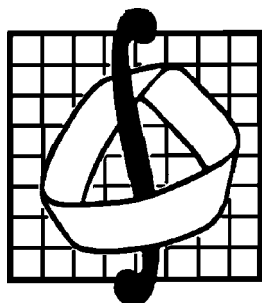


МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА



Механико-математический факультет
Кафедра высшей алгебры

Курс лекций по алгебре

Е.С. Голод

Москва 2004 год

Е.С. Голод

Курс лекций по алгебре. I семестр.

Пособие содержит часть материала курса высшей алгебры, читаемого в первом семестре.

Для студентов начальных курсов университетов.

© Механико-математический факультет МГУ, 2004 г.

© Е.С. Голод, 2004 г.

Оглавление

1. Перестановки	5
1.1. Основные понятия	5
1.2. Четность перестановки	9
2. Теорема Крамера	14
2.1. Напоминание об исследовании и решении систем линейных уравнений методом элементарных пре- образований (метод Гаусса)	14
2.2. Ступенчатый вид квадратной матрицы	16
2.3. Критерий определенности квадратной системы ли- нейных уравнений	17
2.4. Другое доказательство теоремы и формул Краме- ра, не использующее приведение матрицы к сту- пенчатому виду	20
3. Базис и ранг системы векторов	22
3.1. Напоминание о линейной зависимости системы векторов	22
3.2. Базис системы векторов	26
3.3. Алгоритм нахождения некоторого базиса конечной системы векторов	30
3.4. Ранг системы векторов	33
3.5. Подпространства в \mathbb{R}^n	34
3.6. Базис и размерность подпространства решений од- нородной системы линейных уравнений	36
4. Операции над матрицами	38
4.1. Сложение матриц и умножение на скаляр	38
4.2. Умножение матриц	39
4.3. Элементарные матрицы	43
4.4. Определитель произведения матриц	46
4.5. Аксиоматическая характеристика определителя и другое доказательство теоремы об определителе произведения матриц	47
4.6. Простейшие линейные матричные уравнения	48
4.7. Обратная матрица	49
4.8. Решение простейших линейных матричных урав- нений и вычисление обратной матрицы с помо- щью элементарных преобразований	51

5. Ранг матрицы	54
5.1. Теорема о ранге матрицы	54
5.2. Критерий совместности для систем линейных уравнений (в терминах рангов матриц)	58
5.3. Выбор главных и свободных неизвестных в совместной системе линейных уравнений	59
6. Понятие группы	61
6.1. Понятия бинарной операции и полугруппы, обобщенный закон ассоциативности	61
6.2. Единица и обратный элемент в полугруппе. Свойства степеней элементов	63
6.3. Определение группы. Порядок элемента группы и его свойства	67
6.4. Понятие подполугруппы и подгруппы. Циклические подгруппы. Циклические группы, их порождающие и их подгруппы.	72
6.5. Понятия гомоморфизма и изоморфизма. Классификация циклических групп с точностью до изоморфизма	75
6.6. Задание конечной группы таблицей Кейли. Теорема Кейли	79
6.7. Разложение группы на смежные классы. Теорема Лагранжа	81
6.8. Нормальные подгруппы. Структура гомоморфизмов. Факторгруппы	84
7. Понятия кольца и поля	89
7.1. Определение кольца. Общие и специальные свойства, примеры	89
7.2. Кольца и поля классов вычетов	93
7.3. Подкольца и подполя. Гомоморфизмы и изоморфизмы колец. Группа автоморфизмов	95
7.4. Характеристика поля	98
8. Комплексные числа	101
8.1. Построение поля комплексных чисел	101
8.2. Тригонометрическая форма комплексного числа. Формула Муавра. Извлечение корней из комплексных чисел	105
8.3. Корни из единицы	107

§1. Перестановки

1.1. Основные понятия

Под *перестановками* на множестве понимаются *биективные отображения* множества на себя. Мы будем рассматривать случай, когда множество конечно. В этом случае, если состоит из n элементов, занумеруем его элементы натуральными числами от 1 до n и отождествим с отрезком натурального ряда $[1, n]$. Таким образом, мы рассматриваем перестановки на множестве $[1, n]$ и обозначаем множество всех таких перестановок через S_n . Число элементов в S_n равно $n!$ Всякую перестановку $\pi \in S_n$ мы можем записывать в виде таблицы

$$\pi = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix},$$

в верхней строке которой записаны в некотором порядке все числа от 1 до n , а под каждым элементом i_k верхней строки записан элемент j_k , в который i_k переходит при отображении π , т.е. $j_k = \pi(i_k)$. Так как отображение π биективное, то в нижней строке таблицы также записаны все числа от 1 до n . Табличная запись перестановки π неоднозначна, так как порядок записи чисел в верхней строке произволен. Две таблицы

$$\begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix}, \quad \begin{pmatrix} s_1 & \dots & s_n \\ t_1 & \dots & t_n \end{pmatrix}$$

задают одну и ту же перестановку в том и только в том случае, если они имеют одинаковые столбцы и отличаются только порядком расположения столбцов. Каждая перестановка имеет запись в виде таблицы, в которой числа в верхней строке расположены в естественном порядке:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

где $k_i = \pi(i)$. Такую запись перестановки будем называть *канонической*. Для элементов множества S_n определена операция умножения, задаваемая композицией отображений: если $\pi, \sigma \in S_n$, то $\pi\sigma$ есть такая перестановка, что $(\pi\sigma)(i) = \pi(\sigma(i))$ для всех $i \in [1, n]$. Эта операция обладает следующими свойствами:

1. *Ассоциативность*: $(\pi\sigma)\tau = \pi(\sigma\tau) \forall \pi, \sigma, \tau \in S_n$.
2. Существует *единичная* перестановка $\varepsilon \in S_n$, т.е. такая, что $\varepsilon\pi = \pi\varepsilon = \pi \forall \pi \in S_n$.
3. Для всякой перестановки $\pi \in S_n$ существует *обратная* перестановка $\pi^{-1} \in S_n$, т.е. такая, что $\pi\pi^{-1} = \pi^{-1}\pi = \varepsilon$.

Тот факт, что умножение перестановок обладает перечисленными свойствами, выражают, говоря, что множество S_n относительно операции умножения является *группой*. Поэтому в дальнейшем мы будем называть S_n *группой перестановок*. Эту группу называют также *симметрической группой* (степени n). Табличная запись единичной перестановки ε , которая представляет собой тождественное отображение множества $[1, n]$, имеет вид

$$\varepsilon = \begin{pmatrix} i_1 & \dots & i_n \\ i_1 & \dots & i_n \end{pmatrix}.$$

Если перестановка $\pi \in S_n$ записывается таблицей

$$\pi = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix},$$

то обратная перестановка задается таблицей

$$\pi^{-1} = \begin{pmatrix} j_1 & \dots & j_n \\ i_1 & \dots & i_n \end{pmatrix}.$$

Для каждой пары различных чисел $i, j \in [1, n]$ можно рассматривать перестановку, обозначаемую через (i, j) и называемую *транспозицией*, которая отображает элементы i, j друг в друга, а все остальные элементы множества $[1, n]$ отображает тождественно, т.е. в табличной записи

$$(i, j) = \begin{pmatrix} i & j & i_1 & i_2 & \dots & i_{n-2} \\ j & i & i_1 & i_2 & \dots & i_{n-2} \end{pmatrix}.$$

Очевидно, $(j, i) = (i, j)$ и S_n содержит $n(n-1)/2$ различных транспозиций. Более широкий класс образуют перестановки, называемые *циклами*. Каждый цикл (длины k) задается выбором из k различных чисел $i_1, \dots, i_k \in [1, n]$ и расположением их в некотором фиксированном порядке. *Циклом*, обозначаемым через (i_1, \dots, i_k) , называется перестановка, задаваемая следующей таблицей:

$$(i_1, \dots, i_k) = \begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k & j_1 & \dots & j_{n-k} \\ i_2 & i_3 & \dots & i_k & i_1 & j_1 & \dots & j_{n-k} \end{pmatrix}.$$

В случае $k = 1$ мы получаем тождественную перестановку. Циклы длины 2 — это транспозиции. Запись цикла в виде (i_1, \dots, i_k) неоднозначна: в случае $k \geq 2$ мы можем записать тот же самый цикл, начав запись с любого элемента i_l из $\{i_1, \dots, i_k\}$, после чего порядок остальных элементов в записи этого цикла определяется единственным образом:

$$(i_1, \dots, i_k) = (i_l, i_{l+1}, \dots, i_k, i_1, \dots, i_{l-1}).$$

Это показывает, что в S_n содержится $\binom{n}{k}(k-1)!$ различных циклов длины $k \geq 2$, где $\binom{n}{k}$ обозначает *биномиальный коэффициент*

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

Два цикла $(i_1, \dots, i_k), (j_1, \dots, j_l) \in S_n$ называются *независимыми*, если множества $\{i_1, \dots, i_k\}$ и $\{j_1, \dots, j_l\}$ не пересекаются (не имеют общих элементов).

Более общо, назовем *носителем* перестановки π множество всех таких $i \in [1, n]$, что $\pi(i) \neq i$. Две перестановки называются *независимыми*, если их носители не пересекаются.

Предложение 1.1. *Независимые перестановки коммутируют.*

Доказательство. Пусть $\{i_1, \dots, i_s\}$ — носитель π , а $\{j_1, \dots, j_t\}$ — носитель σ . Так как эти множества не пересекаются, то эти перестановки можно записать в виде

$$\pi = \begin{pmatrix} i_1 & \dots & i_s & j_1 & \dots & j_t & k_1 & \dots & k_{n-s-t} \\ \pi(i_1) & \dots & \pi(i_s) & j_1 & \dots & j_t & k_1 & \dots & k_{n-s-t} \end{pmatrix},$$

$$\sigma = \begin{pmatrix} i_1 & \dots & i_s & j_1 & \dots & j_t & k_1 & \dots & k_{n-s-t} \\ i_1 & \dots & i_s & \sigma(j_1) & \dots & \sigma(j_t) & k_1 & \dots & k_{n-s-t} \end{pmatrix}$$

и, очевидно, имеем

$$\begin{aligned} \pi\sigma &= \sigma\pi = \\ &= \begin{pmatrix} i_1 & \dots & i_s & j_1 & \dots & j_t & k_1 & \dots & k_{n-s-t} \\ \pi(i_1) & \dots & \pi(i_s) & \sigma(j_1) & \dots & \sigma(j_t) & k_1 & \dots & k_{n-s-t} \end{pmatrix}. \end{aligned}$$

□

Теорема 1.2. *Всякая перестановка обладает разложением в произведение независимых циклов, причем входящие в это произведение циклы длины ≥ 2 определены однозначно (порядок множителей в произведении может быть произвольным, так как независимые циклы коммутируют).*

Доказательство. Пусть $\pi \in S_n$. Если π тождественная, то она является циклом длины 1. Если π не является тождественной, то выбираем произвольное число $i_1 \in [1, n]$, такое что $i_2 = \pi(i_1) \neq i_1$. Далее рассматриваем $i_3 = \pi(i_2), \dots, i_k = \pi(i_{k-1})$ до тех пор, пока пока все числа i_1, i_2, \dots, i_k различны. Так как множество $[1, n]$ конечно, то на некотором шаге мы получим в первый раз, что $\pi(i_k) = i_l$, где $1 \leq l < k$. Допустим, что $l \geq 2$. Тогда $i_l = \pi(i_{l-1})$ и $\pi(i_k) = \pi(i_{l-1})$ откуда $i_k = i_{l-1}$; это противоречит предположению, что числа i_1, \dots, i_k различны. Значит, $l = 1$, $\pi(i_k) = i_1$ и мы получим цикл $\sigma_1 = (i_1, \dots, i_k)$. Если бы в качестве начального элемента был выбран вместо i_1 любой другой элемент i_l из множества $\{i_1, \dots, i_k\}$, то мы получили бы тот же самый цикл в другой записи $\sigma_1 = (i_l, i_{l+1}, \dots, i_k, i_1, \dots, i_{l-1})$. Если $\pi(j) = j \quad \forall j \in [1, n] \setminus \{i_1, \dots, i_k\}$, то $\pi = \sigma_1$. Если же существует $j_1 \in [1, n] \setminus \{i_1, \dots, i_k\}$, такое что $j_2 = \pi(j_1) \neq j_1$, то поступая как выше, мы получим цикл $\sigma_2 = (j_1, \dots, j_l)$. Эти циклы независимы, так как если бы $j_t = i_s$ для некоторых s, t , то начав построение с этого элемента, мы получили бы цикл, который совпадает как с σ_1 , так и с σ_2 , и, следовательно, $j_1 \in \{i_1, \dots, i_k\}$, вопреки предположению. Продолжая этот процесс до исчерпания элементов множества $[1, n]$, мы получаем разложение π в произведение независимых циклов. Согласно построению, эти циклы определены однозначно. □

Замечание 1.3. Циклы длины 1 можно как включать, так и не включать в разложение, даваемое теоремой 1.2. Их включение целесообразно, когда нужно указать все элементы множества, на котором действует перестановка.

Предложение 1.4. *Всякий цикл длины k можно представить (многими разными способами) в виде произведения $k - 1$ транспозиций.*

Действительно, имеем, например, разложение:

$$(i_1, \dots, i_k) = (i_1, i_2) (i_2, i_3) \dots (i_{k-1}, i_k).$$

Теорема 1.5. *Всякая перестановка из S_n обладает разложением в произведение транспозиций.*

Доказательство непосредственно следует из теоремы 1.2 и предложения 1.4.

Заметим, что разложение в произведение транспозиций не единственно, транспозиции в этом произведении могут не коммутировать и, более того, одна и та же транспозиция может входить в это произведение несколько раз.

1.2. Четность перестановки

Пусть задана $\pi \in S_n$ и $\{i, j\}$ — любая неупорядоченная пара (т.е. $\{j, i\}$ считается той же самой парой) разных элементов из $[1, n]$. Будем называть пару $\{i, j\}$ *правильной* для перестановки π , если π сохраняет естественный порядок между числами i, j , т.е. при $i < j$ имеем $\pi(i) < \pi(j)$, и будем называть пару $\{i, j\}$ *неправильной* для π , если π обращает естественный порядок, т.е. при $i < j$ имеем $\pi(i) > \pi(j)$.

