числовыми матрицами).

Множество всех матриц размера $m \times n$ и квадратных матриц n-го порядка с вещественными элементами будем обозначать $M_{m\times n}(\mathbb{R})$ и $M_n(\mathbb{R})$ соответственно.

Рассматривая произвольную СЛУ

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + \dots + a_{2n}x_n = b_2, \\ \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m, \end{cases}$$

мы сопоставим ей две матрицы: матрицу (1), называемую *матрицей* СЛУ, и матрицу

$$\overline{A} = \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \dots\dots\dots\dots & & & \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix}$$

размера $m \times (n+1)$, называемую *расширенной матрицей* СЛУ. Элементарным преобразованиям над уравнениями будут соответствовать (понятно, какие) *элементарные* преобразования над строками расширенной матрицы $\overline{A}$.

Упражнение 1. Аккуратно сформулируйте эти четыре типа элементарных преобразований над строками матрицы.

Матрица называется *ступенчатой*, если она не содержит нулевых строк и в каждой её строке первый ненулевой элемент расположен правее, чем первый ненулевой элемент в предыдущей строке. Очевидно, для ступенчатой СЛУ соответствующие ей матрицы A и $\overline{A}$ будут ступенчататыми.

Замечание. Выполняя элементарные преобразования над строками по тому же алгоритму, по которому в методе Гаусса мы совершаем элементарные преобразования над уравнениями, мы сможем любую матрицу привести к ступенчатому виду.

II. Строчечный ранг матрицы. Для матрицы (1) обозначим через S систему её строк

$$(a_{i1}, \ldots, a_{in}) \in \mathbb{R}^n, \quad i = 1, \ldots, m.$$

Определение 2. *Строчечным* рангом матрицы A называется $\operatorname{rank}(S)$.

Далее мы покажем, как можно вычислить строчечный ранг матрицы. Предварительно докажем одно вспомогательное утверждение.

Лемма. Пусть S_1 и S_2 — две системы векторов в пространстве $\mathbb{R}^n$, причём S_2 линейно выражается через S_1. Тогда $\operatorname{rank}(S_2) \leqslant \operatorname{rank}(S_1)$.

Доказательство. Пусть B_1, B_2 — базисы систем векторов S_1, S_2 соответственно. Из условия и определений легко следует, что B_2 линейно выражается через B_1, и нам остаётся сослаться на следствие 1 теоремы 2 из § 2. □

Теорема 1. При элементарных преобразованиях строк матрицы её строчечный ранг не меняется.

Доказательство. Проделаем с матрицей (1), например, следующее элементарное преобразование третьего типа: ко второй её строке прибавим первую строку, умноженную на число λ. Получим матрицу

$$A' = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} + \lambda a_{11} & \ldots & a_{2n} + \lambda a_{1n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}.$$

Обозначим системы строк матриц A и A' через S и S' соответственно и пусть S: a_1, a_2, a_3, …, a_m. Тогда, очевидно, S': a_1, $a_2 + \lambda a_1$, a_3, …, a_m. Поскольку S' линейно выражается через S, по лемме $\operatorname{rank}(S') \leqslant \operatorname{rank}(S)$. Но и S в свою очередь можно линейно выразить через S', поэтому $\operatorname{rank}(S) \leqslant \operatorname{rank}(S')$. Значит, $\operatorname{rank}(S') = \operatorname{rank}(S)$.

Для элементарных преобразований других типов утверждение очевидно. □

Как уже отмечалось, при помощи элементарных преобразований данную матрицу можно привести к ступенчатому виду. Осталось понять, чему равен строчечный ранг ступенчатой матрицы.

Теорема 2. Строчечный ранг ступенчатой матрицы равен числу её строк.

ДОКАЗАТЕЛЬСТВО. Для удобства обозначений предположим, что нам дана *трапецевидная* ступенчатая матрица (это не ограничивает общности рассуждений):

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2r} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr} & \dots & a_{rn} \end{pmatrix},$$

при этом $a_{ii} \neq 0\,(i = 1, \dots, r)$. Требуемое равенство $\operatorname{rank}(S) = r$ означает, что система строк S матрицы A является линейно независимой. Последнее нетрудно проверить. □

Упражнение 2. Обязательно проверьте.

Из теорем 1 и 2 вытекает следующий способ вычисления строчечного ранга матрицы: привести данную матрицу к ступенчатому виду и подсчитать число строк в получившейся ступенчатой матрице.

Отметим, что этот способ отличается от того способа вычисления $\operatorname{rank}(S)$, который основан на теореме 2 из § 3. Далее мы сопоставим эти два способа и в результате получим нетривиальный факт.

III. Столбцовый ранг матрицы. Наряду с системой строк матрицы (1) можно рассмотреть и систему T её столбцов

$$(a_{1j}, \dots, a_{mj}) \in \mathbb{R}^m, \quad j = 1, \dots, n.$$

Определение 3. *Столбцовым* рангом матрицы A называется $\operatorname{rank}(T)$.

Справедлива следующая

Теорема 3. Столбцовый ранг матрицы равен её строчечному рангу.

ДОКАЗАТЕЛЬСТВО. Будем вычислять строчечный ранг матрицы A, т. е. $\operatorname{rank}(S)$ системы её строк S, в соответствии с теоремой 2 из § 3. Очевидно, для этого мы должны привести к ступенчатому виду матрицу

$$A^t = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \dots & \dots & \dots \\ a_{1n} & \dots & a_{mn} \end{pmatrix},$$

столбцы которой являются строками матрицы A. Но, как было показано в п. **II**, такая процедура вычисляет строчечный ранг матрицы A^t, который одновременно оказывается и столбцовым рангом матрицы A. Поэтому $\operatorname{rank}(S) = \operatorname{rank}(T)$. □

Общее значение строчечного и столбцового рангов матрицы A называется просто рангом этой матрицы и обозначается $\operatorname{rank}(A)$. Очевидно неравенство

$$\operatorname{rank}(A) \leqslant \min\{m, n\}.$$

В случае равенства матрицу A называют матрицей *полного ранга*.

§ 6. Теорема Кронекера — Капелли

Теорема Кронекера — Капелли (критерий совместности СЛУ). Теорема об однозначной разрешимости СЛУ.

Опираясь на понятие ранга матрицы, можно легко дать необходимые и достаточные условия совместности, а также однозначной разрешимости данной СЛУ.

I. Критерий совместности СЛУ. Пусть дана произвольная СЛУ:

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

Как известно, с этой СЛУ можно связать две матрицы: матрицу A и расширенную матрицу $\overline{A}$. Рассмотрим систему $a_1, \ldots, a_n$ первых n столбцов матрицы $\overline{A}$ (они же — столбцы матрицы A) и пусть b — последний столбец $\overline{A}$. Нетрудно видеть, что СЛУ (1) можно записать в виде одного векторного уравнения

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

Следующая теорема, дающая критерий совместности СЛУ (1), известна как *теорема Кронекера — Капелли*[2)].

Теорема 1. СЛУ (1) совместна тогда и только тогда, когда

$$\operatorname{rank}(\overline{A}) = \operatorname{rank}(A). \tag{3}$$

Доказательство. Глядя на уравнение (2), можно обнаружить, что СЛУ (1) будет совместной в том и только том случае, если вектор b линейно выражается через систему векторов $a_1, \ldots, a_n$. А это условие, как легко видеть, равносильно равенству

$$\operatorname{rank}(a_1, \ldots, a_n, b) = \operatorname{rank}(a_1, \ldots, a_n),$$

т. е. равенству (3), если подразумевать столбцовые ранги матриц. □

Упражнение 1. Увидьте это «легко видеть».

Доказанная теорема имеет важное теоретическое значение, однако на практике она может быть полезна только тогда, когда у нас есть сравнительно простой способ вычислить ранги матриц A и $\overline{A}$ (разумеется, способ вычисления ранга при помощи элементарных преобразований, изложенный в § 5, не принимается в расчёт).

II. Критерий однозначной разрешимости СЛУ. Можно пойти дальше и выяснить, при каких условиях СЛУ (1) будет иметь единственное решение. Это важно, например, для ОСЛУ, для которых желательно иметь критерий наличия ненулевых решений.

[2)] Л. Кронекер (1823 — 1891) — немецкий математик. А. Капелли (1855 — 1910) — итальянский математик.

Теорема 2. СЛУ (1) однозначно разрешима тогда и только тогда, когда

$$\operatorname{rank}(\overline{A}) = \operatorname{rank}(A) = n.$$

Доказательство. Случай однозначной разрешимости СЛУ (1) характеризуется тем, что вектор b должен единственным образом линейно выражаться через систему векторов $a_1, \ldots, a_n$. Как мы уже знаем, условие «должен линейно выражаться» равносильно равенству (3), а условие «единственным образом» равносильно, как нетрудно понять, линейной независимости системы векторов $a_1, \ldots, a_n$, т. е. равенству $\operatorname{rank}(A) = n$. □

Упражнение 2. Поймите то, что «нетрудно понять».

В качестве следствия теоремы 2 получим следующее утверждение: ОСЛУ

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + \ldots + a_{2n}x_n = 0, \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0. \end{cases} \tag{4}$$

имеет только нулевое решение тогда и только тогда, когда $\operatorname{rank}(A) = n$.

Упражнение 3. Сформулируйте необходимые и достаточные условия существования у ОСЛУ (4) ненулевых решений (ср. с теоремой 3 из § 1).

Возвращаясь к методу Гаусса решения СЛУ (1), которую мы предположим совместной, заметим следующее.

Во-первых, число r главных неизвестных, которые будут в равносильной ступенчатой СЛУ, равно $\operatorname{rank}(A)$ и потому не зависит от конкретной последовательности элементарных преобразований.

Во-вторых, набор индексов $1 \leqslant j_1 < j_2 < \ldots < j_r \leqslant n$ главных неизвестных также инвариантен.

Упражнение 4. Убедитесь в справедливости последнего утверждения.

Указание. Проследите за изменением ранга (первоначально пустой) системы векторов, в которую последовательно добавляются векторы-столбцы $a_1, a_2, \ldots, a_n$.

§ 7. Операции над матрицами. Обратная матрица. Решение матричных уравнений

Операции над матрицами: сложение матриц, умножение матрицы на число, умножение матриц. Транспонированная матрица. Обратная матрица. Критерий обратимости матрицы. Запись и решение квадратной СЛУ в матричном виде. Решение матричных уравнений.

I. Операции над матрицами и их свойства. Для работы с матрицами часто используют краткую запись типа $A = (a_{ij})$ (т. е. матрица A с элементами a_{ij}), при этом размер матрицы A обычно ясен из контекста. Иногда, чтобы не вводить дополнительных обозначений, удобно произвольный элемент матрицы A обозначить через $[A]_{ij}$.

Цель этого пункта — ввести стандартные операции над матрицами. Начнём с так называемых «векторных» операций.

Определение 1. Пусть заданы две матрицы $A = (a_{ij})$ и $B = (b_{ij})$ одинакового размера. Матрицы $C = (c_{ij})$ и $D = (d_{ij})$ называются соответственно *суммой* матриц A и B и *произведением* матрицы A на число λ, если

$$c_{ij} = a_{ij} + b_{ij}, \quad d_{ij} = \lambda a_{ij}$$

для всех i, j. Обозначения: $C = A + B$ и $D = \lambda A$.

Таким образом, сложение матриц и умножение матрицы на число происходит поэлементно, при этом результирующие матрицы имеют тот же размер, что и исходные. Если матрицы «вытянуть» в арифметические векторы, то эти операции ничем не будут отличаться от соответствующих операций над векторами. В частности, они будут обладать такими же свойствами, что и операции сложения векторов и умножения вектора на число, перечисленные нами в п. **I** § 2.

Упражнение 1. Сформулируйте эти свойства сложения матриц и умножения матрицы на число.

Отметим ещё, что *нулевой* матрицей называется матрица, все элементы которой суть нули, а матрицей, *противоположной* матрице $A = (a_{ij})$ — матрица $-A = (-a_{ij})$.

Перейдём к определению действительно «матричных» операций.

Определение 2. Пусть даны матрицы $A = (a_{ij})$ и $B = (b_{jk})$ размеров $m \times n$ и $n \times p$ соответственно. Матрица $C = (c_{ik})$ называется *произведением* матрицы A на матрицу B, если

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

для всех i, k. Обозначение: $C = AB$.

Можно сказать, что матрицы перемножаются по правилу «строка на столбец»: чтобы вычислить элемент c_{ik} произведения, нужно i-ю строку левого сомножителя A умножить на k-й столбец правого сомножителя B. Смысл именно такого способа умножения матриц проясняет следующий

Пример 1. Рассмотрим системы векторов S: u_1, u_2, T: v_1, v_2, v_3 и R: w_1, w_2. Предположим, что S линейно выражается через T, а T — через R:

$$\begin{array}{l} u_1 = a_{11}v_1 + a_{12}v_2 + a_{13}v_3, \\ u_2 = a_{21}v_1 + a_{22}v_2 + a_{23}v_3, \end{array} \quad ; \quad \begin{array}{l} v_1 = b_{11}w_1 + b_{12}w_2, \\ v_2 = b_{21}w_1 + b_{22}w_2, \\ v_3 = b_{31}w_1 + b_{32}w_2. \end{array}$$

Составим из коэффициентов этих линейных комбинаций матрицы A и B соответственно. Ясно, что система S должна линейно выражаться через систему R. Нетрудно проверить, что матрица C коэффициентов соответствующих линейных комбинаций оказывается ни чем иным, как произведением AB. □

Упражнение 2. Проверьте это.

Очевидно, размеры перемножаемых матриц не могут быть произвольными, но, например, всегда можно перемножить две квадратные матрицы одного размера. Перечислим теперь основные свойства операции умножения матриц.

1. Умножение матриц *некоммутативно*, т. е., вообще говоря, $AB \neq BA$.

В самом деле, наугад взятые две квадратные матрицы (например, 2-го порядка) подтверждают это.

Упражнение 3. Проведите этот эксперимент и убедитесь.

2. Умножение матриц *ассоциативно*: $(AB)C = A(BC)$.

Действительно, пусть $A = (a_{ij})$, $B = (b_{jk})$, $C = (c_{kl})$ — три матрицы согласованных размеров $m \times n$, $n \times p$, $p \times q$ соответственно. Тогда

$$[(AB)C]_{il} = \sum_{k=1}^{p} [AB]_{ik} c_{kl} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) c_{kl} = \sum_{k=1}^{p} \sum_{j=1}^{n} a_{ij} b_{jk} c_{kl}$$

и совершенно аналогично

$$[A(BC)]_{il} = \sum_{j=1}^{n} a_{ij} [BC]_{jl} = \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{p} b_{jk} c_{kl} \right) = \sum_{j=1}^{n} \sum_{k=1}^{p} a_{ij} b_{jk} c_{kl}.$$

При любых фиксированных i, l две полученные суммы отличаются лишь порядком суммирования произведений $a_{ij} b_{jk} c_{kl}$ и потому равны, т. е. $[(AB)C]_{il} = [A(BC)]_{il}$.

3. Умножение матриц *дистрибутивно* относительно сложения:

$$A(B + C) = AB + AC, \quad (B + C)A = BA + CA.$$

Докажем, например, первое из этих равенств. Пусть матрица $A = (a_{ij})$ имеет размер $m \times n$, а матрицы $B = (b_{jk})$, $C = (c_{jk})$ — размер $n \times p$. Имеем

$$[A(B + C)]_{ik} = \sum_{j=1}^{n} a_{ij}(b_{jk} + c_{jk}) = \sum_{j=1}^{n} a_{ij} b_{jk} + \sum_{j=1}^{n} a_{ij} c_{jk} = [AB]_{ik} + [AC]_{ik},$$

что и требовалось.

Из-за некоммутативности умножения при действиях с матрицами следует соблюдать бóльшую аккуратность, чем при аналогичных действиях с числами.

Пример 2. Привычное для чисел тождество

$$(A+B)^2 = A^2 + 2AB + B^2$$

не выполняется для квадратных матриц одинакового порядка. Мы получим правильный вариант

$$(A+B)^2 = A^2 + AB + BA + B^2$$

этого тождества, если аккуратно раскроем скобки в произведении $(A+B)(A+B)$. □

Операция умножения матриц связана с операцией умножения матрицы на число следующим образом:

$$(\lambda A)(\mu B) = (\lambda\mu)AB$$

для любых чисел λ, μ и матриц A, B согласованных размеров.

Определение 3. Для матрицы $A = (a_{ij})$ размера $m \times n$ *транспонированной* матрицей называется матрица $A^t = (a^t_{ij})$ размера $n \times m$, где $a^t_{ij} = a_{ji}$ для любых i, j.

Очевидно, при транспонировании строки (столбцы) матрицы A становятся столбцами (строками) матрицы A^t. Перечислим свойства операции транспонирования.

1. $(A+B)^t = A^t + B^t$.
2. $(\lambda A)^t = \lambda A^t$.
3. $(AB)^t = B^t A^t$.

Первые два из них довольно очевидны, а доказательство третьего выглядит так:

$$[(AB)^t]_{ik} = [AB]_{ki} = \sum_{j=1}^{n} a_{kj} b_{ji} = \sum_{j=1}^{n} b^t_{ij} a^t_{jk} = [B^t A^t]_{ik}.$$

Упражнение 4. Пусть $C = AB$. Докажите, что система столбцов матрицы C линейно выражается через систему столбцов матрицы A, а система строк матрицы C — через систему строк матрицы B. Как следствие, $\operatorname{rank}(C) \leqslant \min\{\operatorname{rank}(A), \operatorname{rank}(B)\}$.

II. Обратная матрица. Умножение (как, впрочем, и сложение) квадратных матриц одного порядка имеет особое значение, поскольку множество всех таких матриц замкнуто относительно этой операции. В этом пункте мы всюду будем иметь дело только с квадратными матрицами n-го порядка.

Прежде всего отметим, что существует такая матрица E, при умножении на которую (как слева, так и справа) ничего не происходит:

$$AE = EA = A$$

для любой матрицы A. Это *единичная* матрица $E = (e_{ij})$, где

$$e_{ij} = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j. \end{cases}$$

В умножении матриц она играет ту же роль, что и единица в умножении чисел.

Определение 4. Матрица A называется *обратимой*, если существует такая матрица B, что $AB = BA = E$. Эта матрица B называется *обратной* к матрице A.

Конечно, произвольно взятая матрица A может оказаться и необратимой (например, такова нулевая матрица, но не только она). Однако если же A обратима, то для неё существует лишь одна обратная матрица B. В самом деле, если B_1, B_2 — матрицы, обратные к матрице A, то

$$B_1 = B_1E = B_1(AB_2) = (B_1A)B_2 = EB_2 = B_2.$$

Эту единственную обратную матрицу B будем обозначать A^{-1}.

Далее мы сформулируем критерий обратимости матрицы A, а также укажем способ найти обратную матрицу A^{-1}.

Теорема 1. Матрица A обратима тогда и только тогда, когда $\operatorname{rank}(A) = n$.

Доказательство. Пусть $a_1, \ldots, a_n$ — система столбцов матрицы A. Предположим, что $\operatorname{rank}(A) = n$. Тогда по теореме 5 из § 3 система $a_1, \ldots, a_n$ есть базис пространства $\mathbb{R}^n$. Следовательно, существуют такие числа b_{ij}, что

$$b_{1j}a_1 + \ldots + b_{nj}a_n = e_j, \quad j = 1, \ldots, n, \tag{1}$$

где e_j — единичные векторы. Положим $B = (b_{ij})$. Тогда n векторных равенств (1) можно объединить в одно матричное равенство

$$AB = E,$$

где E — матрица, составленная из e_j как из столбцов, т. е. единичная матрица. Покажем, что $B = A^{-1}$.

Из упражнения 4 следует, что $\operatorname{rank}(B) = n$. Значит, к матрице B применимы предыдущие рассуждения и существует такая матрица C, что

$$BC = E.$$

Но $C = EC = (AB)C = A(BC) = AE = A$, и равенство $B = A^{-1}$ обосновано.

Итак, мы доказали, что условие $\operatorname{rank}(A) = n$ является достаточным для обратимости матрицы A. То, что оно является и необходимым, вытекает из упражнения 4. □

Упражнение 5. Объясните, как именно вытекает.

Из доказательства теоремы 1 следует, что для нахождения обратной матрицы A^{-1} нужно решить n векторных уравнений (1) с неизвестными b_{ij}. Каждое такое уравнение равносильно СЛУ с одной и той же матрицей A, поэтому их все можно решать методом Гаусса одновременно. Для этого обычно составляют расширенную матрицу вида $(A \mid E)$ и при помощи элементарных преобразований строк пытаются привести её к виду $(E \mid B)$, попутно вычисляя $\operatorname{rank}(A)$. Если выясняется, что $\operatorname{rank}(A) = n$, то такой переход возможен и тогда $B = A^{-1}$.

Упражнение 6. Пусть A, B — обратимые матрицы, λ — ненулевое число. Докажите, что: а) $(AB)^{-1} = B^{-1}A^{-1}$; б) $(A^t)^{-1} = (A^{-1})^t$; в) $(\lambda A)^{-1} = \lambda^{-1}A^{-1}$.

III. Матричные уравнения. В очередной раз вернёмся к решению СЛУ. Ранее (см. п. **I** § 6) мы заметили, что произвольную СЛУ можно представить в виде одного векторного уравнения. Ещё более компактной будет запись произвольной СЛУ

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

в виде *матричного* уравнения

$$AX = B. \tag{3}$$

Здесь $A = (a_{ij})$ — это матрица СЛУ (2) размера $m \times n$, X — матрица-столбец размера $n \times 1$, заполненная неизвестными, и B — матрица-столбец размера $m \times 1$ из свободных коэффициентов:

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Если $m = n$ и матрица A обратима, то X можно найти по формуле

$$X = A^{-1}B,$$

получающейся, если обе части уравнения (3) умножить слева на A^{-1}. Разумеется, практическая ценность этой формулы определяется наличием альтернативного методу Гаусса способа вычисления обратной матрицы.

Более общий, нежели (3), тип матричных уравнений

$$AXB = C, \tag{4}$$

где A, B — квадратные матрицы (не обязательно одного порядка), можно исследовать аналогичным образом. Для осмысленности уравнения (4) размер матрицы C должен быть согласован с размерами матриц A и B (подумайте, как именно). Тогда в наиболее благоприятной ситуации — когда обе матрицы A и B обратимы — уравнение (4) будет иметь единственное решение

$$X = A^{-1}CB^{-1}$$

(Запоминать эту формулу не следует, поскольку «бутерброд» в её правой части можно правильно приготовить только одним способом.) Если обратимой является, например, лишь матрица A, то уравнение (4) можно всего лишь упростить, заменив уравнением

$$XB = A^{-1}C.$$

Теперь, чтобы найти неизвестную матрицу X, можно составить СЛУ, где в роли неизвестных будут элементы матрицы X, и применить к этой СЛУ метод Гаусса.

§ 8. Перестановки и подстановки. Чётность подстановки

Перестановки и подстановки. Умножение подстановок. Циклические подстановки (циклы). Теорема о разложении подстановки в произведение независимых циклов. Разложение подстановки в произведение транспозиций. Декремент и чётность подстановки.

Этот параграф носит вспомогательный характер и необходим, прежде всего, для построения теории определителей, которая будет изложена в § 9 — 12.

I. Перестановки и подстановки. Начнём с определений этих понятий.

Определение 1. Пусть задано некоторое конечное множество Ω из n элементов. *Перестановкой* элементов множества Ω называется их запись в каком-либо порядке.

Поскольку в дальнейшем природа элементов множества будет не важна, примем за Ω множество первых n натуральных чисел:

$$\Omega = \{1, 2, \ldots, n\}.$$

Таким образом, произвольная перестановка элементов множества Ω — это последовательность $i_1, \ldots, i_n$, в которой $i_k \neq i_l$ при $k \neq l$, так что $\Omega = \{i_1, \ldots, i_n\}$.

Нетрудно видеть, что при $n = 1$ имеется одна перестановка, при $n = 2$ их будет две, а при $n = 3$ — шесть. В общем случае ответ на вопрос о количестве перестановок даёт

Теорема 1. Число всех перестановок элементов множества Ω равно $n!$ — произведению первых n натуральных чисел.

Доказательство. Это хорошо известный факт из элементарной комбинаторики. Он может быть доказан, например, индукцией по n. □

Упражнение 1. Приведите доказательство.

Определение 2. *Подстановкой* на множестве Ω называется взаимно однозначное соответствие между элементами множества Ω.

Всякая подстановка записывается в виде таблицы

$$\alpha = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix} \tag{1}$$

из двух строк, нижняя строка которой есть некоторая перестановка верхней. При этом произвольному элементу k верхней строке соответствует элемент i_k нижней строки, что записывается следующим образом:

$$\alpha(k) = i_k, \quad k = 1, \ldots, n.$$

Если для некоторого $k \in \Omega$ имеем $\alpha(k) = k$, то элемент k называется *неподвижным* относительно подстановки α. Столбцы таблицы (1) можно переставлять, не меняя смысла подстановки α. Запись подстановки в виде (1) будем называть *стандартной*. Из теоремы 1 следует, что число всех подстановок α на множестве Ω равно $n!$.

Обозначим через S_n множество всех подстановок на множестве Ω (или, как ещё говорят, подстановок n-й степени). На множестве S_n можно задать естественную операцию — так называемое умножение подстановок.

Определение 3. Пусть $\alpha,\ \beta \in S_n$. *Произведением* подстановки α на подстановку β называется такая подстановка $\gamma \in S_n$, выполнение которой эквивалентно последовательному выполнению подстановки α, а затем подстановки β. Обозначение: $\gamma = \alpha\beta$.

Иными словами, произведение двух подстановок есть их композиция, т. е. последовательное применение в указанном порядке.

Пример 1. Пусть $n = 4$. Рассмотрим две подстановки:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$

Тогда

$$\gamma_1 = \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \gamma_2 = \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

Так, например, $\gamma_1(3) = 1$, поскольку $\alpha(3) = 4$, а $\beta(4) = 1$. □

Как видно из этого примера, умножение подстановок *некоммутативно*, т. е., вообще говоря, $\alpha\beta \neq \beta\alpha$. Исключения составляют лишь случаи $n = 1$ и $n = 2$.

Однако умножение подстановок, очевидно, обладает свойством *ассоциативности*: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ для любых подстановок α, β, γ.

Упражнение 2. Объясните, почему.

Подстановку

$$\varepsilon = \begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix}$$

будем называть *тождественной*. Очевидно, $\alpha\varepsilon = \varepsilon\alpha = \alpha$ для любой $\alpha \in S_n$.

Для данной подстановки $\alpha \in S_n$ подстановка $\beta \in S_n$ называется *обратной*, если

$$\alpha\beta = \beta\alpha = \varepsilon.$$

В отличие, скажем, от умножения матриц, здесь проблем с обратимостью нет: для подстановки α, заданной таблицей (1), можно взять

$$\beta = \begin{pmatrix} i_1 & \dots & i_n \\ 1 & \dots & n \end{pmatrix}$$

(такая запись подстановки, конечно, не будет стандартной, но подходящей перестановкой столбцов она приводится к стандартному виду). Обратная подстановка обозначается стандартно: $\beta = \alpha^{-1}$.

Упражнение 3. Докажите следующее правило обращения произведения нескольких подстановок: $(\alpha\beta\dots\gamma)^{-1} = \gamma^{-1}\dots\beta^{-1}\alpha^{-1}$.

II. Циклические подстановки. Результат применения «нетривиальной» подстановки $\alpha \in S_n$ к элементам множества Ω было бы желательно представить в виде результата последовательного выполнения нескольких «простейших» подстановок.

Определение 4. Подстановка $\sigma \in S_n$ называется *циклической* (или *циклом*), если существуют такие различные элементы $i_1, i_2, \ldots, i_k$ из Ω, что

$$\sigma(i_l) = i_{l+1}, \quad l = 1, \ldots, k$$

(считаем $i_{k+1} = i_1$), а все остальные элементы $i \in \Omega$ являются неподвижными.

Число $k \geqslant 2$ называется *длиной* цикла σ, сам цикл обычно записывают в виде

$$\sigma = (i_1 i_2 \ldots i_k), \tag{2}$$

а про элементы $i_1, i_2, \ldots, i_k$ говорят, что они составляют *тело* цикла (эта запись неоднозначна и, кроме того, требует уточнения значения n). Циклы длины 2 принято называть *транспозициями*. Имеем

$$\sigma^k = \varepsilon, \quad \sigma^{-1} = (i_k i_{k-1} \ldots i_1).$$

Два цикла $\sigma_1, \sigma_2 \in S_n$ называются *независимыми*, если их тела не пересекаются. Очевидно, это условие равносильно тому, что они коммутируют: $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Теорема 2. Любую подстановку можно разложить в произведение попарно независимых циклов. Это разложение единственно, если не учитывать порядок сомножителей в произведении.

Циклические подстановки, таким образом, представляют своего рода кирпичики, из которых можно сложить, причём единственным способом, произвольную подстановку. Мы не станем доказывать этот довольно очевидный факт, а ограничимся одним примером, где покажем, как практически находить такое разложение.

Пример 2. Пусть $n = 7$. Разложим подстановку

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 7 & 2 & 6 & 1 \end{pmatrix}$$

в произведение независимых циклов. Стартуем, например, с элемента 1:

$$\alpha(1) = 3, \quad \alpha(3) = 4, \quad \alpha(4) = 7, \quad \alpha(7) = 1,$$

и первый цикл определился: $\sigma_1 = (1347)$. Далее выберем какой-нибудь элемент, не принадлежащий телу цикла σ_1, и для него проделаем аналогичное:

$$\alpha(2) = 5, \quad \alpha(5) = 2,$$

откуда второй цикл $\sigma_2 = (25)$. Единственный оставшийся (т. е. не принадлежащий телам циклов σ_1, σ_2) элемент 6 является неподвижным относительно подстановки α, и мы можем записать следующее разложение:

$$\alpha = \sigma_1\sigma_2 = (1347)(25).$$

По построению оно и будет искомым. □

Поскольку каждый цикл (2) можно представить в виде произведение

$$\sigma = \tau_1 \dots \tau_{k-1}, \tag{3}$$

где $\tau_l = (i_1 i_{l+1})$ — транспозиции, то получаем такое

Следствие. Любую подстановку можно разложить в произведение транспозиций.

Так, для подстановки α из примера 2 имеем $\alpha = (13)(14)(17)(25)$.

Упражнение 4. Убедитесь в справедливости равенства (3). Обязано ли разложение подстановки в произведение транспозиций быть однозначным? содержать попарно независимые транспозиции?

III. Чётность подстановки. Эта характеристика произвольной подстановки может быть определена разными эквивалентными способами. Мы выберем следующий.

Определение 5. *Декрементом* подстановки $\alpha \in S_n$ называется целое число

$$d(\alpha) = n - (s + t),$$

где s — число независимых циклов, в произведение которых разлагается α, а t — число элементов, неподвижных относительно α. Подстановка α называется *чётной* (*нечётной*), если её декремент $d(\alpha)$ чётен (нечётен).

Например, для подстановки α из примера 2 имеем $d(\alpha) = 7 - (2 + 1) = 4$, так что эта подстановка является чётной.

Тождественная подстановка ε является чётной, а чётность цикла σ длины k противоположна чётности числа k (в частности, любая транспозиция τ является нечётной подстановкой). Подстановки α и α^{-1} имеют одинаковую чётность.

Упражнение 5. Докажите эти утверждения, вычислив декременты соответствующих подстановок.

Ещё одно важное свойство чётности описывает следующая

Теорема 3. При умножении подстановки на транспозицию (как слева, так и справа) чётность подстановки меняется.

Доказательство. Пусть $\alpha \in S_n$ — данная подстановка и $\beta = \tau\alpha$, где $\tau = (ij)$ — некоторая транспозиция. Покажем, что чётности подстановок α и β различны.

Пусть $\alpha = \sigma_1 \dots \sigma_s$ — разложение подстановки α в произведение независимых циклов. Рассмотрим различные варианты.

а) Оба элемента i, j принадлежат телу какого-то одного цикла, например σ_s. Запишем этот цикл в виде

$$\sigma_s = (i i_1 \dots i_k j j_1 \dots j_l)$$

и найдём разложение подстановки β в произведение независимых циклов. Имеем

$$\beta = \tau\sigma_1 \dots \sigma_{s-1}\sigma_s = \sigma_1 \dots \sigma_{s-1}\tau\sigma_s = \sigma_1 \dots \sigma_{s-1}(ij)(i i_1 \dots i_k j j_1 \dots j_l) = \\ = \sigma_1 \dots \sigma_{s-1}(i j_1 \dots j_l)(j i_1 \dots i_k),$$

т. е. количество независимых циклов увеличилось на один. Значит, $d(\beta) = d(\alpha) - 1$.

б) Оба элемента i, j являются неподвижными относительно подстановки α. Тогда

$$\beta = \tau\sigma_1 \dots \sigma_s$$

есть разложение в произведение независимых циклов, т. е. опять $d(\beta) = d(\alpha) - 1$.

в) Элементы i, j принадлежат телам разных циклов. Пусть, к примеру, i принадлежит телу σ_{s-1}, а j — телу σ_s. Тогда можно записать

$$\sigma_{s-1} = (ii_1 \dots i_k), \quad \sigma_s = (jj_1 \dots j_l).$$

В этом случае имеем

$$\beta = \tau\sigma_1 \dots \sigma_{s-2}\sigma_{s-1}\sigma_s = \sigma_1 \dots \sigma_{s-2}\tau\sigma_{s-1}\sigma_s = \sigma_1 \dots \sigma_{s-2}(ij)(ii_1 \dots i_k)(jj_1 \dots j_l) = \\ = \sigma_1 \dots \sigma_{s-2}(ii_1 \dots i_k jj_1 \dots j_l),$$

и количество независимых циклов уменьшилось на один, т. е. $d(\beta) = d(\alpha) + 1$.

г) Этот последний вариант читатель может рассмотреть самостоятельно. Здесь также $d(\beta) = d(\alpha) + 1$.

Итак, всегда $d(\beta) = d(\alpha) \pm 1$, поэтому чётности подстановок α и $\beta = \tau\alpha$ противоположны. Так же обстоит дело и тогда, когда подстановка α умножается на транспозицию τ справа. Действительно, $(\alpha\tau)^{-1} = \tau^{-1}\alpha^{-1} = \tau\alpha^{-1}$, а чётности α и α^{-1} совпадают. □

Доказанная теорема делает очевидным следующий критерий чётности подстановки, который иногда принимают за определение: подстановка α является чётной тогда и только тогда, когда она разлагается в произведение чётного количества транспозиций. Отсюда в качестве следствия получим такое интуитивно ожидаемое утверждение: произведение двух подстановок одинаковой чётности будет чётной подстановкой, а произведение двух подстановок разной чётности — нечётной.

Ещё одно следствие теоремы 3: при $n > 1$ в множестве S_n чётных и нечётных подстановок поровну, т. е. по $n!/2$ штук.

Упражнение 6. Докажите это утверждение, сопоставив каждой чётной подстановке α нечётную подстановку $\beta = \tau\alpha$, где τ — некоторая фиксированная транспозиция.

Сделаем несколько заключительных замечаний.

1. Декремент $d(\alpha)$ подстановки α — это наименьшее число транспозиций, в произведение которых можно разложить эту подстановку. Действительно, если $\tau_1, \dots, \tau_t$ — транспозиции, то $d(\tau_1 \dots \tau_t) \leqslant t$ (доказательство проводится индукцией по t). С другой стороны, α допускает разложение в произведение $d(\alpha)$ транспозиций — так, как было описано выше.

2. Опишем ещё один способ определить чётность подстановки. Пусть дана некоторая перестановка $i_1, \dots, i_n$. Говорят, что индексы i_k и i_l образуют *инверсию*, если $k < l$, но $i_k > i_l$ (иными словами, инверсия есть беспорядок, отсутствие естественного порядка). Оказывается, чётность подстановки α, записанной в стандартном виде (1), совпадает с чётностью количества инверсий в нижней строке $i_1, \dots, i_n$.

Для доказательства достаточно понять, что при транспозиции двух элементов i и j в перестановке чётность числа инверсий поменяется на противоположную. Если i и j — соседние элементы, то число инверсий, как легко понять, изменится на единицу; если же между i и j в точности k других элементов, то потребуется ровно $2k + 1$ транспозиций соседних элементов, чтобы поменять местами i и j.

3. Интересный пример, в котором хорошо работает понятие чётности подстановки, представляет известная «игра в 15» (см. `https://en.wikipedia.org/wiki/15_puzzle`).

§ 9. Определитель квадратной матрицы

Определитель (детерминант) квадратной матрицы. Вычисление определителей матриц малых порядков. Свойства определителей.

Рассмотрим простейшую квадратную СЛУ, в которой два уравнения и два неизвестных:

$$\begin{cases} ax + by = c, \\ dx + ey = f. \end{cases}$$

Естественно пытаться найти общие формулы, позволяющие выразить неизвестные x, y через коэффициенты $a, b, \ldots, f$. Это нетрудно сделать, по очереди исключив неизвестные с помощью элементарных преобразований:

$$x = \frac{ce - bf}{ae - bd}, \quad y = \frac{af - cd}{ae - bd}.$$

Легко заметить, что выражения в числителях и (общем) знаменателе устроены по одному принципу. А именно, сопоставим каждой матрице

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

число $\det(A) = a_{11}a_{22} - a_{12}a_{21}$ — так называемый определитель матрицы A. Тогда наши формулы примут вид

$$x = \frac{\Delta_x}{\Delta}, \quad y = \frac{\Delta_y}{\Delta}, \tag{1}$$

где

$$\Delta = \det \begin{pmatrix} a & b \\ d & e \end{pmatrix}, \quad \Delta_x = \det \begin{pmatrix} c & b \\ f & e \end{pmatrix}, \quad \Delta_y = \det \begin{pmatrix} a & c \\ d & f \end{pmatrix}.$$

Формулы, аналогичные (1), существуют для любой квадратной СЛУ и называются формулами Крамера. Мы их получим в § 12, а здесь и в следующих двух параграфах рассмотрим необходимые для этого факты из теории определителей — выражений вида $\det(A)$ для квадратных матриц A любого порядка.