Определение 1.6. Четность числа неправильных пар для перестановки π называется *четностью перестановки π* .

Рассмотрим каноническую запись перестановки π :

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ k_1 & k_2 & \dots & k_i & \dots & k_j & \dots & k_n \end{pmatrix}.$$

Скажем, что пара чисел (k_i, k_j) , записанных в том же порядке, в каком они расположены в строке $(k_1, k_2, \dots, k_i, \dots, k_j, \dots, k_n)$,

т.е. $i < j$, образует *инверсию* в этой строке, если $k_i > k_j$. Мы видим, что пара $\{i, j\}$ является неправильной для π , если и только если соответствующие элементы в нижней строке образуют инверсию. Таким образом, мы получаем

Предложение 1.7. *Четность перестановки π равна четности числа инверсий в нижней строке ее канонической записи.*

Покажем, что имеет место более общее утверждение:

Предложение 1.8. *Четность перестановки равна четности суммарного числа инверсий в верхней и нижней строках произвольной табличной записи этой перестановки.*

Доказательство. Пусть

$$\pi = \begin{pmatrix} i_1 & \dots & i_k & \dots & i_l & \dots & i_n \\ j_1 & \dots & j_k & \dots & j_l & \dots & j_n \end{pmatrix}.$$

Будем рассматривать всевозможные пары чисел из $[1, n]$, записывая их в том порядке, в котором они встречаются в верхней строке рассматриваемой записи π , и соответствующие пары чисел из нижней строки. Возможны три случая:

1. Обе пары (i_k, i_l) и (j_k, j_l) не образуют инверсий в своих строках, т.е. $i_k < i_l$ и $j_k < j_l$. Такие пары (i_k, i_l) являются правильными.
2. Обе пары (i_k, i_l) и (j_k, j_l) образуют инверсии в своих строках, т.е. $i_k > i_l$ и $j_k > j_l$. Такие пары (i_k, i_l) также являются правильными, но, если их число равно t , то мы получаем $2t$ инверсий в верхней и нижней строках.
3. Одна из пар (i_k, i_l) , (j_k, j_l) образует инверсию в своей строке, а другая нет, т.е. $i_k < i_l$ и $j_k > j_l$, или $i_k > i_l$ и $j_k < j_l$. В этом случае пара (i_k, i_l) является неправильной. Пусть число таких пар (i_k, i_l) равно s . Тогда мы имеем еще s инверсий в верхней и нижней строках.

Таким образом, число неправильных пар равно s , а суммарное число инверсий в верхней и нижней строках записи равно $s + 2t$, т.е. эти числа имеют одинаковую четность. \square

Из предложения 1.7 (или непосредственно из определения 1.6) мы видим, что тождественная перестановка является четной и что любая перестановка π и обратная к ней π^{-1} имеют одинаковую четность.

Предложение 1.9. *При умножении перестановок четности суммируются.*

Доказательство. Докажем это для произведения двух перестановок $\pi_1, \pi_2 \in S_n$ (тогда для произведения любого конечного числа перестановок доказательство сразу получается по индукции). Пусть

$$\pi_2 = \begin{pmatrix} i_1 & \dots & i_n \\ j_1 & \dots & j_n \end{pmatrix}.$$

Используем для π_1 запись, в которой верхняя строка совпадает с нижней строкой записи π_2 :

$$\pi_1 = \begin{pmatrix} j_1 & \dots & j_n \\ k_1 & \dots & k_n \end{pmatrix}.$$

Тогда

$$\pi_1\pi_2 = \begin{pmatrix} i_1 & \dots & i_n \\ k_1 & \dots & k_n \end{pmatrix}.$$

Пусть s, t, u обозначают число инверсий в строках (i_1, \dots, i_n) , (j_1, \dots, j_n) , (k_1, \dots, k_n) соответственно. Тогда четность π_1 равна четности числа $t + u$, четность π_2 равна четности числа $s + t$ и, наконец, четность $\pi_1\pi_2$ равна четности числа $s + u$, имеющего ту же четность, что и сумма $(s + t) + (t + u)$. \square

Определение 1.10. Пусть четность перестановки π равна четности некоторого числа t . Тогда число $s(\pi) = (-1)^t$ будем называть *знаком перестановки* π .

Предложение 1.9 можно переформулировать следующим образом:

Предложение 1.11. *Для любых перестановок $\pi_1, \dots, \pi_k \in S_n$*

$$s(\pi_1 \dots \pi_k) = s(\pi_1) \dots s(\pi_k).$$

Предложение 1.12. Любая транспозиция является нечетной перестановкой.

Доказательство. Определим четность суммарного числа инверсий в записи

$$(i, j) = \begin{pmatrix} i & j & i_1 & \dots & i_{n-2} \\ j & i & i_1 & \dots & i_{n-2} \end{pmatrix}.$$

Пары (i_k, i_l) , (i, i_l) , (j, i_l) расположены в верхней и нижней строках в одинаковом порядке, а потому те, которые образуют инверсии, дают в сумме четное число инверсий. В то же время из оставшихся пар (i, j) (в верхней строке) и (j, i) (в нижней строке) одна образует инверсию, а другая нет. Поэтому суммарное число инверсий нечетно. \square

Следствие 1.13. Четность перестановки совпадает с четностью числа множителей в любом представлении этой перестановки в виде произведения транспозиций.

Принимая во внимание предложение 1.4, получаем:

Следствие 1.14. Четность цикла длины k совпадает с четностью числа $k - 1$.

Следствие 1.15. Если перестановка π разлагается в произведение независимых циклов длин k_1, \dots, k_s , то ее четность совпадает с четностью числа $d(\pi) = \sum_{i=1}^s (k_i - 1)$ (называемого декрементом перестановки).

Предложение 1.16. Количество четных и нечетных перестановок в S_n одинаково и равно $n!/2$.

Доказательство. Пусть число четных перестановок равно N и $\{\pi_1, \pi_2, \dots, \pi_N\}$ — список всех четных перестановок. Пусть τ — некоторая нечетная перестановка (например, транспозиция). Тогда перестановки $\tau\pi_1, \tau\pi_2, \dots, \tau\pi_N$ нечетные. Они все разные, так как если бы $\tau\pi_i = \tau\pi_j$ для некоторых $i \neq j$, то, умножая это равенство слева на τ^{-1} , мы получили бы, что $\pi_i = \pi_j$. Наконец, всякая нечетная перестановка $\sigma \in S_n$ равна некоторой $\tau\pi_i$, $1 \leq i \leq N$. Действительно, $\tau^{-1}\sigma$ — четная перестановка, а потому $\tau^{-1}\sigma = \pi_i$ для некоторого i , откуда $\sigma = \tau\pi_i$.

Таким образом, $\{\tau\pi_1, \tau\pi_2, \dots, \tau\pi_N\}$ есть список всех нечетных перестановок в S_n и их число также равно N . Так как $2N = n!$, то $N = n!/2$. \square

- 1) все нулевые строки, если такие имеются, расположены в нижней части матрицы;
- 2) главный элемент каждой следующей ненулевой строки находится строго правее главного элемента предыдущей строки (*главным элементом* ненулевой строки мы называем ее первый ненулевой элемент).

Систему линейных уравнений с расширенной матрицей такого вида будем называть *ступенчатой*.

Теорема 2.1. Система линейных уравнений (2.1) совместна в том и только том случае, если в эквивалентной ей ступенчатой системе нет “экзотических” уравнений вида

$$0x_1 + \dots + 0x_n = b, \quad b \neq 0$$

(другими словами, в расширенной матрице ступенчатой системы нет строк вида $(0, \dots, 0, b)$, $b \neq 0$).

В случае совместной системы неизвестные разделяются на *главные* и *свободные*. Главными считаются те неизвестные, которые в эквивалентной ступенчатой системе встречаются с коэффициентами, являющимися главными элементами ненулевых строк ступенчатой матрицы. Число главных неизвестных равно числу ненулевых строк. Остальные неизвестные считаются свободными. Каждому набору значений свободных неизвестных соответствует единственный набор значений главных неизвестных, дающий решение системы.

Теорема 2.2. Совместимая система линейных уравнений является определенной в том и только том случае, если все неизвестные являются главными (другими словами, число неизвестных равно числу ненулевых строк в ступенчатом виде).

С помощью элементарных преобразований I типа можно привести матрицу к еще более специальному виду, который будем называть *сильно ступенчатым*. Ступенчатая матрица называется *сильно ступенчатой*, если в ней над всеми главными элементами стоят только нули. В системе линейных уравнений с сильно ступенчатой расширенной матрицей каждое (ненулевое) уравнение содержит только одно главное неизвестное.

2.2. Ступенчатый вид квадратной матрицы

Квадратная матрица $A = (a_{ij})$ называется (*верхней*) *треугольной*, если в ней все элементы под главной диагональю равны нулю (т.е. $a_{ij} = 0$ при $i > j$). Будем называть такую матрицу *строго треугольной*, если все ее диагональные элементы a_{ii} отличны от нуля.

Предложение 2.3. *Ступенчатая квадратная матрица является треугольной, причем если в одной из ненулевых строк главный элемент расположен правее главной диагонали, то и во всех следующих ненулевых строках главные элементы находятся правее главной диагонали.*

Доказательство. Нам нужно показать, что в ступенчатой квадратной матрице все главные элементы ненулевых строк расположены на или правее главной диагонали. Доказываем это индукцией по номеру строки. Для первой строки это очевидно. Предположим, что утверждение доказано для первых k строк. Тогда для главного элемента a_{kj_k} k -й строки имеем: $j_k \geq k$. Так как главный элемент $a_{k+1, j_{k+1}}$ $k+1$ -й строки (если она ненулевая) стоит строго правее a_{k, j_k} , то $j_{k+1} > j_k$, а потому $j_{k+1} \geq k+1$. Если в k -й строке главный элемент находится строго правее главной диагонали, т.е. $j_k \geq k+1$, то $j_{k+1} \geq k+2$, т.е. и в следующей строке главный элемент также расположен правее главной диагонали. \square

Предложение 2.4. *Ступенчатый вид квадратной матрицы либо является строго треугольной матрицей, либо в нем последняя строка нулевая.*

Действительно, согласно предложению 2.3, ступенчатый вид является треугольной матрицей. Если она не оказывается строго треугольной, то начиная с некоторой строки на главной диагонали стоят нули, а потому последняя строка нулевая.

Учитывая, что при элементарных преобразованиях свойство определителя матрицы быть или не быть равным нулю сохраняется, мы получаем

Следствие 2.5. *Определитель матрицы равен нулю в том и только том случае, если в ее ступенчатом виде имеется*

Доказательство. Рассмотрим квадратную систему (2.2).

Пусть $|A| \neq 0$. Тогда согласно следствию 2.6 расширенную матрицу системы можно привести к виду

$$\left(\begin{array}{ccc|c} 1 & \dots & 0 & \tilde{b}_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & \tilde{b}_n \end{array} \right) \quad (2.3)$$

и, соответственно, ступенчатая система будет иметь вид

$$\begin{cases} x_1 = \tilde{b}_1, \\ \dots\dots\dots \\ x_n = \tilde{b}_n. \end{cases}$$

Следовательно, система (2.2) имеет единственное решение $(\tilde{b}_1, \dots, \tilde{b}_n)$.

Пусть $|A| = 0$. Тогда согласно следствию 2.5 расширенная матрица системы приводится к виду, в котором матрица коэффициентов имеет хотя бы одну нулевую строку. Поэтому система (2.2) либо несовместна (если в ступенчатой системе имеется “экзотическое” уравнение), либо совместна, но неопределена, поскольку число главных неизвестных меньше n . \square

Следствие 2.8. *Однородная квадратная система линейных уравнений имеет ненулевое решение в том и только том случае, если определитель ее матрицы равен нулю.*

Доказательство. Действительно, однородная система всегда совместна и наличие ненулевого решения означает, что она неопределена. Согласно теореме Крамера, это имеет место в том и только том случае, если определитель матрицы равен нулю. \square

Теорема 2.9 (формулы Крамера). *Пусть определитель матрицы A квадратной системы (2.2) не равен 0. Введем вспомогательные матрицы*

$$A_i = \begin{pmatrix} a_{11} & \dots & a_{1,i-1} & b_1 & a_{1,i+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,i-1} & b_n & a_{n,i+1} & \dots & a_{nn} \end{pmatrix},$$

где $i = 1, \dots, n$. Тогда единственное решение системы (2.2) задается формулами:

$$x_1 = \frac{|A_1|}{|A|}, \dots, x_n = \frac{|A_n|}{|A|}.$$

Доказательство. Если над строками расширенной матрицы произвести одно элементарное преобразование и для преобразованной расширенной матрицы рассмотреть соответствующие матрицы A', A'_1, \dots, A'_n , то либо (при преобразовании I типа) все определители не изменяются: $|A'| = |A|$, $|A'_i| = |A_i|$, либо все определители умножаются на одно и то же число: $|A'| = c|A|$, $|A'_i| = c|A_i|$, где $c = -1$ при преобразовании II типа и c — некоторое ненулевое число при преобразовании III типа. Поэтому при любом элементарном преобразовании отношения $\frac{|A_i|}{|A|}$ не изменяются. С помощью последовательности элементарных преобразований приведем расширенную матрицу системы к виду (2.3). Тогда решением системы (2.2) будет $x_1 = (\tilde{b}_1, \dots, \tilde{b}_n)$. С другой стороны, теперь матрица коэффициентов есть единичная матрица E , а вспомогательные матрицы \tilde{A}_i имеют вид

$$\tilde{A}_i = \begin{pmatrix} 1 & \dots & 0 & \tilde{b}_1 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \tilde{b}_{i-1} & 0 & \dots & 0 \\ 0 & \dots & 0 & \tilde{b}_i & 0 & \dots & 0 \\ 0 & \dots & 0 & \tilde{b}_{i+1} & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \tilde{b}_n & 0 & \dots & 1 \end{pmatrix}.$$

Непосредственно из определения определителя получаем $|\tilde{A}_i| = \tilde{b}_i$. Следовательно, для всякого $i = 1, \dots, n$

$$\frac{|A_i|}{|A|} = \frac{|\tilde{A}_i|}{|E|} = \tilde{b}_i.$$

□

2.4. Другое доказательство теоремы и формул Крамера, не использующее приведение матрицы к ступенчатому виду

Лемма 2.10. Пусть дана однородная система из r уравнений с $r+1$ неизвестным и матрицей коэффициентов B размера $r \times (r+1)$. Обозначим через M_j , $j = 1, \dots, r+1$, минор матрицы B , получаемый вычеркиванием j -го столбца. Тогда набор (x_1, \dots, x_r) , где $x_j = (-1)^{j-1} M_j$, является решением данной системы.