I. Определение и примеры. Пусть дана квадратная матрица n-го порядка:

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}.$$

Рассмотрим всевозможные произведения по n элементов этой матрицы, расположенных в разных строках и разных столбцах. Очевидно, каждое такое произведение представляется в виде $a_{1i_1} \ldots a_{ni_n}$ и соответствует некоторой подстановке

$$\alpha = \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}.$$

Всего таких произведений $a_{1i_1} \ldots a_{ni_n}$ имеется $n!$ штук.

Определение 1. *Детерминантом* (*определителем*) матрицы A называется число

$$\det(A) = \sum_{\alpha \in S_n} \pm a_{1i_1} \dots a_{ni_n}. \tag{2}$$

Знак плюс или минус перед каждым произведением в сумме выбирается в зависимости от того, является подстановка α чётной или нечётной.

Число слагаемых в правой части формулы (2) равно $n!$, а значит, быстро возрастает с ростом n. Вместо обозначения $\det(A)$ часто используют более простое $|A|$.

Пример 1. Для матрицы

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

второго порядка получим $\det(A) = a_{11}a_{22} - a_{12}a_{21}$. □

Пример 2. Для матрицы

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

третьего порядка выражение для определителя будет таким:

$$\det(A) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{32}a_{21} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

Для запоминания этой громоздкой формулы существует мнемоническое *правило треугольников*. □

Упражнение 1. Проверьте правильность выражений для $\det(A)$, полученных в примерах 1 и 2. Научитесь правильно пользоваться правилом треугольников.

При $n > 3$ формулу (2) в явном виде выписывать нецелесообразно, так как на практике пользоваться такой формулой было бы затруднительно.

II. Свойства определителей. В этом пункте мы рассмотрим некоторые свойства определителей, которые можно использовать при их вычислении.

1. При транспонировании матрицы определитель не меняется:

$$\det(A^t) = \det(A).$$

В самом деле, имеем

$$\det(A^t) = \sum_{\alpha \in S_n} \pm a^t_{1i_1} \dots a^t_{ni_n} = \sum_{\alpha \in S_n} \pm a_{i_1 1} \dots a_{i_n n} = \sum_{\beta \in S_n} \pm a_{1j_1} \dots a_{nj_n} = \det(A),$$

где подстановка β связана с подстановкой α следующим образом:

$$\beta = \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix} = \begin{pmatrix} i_1 & \dots & i_n \\ 1 & \dots & n \end{pmatrix} = \alpha^{-1},$$

в частности, эти подстановки имеют одинаковую чётность.

В силу этого свойства всякое утверждение, справедливое для определителей и сформулированное в терминах строк матрицы, останется верным, если его переформулировать в терминах столбцов матрицы. В дальнейшем мы будем явно приводить только один вариант утверждения — в терминах строк.

2. При перестановке двух строк матрицы определитель меняет только знак:

$$\det(A') = -\det(A),$$

где A' — матрица, полученная из матрицы A перестановкой некоторых двух строк. Как следствие, определитель матрицы, имеющей две одинаковых строки, равен нулю.

Упражнение 2. Докажите это свойство, следуя схеме доказательства свойства **1**.

3. Если строку матрицы умножить на число λ, то определитель также умножится на это число:

$$\det(A') = \lambda \det(A),$$

где A' — матрица, полученная из матрицы A умножением некоторой строки на число λ. В частности, если матрица содержит нулевую строку, то её определитель равен нулю.

Это свойство довольно очевидно вытекает из формулы (2).

Упражнение 3. Приведите доказательство.

4. Фиксируем номер t и предположим, что каждая из матриц $A^{(1)}, \ldots, A^{(s)}$ совпадает с матрицей A всюду, кроме t-й строки, при этом сумма t-х строк матриц $A^{(1)}, \ldots, A^{(s)}$ равна t-й строке матрицы A:

$$a_{tj} = a_{tj}^{(1)} + \ldots + a_{tj}^{(s)}, \quad j = 1, \ldots, n.$$

Тогда справедлива *формула сложения* определителей:

$$\det(A) = \det(A^{(1)}) + \ldots + \det(A^{(s)}).$$

И здесь утверждение является прямым следствием формулы (2). Имеем

$$\begin{aligned}\det(A) &= \sum_{\alpha\in S_n} \pm a_{1i_1}\ldots a_{ti_t}\ldots a_{ni_n} = \sum_{\alpha\in S_n} \pm a_{1i_1}\ldots(a_{ti_t}^{(1)} + \ldots + a_{ti_t}^{(s)})\ldots a_{ni_n} = \\ &= \sum_{\alpha\in S_n} \pm a_{1i_1}\ldots a_{ti_t}^{(1)}\ldots a_{ni_n} + \ldots + \sum_{\alpha\in S_n} \pm a_{1i_1}\ldots a_{ti_t}^{(s)}\ldots a_{ni_n} = \\ &= \det(A^{(1)}) + \ldots + \det(A^{(s)}),\end{aligned}$$

что и требовалось.

§ 10. Основные свойства определителя

Свойства определителя (продолжение). Вычисление определителя приведением к треугольному виду. Определитель Вандермонда. Критерий равенства определителя нулю.

Продолжим обсуждение свойств определителей, начатое в предыдущем параграфе. Будем использовать те же обозначения.

I. Свойства определителей (продолжение). Следующее свойство играет важную роль при вычислении определителей и им приходится пользоваться наиболее часто.

5. Определитель матрицы не изменится, если к некоторой строке матрицы прибавить другую её строку, предварительно умноженную на какое-нибудь число λ:

$$\det(A') = \det(A),$$

где A' — матрица, полученная из A описанным выше преобразованием.

Действительно, пользуясь формулой сложения (см. свойство **4**), получим

$$\det(A') = \det(A) + \lambda \det(A^{(1)}),$$

где у матрицы $A^{(1)}$ две одинаковые строки. Но тогда $\det(A^{(1)}) = 0$, и равенство доказано.

Это свойство допускает следующее обобщение: определитель матрицы не изменится, если к некоторой строке матрицы прибавить произвольную линейную комбинацию её остальных строк.

Упражнение 1. Докажите это более общее утверждение.

6. Определитель *треугольной* матрицы равен произведению её диагональных элементов:

$$\det \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix} = a_{11}a_{22}\dots a_{nn}.$$

Это очевидным образом следует из явной формулы (2) из § 9, поскольку единственным ненулевым произведением в сумме справа может быть только произведение диагональных элементов, соответствующее тождественной подстановке.

В свойствах **2**, **3** и **5** объяснено, что происходит с определителем матрицы после применения к ней элементарных преобразований строк. Учитывая и свойство **6**, мы можем предложить такой алгоритм вычисления определителей, который не апеллирует к явной формуле, а именно: с помощью элементарных преобразований строк привести данную матрицу к треугольному виду, следя при этом за изменениями определителя, и затем вычислить определитель получившийся треугольной матрицы.

Примеры применения этого алгоритма вычисления определителей будут разобраны на практических занятиях. Здесь мы ограничимся вычислением так называемого *определителя Вандермонда*[3)], который естественным образом возникает в различных задачах алгебры и математического анализа.

[3)] А. Т. Вандермонд (1735 — 1796) — французский математик и музыкант.

Пример 1. Речь идёт об определителе

$$V_{n+1}(x_0, x_1, \ldots, x_n) = \det \begin{pmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{pmatrix},$$

где $x_0, x_1, \ldots, x_n$ — произвольные числа. Мы докажем следующую формулу:

$$V_{n+1}(x_0, x_1, \ldots, x_n) = \prod_{0 \leqslant i < j \leqslant n} (x_j - x_i). \tag{1}$$

Для доказательства совершим такую серию преобразований над $V_{n+1}(x_0, x_1, \ldots, x_n)$: для каждого j, начиная с $j = n - 1$ и до $j = 1$, умножим j-й столбец на $-x_0$ и прибавим к $(j + 1)$-му столбцу. В результате получим равенство

$$V_{n+1}(x_0, x_1, \ldots, x_n) = \det \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & x_1 - x_0 & x_1^2 - x_0 x_1 & \ldots & x_1^n - x_0 x_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & x_n - x_0 & x_n^2 - x_0 x_n & \ldots & x_n^n - x_0 x_n^{n-1} \end{pmatrix}.$$

Непосредственно из определения детерминанта можно заметить, что последний определитель равен

$$\det \begin{pmatrix} x_1 - x_0 & x_1^2 - x_0 x_1 & \ldots & x_1^n - x_0 x_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ x_n - x_0 & x_n^2 - x_0 x_n & \ldots & x_n^n - x_0 x_n^{n-1} \end{pmatrix} \tag{2}$$

(это наблюдение далее будет обобщено, см. лемму 1 в § 12). Если теперь в определителе (2) вынести из каждой строки множитель $x_i - x_0$, то он превратится в определитель

$$\det \begin{pmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & x_n & \ldots & x_n^{n-1} \end{pmatrix} = V_n(x_1, \ldots, x_n).$$

Таким образом, мы пришли к рекуррентному соотношению

$$V_{n+1}(x_0, x_1, \ldots, x_n) = (x_1 - x_0) \ldots (x_n - x_0) V_n(x_1, \ldots, x_n).$$

Применяя к определителю $V_n(x_1, \ldots, x_n)$ аналогичные рассуждения, в конечном итоге получим формулу (1). □

Замечание. Существуют и другие способы вычисления определителя Вандермонда.

Несколько более экономный алгоритм вычисления определителей будет предложен далее в § 12.

II. Критерий равенства определителя нулю. Часто бывает нужно знать, равен нулю данный определитель или нет. Следующая теорема предоставляет такой критерий.

Теорема 1. $\det(A) = 0$ тогда и только тогда, когда $\operatorname{rank}(A) < n$.

ДОКАЗАТЕЛЬСТВО. Предположим сначала, что $\operatorname{rank}(A) < n$. Это означает, например, что строки $a_1, a_2, \ldots, a_n$ матрицы A линейно зависимы. Для определённости будем считать, что первая строка линейно выражается через остальные строки:

$$a_1 = \lambda_2 a_2 + \ldots + \lambda_n a_n$$

для некоторых чисел $\lambda_2, \ldots, \lambda_n$. Прибавим к первой строке a_1 линейную комбинацию

$$(-\lambda_2)a_2 + \ldots + (-\lambda_n)a_n$$

остальных строк, не изменив при этом $\det(A)$. В результате получим матрицу с нулевой строкой и, следовательно, нулевым определителем.

Предположим теперь, что $\operatorname{rank}(A) = n$. Тогда матрицу A можно привести к треугольному виду с ненулевыми диагональными элементами. Поскольку используемые при этом элементарные преобразования либо не меняют определителя, либо меняют только его знак, определитель Δ полученной треугольной матрицы будет отличаться от $\det(A)$ разве что знаком. Но $\Delta \neq 0$, поэтому и $\det(A) \neq 0$. □

Матрица A, для которой $\det(A) \neq 0$, называется *невырожденной*. Как видим, критерием невырожденности матрицы A является полнота её ранга: $\operatorname{rank}(A) = n$. Но это же условие является и критерием обратимости матрицы A (см. теорему 1 из § 7), поэтому матрица A обратима тогда и только тогда, когда она невырождена. В § 12 мы получим явную формулу для обратной матрицы A^{-1} в терминах теории определителей.

§ 11. Мультипликативное свойство определителя

Мультипликативное свойство определителя: $\det(AB) = \det(A)\det(B)$.

Цель этого параграфа — доказать следующее свойство определителя:

$$\det(AB) = \det(A)\det(B), \tag{1}$$

где A, B — произвольные квадратные матрицы одного порядка. Это можно сделать разными способами. Мы выберем тот, который естественным образом вытекает из ранее доказанных свойств определителя и алгоритма вычисления определителя приведением к треугольному виду.

I. Элементарные матрицы. Рассмотрим матрицы специального вида, при помощи которых можно описать элементарные преобразования над строками (столбцами) произвольной матрицы в терминах матричного умножения.

Пусть E — единичная матрица m-го порядка, а E_{kl} — квадратная матрица того же порядка, у которой на пересечении k-й строки и l-го столбца стоит единица, а на всех остальных местах находятся нули.

Определение 1. *Элементарные* матрицы m-го порядка — это матрицы вида

$$F_{kl}(\lambda) = E + \begin{cases} \lambda E_{kl}, & \text{если } k \neq l, \\ (\lambda - 1)E_{kl}, & \text{если } k = l, \end{cases}$$

где λ — произвольное число.

Такое название объясняется следующим: если A — матрица размера $m \times n$, то матрица

$$A' = F_{kl}(\lambda)A$$

получается из A при помощи одного элементарного преобразования над строками.

Упражнение 1. Докажите, что при $k \neq l$ к k-й строке матрицы A прибавляется l-я строка, умноженная на λ, а если $k = l$, то l-я строка матрицы A умножается на λ.

Заметим, что для матрицы A', полученной из A переменой местами k-й и l-й строк, имеет место равенство

$$A' = F_{kl}(-1)F_{lk}(1)F_{ll}(-1)F_{kl}(1)A = G_{kl}A,$$

где G_{kl} — матрица, получающаяся из E перестановкой k-й и l-й строк (матрицы такого вида также будем называть элементарными).

Упражнение 2. Убедитесь в этом.

Указание. Вспомните про упражнение 1 из § 1.

Итак, любое элементарное преобразование над строками матрицы A размера $m \times n$ можно представить как умножение матрицы A слева на элементарную матрицу m-го порядка. Нетрудно видеть, что аналогичное утверждение справедливо и относительно столбцов, только матрицу A теперь нужно умножать справа на элементарную матрицу n-го порядка.

II. Доказательство свойства мультипликативности. Во-первых, заметим, что равенство (1) верно, когда одна из матриц A или B является элементарной. Это вытекает из соответствующих свойств определителей и очевидных формул

$$\det(F_{kl}(\lambda)) = \begin{cases} 1, & \text{если } k \neq l, \\ \lambda, & \text{если } k = l, \end{cases} \qquad \det(G_{kl}) = -1$$

для определителя элементарных матриц.

Во-вторых, равенство (1) справедливо для треугольных матриц A, B, так как произведение AB также является треугольной матрицей с диагональными элементами, равными произведению соответствующих диагональных элементов матриц A и B.

Упражнение 3. Убедитесь в этом.

Рассмотрим теперь общий случай. Представим матрицы A и B в виде

$$A = A_s \dots A_1 A^*, \quad B = B^* B_1 \dots B_t,$$

где A_i, B_j — элементарные матрицы, а A^*, B^* — треугольные матрицы.

Упражнение 4. Объясните, как добиться таких представлений.

Теперь имеем

$$\det(A) = \det(A_s \dots A_1 A^*) =$$
$$= \det(A_s) \det(A_{s-1} \dots A_1 A^*) = \dots = \det(A_s) \dots \det(A_1) \det(A^*)$$

и совершенно аналогично

$$\det(B) = \det(B^*) \det(B_1) \dots \det(B_t),$$
$$\det(AB) = \det(A_s) \dots \det(A_1) \det(A^* B^*) \det(B_1) \dots \det(B_t).$$

Поскольку $\det(A^* B^*) = \det(A^*) \det(B^*)$, равенство (1) можно считать доказанным.

Упражнение 5. Пусть матрица A обратима. Докажите равенство

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

Можно предложить иное доказательство, которое использует правило сложения определителей и (непосредственно) явную формулу (2) из § 9.

Пусть $C = AB$. Согласно упражнению 4 из § 7, система строк $c_1, \dots, c_n$ матрицы C линейно выражается через систему строк $b_1, \dots, b_n$ матрицы B, при этом в роли коэффициентов линейных комбинаций выступают элементы a_{ij} матрицы A:

$$c_i = a_{i1} b_1 + \dots + a_{in} b_n, \quad i = 1, \dots, n.$$

Применив несколько раз правило сложения определителей, мы получим следующее:

$$\det(C) = \det \begin{pmatrix} a_{11} b_1 + \dots + a_{1n} b_n \\ \dots\dots\dots\dots\dots \\ a_{n1} b_1 + \dots + a_{nn} b_n \end{pmatrix} = \sum_{(i_1, \dots, i_n)} \det \begin{pmatrix} a_{1 i_1} b_{i_1} \\ \dots\dots \\ a_{n i_n} b_{i_n} \end{pmatrix} = \Sigma.$$

В сумме Σ имеется ровно n^n определителей, но почти все они равны нулю. Более точно,

$$\det \begin{pmatrix} a_{1i_1} b_{i_1} \\ \dots\dots\dots \\ a_{ni_n} b_{i_n} \end{pmatrix} = a_{1i_1} \dots a_{ni_n} \det \begin{pmatrix} b_{i_1} \\ \dots \\ b_{i_n} \end{pmatrix} =$$

$$= a_{1i_1} \dots a_{ni_n} \begin{cases} 0, & \text{если среди } i_1, \dots, i_n \text{ есть одинаковые,} \\ \pm \det(B), & \text{если } i_1, \dots, i_n \text{ — перестановка } \Omega = \{1, \dots, n\}. \end{cases}$$

Очевидно, знак перед $\det(B)$ определяется чётностью подстановки

$$\alpha = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$$

и равен плюсу, если эта подстановка чётная, и минусу в противном случае. В итоге получим

$$\Sigma = \sum_{\alpha \in S_n} a_{1i_1} \dots a_{ni_n} (\pm \det(B)) = \det(B) \sum_{\alpha \in S_n} \pm a_{1i_1} \dots a_{ni_n} = \det(B) \det(A),$$

и равенство (1) установлено.

§ 12. Миноры и алгебраические дополнения. Теорема Крамера

Миноры и алгебраические дополнения в определителе. Теорема о разложении определителя по строке либо столбцу. Формула для обратной матрицы. Теорема Крамера. Вычисление ранга матрицы методом окаймляющих миноров.

I. Миноры и алгебраические дополнения. Пусть A — произвольная матрица размера $m \times n$. Зафиксируем два набора по k различных индексов:

$$I = \{i_1, \ldots, i_k\} \subset \{1, 2, \ldots, m\}, \quad J = \{j_1, \ldots, j_k\} \subset \{1, 2, \ldots, n\}.$$

Обозначим через $A(I, J)$ подматрицу, состоящую из элементов матрицы A, расположенных на пересечении строк с номерами из I и столбцов с номерами из J.

Определение 1. *Минором* $M(I, J)$ матрицы A, расположенным в строках с номерами из I и столбцах с номерами из J, называется $\det(A(I, J))$.