Доказательство. Результат подстановки этих значений неизвестных в i -е уравнение $\sum_{j=1}^{r+1} (-1)^{j-1} a_{ij} M_j$ равен нулю, так как левая часть представляет собой разложение по 1-й строке определителя матрицы порядка $r+1$, полученной из матрицы B добавлением в качестве первой строки ее i -й строки. \square

Предложение 2.11. Пусть дана произвольная однородная система линейных уравнений с матрицей коэффициентов A , и пусть M — некоторый минор порядка r матрицы A , такой что $M \neq 0$, а всякий минор порядка $r+1$, получаемый добавлением к M одной строки и одного столбца (такие миноры называют окаймляющими) равен нулю. Если число неизвестных n больше r , то система имеет ненулевое решение.

Доказательство. Переставляя уравнения и изменяя нумерацию неизвестных, можем считать, что минор M находится в нижнем левом углу матрицы A . Пусть B — матрица размера $r \times (r+1)$, составленная из элементов последних r строк и первых $r+1$ столбцов матрицы A . Обозначим через M_j , $j = 1, \dots, r+1$, минор матрицы B , полученный вычеркиванием j -го столбца. Покажем, что

$$x_j = (-1)^{j-1} M_j, \quad j = 1, \dots, r+1,$$

$$x_{r+2} = \dots = x_n = 0$$

§3. Базис и ранг системы векторов

3.1. Напоминание о линейной зависимости системы векторов

Под *системой векторов* (столбцов или строк) понимается индексированная совокупность векторов, т.е. система может содержать равные между собой векторы, которые считаются разными элементами системы, если наделены разными индексами. Всякое множество векторов может рассматриваться как система векторов; в этом случае множество индексов находится в биективном соответствии с рассматриваемым множеством векторов. В частности, допускается к рассмотрению пустое множество векторов (с пустым множеством индексов).

Мы будем рассматривать, как правило, системы векторов-столбцов из пространства \mathbb{R}^n . Разумеется, все сказанное в равной степени можно отнести также к системам векторов-строк.

Пусть дана конечная система векторов $\mathbf{a} = (a_1, \dots, a_s)$. *Линейная комбинация* $\lambda_1 a_1 + \dots + \lambda_s a_s$ называется *нетривиальной*, если хотя бы один из коэффициентов $\lambda_i \in \mathbb{R}$ отличен от нуля. В противном случае линейная комбинация называется *тривиальной*. Тривиальная линейная комбинация любой конечной системы векторов равна нулю (т.е. нулевому вектору).

Определение 3.1. Конечная система векторов называется *линейно независимой*, если только тривиальная линейная комбинация этой системы равна нулю. Конечная система векторов называется *линейно зависимой*, если существует нетривиальная линейная комбинация этой системы, которая равна нулю.

Таким образом, если дана система векторов $\mathbf{a} = (a_1, \dots, a_s)$, то эта система линейно зависима, если существуют числа $\lambda_1, \dots, \lambda_s \in \mathbb{R}$, не все равные нулю, такие что

$\lambda_1 a_1 + \dots + \lambda_s a_s = 0$. Система \mathbf{a} линейно независима, если из того, что для какого-то набора коэффициентов $\lambda_1, \dots, \lambda_s \in \mathbb{R}$ линейная комбинация $\lambda_1 a_1 + \dots + \lambda_s a_s = 0$ следует, что все числа $\lambda_1, \dots, \lambda_s$ равны 0.

В соответствии с этим определением пустая система векторов линейно независима. Для единообразия формулировок удобно считать, что пустая система векторов обладает тривиальной линейной комбинацией, которая (как всякая тривиальная линейная комбинация) равна 0.

Говорят, что вектор $b \in \mathbb{R}^n$ *линейно выражается* через систему векторов $\mathbf{a} \subset \mathbb{R}^n$, если b представляется как линейная комбинация некоторой конечной подсистемы векторов из \mathbf{a} .

То, что вектор b представляется в виде линейной комбинации

$$\lambda_1 a_1 + \dots + \lambda_s a_s = b,$$

означает что набор $(\lambda_1, \dots, \lambda_s)$ является решением системы линейных уравнений, в которой столбцами матрицы коэффициентов служат векторы a_1, \dots, a_s , а столбцом свободных членов — вектор b . Таким образом, вектор b линейно выражается через систему a_1, \dots, a_s в том и только том случае, если указанная система линейных уравнений совместна.

Для краткости всякое равенство вида

$$\lambda_1 a_1 + \dots + \lambda_s a_s = 0$$

мы будем называть *линейным соотношением* между векторами системы (a_1, \dots, a_s) с коэффициентами $\lambda_1, \dots, \lambda_s$. Естественно, различаются *тривиальное* и *нетривиальные* линейные соотношения. На этом языке можно сказать, что линейно зависимая система — это система, которая обладает нетривиальными линейными соотношениями, а линейно независимая система — это система, для которой имеется только тривиальное линейное соотношение. Наборы коэффициентов для линейных соотношений между векторами (a_1, \dots, a_s) — это в точности решения однородной системы линейных уравнений, столбцами матрицы которой служат векторы a_1, \dots, a_s . Таким образом, система (a_1, \dots, a_s) линейно зависима в том и только том случае, если указанная однородная система линейных уравнений име-

ет ненулевое решение. В частности мы получаем следующую теорему:

Теорема 3.2 (критерий равенства определителя нулю). *Для квадратной матрицы A следующие условия равносильны:*

1. $\det A = 0$;
2. система столбцов матрицы A линейно зависима;
3. система строк матрицы A линейно зависима.

Доказательство. Действительно, согласно следствию 2.8 теоремы Крамера, условие $\det A = 0$ равносильно тому, что однородная система линейных уравнений с матрицей A имеет ненулевое решение, а последнее условие, согласно предыдущему, равносильно тому, что система столбцов матрицы A линейно зависима. Равносильность условий 1) и 3) следует из равносильности условий 1) и 2) для транспонированной матрицы A^T . \square

Сформулируем ряд свойств понятия линейной зависимости векторов.

Предложение 3.3. *Система векторов (a_1, \dots, a_s) линейно зависима в том и только том случае, если хотя бы один из ее векторов линейно выражается через остальные.*

Предложение 3.4. *Любая подсистема линейно независимой системы линейно независима. Если некоторая подсистема данной конечной системы векторов линейно зависима, то и вся эта система линейно зависима.*

Пусть дана система n -мерных векторов (a_1, \dots, a_s) . Систему (a'_1, \dots, a'_s) $(n - r)$ -мерных векторов, которые получаются из векторов a_1, \dots, a_s вычеркиванием r компонент с одними и теми же номерами i_1, \dots, i_r , будем называть *укороченной* системой векторов.

Предложение 3.5. *Если данная система векторов линейно зависима, то и любая ее укороченная система линейно зависима. Если некоторая укороченная система линейно независима, то и данная система линейно независима.*

Так как по предположению число неизвестных r в этой системе больше числа уравнений s , то она имеет ненулевое решение. Следовательно, существует нетривиальное соотношение вида (3.1). \square

3.2. Базис системы векторов

Определение 3.8. *Базисом* системы векторов называется всякая ее конечная подсистема, которая линейно независима и через которую линейно выражается вся данная система.

В этом определении данная система векторов может быть конечной или бесконечной, в частности, может совпадать со всем пространством \mathbb{R}^n .

Теорема 3.9. *Все базисы данной системы векторов содержат одинаковое количество векторов. Число векторов в любой линейно независимой подсистеме данной системы векторов не превосходит числа векторов в ее базисе.*

Доказательство. Докажем сначала второе утверждение. Пусть (b_1, \dots, b_r) — линейно независимая подсистема данной системы векторов и (a_1, \dots, a_s) — некоторый ее базис. Тогда система (b_1, \dots, b_r) линейно выражается через (a_1, \dots, a_s) и согласно основной лемме о линейной зависимости $r \leq s$. Если теперь (a_1, \dots, a_r) и (a'_1, \dots, a'_s) — два базиса данной системы векторов, то согласно предыдущему $r \leq s$ и $s \leq r$. Следовательно, $r = s$. \square

Определение 3.10. Конечная подсистема векторов данной системы векторов называется *максимальной линейно независимой* подсистемой, если она линейно независима и ее нельзя включить ни в какую строго большую линейно независимую подсистему данной системы, т.е. если при добавлении к ней хотя бы одного произвольного вектора из данной системы получается линейно зависимая подсистема.

Предложение 3.11. *Конечная подсистема данной системы векторов является ее базисом в том и только том случае, если она представляет собой максимальную линейно независимую подсистему.*

Доказательство. Так как любой вектор данной системы линейно выражается через базис, то при добавлении к базису любого вектора системы получается линейно зависимая подсистема. Поэтому базис является максимальной линейно независимой подсистемой.

Обратно, пусть (a_1, \dots, a_r) — максимальная линейно независимая подсистема и b — произвольный вектор из данной системы. Если $b \in \{a_1, \dots, a_r\}$, то b линейно выражается через (a_1, \dots, a_r) . Если $b \notin \{a_1, \dots, a_r\}$, то (a_1, \dots, a_r, b) — линейно зависимая подсистема и согласно предложению 3.6 вектор b линейно выражается через (a_1, \dots, a_r) . Следовательно, (a_1, \dots, a_r) — базис данной системы векторов. \square

Замечание 3.12. Максимальность линейно независимой подсистемы можно понимать в двух разных по своему содержанию смыслах: 1) согласно данному выше определению максимальность понимается *по включению*: нельзя включить в строго большую линейно независимую подсистему; 2) *максимальность по количеству* векторов в подсистеме. Ясно, что максимальная по количеству векторов линейно независимая подсистема является максимальной и по включению. Однако, в данном случае верно и обратное, поскольку всякая максимальная по включению линейно независимая подсистема является базисом и, согласно теореме 3.9 содержит максимальное возможное число векторов.

Пример 3.13 (очень важный). Рассмотрим в качестве системы векторов все пространство \mathbb{R}^n и в нем следующую подсистему:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Предложение 3.14. Система (e_1, \dots, e_n) является базисом пространства \mathbb{R}^n .

Доказательство. Всякий вектор

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$$

представляется в виде линейной комбинации системы (e_1, \dots, e_n) :

$$x = x_1 e_1 + \dots + x_n e_n$$

(коэффициентами в этой линейной комбинации служат компоненты вектора x).

Система (e_1, \dots, e_n) линейно независима, так как если некоторая их линейная комбинация равна нулю:

$$\lambda_1 e_1 + \dots + \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

то все коэффициенты равны нулю: $\lambda_1 = \dots = \lambda_n = 0$. □

Этот базис (e_1, \dots, e_n) мы будем называть *стандартным базисом* пространства \mathbb{R}^n .

Из этого примера, применяя теорему 3.9, мы получаем

Предложение 3.15. Всякая линейно независимая система векторов в \mathbb{R}^n содержит не более чем n векторов.

Пример 3.16 (тривиальный). Если система векторов пустая или если все ее векторы равны нулю, то базисом такой системы является пустая подсистема. Действительно, пустая система векторов линейно независима и нулевой вектор, в соответствии с принятым соглашением, представляется как (тривиальная) линейная комбинация пустой системы векторов.

Теорема 3.17. Любая система векторов в \mathbb{R}^n обладает базисом. Более того, любую линейно независимую подсистему данной системы векторов можно дополнить до базиса всей системы.

Доказательство. Достаточно доказать второе утверждение, поскольку всякая система векторов содержит линейно независимую подсистему (например, пустую). Пусть \mathbf{a} — произвольная система векторов в \mathbb{R}^n и задана некоторая ее линейно независимая подсистема (a_1, \dots, a_k) . Если эта подсистема еще не является максимальной, то найдется вектор $a_{k+1} \in \mathbf{a}$ такой, что подсистема $(a_1, \dots, a_k, a_{k+1})$ линейно независима. Продолжая эту процедуру, мы, поскольку любая линейно независимая система векторов в \mathbb{R}^n содержит не более чем n векторов, после конечного числа шагов получим максимальную линейно независимую подсистему в \mathbf{a} , т.е. базис. \square

Дадим еще одну характеристику базиса системы векторов.

Предложение 3.18. *Конечная подсистема (a_1, \dots, a_r) системы векторов \mathbf{a} является ее базисом в том и только в том случае, если всякий вектор из \mathbf{a} единственным образом линейно выражается через (a_1, \dots, a_r) .*

Единственность означает, что если для некоторого вектора b получены два представления в виде линейной комбинации

$$\begin{aligned} b &= \beta_1 a_1 + \dots + \beta_r a_r, \\ b &= \beta'_1 a_1 + \dots + \beta'_r a_r, \end{aligned} \tag{3.2}$$

то все коэффициенты в этих линейных комбинациях совпадают: $\beta_1 = \beta'_1, \dots, \beta_r = \beta'_r$.

Доказательство. Пусть (a_1, \dots, a_r) — базис и допустим, что для некоторого вектора $b \in \mathbf{a}$ имеются два представления (3.2). Вычитая эти равенства почленно, получаем:

$$(\beta_1 - \beta'_1)a_1 + \dots + (\beta_r - \beta'_r)a_r = 0.$$

Так как система a_1, \dots, a_r линейно независима, то

$$\beta_1 - \beta'_1 = \dots = \beta_r - \beta'_r = 0,$$

т.е. представление любого вектора $b \in \mathbf{a}$ единственно.

Обратно, предположим, что векторы из \mathbf{a} единственным образом линейно выражаются через (a_1, \dots, a_r) . Чтобы установить, что подсистема (a_1, \dots, a_r) является базисом, нужно показать, что она линейно независима. Допустим, что имеется некоторое линейное соотношение

$$\lambda_1 a_1 + \dots + \lambda_s a_s = 0, \quad (3.3)$$

и рассмотрим представление некоторого вектора $b \in \mathbf{a}$ в виде

$$\beta_1 a_1 + \dots + \beta_r a_r = b. \quad (3.4)$$

Складывая почленно равенства (3.3) и (3.4), получаем

$$(\lambda_1 + \beta_1) a_1 + \dots + (\lambda_r + \beta_r) a_r = b. \quad (3.5)$$

В силу единственности линейного выражения для вектора b из (3.4) и (3.5) следует, что

$$\beta_1 = \beta_1 + \lambda_1, \dots, \beta_r = \beta_r + \lambda_r,$$

откуда $\lambda_1 = \dots = \lambda_r = 0$. Таким образом, подсистема (a_1, \dots, a_r) линейно независима и, следовательно, является базисом системы \mathbf{a} . \square

Однозначно определенные коэффициенты линейного выражения вектора через данный базис называются его *координатами* относительно этого базиса.

3.3. Алгоритм нахождения некоторого базиса конечной системы векторов

Пусть задана система из s n -мерных векторов-столбцов; составив из этих столбцов матрицу A размером $n \times s$, мы можем далее считать, что нам надо найти базис системы столбцов матрицы A , которые мы будем обозначать через A_1, \dots, A_s . Пусть матрица A' получена из матрицы A элементарными преобразованиями над строками. Столбцы матрицы A' будем обозначать через A'_1, \dots, A'_s .

Предложение 3.19. Для любого набора номеров j_1, \dots, j_k , $1 \leq k \leq s$, наборы коэффициентов для линейных соотношений между столбцами A_{j_1}, \dots, A_{j_k} и столбцами $A'_{j_1}, \dots, A'_{j_k}$ совпадают, т.е.

$$\lambda_1 A_{j_1} + \dots + \lambda_k A_{j_k} = 0 \iff \lambda_1 A'_{j_1} + \dots + \lambda_k A'_{j_k} = 0.$$

В частности, система $(A_{j_1}, \dots, A_{j_k})$ линейно зависима (соответственно линейно независима, является базисом системы столбцов матрицы A), если и только если система $(A'_{j_1}, \dots, A'_{j_k})$ линейно зависима (соответственно линейно независима, является базисом системы столбцов матрицы A'). Столбец $A_{j_{k+1}}$ линейно выражается через столбцы A_{j_1}, \dots, A_{j_k} с коэффициентами $\alpha_1, \dots, \alpha_k$ в том и только в том случае, если столбец $A'_{j_{k+1}}$ линейно выражается через столбцы $A'_{j_1}, \dots, A'_{j_k}$ с теми же коэффициентами.

Доказательство. Множества наборов коэффициентов для линейных соотношений между A_{j_1}, \dots, A_{j_k} и между $A'_{j_1}, \dots, A'_{j_k}$ являются множествами решений однородных систем линейных уравнений с матрицами, составленными соответственно из столбцов A_{j_1}, \dots, A_{j_k} и $A'_{j_1}, \dots, A'_{j_k}$. Так как эти матрицы получаются друг из друга элементарными преобразованиями над строками, то эти системы линейных уравнений эквивалентны и множества их решений совпадают. Аналогично, наборы коэффициентов $\alpha_1, \dots, \alpha_k$ для линейного выражения $A_{j_{k+1}}$ через A_{j_1}, \dots, A_{j_k} (соответственно $A'_{j_{k+1}}$ через $A'_{j_1}, \dots, A'_{j_k}$) являются решениями систем линейных уравнений с расширенными матрицами, составленными из столбцов $A_{j_1}, \dots, A_{j_k}, A_{j_{k+1}}$ и соответственно из $A'_{j_1}, \dots, A'_{j_k}, A'_{j_{k+1}}$. Эти системы линейных уравнений эквивалентны: множества их решений совпадают. \square

Алгоритм 3.20. Приведем матрицу A элементарными преобразованиями над строками к сильно ступенчатому виду, а затем разделим ненулевые строки на их главные элементы. По-

лучим матрицу вида

$$A' = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots \\ 0 & 1 & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Пусть число ненулевых строк этой матрицы равно r и j_1, \dots, j_r — номера столбцов, в которых стоят главные элементы ненулевых строк. Отбрасывая последние $n - r$ нулевых компонент столбцов, которые ни на что не влияют, мы можем рассматривать столбцы матрицы A' как r -мерные векторы. Столбцы с номерами j_1, \dots, j_r имеют вид

$$A'_{j_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad A'_{j_2} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad A'_{j_r} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

т.е. составляют стандартный базис пространства r -мерных столбцов. Следовательно, они образуют также базис системы столбцов матрицы A' и j -й столбец матрицы A'

$$A'_j = \begin{pmatrix} a'_{1j} \\ a'_{2j} \\ \vdots \\ a'_{rj} \end{pmatrix}$$

линейно выражается через этот базис с коэффициентами $a'_{1j}, a'_{2j}, \dots, a'_{rj}$:

$$A'_j = a'_{1j}A'_{j_1} + a'_{2j}A'_{j_2} + \dots + a'_{rj}A'_{j_r}.$$

Возвращаясь к данной матрице, мы получаем, что ее столбцы с теми же номерами A_{j_1}, \dots, A_{j_r} образуют базис ее системы столбцов и j -й столбец A_j матрицы A линейно выражается через этот базис с теми же коэффициентами:

$$A_j = a'_{1j}A_{j_1} + a'_{2j}A_{j_2} + \dots + a'_{rj}A_{j_r}.$$

Замечание 3.21. Базис, который находит этот алгоритм, зависит от нумерации векторов в системе: на каждом шаге построения максимальной линейно независимой подсистемы он выбирает вектор с наименьшим возможным номером.

3.4. Ранг системы векторов

Определение 3.22. Рангом системы векторов называется число векторов в любом базисе этой системы.

Ранг системы векторов \mathbf{a} обозначается через $\text{rk}(\mathbf{a})$. Следующее предложение очевидно:

Предложение 3.23. Ранг любой системы векторов не превосходит числа векторов в системе. Ранг равен числу векторов системы, если и только если система линейно независима. Ранг системы равен 0, если и только если система пустая или все ее векторы равны нулю.

Предложение 3.24. Если система \mathbf{b} линейно выражается через систему \mathbf{a} , то $\text{rk}(\mathbf{b}) \leq \text{rk}(\mathbf{a})$

Доказательство. Пусть $\text{rk}(\mathbf{a}) = s$, $\text{rk}(\mathbf{b}) = r$, (a_1, \dots, a_s) — базис системы \mathbf{a} , (b_1, \dots, b_r) — базис системы \mathbf{b} . Тогда система (b_1, \dots, b_r) линейно выражается через систему (a_1, \dots, a_s) и, согласно основной лемме о линейной зависимости (теорема 3.7), $r \leq s$. \square

Две системы векторов в \mathbb{R}^n называются *эквивалентными*, если каждая из них линейно выражается через другую. Например, всякая система векторов эквивалентна любому своему базису. Из предположения 3.24 получаем

Предложение 3.25. Эквивалентные системы векторов имеют одинаковый ранг.

Обратное, разумеется, неверно. Однако имеет место

Предложение 3.26. Если система векторов \mathbf{b} линейно выражается через систему \mathbf{a} (в частности, если \mathbf{b} содержится в \mathbf{a}) и $\text{rk}(\mathbf{a}) = \text{rk}(\mathbf{b})$, то системы \mathbf{a} и \mathbf{b} эквивалентны.

Доказательство. Пусть $r = \text{rk}(\mathbf{a}) = \text{rk}(\mathbf{b})$. Рассмотрим систему $\mathbf{c} = \mathbf{a} \cup \mathbf{b}$. Системы \mathbf{a} , \mathbf{c} эквивалентны, а потому $\text{rk}(\mathbf{c}) = \text{rk}(\mathbf{a}) = r$. Пусть (b_1, \dots, b_r) — базис системы \mathbf{b} . Так как $\text{rk}(\mathbf{c}) = r$, то (b_1, \dots, b_r) — максимальная линейно независимая подсистема в \mathbf{c} , т.е. базис системы \mathbf{c} . Таким образом, каждый вектор системы \mathbf{c} , в том числе каждый вектор системы \mathbf{a} , линейно выражается через векторы b_1, \dots, b_r и, следовательно, системы \mathbf{a} и \mathbf{b} эквивалентны. \square

Ранг системы векторов обладает свойством максимальности: он равен наибольшему числу векторов в линейно независимых подсистемах рассматриваемой системы. Следующее предложение дает некоторое свойство минимальности ранга:

Предложение 3.27. *Ранг системы векторов $\mathbf{a} \subset \mathbb{R}^n$ равен наименьшему числу векторов в подсистемах пространства \mathbb{R}^n , через которые система \mathbf{a} линейно выражается.*

Доказательство. Пусть $\text{rk}(\mathbf{a}) = r$. С одной стороны, система \mathbf{a} линейно выражается через свой базис, который содержит r векторов. С другой стороны, если система \mathbf{a} линейно выражается через какую-то систему векторов $(b_1, \dots, b_s) \subset \mathbb{R}^n$, содержащую s векторов, то, согласно предложениям 3.23 и 3.24, $r \leq s$. Таким образом, систему \mathbf{a} можно линейно выразить через r векторов и нельзя линейно выразить через меньшее число векторов. \square

3.5. Подпространства в \mathbb{R}^n

Определение 3.28. Подмножество $L \subset \mathbb{R}^n$ называется *подпространством*, если оно удовлетворяет следующим условиям:

- 1) $L \neq \emptyset$;
- 2) если $a, b \in L$, то $a + b \in L$;
- 3) если $a \in L$, то $\lambda a \in L \quad \forall \lambda \in \mathbb{R}$.

Всякое подпространство содержит нулевой вектор, так как, взяв в условии 3) $\lambda = 0$, получаем: $0 = 0a \in L$. Можно дать эквивалентное определение: подпространством называется такое подмножество $L \in \mathbb{R}^n$, которое вместе с каждой своей подсистемой $a_1, \dots, a_s \in L$ содержит любую ее линейную комбинацию. Тривиальными примерами подпространств служат все пространство \mathbb{R}^n и нулевое подпространство, состоящее только из нулевого вектора. Известные свойства множеств решений однородных систем линейных уравнений означают в точности, что такие множества являются подпространствами. Обратное, если множество решений системы линейных уравнений представляет собой подпространство, то эта система однородная (так как нулевой вектор является решением).

Определение 3.29. *Линейной оболочкой системы векторов $\mathbf{a} \subseteq \mathbb{R}^n$ называется множество всех тех векторов из \mathbb{R}^n , которые представляются в виде линейных комбинаций векторов из \mathbf{a} . Линейная оболочка системы \mathbf{a} обозначается через $\langle \mathbf{a} \rangle$. Если \mathbf{a} — конечная система (a_1, \dots, a_s) , то ее линейная оболочка обозначается через $\langle a_1, \dots, a_s \rangle$ и состоит из всевозможных линейных комбинаций $\lambda_1 a_1 + \dots + \lambda_s a_s$. В следующем предложении собран ряд утверждений, каждое из которых непосредственно вытекает из соответствующих определений.*

Предложение 3.30. *а) Линейная оболочка любой системы векторов является подпространством.*

б) Всякое подпространство является линейной оболочкой любого своего базиса.

в) Все векторы системы \mathbf{a} содержатся в ее линейной оболочке $\langle \mathbf{a} \rangle$.

(Если все векторы системы \mathbf{a} содержатся в подпространстве L , то $\langle \mathbf{a} \rangle \subseteq L$; следовательно, линейная оболочка — это наименьшее подпространство, содержащее все векторы рассматриваемой системы.)

г) Условие, что система \mathbf{b} линейно выражается через систему \mathbf{a} , равносильно тому, что $\langle \mathbf{b} \rangle \subseteq \langle \mathbf{a} \rangle$.

д) Две системы векторов эквивалентны в том и только том случае, если их линейные оболочки совпадают.

Если система векторов представляет собой подпространство, то вместо термина “ранг подпространства” принято употреблять термин *размерность подпространства*. Размерность подпространства L обозначается через $\dim L$. Как было установлено (предложение 3.14), $\dim \mathbb{R}^n = n$. Поскольку, по определению линейной оболочки, любая систему векторов эквивалентна своей линейной оболочке, получаем

Предложение 3.31. Для всякой системы векторов $\mathbf{a} \subseteq \mathbb{R}^n$

$$\dim \langle \mathbf{a} \rangle = \text{rk}(\mathbf{a}).$$

3.6. Базис и размерность подпространства решений однородной системы линейных уравнений

Пусть дана однородная система линейных уравнений с n неизвестными x_1, \dots, x_n . Обозначим через L ее подпространство решений. Если система имеет только нулевое решение, т.е. $L = 0$, то базисом L является пустая система векторов. Если система имеет ненулевые решения, то неизвестные разделяются на главные и свободные и каждому набору значений свободных неизвестных соответствует единственное решение системы. Для упрощения обозначений будем считать, что главными неизвестными являются x_1, \dots, x_r (их число r равно, как мы знаем, числу ненулевых строк в ступенчатом виде матрицы системы), а x_{r+1}, \dots, x_n — свободные неизвестные (их число равно $n - r$). Мы хотим построить базис подпространства решений L , т.е. набор решений, который линейно независим и через который выражаются все решения системы. Для этого придаем значения свободным неизвестным так, как это указано в таблице ниже, находим значения главных неизвестных и записываем получившиеся решения в виде векторов-строк:

$$\begin{array}{l} U_1 = \\ U_2 = \\ \dots \\ U_{n-r} = \end{array} \left(\begin{array}{cccccccc} x_1 & \dots & x_r & x_{r+1} & x_{r+2} & \dots & x_n \\ a_{11} & \dots & a_{1r} & 1 & 0 & \dots & 0 \\ a_{21} & \dots & a_{2r} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n-r,1} & \dots & a_{n-r,r} & 0 & 0 & \dots & 1 \end{array} \right)$$

Предложение 3.32. Система решений

$$(u_1, \dots, u_{n-r})$$

является базисом подпространства решений. Размерность подпространства решений равна $n-r$, где n — число неизвестных, r — число ненулевых строк в ступенчатом виде матрицы системы.