Число $k \leqslant \min\{m, n\}$ называется порядком минора $M(I, J)$. Если $A = (a_{ij})$ — квадратная матрица n-го порядка, то мы будем также использовать следующее

Определение 2. *Минором* M_{ij} матрицы A, соответствующим элементу a_{ij}, называется определитель подматрицы, получающейся из A вычёркиванием i-й строки и j-го столбца. Число

$$A_{ij} = (-1)^{i+j} M_{ij} \tag{1}$$

называется *алгебраическим дополнением* элемента a_{ij}.

Отметим, что порядок минора M_{ij} равен $n - 1$.

Упражнение 1. Подсчитайте число всех миноров k-го порядка матрицы A размера $m \times n$. Сколько из них будет иметь максимальный порядок?

II. Разложение определителя по строке (столбцу). Следующая теорема является основой ещё одного способа вычисления определителей. Пусть $A = (a_{ij})$ — произвольная квадратная матрица n-го порядка.

Теорема 1. Справедливы следующие формулы:

$$\det(A) = \sum_{j=1}^{n} a_{ij} A_{ij}, \quad i = 1, \ldots, n; \tag{2}$$

$$\det(A) = \sum_{i=1}^{n} a_{ij} A_{ij}, \quad j = 1, \ldots, n. \tag{3}$$

Формулы (2) и (3) называются *разложением определителя* по i-й строке и j-му столбцу соответственно. Поскольку при транспонировании определитель матрицы не меняется, достаточно доказать, например, формулу (2), что мы и сделаем далее.

Предварительно докажем две леммы.

Лемма 1. Если

$$A = \begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix},$$

то $\det(A) = a_{11} A_{11}$.

Доказательство. Воспользуемся формулой (2) из § 9, которая, если учесть специфику первой строки матрицы A, примет следующий вид:

$$\det(A) = \sum_{\alpha \in S_n} \pm a_{11} a_{2i_2} \dots a_{ni_n} = a_{11} \sum_{\alpha \in S_n} \pm a_{2i_2} \dots a_{ni_n},$$

где суммирование распространено только на подстановки $\alpha \in S_n$ вида

$$\alpha = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & i_2 & \dots & i_n \end{pmatrix}.$$

Каждую такую подстановку можно отождествить с подстановкой $\alpha' \in S_{n-1}$, действующей на множестве $\{2, 3, \dots, n\}$, где

$$\alpha' = \begin{pmatrix} 2 & \dots & n \\ i_2 & \dots & i_n \end{pmatrix},$$

при этом, очевидно, чётности подстановок α и α' совпадают. Следовательно,

$$\det(A) = a_{11} \sum_{\alpha' \in S_{n-1}} \pm a_{2i_2} \dots a_{ni_n} = a_{11} \det \begin{pmatrix} a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{n2} & \dots & a_{nn} \end{pmatrix} = a_{11} M_{11} = a_{11} A_{11},$$

и утверждение доказано. □

Лемма 2. Если

$$A = \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & a_{1j} & a_{1,j+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_{ij} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,j-1} & a_{nj} & a_{n,j+1} & \dots & a_{nn} \end{pmatrix},$$

то $\det(A) = a_{ij} A_{ij}$.

Доказательство. Приведём матрицу A к виду, рассмотренному в лемме 1, меняя местами соседние строки и соседние столбцы. Для того, чтобы таким способом загнать элемент a_{ij} в левый верхний угол, всего потребуется

$$(i-1) + (j-1) = i + j - 2$$

перемен местами строк и столбцов. В результате получится матрица

$$A' = \begin{pmatrix} a_{ij} & 0 & \dots & 0 & 0 & \dots & 0 \\ a_{1j} & a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i-1,j} & a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i+1,j} & a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{nj} & a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{pmatrix}.$$

По лемме 1 имеем $\det(A') = a'_{11}A'_{11}$. Но $a'_{11} = a_{ij}$ и $A'_{11} = M'_{11} = M_{ij}$, поэтому

$$\det(A') = a_{ij}M_{ij}.$$

С другой стороны, $\det(A') = (-1)^{i+j-2}\det(A) = (-1)^{i+j}\det(A)$. Значит,

$$(-1)^{i+j}\det(A) = a_{ij}M_{ij},$$

и требуемое равенство следует из формулы (1) для алгебраических дополнений. □

Теперь можно приступить к рассмотрению общего случая.

Доказательство теоремы 1. Применив при фиксированном i правило сложения, представим определитель данной матрицы A в виде суммы n определителей:

$$\det(A) = \Delta_1 + \ldots + \Delta_n, \quad \Delta_j = \det\begin{pmatrix} a_{11} & \ldots & a_{1,j-1} & a_{1j} & a_{1,j+1} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & a_{ij} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{n,j-1} & a_{nj} & a_{n,j+1} & \ldots & a_{nn} \end{pmatrix}.$$

По лемме 2 имеем $\Delta_j = a_{ij}A_{ij}$ при любом $j = 1, \ldots, n$. Суммируя эти равенства, получим формулу (2). □

Замечание. Доказанная теорема представляет собой частный случай так называемой *теоремы Лапласа*[4]. Формулировку, а также доказательство этой теоремы можно найти, например, в книге [11], стр. 58.

Теорема 1 позволяет свести вычисление определителя матрицы n-го порядка к вычислению n определителей матриц $(n-1)$-го порядка. Если процесс понижения порядка продолжить далее, то в конечном итоге получим $n!/2$ определителей матриц второго порядка. Это слишком много, поэтому на практике такую редукцию рекомендуется комбинировать с элементарными преобразованиями строк и столбцов: сначала обнулив все элементы какой-нибудь строки (столбца), за исключением одного, затем разлагают определитель по этой строке (столбцу); к полученному определителю меньшего порядка применяют такую же стратегию и т. д.

Примеры вычисления определителей таким способом будут разобраны на практических занятиях. Следующая теорема является одновременно и следствием, и обобщением теоремы 1.

Теорема 2. Имеют место следующие равенства:

$$\sum_{j=1}^{n} a_{ij}A_{kj} = \begin{cases} \det(A), & \text{если } k = i, \\ 0, & \text{если } k \neq i; \end{cases} \tag{4}$$

$$\sum_{i=1}^{n} a_{ik}A_{ij} = \begin{cases} \det(A), & \text{если } k = j, \\ 0, & \text{если } k \neq j. \end{cases} \tag{5}$$

[4] П. С. Лаплас (1749 — 1827) — французский математик, физик и астроном.

ДОКАЗАТЕЛЬСТВО. Докажем, например, формулу (4). При $k = i$ это есть формула (2), поэтому будем считать $k \neq i$.

Рассмотрим матрицу A', которая получается из матрицы A заменой k-й строки на её i-ю строку. С одной стороны, имеем

$$\det(A') = 0,$$

поскольку A' содержит две одинаковых строки. С другой стороны, если этот определитель разложить по k-й строке, получим

$$\det(A') = \sum_{j=1}^{n} a'_{kj} A'_{kj} = \sum_{j=1}^{n} a_{ij} A_{kj},$$

так как $a'_{kj} = a_{ij}$ и $A'_{kj} = A_{kj}$ по построению матрицы A'. □

Далее мы рассмотрим некоторые приложения теории определителей.

III. Формула для обратной матрицы. Теорема Крамера. Сначала получим явную формулу для обратной матрицы. Пусть A — произвольная квадратная матрица n-го порядка.

Определение 3. Матрица

$$A^r = \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}$$

составленная из алгебраических дополнений к элементам матрицы A, называется *присоединённой* или *взаимной* к матрице A.

Нетрудно видеть, что формулы (4) и (5) можно «упаковать» в следующие матричные равенства:

$$AA^r = \det(A)E, \quad A^r A = \det(A)E,$$

где E — единичная матрица n-го порядка. Для невырожденной матрица A отсюда следует формула для обратной матрицы:

$$A^{-1} = \frac{1}{\det(A)} A^r = \frac{1}{\det(A)} \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}. \tag{6}$$

Формула (6) имеет скорее теоретическое значение: с вычислительной точки зрения, особенно при больших n, для отыскания A^{-1} удобнее пользоваться методом, изложенным в п. **II** § 7.

Рассмотрим теперь произвольную квадратную СЛУ

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1, \\ \dots \\ a_{n1}x_1 + \dots + a_{nn}x_n = b_n, \end{cases} \tag{7}$$

которую запишем в матричной форме:

$$AX = B \tag{8}$$

(см. п. **III** § 7). Обозначим $\Delta = \det(A)$ и пусть Δ_j ($j = 1, \ldots, n$) обозначает определитель матрицы, получающейся из матрицы A заменой j-го столбца столбцом свободных коэффициентов B. В этих обозначениях справедлива следующая теорема, известная как *теорема Крамера*[5)].

Теорема 3. Если $\Delta \neq 0$, то СЛУ (7) имеет единственное решение, которое находится по формулам

$$x_j = \frac{\Delta_j}{\Delta}, \quad j = 1, \ldots, n. \tag{9}$$

Если $\Delta = 0$, но хотя бы один из $\Delta_j \neq 0$, то СЛУ (7) несовместна.

Доказательство. Предположим, что СЛУ (7) совместна. Если умножить обе части уравнения (8) слева на присоединённую матрицу A^r, то получим

$$\Delta \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \det(A) X = A^r B = \begin{pmatrix} A_{11} & \ldots & A_{n1} \\ \ldots\ldots\ldots\ldots \\ A_{1n} & \ldots & A_{nn} \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix},$$

откуда найдём

$$\Delta x_j = b_1 A_{1j} + \ldots + b_n A_{nj} = \Delta_j, \quad j = 1, \ldots, n.$$

При $\Delta \neq 0$ отсюда следуют формулы (9), а при $\Delta = 0$ и некотором $\Delta_j \neq 0$ — необходимое для завершения доказательства теоремы противоречие. □

Упражнение 2. Объясните, почему верно равенство $b_1 A_{1j} + \ldots + b_n A_{nj} = \Delta_j$.

Формулы (9) называются *формулами Крамера*. При

$$\Delta = \Delta_1 = \ldots = \Delta_n = 0$$

СЛУ (7) требует дополнительного исследования — в этом случае она может оказаться как несовместной, так и неопределённой. Отметим, что с практической точки зрения формулы Крамера малопригодны ввиду большого объёма вычислений.

IV. Метод окаймляющих миноров. Теория определителей позволяет взглянуть на понятие ранга матрицы более симметричным образом. Пусть, как и в начале параграфа, A — любая матрица размера $m \times n$ и $M(I, J)$ — некоторый её минор k-го порядка.

Определение 4. Минор $M(I^*, J^*)$, порядок которого равен $k+1$, называют *окаймляющим* минор $M(I, J)$, если $I \subset I^*$, $J \subset J^*$.

Определение 5. Минор $M(I, J)$ называется *базисным* для матрицы A, если он отличен от нуля, а любой его окаймляющий минор равен нулю.

[5)] Г. Крамер (1704 — 1752) — швейцарский математик.

Базисные миноры всегда существуют — в качестве такового годится любой минор, имеющий наибольший порядок среди всех ненулевых миноров данной матрицы (будем называть такие миноры *максимальными*). Apriori могут существовать базисные миноры, не являющиеся максимальными. Следующая теорема показывает, что на самом деле этого нет.

Теорема 4. Порядок любого базисного минора равен рангу матрицы.

Доказательство. Пусть $\Delta = M(I, J)$ — некоторый базисный минор матрицы A, имеющий порядок r. Требуется доказать, что $r = \operatorname{rank}(A)$. Для упрощения обозначений далее будем считать $I = J = \{1, \ldots, r\}$.

Нам достаточно показать, что первые r столбцов

$$a_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}, \quad j = 1, \ldots, r,$$

матрицы A образуют базис всей системы столбцов этой матрицы. Линейная независимость $a_1, \ldots, a_r$ следует из линейной независимости укороченных столбцов

$$a'_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{rj} \end{pmatrix}, \quad j = 1, \ldots, r, \tag{10}$$

которая имеет место ввиду $\Delta \neq 0$. Фиксируем $j_0 > r$ и убедимся, что столбец a_{j_0} линейно выражается через $a_1, \ldots, a_r$. Обозначим через A' матрицу r-го порядка, составленную из столбцов (10), так что $\det(A') = \Delta$. Для укороченного столбца a'_{j_0} имеем

$$a'_{j_0} = \lambda_1 a'_1 + \ldots + \lambda_r a'_r,$$

где коэффициенты линейной комбинации находятся по формулам Крамера:

$$\lambda_j = \frac{\Delta_j}{\Delta}, \quad j = 1, \ldots, r.$$

Здесь Δ_j — определитель матрицы, получающейся из матрицы A' заменой j-го столбца столбцом a'_{j_0}. Докажем равенство

$$a_{j_0} = \lambda_1 a_1 + \ldots + \lambda_r a_r.$$

Достаточно проверить, что для любого $i > r$ справедливо равенство

$$a_{ij_0} = \lambda_1 a_{i1} + \ldots + \lambda_r a_{ir}. \tag{11}$$

Рассмотрим окаймляющий минор

$$\Delta_i^* = \det \begin{pmatrix} a_{11} & \ldots & a_{1r} & a_{1j_0} \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} & a_{rj_0} \\ a_{i1} & \ldots & a_{ir} & a_{ij_0} \end{pmatrix} = 0.$$

Разложив его по последней строке, получим

$$0 = a_{i1}\mu_1 + \ldots + a_{ir}\mu_r + a_{ij_0}\Delta,$$

где μ_j — соответствующие алгебраические дополнения. Заметим теперь, что

$$\mu_j = -\Delta_j = -\lambda_j\Delta, \quad j = 1, \ldots, r,$$

откуда и следует равенство (11). □

Упражнение 3. Объясните, почему верно равенство $\mu_j = -\Delta_j$.

Замечание. Более короткое доказательство теоремы 4 см. в книге [4], стр. 126.

Поскольку всякий максимальный минор является базисным, ранг матрицы совпадает с порядком максимального минора, т. е. равен наибольшему порядку всех ненулевых миноров этой матрицы.

На теореме 4 основан ещё один способ вычисления ранга матрицы A, называемый *методом окаймления миноров*. Стартовав с произвольного ненулевого элемента матрицы (ненулевого минора 1-го порядка), мы будем искать окаймляющий его ненулевой минор 2-го порядка и т. д. Когда все окаймляющие миноры для очередного ненулевого минора r-го порядка окажутся равными нулю, ранг будет найден: $\operatorname{rank}(A) = r$.

Глава 3
Основные алгебраические структуры

§ 13. Отображения множеств. Бинарные отношения. Отношение эквивалентности

Понятие отображения множеств. Сюръективные, инъективные и биективные отображения. Композиция отображений. Обратное отображение. Декартово произведение множеств. Понятие бинарного отношения. Отношение эквивалентности и разбиение на классы эквивалентных элементов. Фактормножество.

Современная математика базируется на *теории множеств*.

На интуитивном уровне с понятием множества мы уже сталкивались в предыдущих параграфах (числовые множества $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$, множество решений СЛУ, множество n-мерных арифметических векторов $\mathbb{R}^n$ и т. п.). Напомним основные определения, связанные с интуитивным понятием множества.

Под *множеством* понимают любую совокупность объектов, называемых *элементами* множества. Если множество содержит конечное число элементов, то оно называется *конечным*; иначе его называют *бесконечным*. Число элементов конечного множества S обозначают $|S|$. Конечное множество можно задать перечислением всех его элементов: $\{0, 1, 2, \ldots, 9\}$ — множество цифр в десятичной системе счисления. Запись $a \in S$ означает, что a есть элемент множества S; в противном случае пишут $a \notin S$.

Говорят, что множество S является *подмножеством* множества T и пишут $S \subset T$, если всякий элемент S является элементом T. Два множества S и T считаются равными, если у них одни и те же элементы: $S \subset T$ и $T \subset S$.

Пустое множество $\emptyset$, не содержащее никаких элементов, считается подмножеством любого множества. Для выделения подмножества S в множестве T часто используют какое-либо свойство, присущее только элементам из S:

$$S = \{x \in T : P(x)\},$$

где $P(x)$ означает, что элемент x обладает неким свойством P.

Под *пересечением* и *объединением* множеств S и T понимают множества

$$S \cap T = \{x : x \in S \text{ и } x \in T\}, \quad S \cup T = \{x : x \in S \text{ или } x \in T\}$$

соответственно. *Разностью* между T и S называется множество

$$T \setminus S = \{x : x \in T \text{ и } x \notin S\}.$$

Если $S \subset T$, то разность $T \setminus S$ называют *дополнением* к S в T и обозначают S^c.

Упражнение 1. Докажите следующие тождества:
а) $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$ и $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$;
б) если $A \subset S$ и $B \subset S$, то $(A \cup B)^c = A^c \cap B^c$ и $(A \cap B)^c = A^c \cup B^c$.

Обычно какое-либо множество X задают при помощи *словесного описания* его элементов. Но использование для этой цели совершенно произвольных словосочетаний может быть чревато разными странными ситуациями типа известного *парадокса брадобрея*, который можно сформулировать в виде вопроса: бреет ли себя брадобрей, если он бреет тех и только тех, кто себя не бреет?

Упражнение 2. Попробуйте ответить на естественный вопрос, принадлежит ли брадобрей множеству $X = \{$те и только те, кто не бреется сам$\}$.

Наивная теория множеств, придуманная Кантором[6)], просто запрещает «сомнительные» действия при конструировании множеств, которые могут привести к подобным парадоксальным ситуациям, и разрешает работать только с «разумными» множествами (например, множество X из упражнения 2 таковым не является). Ещё один способ избежать неприятных моментов состоит в применении *аксиоматического подхода*. При таком подходе множество — это нечто, удовлетворяющее определённой системе аксиом, например *системе аксиом Цермело — Френкеля*[7)]. Однако и в этом случае некоторые естественные и на первый взгляд безобидные аксиомы типа *аксиомы выбора* могут иметь вполне законные парадоксальные следствия в духе *теоремы Банаха — Тарского*[8)] о том, что из одного апельсина, «разрезав» его, можно сделать два точно таких же.

Более подробно обо всём этом можно прочитать в брошюре: *Ященко И.В.* Парадоксы теории множеств. М.: МЦНМО, 2002.

I. Отображение множеств. Понятие отображения или функции, как и понятие множества, играет центральную роль в математике.

При заданных множествах X и Y под *отображением*

$$f : X \to Y \tag{1}$$

с *областью определения* X и *областью значений* Y понимается соответствие (правило), при котором каждому элементу $x \in X$ сопоставляется вполне определённый элемент $y \in Y$, называемый *образом* элемента x и обозначаемый $y = f(x)$.

В случае $Y = X$ говорят об отображении множества X в себя или *преобразовании* множества X. Если множество Y имеет числовую природу, то отображение (1) обычно называют *функцией*.

Образом множества $A \subset X$ при отображении (1) называется множество

$$f(A) = \{y \in Y : y = f(x) \text{ для некоторого } x \in A\} \subset Y.$$

Множество $f(X)$ называют также образом всего отображения (1) и обозначают $\mathrm{Im}\,(f)$. Множество

$$f^{-1}(B) = \{x \in X : f(x) \in B\} \subset X$$

называется *прообразом* множества $B \subset Y$. Если $y \in Y \setminus \mathrm{Im}\,(f)$, то $f^{-1}(y) = \emptyset$.