Доказательство. Система строк (u_1, \dots, u_{n-r}) линейно независима, поскольку укороченная система, в которой строки составлены из значений свободных неизвестных (см. предложение 3.5), является линейно независимой. Покажем, что любое решение линейно выражается через систему (u_1, \dots, u_{n-r}) . Пусть $u \in L$ — любое решение, $u = (a_1, \dots, a_r, a_{r+1}, a_{r+2}, \dots, a_n)$. Так как множество решений L — подпространство, то вектор $u' = a_{r+1}u_1 + a_{r+2}u_2 + \dots + a_n u_{n-r}$ также является решением. Мы видим, что в u' свободные неизвестные принимают те же значения, что и в решении u . Но такие два решения должны совпадать, т.е. $u = u'$ представляется как линейная комбинация построенной системы решений. Следовательно, (u_1, \dots, u_{n-r}) — базис L и $\dim L = n - r$. \square

Замечание 3.33. Такое же рассуждение показывает, что базисом подпространства решений служит любая система решений, для которой укороченная система, составленная из значений свободных неизвестных, является базисом в пространстве всех $(n - r)$ -мерных векторов.

Базис подпространства решений однородной системы линейных уравнений принято также называть *фундаментальной системой решений* этой системы уравнений. Подчеркнем, что это понятие вводится только для однородных линейных систем.

§4. Операции над матрицами

4.1. Сложение матриц и умножение на скаляр

Сложение определено только для матриц одинакового размера. Если $A = (a_{ij})$ и $B = (b_{ij})$ — две матрицы размера $m \times n$, то их *сумма* $A + B$, по определению, есть матрица, в которой на пересечении i -ой строки и j -го столбца находится элемент $a_{ij} + b_{ij}$, т.е. $A + B = (a_{ij} + b_{ij})$. *Произведение* λA *матрицы* $A = (a_{ij})$ *на скаляр* $\lambda \in \mathbb{R}$ есть, по определению, матрица, в которой на пересечении i -ой строки и j -го столбца находится элемент λa_{ij} , т.е. $\lambda A = (\lambda a_{ij})$. Таким образом, на множестве $M_{m \times n}(\mathbb{R})$ всех матриц размера $m \times n$ определены две операции: внутренняя — сложение и внешняя — умножение на скаляр. Непосредственно из определения этих операций видно, что они обладают следующими свойствами:

- 1) $(A + B) + C = A + (B + C) \quad \forall A, B, C \in M_{m \times n}(\mathbb{R});$
- 2) $\exists 0 \in M_{m \times n}(\mathbb{R}) : \quad \forall A \in M_{m \times n}(\mathbb{R}) \quad 0 + A = A + 0 = A$
(0 — это матрица, у которой все элементы равны 0);
- 3) $\forall A \in M_{m \times n}(\mathbb{R}) \quad \exists -A \in M_{m \times n}(\mathbb{R}) :$
 $A + (-A) = (-A) + A = 0$
(если $A = (a_{ij})$, то $-A$ есть матрица $(-a_{ij})$);
- 4) $A + B = B + A \quad \forall A, B \in M_{m \times n}(\mathbb{R});$
- 5) $\lambda(A + B) = \lambda A + \lambda B \quad \forall A, B \in M_{m \times n}(\mathbb{R}), \lambda \in \mathbb{R}$
- 6) $(\lambda + \mu)A = \lambda A + \mu A \quad \forall A \in M_{m \times n}(\mathbb{R}), \lambda, \mu \in \mathbb{R};$
- 7) $(\lambda\mu)A = \lambda(\mu A) \quad \forall A \in M_{m \times n}(\mathbb{R}), \lambda, \mu \in \mathbb{R};$
- 8) $1A = A \quad \forall A \in M_{m \times n}(\mathbb{R}).$

Из этих восьми основных свойств или непосредственно из определения можно вывести также следующие свойства:

$$0A = 0 \quad \forall A \in M_{m \times n}(\mathbb{R})$$

(слева 0 — скаляр, справа 0 — матрица);

$$\lambda 0 = 0 \quad \forall \lambda \in \mathbb{R} \quad (0 \text{ справа и слева это матрица});$$

$$-(\lambda A) = (-\lambda)A \quad \forall A \in M_{m \times n}(\mathbb{R}), \lambda \in \mathbb{R}.$$

Введя, как обычно, операцию *вычитания матриц*

$$A - B = A + (-B),$$

будем иметь следующие свойства:

$$\lambda(A - B) = \lambda A - \lambda B \quad \forall A, B \in M_{m \times n}(\mathbb{R}), \lambda \in \mathbb{R};$$

$$(\lambda - \mu)A = \lambda A - \mu A \quad \forall A \in M_{m \times n}(\mathbb{R}), \lambda, \mu \in \mathbb{R}.$$

Отметим, что выполнение свойств 1)–4) означает, что множество $M_{m \times n}(\mathbb{R})$ является *абелевой группой* относительно сложения.

Матрица, в которой на (i, j) -м месте стоит 1, а остальные элементы равны 0, обозначается через E_{ij} . Такие матрицы называются матричными единицами. Всякая матрица $A = (a_{ij})$ размера $m \times n$ однозначно представляется в виде линейной комбинации матричных единиц того же размера: $A = \sum_{i=1}^m \sum_{j=1}^n a_{ij} E_{ij}$.

4.2. Умножение матриц

Произведение AB определяется (при любых $p, n, q \geq 1$) для матриц A, B размера соответственно $p \times n$ и $n \times q$, т.е. когда число столбцов (длина строк) в первом множителе равно числу строк (длине столбцов) во втором множителе; произведение таких матриц представляет собой матрицу размера $p \times q$. Сначала рассмотрим частный случай, когда $p = q = 1$, т.е. определим произведение строки длины n на столбец длины n , которое будет представлять собой матрицу размера 1×1 , т.е. скаляр,

и поэтому будет называться также скалярным произведением строки на столбец (имеющих одинаковую длину):

$$(a_1, a_2, \dots, a_n) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1 b_1 + a_2 b_2 + \dots + a_n b_n.$$

Пусть теперь даны матрица $A = (a_{ik})$ размера $p \times n$ и $B = (b_{kj})$ размера $n \times q$. Матрицу A рассматриваем как систему строк $A^{(1)}, \dots, A^{(p)}$, а матрицу B как систему столбцов B_1, \dots, B_q . Их произведение AB есть матрица $C = (c_{ij})$ размера $p \times q$, элементами которой являются произведения всех строк матрицы A на все столбцы матрицы B :

$$c_{ij} = A^{(i)} B_j, \quad i = 1, \dots, p, \quad j = 1, \dots, q. \quad (4.1)$$

Поскольку $A^{(i)} = (a_{i1}, \dots, a_{in})$,

$$B_j = \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix},$$

то

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}, \quad i = 1, \dots, p, \quad j = 1, \dots, q. \quad (4.2)$$

Предложение 4.1. *Для матричных единиц надлежащего размера выполняются соотношения:*

$$\begin{aligned} E_{ik} E_{kj} &= E_{ij}, \\ E_{ik} E_{lj} &= 0 \quad \text{при } k \neq l. \end{aligned}$$

Предложение 4.2. *Умножение матриц связано со сложением матриц законами дистрибутивности (когда указанные сумма и произведение определены):*

$$A(B + C) = AB + AC, \quad (4.3)$$

$$(A + B)C = AC + BC. \quad (4.4)$$

Доказательство. Докажем, например, (4.3). Пусть $A = (a_{ik})$, $B = (b_{kj})$, $C = (c_{kj})$, $k = 1, \dots, n$. Тогда, согласно формуле (4.2), в матрице $A(B+C)$ на (i, j) -м месте находится элемент

$$\sum_{k=1}^n a_{ik}(b_{kj} + c_{kj}) = \sum_{k=1}^n a_{ik}b_{kj} + \sum_{k=1}^n a_{ik}c_{kj};$$

последняя сумма есть элемент, стоящий на (i, j) -м месте в матрице $AB + AC$. \square

Предложение 4.3. *Умножение матриц связано с умножением на скаляр соотношениями*

$$\lambda(AB) = (\lambda A)B = A(\lambda B) \quad \forall \lambda \in \mathbb{R}.$$

Эти соотношения проверяются непосредственно.

Предложение 4.4. *Умножение матриц ассоциативно, т.е. если для матриц A, B, C одно из произведений $(AB)C$ или $A(BC)$ определено, то определено и другое и имеет место равенство:*

$$(AB)C = A(BC). \quad (4.5)$$

Доказательство. Каждое из произведений в (4.5) определено в том и только том случае, если матрицы A, B, C имеют соответственно размеры вида $p \times m$, $m \times n$, $n \times q$; поэтому если определено одно произведение, то определено и другое.

Пусть $A = (a_{ij})$, $B = (b_{kl})$, $C = (c_{rs})$. Тогда $A = \sum_{i,j} a_{ij}E_{ij}$, $B = \sum_{k,l} b_{kl}E_{kl}$, $C = \sum_{r,s} c_{rs}E_{rs}$ (в каждом случае рассматриваются матричные единицы надлежащего размера). В силу свойств дистрибутивности и связи между произведением матриц и умножением на скаляр, имеем:

$$A(BC) = \sum_{i,j} \sum_{k,l} \sum_{r,s} a_{ij}b_{kl}c_{rs} E_{ij}(E_{kl}E_{rs}),$$

$$(AB)C = \sum_{i,j} \sum_{k,l} \sum_{r,s} a_{ij}b_{kl}c_{rs} (E_{ij}E_{kl})E_{rs}.$$

Поэтому достаточно проверить ассоциативность умножения матричных единиц

$$E_{ij}(E_{kl}E_{rs}) = (E_{ij}E_{kl})E_{rs},$$

которая сразу следует из правила их умножения (предложение 4.1): оба произведения равны 0, за исключением случаев, когда $j = k$ и $l = r$, а в этих случаях оба они равны E_{is} . \square

Предложение 4.5. Для всякого n существует и притом единственная матрица $E_n \in M_{n \times n}(\mathbb{R})$, называемая единичной и обладающая следующим свойством:

$$E_n A = A, \quad B E_n = B \quad \forall A \in M_{n \times q}(\mathbb{R}), B \in M_{p \times n}(\mathbb{R}).$$

Доказательство. Если бы существовали матрицы E'_n и E''_n с этим свойством, то мы бы имели, с одной стороны, $E'_n E''_n = E''_n$, а с другой $E'_n E''_n = E'_n$, откуда $E'_n = E''_n$. Существование устанавливаем, явно указав матрицу E_n :

$$E_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}.$$

\square

В тех случаях, когда размер единичной матрицы ясен из контекста, она обозначается просто E .

Замечание 4.6. На множестве $M_{n \times n}(\mathbb{R})$ квадратных матриц определены одновременно все три указанные выше операции, т.е. это множество наделено сразу тремя операциями: двумя внутренними (сложение и умножение матриц) и одной внешней (умножение на скаляр).

Замечание 4.7. Простейшие примеры показывают, что умножение матриц некоммутативно:

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

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

Второй пример также показывает, что произведение двух ненулевых матриц может быть нулевой матрицей. Такие матрицы называются *делителями нуля*.

Матрицы вида λE , $\lambda \in \mathbb{R}$, называются *скалярными матрицами*, поскольку умножение на такую матрицу равносильно умножению на соответствующий скаляр:

$$(\lambda E)A = \lambda A, \quad B(\lambda E) = \lambda B.$$

Из этого, в частности, видно, что скалярные матрицы λE_n коммутируют со всеми матрицами в $M_{n \times n}(\mathbb{R})$.

Задача 4.8. Доказать, что только скалярные матрицы обладают последним свойством.

Следующее предложение описывает поведение произведения матриц при транспонировании.

Предложение 4.9. $(AB)^T = B^T A^T$.

Доказательство. Пусть $A^{(j)}$, B_i обозначают соответственно строки и столбцы матриц A , B . Тогда B_i^T , $A^{(j)T}$ представляют собой соответственно строки и столбцы матриц B^T , A^T . Очевидно, имеем: $A^{(j)}B_i = B_i^T A^{(j)T}$, т.е. получаем совпадение (i, j) -ых элементов в матрицах $(AB)^T$ и $B^T A^T$. \square

4.3. Элементарные матрицы

Определение 4.10. *Элементарной матрицей*, соответствующей данному элементарному преобразованию (над строками или столбцами матриц) называется матрица, получающаяся применением этого элементарного преобразования к единичной матрице.

Согласно этому определению, имеем три типа элементарных матриц:

применению к строкам (соответственно столбцам) матрицы A соответствующего элементарного преобразования, т.е. если матрица A' получена некоторым элементарным преобразованием над строками (соответственно столбцами) матрицы A и U — соответствующая элементарная матрица, то $A' = UA$ (соответственно, $A' = AU$).

Доказательство. Следует непосредственно из определения элементарных преобразований и умножения матриц. \square

Предложение 4.12. *Всякая невырожденная матрица представляется в виде произведения элементарных матриц. Всякая вырожденная матрица представляется в виде произведения элементарных матриц и матрицы, имеющей нулевую строку.*

Доказательство. Пусть A — квадратная матрица. Если A невырожденная, то она посредством последовательности элементарных преобразований над строками может быть приведена к единичной. Рассматривая обратные элементарные преобразования, мы можем перейти от единичной матрицы к A :

$$E \xrightarrow{U_1} \dots \xrightarrow{U_n} A.$$

Если U_1, \dots, U_n — соответствующие элементарные матрицы, получаем:

$$U_n \dots U_2 U_1 E = A,$$

откуда

$$A = U_n \dots U_2 U_1.$$

Аналогично, если A вырожденная, то она элементарными преобразованиями над строками приводится к матрице A' с нулевой строкой и, рассматривая элементарные матрицы U_1, \dots, U_n , соответствующие обратным элементарным преобразованиям:

$$A' \xrightarrow{U_1} \dots \xrightarrow{U_n} A,$$

получаем $A = U_n \dots U_1 A'$. \square

4.4. Определитель произведения матриц

Теорема 4.13. *Определитель произведения матриц равен произведению определителей:*

$$\det(AB) = \det A \det B. \quad (4.6)$$

Доказательство. Рассмотрим три случая.

1) A — элементарная матрица. Тогда AB получается из B соответствующим преобразованием над строками. Если это преобразование I типа, то $\det(AB) = \det B$ и $\det A = 1$. Если оно II типа, то $\det(AB) = -\det B$ и $\det A = -1$. Наконец, если оно III типа (умножение строки на число $\alpha \neq 0$), то $\det(AB) = \alpha \det B$ и $\det A = \alpha$. Таким образом, для любого из трех типов элементарной матрицы A равенство (4.6) выполняется.

2) A — невырожденная матрица. Тогда согласно предложению 4.12 матрица A представляется в виде произведения элементарных матриц:

$$A = U_n U_{n-1} \dots U_1.$$

Применяя (4.6) в случае, когда первый множитель — элементарная матрица, получаем:

$$\begin{aligned} \det(AB) &= \det(U_n U_{n-1} \dots U_1 B) = \\ &= \det U_n \det(U_{n-1} \dots U_1 B) = \dots = \\ &= \det U_n \det U_{n-1} \dots \det U_1 \det B, \end{aligned}$$

$$\det A = \det(U_n U_{n-1} \dots U_1) = \dots = \det U_n \det U_{n-1} \dots \det U_1,$$

откуда $\det(AB) = \det A \det B$.

3) A — вырожденная матрица. Согласно предложению 4.12, $A = U_n \dots U_1 A'$ где A' — матрица с нулевой строкой и U_i — элементарные матрицы. Тогда, как и выше,

$$\det(AB) = \det(U_n \dots U_1 A' B) = \det U_n \dots \det U_1 \det(A' B) = 0,$$

так как матрица $A' B$ содержит нулевую строку (с тем же номером, что и A'). Поскольку $\det A = 0$, равенство (4.6) выполняется. \square

4.5. Аксиоматическая характеристика определителя и другое доказательство теоремы об определителе произведения матриц

Пусть F — функция на множестве квадратных матриц порядка n , которая является полилинейной и кососимметричной как функция от столбцов матрицы.

Теорема 4.14. *Для любых квадратных матриц A, B порядка n*

$$F(AB) = F(A) \det B.$$

Доказательство. Пусть a_1, \dots, a_n — столбцы матрицы A . Тогда столбцы матрицы AB представляются в виде $\sum_{i=1}^n b_{ij}a_i$. Имеем:

$$\begin{aligned} F(AB) &= F\left(\sum_i b_{i1}a_i, \dots, \sum_i b_{in}a_i\right) = \\ &= \sum_{\substack{(i_1, \dots, i_n) \\ i_1, \dots, i_n \text{ все различны}}} F(b_{i_1 1}a_{i_1}, \dots, b_{i_n n}a_{i_n}) = \\ &= \sum_{\substack{(i_1, \dots, i_n) \\ i_1, \dots, i_n \text{ все различны}}} b_{i_1 1} \dots b_{i_n n} F(a_{i_1}, \dots, a_{i_n}) = \\ &= \sum_{\sigma \in S_n} b_{1\sigma(n)} \dots b_{n\sigma(1)} \operatorname{sgn}(\sigma) F(A) = \\ &= F(a) \det B, \quad \text{где } \sigma = \begin{pmatrix} i_1 & \dots & i_n \\ 1 & \dots & n \end{pmatrix}. \end{aligned}$$

□

Следствие 4.15. $\det(AB) = \det A \det B$.

Следствие 4.16. *Пусть F — функция на множестве квадратных матриц порядка n , которая является полилинейной и кососимметрической как функция от столбцов матрицы и такая, что $F(E) = 1$. Тогда $F(A) = \det A$ для любой матрицы A .*

Доказательство. Действительно, $F(A) = F(EA) = F(E) \det A = \det A$. \square

4.6. Простейшие линейные матричные уравнения

Мы рассматриваем уравнение

$$AX = B, \quad (4.7)$$

в котором A и B — данные матрицы размеров $p \times n$ и $p \times q$, а X — неизвестная матрица размера $n \times q$. Это уравнение можно рассматривать как обобщение обычной системы линейных уравнений, так в случае, когда X и B состоят из одного столбца ($q = 1$):

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

уравнение (4.7) представляет собой записанную в матричной форме систему из p линейных уравнений с n неизвестными. В случае произвольного q пусть (X_1, \dots, X_q) и (B_1, \dots, B_q) — системы столбцов матриц X и B соответственно. Тогда решение уравнения равносильно решению q обычных систем линейных уравнений:

$$AX_1 = B_1, \quad \dots, \quad AX_q = B_q.$$

Пусть A — квадратная матрица. Согласно теореме Крамера, эти системы уравнений имеют и притом единственное решение в том и только том случае, если A — невырожденная. Поэтому получаем

Предложение 4.17. *Матричное уравнение $AX = B$ с квадратной матрицей A имеет и притом единственное решение, если и только если матрица A невырожденная. В этом случае элементы матрицы $X = (x_{ij})$ находятся по формулам:*

$$x_{ij} = \Delta_{ij} / \det A,$$

где Δ_{ij} — определитель матрицы, полученной из A заменой ее i -го столбца j -м столбцом матрицы B .

Линейное уравнение

$$YA = C \quad (4.8)$$

сводится к уравнению вида (4.7), если к обеим его частям применить транспонирование:

$$A^T Y^T = C^T.$$

В частности, имеем

Следствие 4.18. *Матричное уравнение $YA = C$ с квадратной матрицей A имеет и притом единственное решение, если и только если матрица A невырожденная.*

4.7. Обратная матрица

Определение 4.19. Пусть A — матрица размера $m \times n$. Матрица B размера $n \times m$ называется *обратной* для A , если выполняются условия

$$AB = E_m \quad \text{и} \quad BA = E_n.$$

В §5 (предложение 5.16) будет показано, что при $m > n$ матриц B , удовлетворяющих условию $AB = E_m$, не существует, так что неквадратные матрицы не могут иметь обратных. Поэтому далее в этом разделе мы рассматриваем только квадратные матрицы некоторого порядка n .

Предложение 4.20. *Если квадратная матрица A имеет обратную, то обратная матрица единственна.*

Это предложение вытекает из следующего несколько более общего утверждения:

Предложение 4.21. *Пусть для данной матрицы A матрицы B' , B'' удовлетворяют условиям: $AB' = E$ и $B''A = E$. Тогда $B' = B''$.*

Доказательство. Используя ассоциативность умножения матриц, с одной стороны, получаем

$$B''AB' = (B''A)B' = EB' = B',$$

пересекающихся с матрицей A' по нулевой строке (другими словами, число ненулевых строк в матрицах A' и $(A' \mid B')$ одинаково).

Если это условие выполнено, то как и в случае обычной линейной системы разделяем неизвестные на главные и свободные. При этом главными или свободными оказываются все неизвестные каждой строки матрицы X в зависимости от ее номера: строки, номера которых совпадают с номерами столбцов матрицы A' , в которых стоят главные элементы ее ненулевых строк, состоят из главных неизвестных, а остальные строки — из свободных. Выражая строки, состоящие из главных неизвестных, через строки, состоящие из свободных, получаем общее решение уравнения (4.7).

Особенно интересен случай, когда в уравнении (4.7) матрица A невырожденная (квадратная).

Предложение 4.25. Пусть в уравнении (4.7) матрица A невырожденная квадратная. Приведем расширенную матрицу $(A \mid B)$ элементарными преобразованиями над строками к виду $(E \mid B')$. Тогда $X = B'$ есть (единственное) решение матричного уравнения (4.7).

Доказательство. Действительно, в этом случае уравнение (4.7) эквивалентно уравнению $EX = B'$. \square

Применим этот способ для вычисления обратной матрицы. Если A — невырожденная, то она имеет обратную, которая является (единственным) решением матричного уравнения $AX = E$. Поэтому получаем

Предложение 4.26. Пусть A — невырожденная матрица. Составим расширенную матрицу $(A \mid E)$ и с помощью элементарных преобразований над строками приведем ее к виду $(E \mid B')$. Тогда B' — обратная матрица для A .

Кратко способ вычисления обратной матрицы, даваемый предложением 4.26, можно записать так:

$$(A \mid E) \longrightarrow (E \mid A^{-1}),$$

где стрелка обозначает выполнение последовательности элементарных преобразований над строками.

Замечание 4.27. Если A — невырожденная матрица, то решение матричного уравнения $AX = B$ записывается в виде $X = A^{-1}B$. Однако этот способ решения, включающий нахождение обратной матрицы, а затем произведения матриц, требует, как правило, большего объема вычисления, чем непосредственное применение элементарных преобразований

$$(A \mid B) \longrightarrow (E \mid X).$$

§5. Ранг матрицы

5.1. Теорема о ранге матрицы

Определение 5.1. Матрица имеет ранг 0, если (и только если) она нулевая. Ненулевая матрица имеет ранг 1, если ее можно представить в виде произведения столбца и строки. Рангом произвольной ненулевой матрицы A называется наименьшее положительное целое число r , такое что A можно представить в виде суммы r матриц ранга 1.

Ранг матрицы A обозначается через $\text{rk}(A)$.

Предложение 5.2. Матрица A имеет ранг 1, если и только если все ее строки (столбцы) пропорциональны некоторой фиксированной ненулевой строке (столбцу).

Доказательство. Пусть $a^{(1)}, \dots, a^{(m)}$ — строки матрицы A и $a^{(i)} = \alpha_i b$. Рассмотрим столбец $a = (\alpha_1, \dots, \alpha_m)^T$. Тогда $A = ab$. \square

Следующие два предложения очевидны.

Предложение 5.3. Если A — матрица размера $m \times n$, то $\text{rk}(A) \leq \min\{m, n\}$.

Предложение 5.4. $\text{rk}(A_1 + \dots + A_s) \leq \text{rk}(A_1) + \dots + \text{rk}(A_s)$.

Предложение 5.5. $\text{rk}(A^T) = \text{rk}(A)$.

Доказательство. Если $\text{rk}(A) = 1$, $A = ab$, a — столбец, b — строка, то $A^T = b^T a^T$, т.е. $\text{rk}(A^T) = 1$.

Пусть $\text{rk}(A) = r$, $A = A_1 + \dots + A_r$, где $\text{rk}(A_i) = 1$. Тогда $A^T = A_1^T + \dots + A_r^T$, а потому $\text{rk}(A^T) \leq \text{rk}(A)$. Так как $A = (A^T)^T$, то $\text{rk}(A) \leq \text{rk}(A^T)$. \square

Предложение 5.6. Ранг матрицы равен рангу системы ее столбцов и равен рангу системы ее строк.

Доказательство. Пусть $\text{rk}(A) = r$ и $\text{rk}\{a_1, \dots, a_n\} = s$ (a_1, \dots, a_n — столбцы матрицы A). Имеем: $A = A_1 + \dots + A_r$, где A_i — матрицы ранга 1. В силу предложения 5.2 существуют столбцы b_1, \dots, b_r , такие что все столбцы матрицы A_i пропорциональны столбцу b_i , $i = 1, \dots, r$. Следовательно, столбцы матрицы A представляются как линейные комбинации столбцов b_1, \dots, b_r , откуда $s \leq r$. С другой стороны, система $\{a_1, \dots, a_n\}$ линейно выражается через некоторую систему столбцов $\{b'_1, \dots, b'_s\}$: $a_j = \sum_{i=1}^s \alpha_{ij} b'_i$. Пусть A_i — матрица со столбцами $\alpha_{i1} b'_1, \dots, \alpha_{in} b'_i$. Тогда $A = A_1 + \dots + A_s$ и $\text{rk}(A_i) \leq 1$. Поэтому $r \leq s$. Итак, $r = s$.

Доказательство для случая строк можно провести аналогично или воспользоваться предложением 5.5 и тем, что ранг системы строк матрицы A равен рангу системы столбцов матрицы A^T . \square

Предложение 5.7. $\text{rk}(A_1 \cdot \dots \cdot A_s) \leq \min_i \{\text{rk}(A_i)\}$.

Доказательство. Пусть сначала $\text{rk}(A_i) = 1$, $A_i = a_i b_i$, a_i — столбец, b_i — строка. Тогда

$$A_1 \dots A_s = (A_1 \dots A_{i-1} a_i)(b_i A_{i+1} \dots A_s),$$

где $A_1 \dots A_{i-1} a_i$ — столбец и $b_i A_{i+1} \dots A_s$ — строка. Следовательно, $\text{rk}(A_1 \dots A_s) \leq 1$. Пусть теперь $\text{rk} A_i = r$ и $A_i = A_{i1} + \dots + A_{ir}$, где A_{i1}, \dots, A_{ir} — матрицы ранга 1. Имеем:

$$A_1 \dots A_s = A_1 \dots A_{i1} \dots A_s + \dots + A_1 \dots A_{ir} \dots A_s,$$

где, согласно предыдущему, все слагаемые являются матрицами ранга 1. Следовательно, $\text{rk}(A_1 \dots A_s) \leq r$. \square

Предложение 5.8. Пусть $B = CAD$, где C, D — невырожденные матрицы. Тогда $\text{rk}(B) = \text{rk}(A)$.