[6)] Г. Кантор (1845 — 1918) — немецкий математик, создатель теории множеств.

[7)] Э. Цермело (1871 — 1953) — немецкий математик. А. Френкель (1891 — 1965) — израильский математик.

[8)] С. Банах (1892 — 1945) — польский математик. А. Тарский (1901 — 1983) — польско-американский математик.

Определение 1. Отображение (1) называется *сюръективным*, если его образ совпадает с областью значений: $\mathrm{Im}\,(f) = Y$; оно называется *инъективным*, если из $x \neq x'$ следует, что $f(x) \neq f(x')$. Наконец, это отображение называется *биективным* или *взаимно однозначным*, если оно сюръективно и инъективно (в случае $Y = X$ также говорят о взаимно однозначном отображении множества X *на себя*).

Пример 1. Всякая подстановка $\alpha \in S_n$ по определению (см. § 8) является взаимно однозначным отображением множества $\Omega = \{1, 2, \ldots, n\}$ на себя. □

Упражнение 3. Может ли инъективное (сюръективное) отображение $\alpha : I \to I$ не быть сюръективным (инъективным)?

Определение 2. Пусть заданы два отображения

$$f : X \to Y, \quad g : Y \to Z. \tag{2}$$

Отображение $h : X \to Z$, задаваемое правилом $h(x) = g(f(x))$ для любого $x \in X$, называется *композицией* или *произведением* отображений (2). Обозначение: $h = g \circ f$.

Отметим, что композиция определяется только для отображений вида (2). Частным случаем композиции отображений является, например, умножение подстановок из S_n. Как мы знаем, умножение подстановок не обладает свойством коммутативности, и это довольно типично.

Пример 2. Рассмотрим функции $f : \mathbb{R} \to \mathbb{R}$ и $g : \mathbb{R} \to \mathbb{R}$, задаваемые формулами

$$f(x) = x + 1, \quad g(x) = x^2.$$

Здесь определены обе композиции $h_1 = g \circ f : \mathbb{R} \to \mathbb{R}$ и $h_2 = f \circ g : \mathbb{R} \to \mathbb{R}$, при этом

$$h_1(x) = (x + 1)^2, \quad h_2(x) = x^2 + 1.$$

Видно, что функции h_1 и h_2 различны. □

Итак, в случае, когда все три множества X, Y, Z совпадают, композиция отображений не обладает свойством коммутативности. Вместе с тем справедлива

Теорема 1. Композиция отображений ассоциативна: если даны три отображения

$$f : X \to Y, \quad g : Y \to Z, \quad h : Z \to W,$$

то $h \circ (g \circ f) = (h \circ g) \circ f$.

Доказательство. Действительно, для любого элемента $x \in X$ имеем

$$\begin{aligned} (h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))), \\ ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) = h(g(f(x))), \end{aligned}$$

откуда и следует равенство отображений $h \circ (g \circ f) : X \to W$ и $(h \circ g) \circ f : X \to W$. □

Очевидно, ассоциативность умножения подстановок из S_n является частным проявлением свойства ассоциативности композиции отображений.

Отображение

$$e_X : X \to X$$

называется *тождественным*, если $e_X(x) = x$ для любого $x \in X$. Ясно, что

$$f \circ e_X = f, \quad e_Y \circ f = f$$

для любого отображения (1).

Определение 3. Отображение $g : Y \to X$ называют *обратным* к отображению (1), если

$$g \circ f = e_X, \quad f \circ g = e_Y. \tag{3}$$

Обозначение: $g = f^{-1}$.

Такое обозначение оправдано тем, что обратное отображение, если оно существует, определено исходным отображением однозначно.

Упражнение 4. Докажите это утверждение, опираясь на теорему 1.

Указание. Вспомните, как доказывается единственность обратной матрицы.

Отображение, имеещее обратное, называется *обратимым*. Критерий обратимости предоставляет

Теорема 2. Отображение (1) обратимо тогда и только тогда, когда оно биективно.

Доказательство. Предварительно заметим: если $g : Y \to X$ — некоторое отображение, для которого имеет место равенство

$$g \circ f = e_X,$$

то f инъективно, а g сюръективно. Действительно, если $f(x) = f(x')$, то

$$x = e_X(x) = g(f(x)) = g(f(x')) = e_X(x') = x',$$

что доказывает инъективность f. Если, далее, $x \in X$ — произвольный элемент, то

$$x = e_X(x) = g(f(x)),$$

т. е. $x = g(y)$, где $y = f(x) \in Y$, а это означает сюръективность g.

Возвращаясь к доказательству теоремы, предположим сначала, что отображение (1) имеет обратное отображение $g = f^{-1}$. Тогда из равенств (3) следует как инъективность, так и сюръективность f, т. е. f биективно.

Наоборот, если предположить f биективным, то для любого элемента $y \in Y$ будет существовать единственный элемент $x \in X$, для которого $f(x) = y$. Положив $g(y) = x$, мы зададим отображение $g : Y \to X$, удовлетворяющее равенствам (3). Значит, $g = f^{-1}$ и f обратимо. □

Из теоремы 2 вытекает довольно очевидное

Следствие. Из биективности отображения (1) следует биективность f^{-1}, причём

$$(f^{-1})^{-1} = f.$$

Если $h : Y \to Z$ — ещё одно биективное отображение, то композиция $h \circ f$ также является биективным отображением и

$$(h \circ f)^{-1} = f^{-1} \circ h^{-1}.$$

Упражнение 5. Докажите это следствие.

II. Бинарные отношения. Отношение эквивалентности. Сначала рассмотрим ещё один способ конструирования множеств. Пусть даны множества $X_1, \ldots, X_n$.

Определение 4. *Декартовым произведением* множеств X_i, $i = 1, \ldots, n$, называется множество, состоящее из всех упорядоченных наборов элементов этих множеств:

$$X_1 \times \ldots \times X_n = \{(x_1, \ldots, x_n) : x_i \in X_i, i = 1, \ldots, n\}.$$

Если $X_i = X$ при $i = 1, \ldots, n$, то говорят о *декартовой n-й степени* множества X:

$$X^n = \{(x_1, \ldots, x_n) : x_i \in X, i = 1, \ldots, n\}.$$

Так, множество всех n-мерных арифметических векторов $\mathbb{R}^n$ по своему определению (см. § 2) есть n-я декартова степень множества $\mathbb{R}$.

Определение 5. Пусть X, Y — два множества. Любое подмножество

$$\omega \subset X \times Y$$

называется *бинарным отношением между* X и Y (или *бинарным отношением на* множестве X, если $Y = X$).

Для упорядоченной пары $(x, y) \in \omega$ обычно используют обозначение $x\omega y$ и говорят, что x находится в отношении ω к y.

Пример 3. 1. Отношение $\omega = <$ (отношение «меньше») на множестве $\mathbb{R}$ — это подмножество

$$< = \{(x, y) \in \mathbb{R}^2 : x < y\}.$$

Вместо $(1, 2) \in <$ мы привычно пишем $1 < 2$.

2. Отношение $\omega = |$ (отношение «быть делителем») на множестве $\mathbb{N}$ — это подмножество

$$| = \{(x, y) \in \mathbb{N}^2 : x \text{ — делитель } y\}.$$

Включение $(4, 12) \in |$ записывают как $4 \mid 12$. □

Определение 6. Отношение $\sim$ на множестве X называется *отношением эквивалентности*, если для любых элементов x, x', x'' множества X выполнены условия:

а) $x \sim x$ (*рефлексивность*);

б) если $x \sim x'$, то $x' \sim x$ (*симметричность*);

в) если $x \sim x'$ и $x' \sim x''$, то $x \sim x''$ (*транзитивность*).

Так, отношения, рассмотренные выше, не являются отношениями эквивалентности.

Упражнение 6. Какими из свойств а) — в) обладают отношения «меньше» и «быть делителем» (см. пример 3), а какими — нет?

Приведём примеры отношений эквивалентности.

Пример 4. Пусть $X = M_{m\times n}(\mathbb{R})$ — множество матриц некоторого фиксированного размера. Будем говорить, что матрица A эквивалентна матрице B, и записывать $A \sim B$, если B получается из A элементарными преобразованиями строк (запретим удаление нулевых строк, которое меняет размер матриц). Возникающее при этом отношение на множестве $M_{m\times n}(\mathbb{R})$ будет именно отношением эквивалентности.

Нетрудно обнаружить, что $A \sim B$ тогда и только тогда, когда $B = CA$ для некоторой обратимой матрицы $C \in M_m(\mathbb{R})$. Понятие эквивалентных матриц можно сделать более естественным, если допустить и элементарные преобразования столбцов: $A \sim B$, если $B = CAD$, где $C \in M_m(\mathbb{R})$, $D \in M_n(\mathbb{R})$ — некоторые обратимые матрицы. □

Пример 5. Пусть $X = \mathbb{Z}$ и m — некоторое фиксированное натуральное число. Скажем, что a *сравнимо* с b по *модулю* m, и запишем

$$a \equiv b \pmod{m},$$

если $a - b$ делится на m. Отношение «быть сравнимыми по модулю m» является отношением эквивалентности на множестве $\mathbb{Z}$. □

Упражнение 7. Докажите утверждения, сформулированные в примерах 4 и 5.

Определение 7. Пусть на множестве X задано отношение эквивалентности $\sim$. Подмножество вида

$$[x]_\sim = \{y \in X : y \sim x\} \subset X$$

называется *классом эквивалентности* с представителем $x \in X$.

Пример 6. Рассмотрим отношение сравнимости по модулю m на $\mathbb{Z}$. Класс эквивалентности с представителем $a \in \mathbb{Z}$ обозначим через $[a]_m$. Таким образом,

$$[a]_m = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}.$$

Чтобы понять, как устроены классы эквивалентности, разделим a на m с остатком:

$$a = mq + r, \quad 0 \leqslant r < m.$$

Тогда $[a]_m = [r]_m$. Значит, различных классов эквивалентности имеется не более m. На самом деле их ровно m, поскольку все классы вида $[r]_m$ попарно различны (класс $[r]_m$ состоит из тех и только тех целых чисел, которые дают остаток r при делении на m). □

На этом примере можно подметить следующее: различные классы эквивалентности $[r]_m$, где $r \in \{0, 1, \ldots, m-1\}$, попарно не пересекаются, а их объединение совпадает со всем множеством $\mathbb{Z}$. То, что это наблюдение не случайно, показывает следующая

Теорема 3. Пусть на множестве задано отношение эквивалентности $\sim$. Тогда множество можно представить в виде объединения попарно не пересекающихся классов эквивалентности. Иными словами, множество классов эквивалентности является *разбиением* множества X.

ДОКАЗАТЕЛЬСТВО. Пусть $x \in X$ — произвольный элемент. В силу рефлексивности $x \in [x]_\sim$. Поэтому X является объединением всех классов эквивалентности.

Докажем теперь, что различные классы эквивалентности не могут иметь общих элементов. Пусть $z \in [x]_\sim \cap [y]_\sim$ и $w \in [x]_\sim$ — произвольный элемент из $[x]_\sim$. Это значит, что $w \sim x$. Кроме того, $z \sim x$. По свойствам симметричности и транзитивности отсюда следует, что $w \sim z$. С другой стороны, $z \sim y$, следовательно, $w \sim y$. Но это означает, что $w \in [y]_\sim$. Таким образом, мы показали, что $[x]_\sim \subset [y]_\sim$. Противоположное включение $[y]_\sim \subset [x]_\sim$ доказывается аналогично. Итак, $[x]_\sim = [y]_\sim$. □

Определение 8. Пусть на множестве X задано некоторое отношение эквивалентности $\sim$. *Фактормножеством* $X/\sim$ называется множество, элементами которого являются классы эквивалентности:

$$X/\sim = \{[x]_\sim : x \in X\}.$$

Если $\sim$ — это отношение сравнимости по модулю m на множестве $\mathbb{Z}$, то соответствующее фактормножество обозначается $\mathbb{Z}_m$:

$$\mathbb{Z}_m = \{[r]_m : r = 0, 1, \ldots, m-1\}.$$

Это фактормножество, рассматриваемое вместе с естественными операциями сложения и умножения (см. далее пример 2 из § 15) играет важную роль в теории чисел. Элементы $[r]_m$ множества $\mathbb{Z}_m$ принято называть *классами вычетов* по модулю m.

§ 14. Бинарные алгебраические операции. Группы

Множество с бинарной алгебраической операцией. Терминология. Понятие группы: определение, примеры и основные свойства. Подгруппа, характеристический признак подгруппы. Изоморфизм групп.

I. Понятие бинарной алгебраической операции. Пусть X — произвольное множество.

Определение 1. *Бинарной алгебраической операцией* или *законом композиции* на X называется произвольное фиксированное отображение $\tau : X^2 \to X$.

Если $a, b \in X$ — два произвольных элемента, то результат применения отображения τ к паре (a, b) будем записывать в виде $a\tau b$ и называть *произведением* элемента a на элемент b. Обычно вместо τ используют специальные символы типа $*$, $\circ$, $\cdot$, $+$ и т. п.

На X может быть задано, вообще говоря, много операций. Желая выделить одну из них, пишут $(X, *)$ и говорят, что операция $*$ определяет на X *алгебраическую структуру* или что $(X, *)$ есть *алгебраическая система*.

Пример 1. На множестве целых чисел $\mathbb{Z}$ есть две естественных операции — сложение и умножение. С их помощью можно задать и другие операции, например

$$m * n = mn - m - n, \quad m \circ n = -m - n.$$

Возникают различные алгебраические структуры: $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, *)$, $(\mathbb{Z}, \circ)$. □

Задача изучения произвольных алгебраических структур была бы слишком общей, поэтому её рассматривают при различных естественных ограничениях.

Определение 2. Пусть на множестве X задана операция $*$. Эта операция называется *ассоциативной*, если

$$(a * b) * c = a * (b * c)$$

для любых элементов $a,\ b,\ c \in X$; она называется *коммутативной*, если

$$a * b = b * a$$

для любых элементов $a,\ b \in X$. Элемент $e \in X$ называется *нейтральным* относительно операции $*$, если

$$a * e = e * a = a$$

для любого элемента $a \in X$.

Нетрудно видеть, что алгебраическая структура $(X, *)$ может иметь не более одного нейтрального элемента: если e' — ещё один нейтральный элемент, то

$$e' = e' * e = e.$$

Алгебраическая структура $(X, *)$ с ассоциативной операцией $*$ называется *полугруппой*. Можно показать, что в любой полугруппе результат последовательного применения операции к нескольким элементам $x_1, \ldots, x_n$ не зависит от расстановки скобок, т. е. в выражениях вида

$$x_1 * \ldots * x_n$$

скобки не обязательны.

Упражнение 1. Докажите это утверждение индукцией по $n \geqslant 3$.

Указание. База индукции есть по определению ассоциативной операции. Делая шаг индукции, докажите равенство

$$(x_1 * \ldots * x_k) * (x_{k+1} * \ldots * x_n) = (x_1 * \ldots * x_l) * (x_{l+1} * \ldots * x_n)$$

при любых $1 \leqslant k < l < n$.

Полугруппу $(X, *, e)$ с нейтральным элементом e принято называть *моноидом* (или *полугруппой с единицей*). Приведём примеры полугрупп и моноидов.

Пример 2. 1. Пусть

$$m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$$

— множество целых чисел, кратных данному натуральному числу m. Тогда $(m\mathbb{Z}, +, 0)$ — коммутативный моноид, а $(m\mathbb{Z}, \cdot)$ — всего лишь полугруппа при $m > 1$.

2. $(\mathbb{R}^n, +, 0)$ и $(M_{m\times n}(\mathbb{R}), +, O)$ — коммутативные моноиды.

3. $(M_n(\mathbb{R}), \cdot, E)$ — некоммутативный моноид.

4. Пусть $M(\Omega)$ — множество всех преобразований множества Ω в себя, т. е. отображений вида $f : \Omega \to \Omega$. Тогда $(M(\Omega), \circ, e_\Omega)$ — некоммутативный моноид при $|\Omega| > 1$.

5. Обозначим через $\mathcal{P}(\Omega)$ множество всех подмножеств данного множества Ω. Тогда $(\mathcal{P}(\Omega), \cup, \emptyset)$ и $(\mathcal{P}(\Omega), \cap, \Omega)$ — коммутативные моноиды. □

Определение 3. Пусть $(X, *, e)$ — моноид и $a \in X$ — произвольный элемент. Элемент $b \in X$ называется *симметричным* элементу a, если

$$a * b = b * a = e.$$

Если симметричный элемент существует, то он определён однозначно. Действительно, пусть b_1 и b_2 — элементы, симметричные элементу a. Тогда

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$$

(сравните с доказательством единственности обратной матрицы).

Когда говорят про некую абстрактную алгебраическую структуру $(X, *)$, обычно используют два типа терминологии: *мультипликативную* и *аддитивную*. Обозначение $(X, *)$ при этом сокращают до X, если понятно, о какой операции идёт речь.

В мультипликативной терминологии операцию называют *умножением* и обозначают знаком $\cdot$ (точка), который обычно не пишут. Результат операции ab называют *произведением*. Нейтральный элемент называют *единичным* и обозначают e или 1. Элемент, симметричный элементу a, называют *обратным* и обозначают a^{-1}.

В аддитивной терминологии операцию называется *сложением* и обозначается знаком $+$. Результат операции $a + b$ называется *суммой*. Нейтральный элемент называется *нулевым* и обозначается 0. Элемент, симметричный элементу a, называется *противоположным* и обозначается $-a$.

В дальнейшем мы будем придерживаться, как правило, мультипликативной терминологии. Для произвольного элемента a моноида X и любого целого $n \geqslant 0$ можно определить *степень* a^n (*кратное* na в аддитивной терминологии), положив $a^0 = e$ и

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$$

при $n \geqslant 1$. Если элемент a имеет обратный (такой элемент называется *обратимым*), то элемент a^{-1} также обратим и, очевидно,

$$(a^{-1})^{-1} = a.$$

Для обратимого элемента a можно положить

$$a^n = (a^{-1})^{-n}$$

при $n < 0$ и тем самым определить степень a^n при любом целом n. Если элементы x и y обратимы, то их произведение xy также обратимо, причём

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Иными словами, множество всех обратимых элементов моноида X *замкнуто* относительно умножения и взятия обратного элемента. Отметим, что с частными проявлениями этих фактов мы уже сталкивались при обращении матриц и подстановок.

II. Понятие группы. Подгруппы. Наиболее широко в различных областях современной математики применяются алгебраические структуры, которые описывает следующее

Определение 4. Моноид G, все элементы которого обратимы, называется *группой*.

Упражнение 2. Дайте развёрнутое определение группы.

Операция, относительно которой G является группой, называется *групповой* операцией. Группа G называется *конечной*, если множество её элементов конечно; число элементов конечной группы принято называть её *порядком*. Если групповая операция коммутативна, то группа называется *абелевой*.[9)] Приведём примеры групп.