Доказательство. Так как $A = C^{-1}BD^{-1}$, то в силу предложения 5.7 $\text{rk}(B) \leq \text{rk}(A)$ и $\text{rk}(A) \leq \text{rk}(B)$. \square

Поскольку элементарное преобразование над строками или столбцами равносильно умножению матрицы слева или справа на элементарную матрицу, которая невырождена, то получаем

Следствие 5.9. *Ранг матрицы не изменяется при элементарных преобразованиях над ее строками и столбцами.*

Предложение 5.10. *Ранг ступенчатой матрицы равен числу ее ненулевых строк.*

Доказательство. Достаточно показать, что ненулевые строки $a^{(1)}, \dots, a^{(i)}$ ступенчатой матрицы линейно независимы. Пусть a_{ij_i} — главный элемент i -й строки. Допустим, что $\lambda_1 a^{(1)} + \dots + \lambda_r a^{(r)} = 0$. Тогда $\lambda_1 a_{1j_1} = 0$, откуда $\lambda_1 = 0$; тогда $\lambda_2 a_{2j_2} = 0$, откуда $\lambda_2 = 0$ и т.д. Последовательно получаем, что все $\lambda_i = 0$. \square

Следствие 5.11. *Ранг матрицы равен числу ненулевых строк в ее ступенчатом виде.*

Предложение 5.12. *Ранг матрицы равен наибольшему порядку ее отличных от нуля миноров.*

Доказательство. Пусть s — максимальный порядок отличных от нуля миноров матрицы A . Тогда $s \leq \text{rk}(A)$, так как у всякого минора порядка $> \text{rk}(A)$ система строк (столбцов) линейно зависима и, следовательно, он равен нулю. Выберем в матрице A минор $M \neq 0$ (пусть его порядок равен r , $r \leq s$), все окаймляющие миноры которого равны 0. Тогда r столбцов матрицы A , проходящих через M , образуют линейно независимую систему, а любая строга содержащая ее система столбцов линейно зависима, так как, согласно предложению 2.11, соответствующая ей однородная система линейных уравнений имеет ненулевое решение. Следовательно, $\text{rk}(A) = r$, откуда $\text{rk}(A) = s$. \square

Объединяя доказанные выше факты, получаем следующую теорему.

Теорема 5.13 (о ранге матрицы). *Для всякой матрицы A следующие ее числовые характеристики равны между собой:*

1. $\text{rk}(A)$;

2. ранг системы столбцов матрицы A ;
3. ранг системы строк матрицы A ;
4. число ненулевых строк в ступенчатом виде матрицы A ;
5. максимальный порядок отличных от 0 миноров матрицы A .

Задача 5.14. Назовем *факторизационным рангом* ненулевой матрицы A (размера $m \times n$) наименьшее положительное целое число s , такое что A представляется в виде произведения $A = BC$, где B — матрица размера $m \times s$ и C — матрица размера $s \times n$. Доказать, что факторизационный ранг матрицы равен ее рангу.

Задача 5.15. Назовем *комбинаторным рангом* матрицы A наименьшее неотрицательное целое число t , такое что после вычеркивания в матрице A t строк и столбцов (в совокупности) в ней не остается ненулевых элементов. Обозначим комбинаторный ранг через $\text{сгк}(A)$. Показать, что $\text{rk}(A) \leq \text{сгк}(A)$, но в то же время матрицы ранга 1 могут иметь сколь угодно большой комбинаторный ранг.

Применим понятие ранга матрицы для доказательства несуществования обратных матриц у неквадратных матриц.

Предложение 5.16. Если A — матрица размера $m \times n$ и $m > n$, то не существует матрицы B , такой что $AB = I_m$.

Доказательство. Действительно, $\text{rk } I_m = m$, а

$$\text{rk}(AB) \leq \text{rk } A \leq n < m.$$

□

Задача 5.17. Пусть A — матрица размера $m \times n$ и $m \leq n$. Доказать, что матрица B , такая что $AB = I_m$, существует в том и только в том случае, если $\text{rk } A = m$.

5.2. Критерий совместности для систем линейных уравнений (в терминах рангов матриц)

Теорема 5.18 (теорема Кронекера–Капелли). Система линейных уравнений совместна в том и только в том случае, если ранг ее матрицы коэффициентов равен рангу расширенной матрицы.

Доказательство. Пусть дана система линейных уравнений с матрицей коэффициентов A , столбцом свободных членов b и расширенной матрицей $(A | b)$. Приведем два доказательства этой теоремы.

1. Приведем расширенную матрицу системы к ступенчатому виду $(A' | b')$. Имеем: система совместна \iff в матрице $(A' | b')$ нет строк вида $(0, \dots, 0, b'_k), b'_k \neq 0 \iff$ число ненулевых строк в матрицах A' и $(A' | b')$ одинаково $\iff \text{rk } A = \text{rk } B$.

2. Имеем: Система совместна \iff столбец b линейно выражается через столбцы матрицы $A \iff$ системы столбцов матриц A и $(A | b)$ эквивалентны $\implies \text{rk } A = \text{rk } B$. Остается доказать, что если $\text{rk } A = \text{rk } B = r$, то системы столбцов матриц A и $(A | b)$ эквивалентны (это уже было доказано в предложении 3.24, но мы не будем на него опираться). Пусть $\text{rk } A = \text{rk } B = r$ и A_{j_1}, \dots, A_{j_r} — базис системы столбцов матрицы A . Так как $\text{rk } B = r$, то это максимальная линейно независимая подсистема системы столбцов матрицы $(A | b)$, следовательно, все столбцы матрицы $(A | b)$ линейно выражаются через систему $(A_{j_1}, \dots, A_{j_r})$, т.е. системы столбцов матриц A и $(A | b)$ эквивалентны. \square

Следствие 5.19. Система линейных уравнений является определенной в том и только в том случае, если ранг ее матрицы коэффициентов равен рангу расширенной матрицы и равен числу неизвестных.

Доказательство. Действительно, совместная система линейных уравнений является определенной в том и только в том случае, если число неизвестных равно числу ненулевых строк в ступенчатом виде ее матрицы, т.е. равно рангу A (равному рангу $(A | b)$). \square

Задача 5.20. Доказать, что матричное уравнение $A = B$ имеет решение в том и только том случае, если $\text{rk } A = \text{rk}(A \mid B)$, и имеет единственное решение в том и только том случае, если эти ранги равны числу столбцов матрицы A .

5.3. Выбор главных и свободных неизвестных в совместной системе линейных уравнений

Пусть дана совместная система линейных уравнений $Ax = b$, $A \in M_{m \times n}(\mathbb{R})$, $b \in \mathbb{R}^m$, $x \in \mathbb{R}^n$. Разбиение множества неизвестных на два непересекающихся подмножества $\{x_{j_1}, \dots, x_{j_r}\}$ и $\{x_{j_{r+1}}, \dots, x_{j_n}\}$ будем называть *выбором* соответственно *главных* и *свободных неизвестных*, если при любом наборе значений неизвестных из второго подмножества $x_{j_{r+1}} = \xi_{j_{r+1}}, \dots, x_{j_n} = \xi_{j_n}$ существует единственный набор значений неизвестных из первого подмножества $x_{j_1} = \xi_{j_1}, \dots, x_{j_r} = \xi_{j_r}$, такой что $x_1 = \xi_1, \dots, x_n = \xi_n$ является решением данной системы.

Предложение 5.21. *Подмножество $\{x_{j_1}, \dots, x_{j_r}\}$ может быть выбрано в качестве набора главных неизвестных (остальные неизвестные при этом считаются свободными) в том и только том случае, если столбцы a_{j_1}, \dots, a_{j_r} образуют базис системы столбцов матрицы A .*

Доказательство. Пусть столбцы a_{j_1}, \dots, a_{j_r} образуют базис системы столбцов матрицы A . Выберем в матрице, образованной этими столбцами, ненулевой минор порядка r . Пусть он расположен в строках с номерами i_1, \dots, i_r . Тогда строки b^{i_1}, \dots, b^{i_r} образуют базис системы строк расширенной матрицы системы, а потому все уравнения системы являются следствиями уравнений с номерами i_1, \dots, i_r . Отбрасывая остальные уравнения и придавая произвольные значения неизвестным, не входящим в подмножество $\{x_{j_1}, \dots, x_{j_r}\}$, получаем квадратную систему с невырожденной матрицей коэффициентов и, по теореме Крамера, имеющую единственное решение.

Пусть теперь $\{x_{j_1}, \dots, x_{j_r}\}$ образуют набор главных неизвестных. При любом выборе значений свободных неизвестных система уравнений со столбцами матрицы коэффициентов a_{j_1}, \dots, a_{j_n} имеет единственное решение, а потому соответствующая однородная система имеет только нулевое решение, т.е. эти столбцы линейно независимы. Допустим, что они не образуют базис системы столбцов, и дополним их до базиса столбцами, например, с номерами j_{r+1}, \dots, j_s . Согласно доказанному, $\{x_{j_1}, \dots, x_{j_r}, x_{j_{r+1}}, \dots, x_{j_s}\}$ есть набор главных неизвестных, т.е. при любом выборе значений остальных неизвестных значения x_{j_1}, \dots, x_{j_s} определяются единственным образом, что противоречит предположению о том, что неизвестным $\{x_{j_{r+1}}, \dots, x_{j_s}\}$ также можно придавать произвольные значения. \square

§6. Понятие группы

6.1. Понятия бинарной операции и полугруппы, обобщенный закон ассоциативности

Пусть G — некоторое множество. *Бинарной операцией* на множестве G называется правило, которое каждой (упорядоченной) паре (a, b) элементов из G сопоставляет некоторый элемент из G . Другими словами, задание бинарной операции на G — это задание отображения декартова квадрата $G \times G$ множества G в G . Образ пары (a, b) при этом отображении, т.е. результат применения операции к паре (a, b) , может обозначаться разными символами: $a \cdot b$, $a + b$, $a \circ b$, $a * b$ и т.д., или просто ab , и называться разными терминами: *умножением* (соответственно результат ее применения называется *произведением*), *сложением* (соответственно *сумма*), *композицией* и др. Множество G с заданной на нем операцией, обозначенной, скажем, \cdot , будем обозначать через (G, \cdot) . Обычно рассматривают операции, обладающие некоторыми специальными свойствами. Когда операция обладает определенным набором таких свойств, множеству с операцией (G, \cdot) присваивается определенное наименование. Например:

Определение 6.1. (G, \cdot) называется *полугруппой*, если операция \cdot удовлетворяет закону ассоциативности:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G.$$

Примеры полугрупп. 1) Неотрицательные целые числа относительно сложения (а также относительно умножения);

2) полугруппа всех отображений данного множества в себя (относительно композиции).

Пусть задан упорядоченный набор элементов $a_1, \dots, a_n \in G$. Если на G задана бинарная операция \cdot , то можно образовать различные произведения из элементов a_1, \dots, a_n (с заданным порядком), используя различные расстановки скобок. Например, при $n = 4$ имеется 5 расстановок скобок: $a_1(a_2(a_3a_4))$, $a_1((a_2(a_3)a_4))$, $(a_1a_2)(a_3a_4)$, $(a_1(a_2a_3))a_4$, $((a_1a_2)a_3)a_4$.

Задача 6.2. Найти формулу для числа расстановок скобок для n множителей.

Ответ: $\frac{2^{n-1}(2n-3)!!}{n!}$.

Обобщенный закон ассоциативности состоит в том, что произведение n элементов (в заданном порядке) не зависит от способа расстановки скобок.

Мы покажем, что выполнение обобщенного закона ассоциативности для любого числа множителей следует из его выполнения для трех множителей, т.е. что обобщенный закон ассоциативности выполняется в любой полугруппе. Для приложений этот факт полезно иметь в более общей ситуации, когда бинарная операция на множестве G является частичной, т.е. определена не обязательно для всех пар $(a, b) \in G \times G$, а на некотором подмножестве $G \times G$ (пример: композиция отображений). В этом случае (обычный) закон ассоциативности состоит в следующем: для любых трех элементов $a, b, c \in G$, если одно из произведений $a(bc)$ или $(ab)c$ определено, то определено также и другое, и эти произведения равны.

Теорема 6.3. Пусть для множества с частичной бинарной операцией (G, \cdot) выполняется закон ассоциативности. Тогда для (G, \cdot) выполняется обобщенный закон ассоциативности: для любого упорядоченного конечного набора элементов из G , если их произведение (в заданном порядке) определено при некоторой расстановке скобок, то оно определено при любой расстановке скобок, и результат не зависит от способа расстановки скобок.

Доказательство. Индукция по числу множителей n . Основание индукции $n = 3$ известно. Пусть $n \geq 4$ фиксировано,

и предположим, что для произведения меньшего чем n числа элементов утверждение доказано. В произведении n элементов a_1, \dots, a_n с заданной расстановкой скобок выделяем скобки, над которыми производится заключительная операция: $(a_1, \dots, a_k) \cdot (a_{k+1}, \dots, a_n)$. Такую расстановку скобок назовем расстановкой типа k . Так как внутри каждой скобки число элементов меньше n , то внутри них допустима любая расстановка скобок. Нам достаточно показать, что для всякого k , $1 \leq k \leq n - 1$, существует расстановка типа k , для которой произведение определено, и что результат одинаков для всех k . Так как нам дано, что для некоторой расстановки скобок наше произведение определено, то достаточно показать, что если произведение определено при расстановке типа k , то оно определено для расстановки типа $k-1$ (при $k \geq 2$) и для расстановки типа $k+1$ (если $k \leq n-2$), и что результаты совпадают. Для перехода от k к $k-1$ (при $k \geq 2$) рассматриваем произведение (которое определено)

$$((a_1, \dots, a_{k-1}) \cdot a_k) \cdot (a_{k+1}, \dots, a_n)$$

и применяем (обычный) закон ассоциативности:

$$\begin{aligned} & ((a_1, \dots, a_{k-1}) \cdot a_k) \cdot (a_{k+1}, \dots, a_n) = \\ & = (a_1, \dots, a_{k-1}) \cdot (a_k \cdot (a_{k+1}, \dots, a_n)), \end{aligned}$$

т.е. произведение определено и совпадает с исходным произведением типа $k-1$. Аналогично производится переход от k к $k+1$. \square

6.2. Единица и обратный элемент в полугруппе. Свойства степеней элементов

Пусть (G, \cdot) — множество с бинарной операцией. Элемент $e \in G$ называется *левой* (соответственно *правой*) *единицей*, если $ea = a$ (соответственно $ae = a$) для всякого $a \in G$, и называется *единицей* (иногда уточняют — *двусторонней*), если $ea = ae = a$. Если G обладает левой единицей e_1 и правой единицей e_2 , то $e_1e_2 = e_1 = e_2$, т.е. этот элемент является единицей. Таким образом, если единица существует, то она единственна.