Пример 3. 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ — абелевы группы относительно сложения чисел.

2. $\mathbb{R}^n$, $M_{m\times n}(\mathbb{R})$ — абелевы группы относительно сложения арифметических векторов и матриц соответственно.

3. Пусть $S(\Omega)$ — множества всех биективных преобразований $f : \Omega \to \Omega$ множества Ω. Тогда $S(\Omega)$ — группа относительно композиции преобразований. В частности, при $|\Omega| = n$ получим S_n — *симметрическую группу* подстановок n-й степени. Эта группа имеет порядок $n!$ и при $n > 2$ не является абелевой.

4. $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$ — группа относительно умножения матриц, называемая *полной линейной группой* степени n над $\mathbb{R}$.

5. $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) = 1\}$ — группа относительно умножения матриц, называемая *специальной линейной группой* степени n над $\mathbb{R}$.

6. *Группа обратимых элементов* произвольного моноида X. Так можно получить группу $GL_n(\mathbb{R})$, если в качестве X рассмотреть $M_n(\mathbb{R})$. □

Упражнение 3. Убедитесь в неабелевости групп $GL_n(\mathbb{R})$ и $SL_n(\mathbb{R})$.

[9)] В честь норвежского математика Н. Х. Абеля (1802—1829). Само понятие группы впервые появилось в исследованиях французского математика Э. Галуа (1811 — 1832), связанных с проблемой разрешимости алгебраических уравнений в радикалах.

Упражнение 4. Докажите, что в любой группе G всякое уравнение вида $ax = b$ или $xa = b$ однозначно разрешимо и найдите x.

Определение 5. Подмножество $H \subset G$ называют *подгруппой* группы G, если относительно групповой операции оно само является группой.

Тривиальными подгруппами группы G являются сама группа G и *единичная подгруппа* $\{e\}$. Для проверки того, будет ли данное подмножество подгруппой, используют следующий характеристический признак подгруппы.

Теорема 1. Подмножество $H \subset G$ является подгруппой тогда и только тогда, когда выполнены следующие условия:
а) из $a,\ b \in H$ следует $ab \in H$;
б) из $a \in H$ следует $a^{-1} \in H$.

Условие а) означает, что H замкнуто относительно групповой операции, а условие б) — что H замкнуто относительно взятия обратного элемента. Совокупность этих двух условий можно заменить одним условием: из $a,\ b \in H$ следует $ab^{-1} \in H$.

Доказательство. Пусть H является подгруппой группы G. Тогда подмножество H должно быть замкнуто относительно групповой операции. Для элемента $a \in H$ существует $a^{-1} \in G$. Так как H является группой относительно той же операции, а обратный элемент единствен, то $a^{-1} \in H$.

Пусть выполнены условия а) и б). Нужно доказать, что H — подгруппа группы G. Из условия а) следует, что групповая операция является алгебраической для множества H. Так как эта операция ассоциативна на всём множестве G, то она обладает этим свойством и на подмножестве H. В качестве единичного элемента в H можно взять единичный элемент $e \in G$, который обязан принадлежать H, ибо $e = aa^{-1}$ для какого-нибудь $a \in H$ и выполнены условия а) и б). Наконец, из условия б) следует, что любой элемент $a \in H$ обратим в H: обратным будет a^{-1} — элемент, обратный a в группе G. □

Следствие. Пусть H_1, H_2 — подгруппы группы G. Тогда $H = H_1 \cap H_2$ также является подгруппой G.

Доказательство. Достаточно проверить для H выполнимость указанных выше условий а) и б), пользуясь тем, что они выполнены для H_1 и H_2. □

Приведём примеры подгрупп.

Пример 4. 1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ — цепочка подгрупп относительно сложения чисел.
2. $A_n \subset S_n$ — подгруппа чётных подстановок n-й степени, которую называют также *знакопеременной группой* подстановок n-й степени.
3. $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$.
4. Подгруппы группы $S(\Omega)$, которые выделяются дополнительными условиями на биективные преобразования множества Ω.

Пусть, например, Ω — евклидова плоскость, а $\rho : \Omega \to \Omega$ — так называемое *движение*, т. е. биективное преобразование плоскости Ω, сохраняющее расстояния:

$$d(\rho(A), \rho(B)) = d(A, B)$$

для любых точек A, B плоскости Ω. Множество всех движений $R(\Omega)$ плоскости Ω образует подгруппу в $S(\Omega)$. Если зафиксировать некоторую фигуру $\Phi \subset \Omega$ и рассматривать только те движения ρ, которые сохраняют эту фигуру:

$$\rho(\Phi) = \Phi,$$

то получим подгруппу $R(\Omega, \Phi)$, называемую *группой симметрий* фигуры Φ. Конкретные фигуры Φ доставляют массу интересных примеров. С другой стороны, отсюда начинаются всевозможные применения теория групп. □

Упражнение 5. Исследуйте группу симметрий правильного треугольника.

III. Изоморфизм групп. Для каждой группы G мы можем, хотя бы в принципе, составить так называемую *таблицу Кэли*[10] — таблицу умножения элементов этой группы. Для конечной группы

$$G = \{g_1, \ldots, g_n\}$$

таблица Кэли — это квадратная матрица n-го порядка $M = (m_{ij})$, где $m_{ij} = g_i g_j$.

Таблица Кэли несёт полную информацию о группе и по ней можно обнаружить многие закономерности группы.

Упражнение 6. Докажите, что конечная группа G абелева тогда и только тогда, когда её таблица Кэли $M = (m_{ij})$ симметрична: $m_{ij} = m_{ji}$ для любых i, j.

Однако сравнивать таблицы Кэли для групп G и G' одинакового порядка, стремясь различить эти группы, было бы затруднительно из-за того, что сами таблицы зависят от нумерации элементов групп G и G'.

Правильный подход к различению (или, наоборот, к отождествлению) групп предлагает понятие изоморфизма.

Определение 6. Говорят, что группа $(G, *)$ *изоморфна* группе $(G', \circ)$, если существует такое биективное отображение $f : G \to G'$, что

$$f(a * b) = f(a) \circ f(b) \tag{1}$$

для любых элементов a, $b \in G$. Обозначение: $G \cong G'$.

Если $G \cong G'$, то и $G' \cong G$. Действительно, последний изоморфизм может быть задан обратным отображением $f^{-1} : G' \to G$. Поэтому говорят просто об изоморфных группах G и G'. При любом изоморфизме $f : G \to G'$ мы имеем $f(e) = e'$, где e и e' — единичные элементы этих групп, а также $f(a^{-1}) = f(a)^{-1}$ для любого $a \in G$.

Упражнение 7. Докажите сформулированные утверждения.

Дадим примеры изоморфных групп.

Пример 5. 1. Группа симметрий правильного треугольника (см. упражнение 4) изоморфна группе S_3. Это можно обнаружить, если проследить за перемещениями вершин треугольника при произвольном движении плоскости, сохраняющем треугольник.

[10] А. Кэли (1821 — 1895) — английский математик.

2. Пусть $\mathbb{R}_{>0}$ обозначает множество всех положительных вещественных чисел. Группа $(\mathbb{R}_{>0}, \cdot)$ изоморфна группе $(\mathbb{R}, +)$. Отображение, осуществляющее этот изоморфизм, есть логарифм $\ln : \mathbb{R}_{>0} \to \mathbb{R}$. Известное свойство логарифма

$$\ln(ab) = \ln(a) + \ln(b)$$

моделирует абстрактное свойство (1) в определении изоморфизма. □

§ 15. Кольца

Понятие кольца: определение, примеры и простейшие свойства. Подкольцо, характеристический признак подкольца. Изоморфизм колец.

I. Понятие кольца. Подкольца. На одном и том же множестве X может быть задано несколько бинарных алгебраических операций $*$, $\circ$ и т. д., при этом между этими операциями обычно имеется некоторая связь.

Определение 1. Говорят, что операция $*$ *дистрибутивна* относительно операции $\circ$, если

$$(a \circ b) * c = (a * c) \circ (b * c), \quad c * (a \circ b) = (c * a) \circ (c * b)$$

для любых элементов $a,\ b,\ c \in X$.

Простейший пример такой ситуации — множество целых чисел $\mathbb{Z}$ с естественными операциями сложения и умножения, связанными законом дистрибутивности. Обобщение этой ситуации приводит к понятию кольца.

Определение 2. Множество R, на котором заданы две операции $+$ (сложение) и $\cdot$ (умножение), называется *кольцом*, если выполнены следующие условия:

а) $(R, +)$ — абелева группа;

б) $(R, \cdot)$ — полугруппа;

в) операция умножения дистрибутивна относительно операции сложения:

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb$$

для любых элементов $a,\ b,\ c \in R$.

Если операция умножения коммутативна, то кольцо R принято называть *коммутативным*. Если же полугруппа $(R, \cdot)$ является моноидом, то кольцо R называют *кольцом с единицей*. Бывает, что условие б) в определении кольца опускают или заменяют каким-то другим условием; в таких случаях говорят о *неассоциативных* кольцах.

Группу $(R, +)$ называют *аддитивной группой* кольца R, а полугруппу $(R, \cdot)$ — его *мультипликативной полугруппой*. Если R — кольцо с единицей, то имеет смысл говорить о *мультипликативной группе* R^* всех обратимых элементов кольца R.

Приведём примеры колец.

Пример 1. 1. В первую очередь это множество целых чисел $\mathbb{Z}$ относительно обычных операций сложения и умножения — *кольцо целых чисел* $\mathbb{Z}$. Это также простейший пример коммутативного кольца с единицей. Множества $\mathbb{Q}$ и $\mathbb{R}$ (рациональных и вещественных чисел соответственно) также являются кольцами, однако они относятся к специальному типу колец, который мы отдельно рассмотрим далее в § 16.

2. $M_n(\mathbb{R})$ — *кольцо квадратных матриц* n-го порядка над $\mathbb{R}$. Это кольцо с единицей, но оно не является коммутативным при $n > 1$. Если здесь $\mathbb{R}$ заменить произвольным коммутативным кольцом R, то получим $M_n(R)$ — кольцо квадратных матриц n-го порядка над R. Конечно, предварительно следует формально распространить действия над вещественными матрицами (см. § 7) на матрицы с элементами из R.

3. Различные *кольца функций*. Пусть X — произвольное множество, R — произвольное кольцо. Рассмотрим множество R^X всех отображений (функций) вида

$$f : X \to R,$$

на котором определим операции *поточечного сложения* и *поточечное умножения* следующим образом:

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x),$$

где $x \in X$ (в правых частях этих равенств задействованы операции в кольце R). Нетрудно убедиться, что относительно этих операций множество R^X оказывается кольцом, при этом «хорошие» свойства кольца R (коммутативность, наличие единицы) наследуются.

В математическом анализе наиболее распространён случай $R = \mathbb{R}$. Все естественные классы функций (ограниченных, непрерывных, дифференцируемых и т. п.) являются, как правило, кольцами.

4. Любую абелеву группу $(R, +)$ можно превратить в *кольцо с нулевым умножением*, положив $ab = 0$ для любых элементов $a,\ b \in R$.

5. Множество 3-мерных арифметических векторов $\mathbb{R}^3$ с обычной операцией сложения и операцией *векторного умножения* $\times$, определяемой для векторов $a = (a_1, a_2, a_3)$ и $b = (b_1, b_2, b_3)$ равенством

$$a \times b = (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1),$$

представляет собой неассоциативное кольцо. *Тождество Якоби*[11)]

$$(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0$$

в некотором смысле заменяет свойство ассоциативности. Кроме того, это кольцо *антикоммутативно* — в нём выполнено тождество $a \times b + b \times a = 0$. □

Упражнение 1. Проверьте: если R — кольцо с единицей, то $M_n(R)$ также является кольцом с единицей. Убедитесь также, что коммутативность может наследоваться только в тривиальных случаях.

Упражнение 2. Пользуясь соответствующими теоремами из анализа, убедитесь, что множество всех функций

$$f : [a, b] \to \mathbb{R},$$

непрерывных на отрезке $[a, b]$, образует коммутативное кольцо с единицей.

Следующий пример имеет большое значение для теории чисел, а в алгебре служит отправным пунктом для разного рода обобщений.

Пример 2. Пусть

$$\mathbb{Z}_m = \{[r]_m : r = 0,\ 1,\ \ldots,\ m-1\}$$

— множество всех классов вычетов по модулю m. Классы вычетов $[a]_m$ и $[a']_m$ совпадают тогда и только тогда, когда их представители сравнимы по модулю m:

$$a \equiv a' \pmod{m},$$

т. е. $a - a'$ делится на m, а значит, $a - a' = mt$ для некоторого $t \in \mathbb{Z}$. Определим теперь сложение и умножение классов вычетов следующим образом:

$$[a]_m + [b]_m = [a+b]_m, \quad [a]_m[b]_m = [ab]_m.$$

[11)] К. Г. Якоби (1804 — 1851) — немецкий математик.

Нетрудно видеть, что так введённые сумма и произведение классов вычетов не зависят от выбора представителей: если $[a]_m = [a']_m$ и $[b]_m = [b']_m$, то

$$[a+b]_m = [a'+b']_m, \quad [ab]_m = [a'b']_m.$$

Таким образом, на множестве $\mathbb{Z}_m$ корректно заданы две бинарные алгебраические операции. Более того, относительно этих операций $\mathbb{Z}_m$ оказывается коммутативным кольцом с единицей.

Упражнение 3. Убедитесь в справедливости сделанных утверждений. Какие классы вычетов играют роль нулевого и единичного элементов в этом кольце?

Кольцо $\mathbb{Z}_m$ называется *кольцом классов вычетов* по модулю m. □

Отметим следующие простейшие свойства операций, которые справедливы в любом кольце R и которые хорошо известны на примере кольца целых чисел $\mathbb{Z}$ (далее a, b и т. п. — произвольные элементы R).

1. $a \cdot 0 = 0 \cdot a = 0$.
2. $(-a)b = a(-b) = -(ab)$.
3. *Общий закон дистрибутивности* (правило раскрытия скобок):

$$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j.$$

Для доказательства свойства **1** заметим, что

$$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0,$$

откуда $a \cdot 0 = 0$. Чтобы доказать свойство **2**, запишем

$$0 = 0 \cdot b = (a + (-a)) \cdot b = ab + (-a)b,$$

откуда получим $(-a)b = -(ab)$. Что касается свойства **3**, то здесь можно рассуждать по индукции.

Упражнение 4. Проведите это рассуждение по индукции. Докажите также, что

$$(na)b = a(nb) = n(ab)$$

для любого $n \in \mathbb{Z}$.

Однако не все очевидные свойства числовых колец можно распространить на общий случай.

Определение 3. Если в кольце R имеем $ab = 0$ при $a \neq 0$ и $b \neq 0$, то a называется *левым*, а b — *правым делителем нуля*. Если таких элементов нет, то R называется *кольцом без делителей нуля*.

В коммутативном кольце R можно говорить просто о делителях нуля. Конечно, в числовых кольцах с обычными операциями сложения и умножения делителей нуля быть не может. Однако в кольце $M_n(\mathbb{R})$ матриц n-го порядка они есть: таковыми будут, например, матрицы E_{kl} из § 11.

Упражнение 5. Пусть $A \in M_n(\mathbb{R})$ — произвольная необратимая матрица, отличная от нулевой. Докажите, что A является как левым, так и правым делителем нуля.

Как показывает следующий пример, делители нуля могут существовать и в коммутативном кольце.

Пример 3. На множестве $\mathbb{R}^2$ введём операцию умножения формулой

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Легко видеть, что вместе с обычной операцией сложения мы получим структуру коммутативного кольца с единицей $e = (1, 1)$. Равенство

$$(1, 0)(0, 1) = (0, 0)$$

свидетельствует о наличии делителей нуля в этом кольце. □

Упражнение 6. Докажите, что в кольце $\mathbb{Z}_m$ нет делителей нуля тогда и только тогда, когда $m = p$ — простое число.

Отсутствие делителей нуля в кольце равносильно выполнению следующего *закона сокращения*: если $ab = ac$ (или $ba = ca$) и $a \neq 0$, то $b = c$. В кольце с единицей никакой обратимый элемент не может быть делителем нуля.

Упражнение 7. Докажите сформулированные утверждения.

Определение 4. Коммутативное кольцо с единицей $e \neq 0$, в котором нет делителей нуля, называется *областью целостности* или *целостным кольцом*.

Равенство $e = 0$ означало бы, что кольцо состоит только из нуля (почему?). В дальнейшем этот тривиальный случай мы исключим из рассмотрения. Стандартными примерами областей целостности служат числовые кольца типа

$$\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}.$$

То, что множество $\mathbb{Z}[\sqrt{2}]$ действительно представляет собой кольцо, можно проверить, воспользовавшись понятием подкольца.

Определение 5. Подмножество $L \subset R$ называется *подкольцом* кольца R, если относительно операций в кольце R оно само является кольцом.

Тривиальные подкольца — это *нулевое* подкольцо $\{0\}$ и само кольцо R. Непосредственно из определения кольца следует, что подкольцо — это ни что иное, как подгруппа аддитивной группы кольца R, замкнутая относительно умножения. С учётом характеристического признака подгруппы (см. теорему 1 из § 14) отсюда вытекает следующий характеристический признак подкольца.

Теорема 1. Подмножество $L \subset R$ является подкольцом тогда и только тогда, когда выполнено следующее условие: если $a,\ b \in L$, то $a - b \in L$ и $ab \in L$.

Эта теорема имеет очевидное

Следствие. Пусть L_1, L_2 — подкольца кольца R. Тогда $L = L_1 \cap L_2$ также является подкольцом R.

Пример 4. Из равенств

$$(m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2}) = (m_1 - m_2) + (n_1 - n_2)\sqrt{2},$$
$$(m_1 + n_1\sqrt{2})(m_2 + n_2\sqrt{2}) = (m_1m_2 + 2n_1n_2) + (m_1n_2 + m_2n_1)\sqrt{2}$$

теперь можно заключить, что подмножество $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ является подкольцом кольца $\mathbb{R}$. Ещё проще проверить, что подмножество $m\mathbb{Z} \subset \mathbb{Z}$ есть подкольцо кольца $\mathbb{Z}$. □

Упражнение 8. Докажите, что любое ненулевое подкольцо кольца $\mathbb{Z}$ имеет вид $m\mathbb{Z}$, где m — натуральное число. Найдите пересечение подколец $m_1\mathbb{Z}$ и $m_2\mathbb{Z}$.

II. Изоморфизм колец. Для сравнения алгебраических свойств различных колец, как и в случае групп, используют соответствующее понятие изоморфизма.

Определение 6. Кольцо $(R, +, \cdot)$ называется *изоморфным* кольцу $(R', \oplus, \odot)$, если существует такое биективное отображение $f : R \to R'$, что

$$f(a + b) = f(a) \oplus f(b), \quad f(a \cdot b) = f(a) \odot f(b)$$

для любых элементов $a,\ b \in R$. Обозначение: $R \cong R'$.

Разумеется, $f(0) = 0'$, а также $f(na) = nf(a)$ для любого $n \in \mathbb{Z}$. Если кольца R и R' имеют единицы e и e' соответственно, то $f(e) = e'$ и $f(a^{-1}) = f(a)^{-1}$ для любого $a \in R^*$.

Пример 5. 1. Пусть $R = \mathbb{Z}[\sqrt{2}]$, а R' — это подкольцо кольца $M_2(\mathbb{Z})$, состоящее из матриц вида

$$\begin{pmatrix} m & 2n \\ n & m \end{pmatrix}, \quad m,\ n \in \mathbb{Z}.$$

Отображение $f : R \to R'$, заданное формулой

$$f(m + n\sqrt{2}) = \begin{pmatrix} m & 2n \\ n & m \end{pmatrix},$$

осуществляет изоморфизм между R и R'.

2. Кольца $R = \mathbb{Z}[\sqrt{2}]$ и $R' = \mathbb{Z}[\sqrt{3}]$ неизоморфны. Действительно, иначе мы получили бы равенство

$$2 = f(2) = f(\sqrt{2} \cdot \sqrt{2}) = f(\sqrt{2})^2 = (m + n\sqrt{3})^2$$

для некоторых $m,\ n \in \mathbb{Z}$, что невозможно. Налицо различие в алгебраических свойствах этих колец: в R есть элемент, квадрат которого равен 2, а в R' такого элемента нет. □

§ 16. Поля

Понятие поля: определение, примеры и простейшие свойства. Подполе, характеристический признак подполя. Изоморфизм полей. СЛУ над произвольным полем.

I. Понятие поля. Конечные поля. В произвольном кольце роли операций сложения и умножения, вообще говоря, существенно различны. В этом параграфе мы рассмотрим специальный класс колец, в которых эти операции почти полностью симметричны.

Определение 1. Ненулевое коммутативное кольцо F с единицей, в котором каждый ненулевой элемент обратим, называется *полем*.

Иными словами, мультипликативная группа поля F состоит из всех ненулевых элементов поля:

$$F^* = F \setminus \{0\},$$

более того, она является абелевой. Единицу поля обычно обозначают символом 1, при этом $1 \neq 0$. Простейшими примерами полей служат поле рациональных чисел $\mathbb{Q}$ и поле вещественных чисел $\mathbb{R}$. Вот более интересный

Пример 1. Пусть $\mathbb{C}'$ — множество всех матриц

$$Z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad a,\, b \in \mathbb{R}.$$

На основании равенств

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} - \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & -b_1 + b_2 \\ b_1 - b_2 & a_1 - a_2 \end{pmatrix},$$
$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - a_2b_1 \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{pmatrix}$$

и теоремы 1 из § 15 мы можем утверждать, что $\mathbb{C}'$ — подкольцо кольца $M_2(\mathbb{R})$. Равенство

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix}$$

означает, что кольцо $\mathbb{C}'$ коммутативно. Единичная матрица E содержится в $\mathbb{C}'$, поэтому $\mathbb{C}'$ — кольцо с единицей. Наконец, равенство

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad (a, b) \neq (0, 0)$$

(см. формулу (6) из § 12) свидетельствует о том, что всякий ненулевой элемент кольца $\mathbb{C}'$ обратим. Таким образом, $\mathbb{C}'$ — поле. □

В поле не может быть делителей нуля: если $ab = 0$ и $a \neq 0$, то

$$0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = b.$$

Иными словами, любое поле является областью целостности. Иногда верно и обратное утверждение.

Теорема 1. Любая конечная область целостности F является полем.

Доказательство. Пусть $a_1, \ldots, a_n$ — все ненулевые элементы F. Требуется доказать, что любой элемент a_i обратим. Рассмотрим произведения $a_i a_j$, $j = 1, \ldots, n$. Они все ненулевые и попарно различны, так как из равенства

$$a_i a_j = a_i a_{j'}, \quad 1 \leqslant j < j' \leqslant n,$$

в силу закона сокращения следовало бы равенство $a_j = a_{j'}$. Следовательно,

$$\{a_i a_1, \ldots, a_i a_n\} = \{a_1, \ldots, a_n\}.$$

В частности, одно из произведений $a_i a_j$ равно единице 1. Но тогда $a_i^{-1} = a_j$. □

Замечание. Можно доказать даже более общий факт: любое конечное коммутативное кольцо без делителей нуля является полем (нужно показать, что в таком кольце есть единичный элемент, а затем сослаться на теорему 1).

Как показывает пример кольца целых чисел $\mathbb{Z}$, для бесконечных областей целостности утверждение теоремы 1 неверно.

Следствие. Кольцо $\mathbb{Z}_m$ является полем тогда и только тогда, когда $m = p$ — простое число.

Доказательство. Достаточно выяснить, при каких m кольцо $\mathbb{Z}_m$ будет областью целостности. Фактически это уже сделано в упражнении 6 из § 15. □

Поле $\mathbb{Z}_p$ классов вычетов по простому модулю p — важный представитель замечательного семейства конечных полей, называемых *полями Галуа*. Эти поля весьма широко используются в различных приложениях: компьютерной алгебре, криптографии, теории кодирования и т. д. Разумеется, арифметика конечных полей сильно отличается от привычной арифметики числовых полей $\mathbb{Q}$ и $\mathbb{R}$.

Упражнение 1. Докажите, что для любого ненулевого элемента $a \in \mathbb{Z}_p$ справедливо равенство $a^{p-1} = 1$. Это утверждение, сформулированное в виде сравнения

$$a^{p-1} \equiv 1 \pmod{p},$$

где $a \in \mathbb{Z}$ не делится на p, в элементарной теории чисел известно как *малая теорема Ферма*.[12)]

Указание. Воспользуйтесь идеей доказательства теоремы 1.

В произвольном поле единственное решение уравнения

$$bx = a,$$

где $b \neq 0$, обычно записывают в виде *дроби* $a/b = ab^{-1} = b^{-1}a$. Нетрудно видеть, что две дроби a/b и c/d равны тогда и только тогда, когда $ad = bc$. Вообще, действия с дробями подчиняются привычным правилам:

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Обосновать эти правила предоставляется читателю как

[12)] П. Ферма (1601 — 1665) — французский математик, юрист по профессии.

Упражнение 2.

Определение 2. Подмножество $L \subset F$ называется *подполем* поля F, если относительно операций в поле F оно само является полем.

По другому говоря, подполе — это подкольцо L, содержащее 1 и обладающее свойством: если $0 \neq b \in L$, то $b^{-1} \in L$. Если учесть характеристический признак подкольца (см. теорему 1 из § 15), то получим характеристический признак подполя.

Теорема 2. Подмножество $L \subset F$ будет подполем тогда и только тогда, когда выполнено следующее условие: если $a,\ b \in L$, то $a - b \in L$, $ab \in L$ и $b^{-1} \in L$ (при $b \neq 0$).

Укажем более экономный вариант этого условия, который обычно используется на практике: если $a,\ b \in L$, то $a - b \in L$ и $a/b \in L$ (при $b \neq 0$). Теорема 2 имеет очевидное

Следствие. Если L_1, L_2 — подполя поля F, то $L = L_1 \cap L_2$ также подполе F.

Пример 2. Докажем, что подмножество

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a,\ b \in \mathbb{Q}\}$$

является подполем поля $\mathbb{R}$. Прежде всего заметим, что запись произвольного числа из $\mathbb{Q}(\sqrt{2})$ в виде $a + b\sqrt{2}$, где $a,\ b \in \mathbb{Q}$, единственна: если

$$a + b\sqrt{2} = a' + b'\sqrt{2},$$

где также $a',\ b' \in \mathbb{Q}$, то $a = a'$ и $b = b'$.

Упражнение 3. Докажите это.
Указание. $\sqrt{2}$ — иррациональное число.

Наше утверждение о подполе следует из равенств

$$(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2},$$
$$\frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} = \frac{a_1a_2 - 2b_1b_2}{a_2^2 - 2b_2^2} + \frac{-a_1b_2 + a_2b_1}{a_2^2 - 2b_2^2}\sqrt{2},$$

первое из которых очевидно, а по поводу второго нужно заметить следующее: при рациональных a_2, b_2 из $a_2 + b_2\sqrt{2} \neq 0$ вытекает $a_2 - b_2\sqrt{2} \neq 0$, поэтому умножение числителя и знаменателя дроби на число $a_2 - b_2\sqrt{2}$ законно. □

Если L — подполе поля F, то говорят также, что F является *расширением* поля L. Так, например, имеем следующую цепочку расширений:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}.$$

В следующем параграфе мы добавим ещё одно важное звено — поле комплексных чисел $\mathbb{C}$, которое является расширением поля $\mathbb{R}$. Любое подполе поля $\mathbb{C}$ принято называть *числовым полем*. Среди числовых полей выделяют поля типа $\mathbb{Q}(\sqrt{2})$, которые называются *полями алгебраических чисел*.

Упражнение 4. Докажите, что поля $\mathbb{Q}$ и $\mathbb{Z}_p$ не имеют собственных (т. е. не совпадающих с ними самими) подполей.

II. Изоморфизм полей. Поле F изоморфно полю F', если они изоморфны как кольца. Если $f : F \to F'$ — изоморфизм, то, в частности, $f(0) = 0'$ и $f(1) = 1'$.

Пример 3. Рассмотрим в качестве F поле $\mathbb{Q}(\sqrt{2})$, и пусть F' — это подкольцо кольца $M_2(\mathbb{Q})$, состоящее из матриц вида

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}, \quad a,\, b \in \mathbb{Q}.$$

Нетрудно проверить, что подкольцо F' на самом деле является полем, при этом отображение $f : F \to F'$, заданное формулой

$$f(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix},$$

осуществляет изоморфизм между F и F'. □

Определение 3. Изоморфизм $f : F \to F$ называется *автоморфизмом* поля F.

Автоморфизмы поля связаны с самыми глубокими его свойствами и являются мощным инструментом при изучении этих свойств в рамках так называемой *теории Галуа*. Отметим кстати, что можно говорить и об автоморфизмах групп и колец.

Упражнение 5. Докажите, что поля $\mathbb{Q}$ и $\mathbb{Z}_p$ имеют только тождественные автоморфизмы.

Не совсем очевидно, что этим свойством обладает и более «богатое» поле $\mathbb{R}$.

Упражнение 6. Докажите, что поле $\mathbb{R}$ тоже не имеет автоморфизмов, отличных от тождественного.

Указание. Предварительно докажите, что всякий автоморфизм $f : \mathbb{R} \to \mathbb{R}$ обладает свойством монотонности: если $a < b$, то $f(a) < f(b)$.

Вместе с тем подполя поля $\mathbb{R}$ сами могут иметь нетривиальные (т. е. отличные от тождественного) автоморфизмы. Таковы, например, некоторые поля алгебраических чисел типа $\mathbb{Q}(\sqrt{2})$.

Пример 4. Отображение $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, заданное формулой

$$f(a + b\sqrt{2}) = a - b\sqrt{2}$$

является автоморфизмом поля $\mathbb{Q}(\sqrt{2})$. Более того, это единственный нетривиальный автоморфизм этого поля. □

Упражнение 7. Докажите утверждения, сформулированные в примере 4.

III. СЛУ над произвольным полем. Теорию СЛУ и выросшую из неё теорию определителей можно обобщить. В роли коэффициентов линейных уравнений

$$a_1x_1 + \ldots + a_nx_n = b,$$

а также элементов матриц $A = (a_{ij})$ у нас были только вещественные числа, но специфику этих чисел никак не использовалась, за исключением того, что их бесконечно много.

Поэтому нет никаких препятствий к тому, чтобы теперь вместо чисел взять элементы некоторого фиксированного поля F. При этом и результаты должны формулироваться в терминах поля F: компоненты решений

$$x^* = (x_1^*, \ldots, x_n^*)$$

СЛУ и значение определителя $\det(A)$ будут принадлежать полю F. Метод Гаусса, вся теория определителей (в частности, формулы Крамера) останутся справедливыми для произвольного поля F. Конечно, в общем случае нельзя будет утверждать, что совместная и неопределённая СЛУ имеет бесконечно много решений, но только потому, что поле F может оказаться конечным (в свете приложений к криптографии и теории кодирования этот случай вызывает особый интерес).

Некоторые примеры решения СЛУ над конечными полями будут даны на практических занятиях.

§ 17. Поле комплексных чисел $\mathbb{C}$

Поле комплексных чисел $\mathbb{C}$. Алгебраическая форма записи комплесных чисел. Автоморфизм сопряжения. Тригонометрическая форма записи комплексных чисел. Формула Муавра. Геометрический смысл операций над комплексными числами.

Исторически комплексные числа возникли в результате попыток найти общую формулу для решения кубических уравнений

$$x^3 + px + q = 0.$$

Такая формула, известная сейчас как *формула Кардано*[13)], была найдена:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Однако применение этой формулы в общем случае требовало действий с абстрактными «мнимыми» величинами — квадратными корнями из отрицательных чисел. Эти абстракции впоследствии привели к строгому понятию комплексного числа.

Более естественной причиной появления комплексных чисел могло бы быть желание расширить запас чисел так, чтобы стало возможным решить любое квадратное уравнение. Пример уравнения

$$x^2 + 1 = 0$$

(можно было бы взять произвольное квадратное уравнение с отрицательным дискриминантом) показывает, что множества $\mathbb{R}$ обычных вещественных чисел для этого недостаточно.

I. Построение поля комплексных чисел. Рассмотрим множество двумерных арифметических векторов $\mathbb{R}^2$. Как мы знаем, для векторов $z_1 = (a_1, b_1)$ и $z_2 = (a_2, b_2)$ определена сумма

$$z_1 + z_2 = (a_1 + a_2, b_1 + b_2),$$

и относительно такой операции сложения $\mathbb{R}^2$ представляет собой абелеву группу. Введём дополнительно операцию умножения, положив

$$z_1 z_2 = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1).$$

Далее множество $\mathbb{R}^2$ будем обозначать через $\mathbb{C}$, а его элементы

$$z = (a, b)$$

будем называть *комплексными числами*, подчёркивая тем самым наличие двух операций — сложения и умножения — на этом множестве. Название «числа» оправдывается тем, что $\mathbb{C}$ оказывается полем относительно этих операций.

Действительно, как показывает непосредственная проверка, операция умножения комплексных чисел коммутативна, ассоциативна и дистрибутивна относительно операции сложения.

[13)] Д. Кардано (1501 — 1576) — итальянский математик, инженер и медик.

Упражнение 1. Докажите, что

$$z_1z_2 = z_2z_1, \quad (z_1z_2)z_3 = z_1(z_2z_3), \quad z_1(z_2 + z_3) = z_1z_2 + z_1z_3$$

для любых комплексных чисел z_1, z_2, z_3.

Комплексное число $(1, 0)$ является единичным элементом: если $z = (a, b)$, то

$$(1, 0)z = (1, 0)(a, b) = (a, b) = z.$$

Таким образом, $\mathbb{C}$ является коммутативным кольцом с единицей. Более того, если комплексное число $z = (a, b) \neq (0, 0)$, то комплексное число

$$w = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2}\right)$$

будет обратным к z.

Упражнение 2. Проверьте, что $w = z^{-1}$, т. е. $zw = (1, 0)$.

Итак, *поле комплексных чисел* $\mathbb{C}$ построено. Объясним, в каком смысле его можно считать расширением поля вещественных чисел $\mathbb{R}$.

Для этого рассмотрим подмножество $\mathbb{R}' \subset \mathbb{C}$ всех комплексных чисел вида $(a, 0)$, где $a \in \mathbb{R}$. Нетрудно видеть, что $\mathbb{R}'$ является подполем, изоморфным полю $\mathbb{R}$. Отображение

$$f : \mathbb{R} \to \mathbb{R}', \quad f(a) = (a, 0),$$

реализующее этот изоморфизм, позволяет отождествить комплексное число $(a, 0)$ с вещественным числом a и тем самым считать поле вещественных чисел $\mathbb{R}$ подполем поля комплексных чисел $\mathbb{C}$. В частности, при таком отождествлении имеем

$$(0, 0) = 0, \quad (1, 0) = 1.$$

Упражнение 3. Докажите, что поле комплексных чисел $\mathbb{C}$ изоморфно полю $\mathbb{C}'$, построенному в примере 1 из § 16.

II. Алгебраическая форма записи. Автоморфизм сопряжения. Введём обозначение:

$$i = (0, 1).$$

Комплексное число i принято называть *мнимой единицей*, что связано со следующим его свойством:

$$i^2 + 1 = 0.$$

Действительно, имеем $i^2 + 1 = (0, 1)(0, 1) + (1, 0) = (-1, 0) + (1, 0) = (0, 0) = 0$. Произвольное комплексное число $z = (a, b)$ теперь можно представить в виде

$$z = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi.$$

Именно так мы дальше и будем записывать комплексные числа.

Определение 1. Формула

$$z = a + bi \tag{1}$$

называется *алгебраической формой* записи комплексного числа z. Вещественные числа a и b называются *вещественной* и *мнимой* частью комплексного числа z.

Обозначение: $a = \operatorname{Re} z$, $b = \operatorname{Im} z$.

Сложение (вычитание) комплексных чисел $z = a + bi$ и $w = c + di$ в алгебраической форме происходит покомпонентно:

$$z \pm w = (a \pm c) + (b \pm d)i.$$

Для того, чтобы перемножить z и w, следует раскрыть скобки, заменить i^2 на -1 и привести подобные:

$$zw = (a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.$$

Для отыскания частного z/w при условии $w \neq 0$ предварительно домножают числитель и знаменатель на число $c - di$:

$$\frac{z}{w} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (-ad + bc)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{-ad + bc}{c^2 + d^2}\, i.$$

Определение 2. Комплексное число

$$\overline{z} = a - bi$$

называется *сопряжённым* комплексному числу $z = a + bi$.

Отображение $\mathbb{C} \to \mathbb{C}$, при котором комплексному числу z сопоставляется его сопряжённое $\overline{z}$, называется (*комплексным*) *сопряжением*. Нетрудно видеть, что сопряжение является автоморфизмом поля $\mathbb{C}$, оставляющим на месте вещественные числа. Действительно, сопряжение — это биективное отображение, при этом $\overline{a} = a$ для любого $a \in \mathbb{R}$. Поэтому достаточно убедиться, что сопряжённое к сумме (произведению) комплексных чисел равно сумме (произведению) сопряжённых к ним.

Упражнение 4. Проверьте это непосредственным вычислением. Докажите, что автоморфизм сопряжения — единственный нетривиальный автоморфизм поля $\mathbb{C}$, относительно которого поле $\mathbb{R}$ неподвижно.

Помимо автоморфизма сопряжения, поле $\mathbb{C}$ имеет очень много других автоморфизмов, но с «плохими» свойствами (так называемые wild automorphisms). «Потрогать руками» такие автоморфизмы нельзя, так как при их построении используется аксиома выбора или что-нибудь, ей эквивалентное (см. начало § 13).

III. Тригонометрическая форма записи. Формула Муавра. Алгебраическая форма записи (1) комплексных чисел плохо приспособлена для совершения мультипликативных действий над ними.

Определение 3. Пусть $z = a + bi$ — комплексное число. Вещественное число

$$\sqrt{a^2 + b^2}$$

называется *модулем* z и обозначается $|z|$. Вещественное число ϕ, для которого

$$\cos\phi = \frac{a}{|z|}, \quad \sin\phi = \frac{b}{|z|}, \tag{2}$$

называется *аргументом* z и обозначается $\phi = \operatorname{Arg} z$ (предполагается, что $z \neq 0$).

Очевидно, $|z| \geqslant 0$, причём $|z| = 0$ только для $z = 0$.

Упражнение 5. Докажите следующие свойства модуля комплексного числа:
а) $|\overline{z}| = |z|$ и $z\overline{z} = |z|^2$;
б) $|zw| = |z||w|$;
в) $|z^n| = |z|^n$, где $n = 1, 2, \ldots$;
г) $|z + w| \leqslant |z| + |w|$.

Аргумент комплексного числа $z \neq 0$ определён неоднозначно, однако если ϕ и ϕ' — два значения $\operatorname{Arg} z$, то

$$\phi - \phi' = 2\pi k$$

для некоторого $k \in \mathbb{Z}$. Однозначность появится, если дополнительно потребовать, чтобы, например, $\phi \in [0, 2\pi)$ (здесь можно взять любой фиксированный полуинтервал длины 2π). В таком случае ϕ называют *главным аргументом* и обозначают $\phi = \arg z$. Для вычисления $\arg z$ используют обратные тригонометрические функции.

Определение 4. Формула

$$z = |z|(\cos\phi + i\sin\phi), \quad \phi = \operatorname{Arg} z,$$

непосредственно вытекающая из равенств (2), называется *тригонометрической формой* записи комплексного числа $z \neq 0$.

Пример 1. Запишем в тригонометрической форме число $z = 1 - i$. Имеем

$$|z| = |1 - i| = \sqrt{2}, \quad \cos\phi = \frac{1}{\sqrt{2}}, \quad \sin\phi = \frac{-1}{\sqrt{2}},$$

откуда $\phi = \arg z = 7\pi/4$. Таким образом, $z = \sqrt{2}\,(\cos(7\pi/4) + i\sin(7\pi/4))$. □

Умножение (деление) комплексных чисел, записанных в тригонометрической форме, происходит по следующим простым правилам. Пусть

$$w = |w|(\cos\psi + i\sin\psi), \quad \psi = \operatorname{Arg} w.$$

Тогда справедливы следующие равенства:

$$zw = |z||w|(\cos(\phi + \psi) + i\sin(\phi + \psi), \quad \frac{z}{w} = \frac{|z|}{|w|}(\cos(\phi - \psi) + i\sin(\phi - \psi)$$

(словами: при умножении модули перемножаются, аргументы складываются, а при делении — делятся и вычитаются, соответственно). Первое из этих равенств доказывается непосредственным перемножением и применением тождеств

$$\cos(\phi + \psi) = \cos\phi\cos\psi - \sin\phi\sin\psi,$$
$$\sin(\phi + \psi) = \sin\phi\cos\psi + \cos\phi\sin\psi.$$

Для доказательства второго нужно записать

$$\frac{z}{w} = \frac{z\overline{w}}{|w|^2},$$

после чего воспользоваться тем, что $\overline{w} = |w|(\cos(-\psi) + i\sin(-\psi))$.

В качестве следствия можно получить *формулу Муавра*[14]:

$$z^n = |z|^n(\cos(n\phi) + i\sin(n\phi)), \quad n = 1, 2, \ldots$$

(доказательство проводится индукцией по n). Эта формула справедлива и для отрицательных целых показателей n.

Упражнение 6. Докажите последнее утверждение.

Указание. Достаточно проверить, что $z^{-1} = |z|^{-1}(\cos(-\phi) + i\sin(-\phi))$.

Пример 2. Вычислим $(1-i)^{100}$. Поскольку

$$1 - i = \sqrt{2}\,(\cos(7\pi/4) + i\sin(7\pi/4))$$

(см. пример 1), по формуле Муавра получим

$$(1-i)^{100} = 2^{50}(\cos(175\pi) + i\sin(175\pi)) = -2^{50}.$$

Другой способ вычисления основан на равенстве $(1-i)^4 = -2^2$, которое можно проверить непосредственным перемножением. □

IV. Геометрический смысл операций над комплексными числами. Рассмотрим евклидову плоскость с некоторой фиксированной прямоугольной системой координат. Комплексному числу (1) можно однозначно сопоставить точку Z этой плоскости, имеющую абсциссу $a = \operatorname{Re} z$ и ординату $b = \operatorname{Im} z$. Саму плоскость при этом называют *комплексной плоскостью* (и обозначают по-прежнему $\mathbb{C}$), подразумевая такую интерпретацию её точек. Комплексное число z, изначально определяемое как арифметический вектор, теперь можно представить как обычный геометрический вектор $\overrightarrow{OZ}$, идущий из начала координат O в точку Z. Понятно, что сложению (вычитанию) комплексных чисел соответствует сложение (вычитание) сопоставляемых им векторов.

Для комплексной плоскости $\mathbb{C}$ справедливы следующие соотношения:

1. $|z|$ — расстояние $d(O, Z)$ от точки O до точки Z или длина вектора $\overrightarrow{OZ}$;

2. $\arg z$ — угол, на который нужно повернуть единичный вектор оси абсцисс, чтобы его направление совпало с направлением вектора $\overrightarrow{OZ}$;[15]

3. $|z_2 - z_1|$ — расстояние между точками Z_1 и Z_2 или длина вектора $\overrightarrow{Z_1Z_2}$.

Указанный геометрический смысл $|z|$ и $\arg z$ позволяет находить атрибуты тригонометрической формы записи комплексного числа z при помощи простых формул школьной тригонометрии.

---

[14] А. Муавр (1667 — 1754) — английский математик французского происхождения.

[15] Ось абсцисс обычно изображают горизонтальной и направленной слева направо, а ось ординат — вертикальной и идущей снизу вверх. Угол поворота считается положительным, если поворот происходит в направлении, противоположном ходу часовой стрелки.

Упражнение 7. Убедитесь, что неравенство п. г) упражнения 5 можно интерпретировать как *неравенство треугольника*: сумма длин двух сторон треугольника больше длины третьей стороны.

Опишем геометрический смысл стандартных операций над комплексными числами. Отображение, сопоставляющее комплексному числу z его сопряжённое $\overline{z}$, есть *осевая симметрия* относительно оси абсцисс. Если зафиксировать комплексное число w, то отображение, сопоставляющее комплексному числу z произведение zw, в геометрических терминах можно описать так: это поворот с центром в начала координат на угол, равный $\arg w$, с последующим растяжением или сжатием в $|w|$ раз. В этом состоит геометрический смысл операции умножения комплексных чисел. Отметим частный случай: если $|w| = 1$, т. е.

$$w = \cos\psi + i\sin\psi, \quad \psi = \arg w,$$

то при умножении на w происходит только поворот на угол ψ. Что касается операции деления, то здесь достаточно понять геометрический смысл отображения, которое сопоставляет комплексному числу z его обратное z^{-1}. Можно показать, что это отображение есть композиция сопряжения и инверсии относительно окружности единичного радиуса с центром в начале координат.

Упражнение 8. Покажите это. (Напомним, что *инверсией* относительно окружности радиуса r с центром в точке O называется преобразование, которое точке X ставит в соответствие точку Y, лежащую на луче OX и такую, что $|OX||OY| = r^2$.)

Такая тесная связь с евклидовой геометрией плоскости позволяет весьма эффективно применять алгебру комплексных чисел к доказательству геометрических теорем. По существу это хорошо известный *координатный метод*, но использующий вместо двух вещественных координат x и y одну комплексную координату $z = x + yi$.

Пример 3. На сторонах произвольного треугольника ABC во внешнюю сторону построены правильные треугольники ABC_1, BCA_1, CAB_1. Тогда их центры образуют ещё один правильный треугольник.

Обозначим эти центры через O_C, O_A, O_B соответственно. Будем считать треугольник ABC расположенным на комплексной плоскости, а его вершины A, B, C — заданными комплексными числами z_1, z_2, z_3 соответственно. Нам ещё понадобится число

$$\zeta = \cos 60^\circ + i\sin 60^\circ = \frac{1 + i\sqrt{3}}{2},$$

которое «отвечает» за поворот на угол в 60°.

Доказательство сформулированного утверждения состоит в последовательном вычислении всех участвующих точек (точнее, соответствующих этим точкам комплексных чисел), после чего проверяется условие правильности треугольника $O_CO_AO_B$.

Сначала вычислим третьи вершины A_1, B_1, C_1:

$$A_1 = C + (B - C)\zeta = -\zeta z_1 + \zeta z_2 + z_3$$

и аналогично для B_1, C_1. Затем вычислим центры O_C, O_A, O_B:

$$O_A = \frac{B + C + A_1}{3} = \frac{-\zeta z_1 + (1 + \zeta)z_2 + 2z_3}{3}$$

и аналогично для O_B, O_C. Условие правильности треугольника $O_CO_AO_B$ на языке комплексных чисел можно записать, например, так:

$$O_C = O_A + (O_B - O_A)\zeta. \tag{3}$$

Проверить это равенство можно механически, просто подставив вместо O_C, O_A, O_B найденные выражения и затем раскрыв скобки.

Треугольник $O_CO_AO_B$ называют *внешним треугольником Наполеона* для исходного треугольника ABC. *Внутренний треугольник Наполеона* $O_C^*O_A^*O_B^*$ определяется аналогичным образом и тоже оказывается правильным.

Интересно отметить, что последний факт не требует отдельного доказательства. Дело в том, что при проверке равенства (3) имело значение только то, что ζ^2 можно было заменить на $\zeta - 1$. Но есть ещё одно число с таким свойством — это

$$\zeta^* = \cos(-60^\circ) + i\sin(-60^\circ) = \frac{1 - i\sqrt{3}}{2},$$

второй корень уравнения $x^2 = x - 1$. Легко видеть, что замена ζ на ζ^* в наших вычислениях приводит к внутреннему треугольнику Наполеона $O_C^*O_A^*O_B^*$. □

§ 18. Корни из комплексных чисел

Извлечение корня n-й степени из комплексных чисел. Группа корней n-й степени из единицы. Первообразные корни из единицы.

I. Понятие корня n-й степени. Пусть $n \geqslant 2$ — фиксированное натуральное число. Напомним, что для любого положительного вещественного числа x однозначно определён *арифметический корень n-й степени* из числа x — такое положительное вещественное число y, для которого $y^n = x$. Обозначение: $y = \sqrt[n]{x}$.[16)]

Это понятие можно расширить следующим образом.

Определение 1. Пусть F — произвольное поле. *Корнем n-й степени* из элемента $z \in F^*$ называется всякий элемент $w \in F^*$, удовлетворяющий уравнению

$$w^n = z. \tag{1}$$

Обозначение: $w = \sqrt[n]{z}$.

Для случая $F = \mathbb{R}$ это новое понятие корня очевидным образом сводится к понятию арифметического корня.

Упражнение 1. Убедитесь в этом. Сколько существует корней n-й степени из данного ненулевого вещественного числа?

В общем случае представляет интерес вопрос о числе различных значений корня n-й степени из данного ненулевого элемента поля. Можно показать, что это число заключено в пределах от 0 до n. Рассмотрим важный частный случай $F = \mathbb{C}$, где всегда достигается верхняя граница.

Пусть

$$z = |z|(\cos\phi + i\sin\phi) \tag{2}$$

— тригонометрическая форма записи комплексного числа z. Выведем формулу, по которой можно найти все корни n-й степени из z. Положим

$$w = |w|(\cos\psi + i\sin\psi)$$

и определим $|w|$ и ψ, исходя из равенства (1). По формуле Муавра

$$w^n = |w|^n(\cos(n\psi) + i\sin(n\psi)).$$

Сравнив с (2), получим $|w|^n = |z|$ и $n\psi - \phi = 2\pi k$ для некоторого $k \in \mathbb{Z}$. Значит,

$$w = \sqrt[n]{|z|}\left(\cos\frac{\phi + 2\pi k}{n} + i\sin\frac{\phi + 2\pi k}{n}\right), \tag{3}$$

где $\sqrt[n]{|z|}$ — арифметический корень n-й степени. Эта формула доставляет все возможные значения корня n-й степени из комплексного числа z. Легко видеть, что будет в точности n различных значений: они получаются, когда k пробегает какой-нибудь отрезок ряда целых чисел $\mathbb{Z}$ длины n. Обычно в формуле (3) полагают $k = 0, 1, \ldots, n-1$.

[16)] При $n = 2$ степень корня не указывают: $y = \sqrt{x}$.

Геометрически все значения $\sqrt[n]{z}$ можно представить как вершины некоторого правильного n-угольника, вписанного в окружность радиуса $\sqrt[n]{|z|}$ с центром в начале координат.

Примеры извлечения корней n-й степени с помощью формулы (3) будут приведены на практических занятиях. Отметим, что для нахождения квадратного корня ($n = 2$) существует альтернативный способ, не требующий записи исходного числа в тригонометрической форме.

Пример 1. Найдём $w = \sqrt{-3 + 4i}$.

Будем искать w в алгебраической форме, т. е. положим $w = x + yi$. Тогда

$$w^2 = (x + yi)^2 = (x^2 - y^2) + 2xyi = -3 + 4i,$$

откуда приходим к системе уравнений

$$x^2 - y^2 = -3, \quad 2xy = 4.$$

Эту систему легко решить школьными методами: подставив $y = 2/x$ в первое уравнение и затем решив биквадратное уравнение относительно x. В итоге получим

$$(x, y) \in \{(-1, -2), (1, 2)\}.$$

Таким образом, $w = \pm(1 + 2i)$. □

II. Корни из единицы. Особый интерес представляет извлечение корней из единичного элемента поля F. Обозначим через U_n множество всех корней n-й степени из элемента $z = 1$. Непосредственно из определения 1 и теоремы 1 из § 14 вытекает, что U_n — это подгруппа мультипликативной группы F^* поля F.

Упражнение 2. Докажите это утверждение.

Группа U_n называется *группой корней n-й степени из единицы* поля F. С помощью группы U_n процедура извлечения корня n-й степени из произвольного элемента $z \in F^*$ сводится к отысканию какого-нибудь одного значения w_0 этого корня. Действительно, тогда любое другое значения w можно получить по формуле

$$w = w_0\zeta, \quad \zeta \in U_n.$$

Упражнение 3. Докажите и это утверждение. В качестве следствия получим следующее: для любого $z \in F^*$ либо не существует ни одного корня n-й степени из z, либо их количество равно порядку группы U_n.

Далее рассмотрим более подробно случай $F = \mathbb{C}$.

Применив формулу (3) к комплексному числу $z = 1$, получим, что группа U_n состоит из комплексных чисел

$$\zeta_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n - 1.$$

В частности, порядок группы U_n равен n. Фактически эта группа ранее нам уже встречалась — как аддитивная группа кольца классов вычетов $\mathbb{Z}_n$. Точнее, речь идёт об изоморфности этих двух групп: изоморфизм $f : U_n \to \mathbb{Z}_n$ можно задать правилом

$$f(\zeta_k) = [k]_n, \quad k = 0, 1, \ldots, n - 1. \tag{4}$$

Упражнение 4. Убедитесь, что отображение (4) действительно осуществляет изоморфизм между указанными группами.

Важное свойство группы U_n состоит в следующем: все её элементы представляются в виде степени одного фиксированного элемента. В самом деле, имеем

$$\zeta_k = \zeta_1^k, \quad k = 0,\, 1,\, \ldots,\, n-1,$$

как это следует из формулы Муавра.

Определение 2. Корень n-й степени из единицы ζ называют *первообразным*, если

$$U_n = \{\zeta^k : k = 0,\, 1,\, \ldots,\, n-1\}.$$

Помимо $\zeta = \zeta_1$, существуют и другие первообразные корни n-й степени из единицы. Эксперименты с конкретными значениями n быстро приводят к следующему описанию всех первообразных корней n-й степени из единицы:

$$\zeta = \zeta_r, \quad \text{НОД}\,(r, n) = 1.$$

Упражнение 5. Убедитесь в корректности такого описания.
Указание. Если $\text{НОД}\,(r, n) = 1$, то в ряду чисел

$$\zeta_r^k = \zeta_1^{rk}, \quad k = 0,\, 1,\, \ldots,\, n-1,$$

не будет совпадающих. Напротив, если $\text{НОД}\,(r, n) > 1$, то совпадения будут.

В заключение отметим, что в случае произвольного поля F группа корней n-й степени из единицы также обладает указанным выше свойством и можно говорить о первообразных корнях n-й степени из единицы в общем случае. В частности, если $F = \mathbb{Z}_p$ — поле классов вычетов по простому модулю p, то утверждение о существовании первообразного корня $(p-1)$-й степени из единицы эквивалентно теореме Гаусса о первообразном корне по простому модулю p.

Упражнение 6. Найдите сумму всех корней n-й степени из единицы.
Указание. Пусть S — искомая сумма, а ζ — фиксированный корень n-й степени из единицы, не равный единице. Рассмотрите произведение ζS.
Другой способ состоит в непосредственном вычислении

$$S = 1 + \zeta + \ldots + \zeta^{d-1},$$

где ζ — фиксированный первообразный корень n-й степени из единицы, а d — порядок группы U_n.

Список литературы

1. *Винберг Э.Б.* Курс алгебры. М.: Изд-во «Факториал Пресс», 2001.
2. *Винберг Э.Б.* Алгебра многочленов. М.: Просвещение, 1980.
3. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. СПб.: Изд-во «Лань», 2015.
4. *Кострикин А.И.* Введение в алгебру. Часть I. Основы алгебры. М.: ФИЗМАТЛИТ, 2004.
5. *Кострикин А.И.* Введение в алгебру. Часть II. Линейная алгебра. М.: ФИЗМАТЛИТ, 2000.
6. *Кострикин А.И.* Введение в алгебру. Часть III. Основные структуры. М.: ФИЗМАТЛИТ, 2004.
7. *Кострикин А.И.* (*ред.*) Сборник задач по алгебре. М.: ФИЗМАТЛИТ, 2001.
8. *Кострикин А.И., Манин Ю.И.* Линейная алгебра и геометрия. М.: Наука, 1986.
9. *Курош А.Г.* Курс высшей алгебры. М.: Наука, 1975.
10. *Проскуряков И.В.* Сборник задач по линейной алгебре. М.: БИНОМ. Лаборатория знаний, 2005.
11. *Тыртышников Е.Е.* Матричный анализ и линейная алгебра. М.: ФИЗМАТЛИТ, 2007.
12. *Фаддеев Д.К., Соминский И.С.* Задачи по высшей алгебре. СПб.: Изд-во «Лань», 1999.