Пусть (G, \cdot) обладает единицей e и $a \in G$. Элемент $a' \in G$ называется *левым* (соответственно *правым*) *обратным* для a , если $a'a = e$ (соответственно $aa' = e$), и называется *обратным* (*двусторонним*) для a , если $a'a = aa' = e$.

Предложение 6.4. Пусть (G, \cdot) — полугруппа с единицей e . Если элемент $a \in G$ обладает левым обратным a' и правым обратным a'' , то $a' = a''$ — обратный элемент для a .

Доказательство. Действительно, $(a'a)a'' = a'(aa'')$ и $(a'a)a'' = ea'' = a''$, $a'(aa'') = a'e = a'$. \square

Таким образом, если элемент a в полугруппе обладает обратным, то обратный элемент единственный. Он обозначается через a^{-1} . Элемент, имеющий обратный, называется *обратимым*.

Задача 6.5. Привести пример полугруппы, обладающей левой (или правой) единицей, но не имеющей единицы. Показать, что левых (или правых) единиц может быть несколько. Привести пример полугруппы с единицей и элемента в ней, имеющего левый (или правый) обратный, но не имеющий обратного. Показать, что элемент может иметь несколько левых (или правых) обратных.

Определение 6.6. Пусть G — полугруппа; назовем элемент $a \in G$ *регулярным* (*корегулярным*, *строго регулярным*) *слева*, если отображение $x \mapsto ax$ инъективно (сюръективно, биективно); это равносильно тому, что для всякого $b \in G$ уравнение $ax = b$ имеет не более одного решения (имеет решение, имеет единственное решение). *Регулярность слева* элемента a равносильна тому, что можно сокращать на a слева, т.е. $ax = ay \implies x = y$. Аналогично определяются правые варианты этих понятий.

Задача 6.7. Показать, что в полугруппе с единицей: если элемент имеет левый (правый) обратный, то он регулярен слева (справа); элемент регулярен слева (справа), если и только если он имеет правый (левый) обратный; элемент строго регулярен (слева, справа или с обеих сторон), если и только если он имеет обратный. Регулярный слева (справа) элемент не обязательно имеет левый (правый) обратный.

Задача 6.8. Показать, что существование в полугруппе строго регулярного слева (справа) элемента равносильно существованию левой (правой) единицы.

Задача 6.9. Показать, что если в полугруппе имеется хотя бы один регулярный слева элемент и хотя бы один строго регулярный справа элемент, то она содержит единицу. В то же время из существования корегулярного слева элемента и строго регулярного справа элемента не следует существование единицы. Однако, если существует элемент, который корегулярен одновременно слева и справа, то единица имеется, и такой элемент обратим.

Предложение 6.10. Если в полугруппе с единицей элементы a_1, \dots, a_n обратимы, то их произведение тоже обратимо и

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}.$$

Для доказательства умножим элементы $a_1 \dots a_n$ и $a_n^{-1} \dots a_1^{-1}$ друг на друга в обоих порядках и воспользуемся ассоциативностью.

Степени элемента в полугруппе. Для всякого элемента a в полугруппе G и всякого положительного целого числа n определена степень

$$a^n = \underbrace{a \cdot \dots \cdot a}_n.$$

n множителей

Если G имеет единицу, то, по определению, $a^0 = e$. Если G имеет единицу и a обратим, то, по определению, для всякого положительного целого числа n

$$a^{-n} = (a^{-1})^n = (a^n)^{-1}$$

(второе равенство получается в силу предложения 6.10).

Предложение 6.11. Для всех целых чисел m, m_1, \dots, m_k, n , для которых соответствующие степени определены,

$$a^{m_1} \cdot a^{m_2} \cdot \dots \cdot a^{m_k} = a^{m_1 + \dots + m_k}, \quad (6.1)$$

$$(a^m)^n = a^{mn}. \quad (6.2)$$

Доказательство. Если все числа m, m_i, n неотрицательны, то равенства очевидны. Пусть a обратим и показатели имеют произвольные знаки. По индуктивным соображениям (6.1) достаточно доказать для $k = 2$. Если m_1 и m_2 имеют одинаковые знаки, то равенство очевидно. Пусть для определенности $m_1 \leq 0$ и $m_2 \geq 0$. Если $m_2 \geq |m_1|$, то запишем $m_2 = (-m_1) + m', m' \geq 0$, и имеем:

$$a^{m_1} a^{m_2} = a^{m_1} (a^{-m_1} a^{m'}) = (a^{m_1} a^{-m_1}) a^{m'} = a^{m'} = a^{m_1+m_2}.$$

Аналогично, если $m_2 < |m_1|$, $m_1 = m' - m_2$, $m' < 0$, имеем:

$$a^{m_1} a^{m_2} = (a^{m'} a^{-m_2}) a^{m_2} = a^{m'} (a^{-m_2} a^{m_2}) = a^{m'} = a^{m_1+m_2}.$$

Итак, (6.1) доказано. Если $n = 0$, то (6.2) очевидно. Если $n > 0$, то применяем (6.1), взяв $k = n$, $m_1 = \dots = m_n = m$. Если $n < 0$, то $-n > 0$ и

$$(a^m)^n = ((a^m)^{-1})^{-n} = (a^{-m})^{-n} = a^{(-m)(-n)} = a^{mn}.$$

□

Определение 6.12. Элементы a и b в множестве с бинарной операцией (G, \cdot) называются *коммутирующими*, или *перестановочными*, если $ab = ba$. Операция (или множество с этой операцией) называется *коммутативной* (*коммутативным*), если любые два элемента коммутируют.

Предложение 6.13. Если элементы a_1, \dots, a_k попарно коммутируют, то

$$(a_1 \dots a_k)^n = a_1^n \dots a_k^n \quad (6.3)$$

для всякого целого n , при котором эти степени определены.

Доказательство очевидно.

Для некоммутирующих элементов это равенство, как правило, не имеет места. Например, если элементы a_1 и a_2 регулярны соответственно слева и справа, то из равенства $(a_1 a_2)^2 = a_1^2 a_2^2$ следует, что $a_1 a_2 = a_2 a_1$.

6.3. Определение группы. Порядок элемента группы и его свойства

Определение 6.14. Множество с бинарной операцией (G, \cdot) называется *группой*, если выполняются следующие свойства:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$ (ассоциативность);
2. $\exists e \in G: e \cdot a = a \cdot e = a \quad \forall a \in G$ (существование единицы);
3. $\forall a \in G \quad \exists a^{-1} \in G: a^{-1} \cdot a = a \cdot a^{-1} = e$ (существование обратного элемента).

Другими словами, группой называется полугруппа с единицей, в которой всякий элемент обратим.

В группе всякий элемент строго регулярен, т.е. для любых a, b каждое из уравнений $ax = b$ и $xa = b$ имеет и притом единственное решение.

Заметим, что единица в группе характеризуется тем, что является *идемпотентом*, т.е. удовлетворяет уравнению $x^2 = x$. Действительно, если в группе $a^2 = a$, то $a^{-1}(a^2) = a^{-1}a \implies a = e$. В полугруппе могут быть идемпотенты, не являющиеся единицей.

- Задача 6.15.**
1. Если в полугруппе имеется левая единица, и относительно нее всякий элемент имеет левый обратный, то полугруппа является группой. Останется ли утверждение верным, если “левый обратный” заменить на “правый обратный”?
 2. Очевидно, в группе всякий элемент сильно регулярен. Показать, что если в полугруппе всякий элемент корегулярен одновременно слева и справа, то она является группой.
 3. Конечная полугруппа, в которой всякий элемент регулярен слева и справа, является группой.

Определение 6.16. Группа G называется *абелевой* (или *коммутативной*), если $ab = ba \quad \forall a, b \in G$.

Замечание 6.17. Выше мы обозначали операцию знаком \cdot и называли умножением (мультипликативная терминология). Если операция в группе называется сложением и обозначается знаком $+$ (аддитивная терминология), то вместо единицы говорят о нуле и обозначают его символом 0 (оба термина “единица” и “нуль” объединяют термином “нейтральный элемент”). Обратный элемент для a относительно сложения обозначают через $-a$ и называют противоположным элементом; вместо $a + (-b)$ пишут $a - b$. Вместо возведения элемента a в степень n в этом случае говорят об умножении a на целое число n , так что если $n > 0$, то:

$$\begin{aligned} na &= \underbrace{a + \dots + a}_{n \text{ слагаемых}}, \\ 0a &= 0, \\ (-n)a &= -(na) = n(-a). \end{aligned}$$

Соотношения (6.1), (6.2), (6.3) переписываются в этом случае в виде:

$$m_1a + m_2a + \dots + m_ka = (m_1 + \dots + m_k)a, \quad (6.1')$$

$$n(ma) = (nm)a, \quad (6.2')$$

$$n(a_1 + \dots + a_k) = na_1 + \dots + na_k. \quad (6.3')$$

Примеры групп:

- 1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ — группы всех целых, рациональных, действительных чисел соответственно относительно операции сложения.
- 2) Пусть $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, \mathbb{Q}_+ — множество всех положительных рациональных чисел и \mathbb{R}^* , \mathbb{R}_+ — аналогичные обозначения для действительных чисел. (\mathbb{Q}^*, \cdot) , (\mathbb{Q}_+, \cdot) , (\mathbb{R}^*, \cdot) , (\mathbb{R}_+, \cdot) — группы относительно умножения.
- 3) Множество все матриц фиксированного размера n , в частности, пространства векторов-столбцов и векторов-строк данной размерности являются группами относительно сложения.

- 4) Множество $GL(n, \mathbb{R})$ всех невырожденных квадратных матриц порядка n и множество $SL(n, \mathbb{R})$ всех квадратных матриц порядка n с определителем $+1$ являются группами относительно умножения (они называются соответственно полной и специальной линейными группами над действительными числами). Аналогично можно рассматривать полную и специальную линейные группы $GL(n, \mathbb{Q})$ и $SL(n, \mathbb{Q})$ над \mathbb{Q} .
- 5) Пусть M — произвольное множество. Тогда множество S_M всех перестановок множества M , т.е. всех биективных отображений множества M на себя, является группой относительно композиции отображений, которая называется *симметрической группой* множества M . Если $M = \{1, \dots, n\}$, то группу S_M обозначают через S_n и называют *симметрической группой степени n* . Подмножество всех четных перестановок в S_n также является группой относительно композиции; эта группа обозначается через A_n и называется *знакопеременной группой степени n* .
- 6) Пусть (G, \cdot) — произвольная полугруппа с единицей. Тогда множество $U(G)$ всех обратимых элементов в G является группой относительно операции \cdot . Группы $GL(n, \mathbb{R})$ и S_M получаются как частные случаи этой конструкции, если в качестве полугруппы взять соответственно множество всех квадратных матриц порядка n с операцией умножения и множество всех отображений M в себя с операцией композиции отображений.

Определение 6.18. Пусть G — группа. *Порядком* $O(a)$ элемента $a \in G$ называется наименьшее среди положительных целых чисел k , таких что $a^k = e$; если таких k нет, то $O(a) = \infty$.

Предложение 6.19. Если $O(a) = \infty$, то $a^k = a^l \iff k = l$ ($k, l \in \mathbb{Z}$). Если $O(a) = n$, то: $a^k = a^l \iff k \equiv l \pmod{n}$, т.е. $n \mid l - k$ (вертикальная черта обозначает слово “делит”). В частности, $a^k = e \iff n \mid k$.

Другими словами, если $O(a) = \infty$, то все степени элемента a различны, а если $O(a) = n$, то среди степеней a имеется точно

n различных и в качестве таковых можно выбрать

$$a^0 = e, a^1 = a, a^2, \dots, a^{n-1}.$$

Доказательство. Пусть $O(a) = \infty$ и $k \neq l$, скажем, $l > k$. Если $a^k = a^l$, то $a^{l-k} = e$ — противоречие. Пусть $O(a) = n$ и k — целое число. Разделим k на n с остатком: $k = qn + r$, $0 \leq r < n$. Тогда

$$a^k = a^{qn+r} = (a^n)^q a^r = a^r,$$

откуда $a^k = e \iff r = 0 \iff n \mid k$. Имеем: $a^k = a^l \iff a^{l-k} = e \iff n \mid l - k$. \square

Предложение 6.20. Пусть G — группа и $a \in G$. Если $O(a) = \infty$, то все элементы $a^k \neq e$ имеют бесконечный порядок. Если a имеет порядок n , то

$$O(a^k) = \frac{n}{(k, n)},$$

где (k, n) обозначает наибольший общий делитель чисел k, n .

Доказательство. Первое утверждение очевидно.

Пусть $O(a) = n$ и m — положительное целое число такое, что $(a^k)^m = e \iff n \mid km$. Поэтому m — наименьший такой показатель, когда km — наименьшее общее кратное чисел k и n , т.е.

$$km = \frac{kn}{(k, n)} \implies m = \frac{n}{(k, n)}.$$

\square

Примеры. В любой группе нейтральный элемент и только он имеет порядок 1. В группах $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, (\mathbb{Q}_+, \cdot) , (\mathbb{R}_+, \cdot) все элементы кроме нейтрального имеют бесконечный порядок. В группах (\mathbb{Q}^*, \cdot) и (\mathbb{R}^*, \cdot) имеется также один элемент порядка 2 — это -1 . В группе $SL(2, \mathbb{R})$ имеются элементы любого порядка. В частности, матрица

$$\begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$$

имеет порядок n . В конечной группе все элементы имеют конечный порядок.

Задача 6.21. Доказать, что если все элементы группы имеют порядок ≤ 2 , то она абелева.

Специально рассмотрим вопрос о порядке элементов в симметрической группе S_n .

Предложение 6.22. Пусть $\pi \in S_n$. Разложим π в произведение независимых циклов $\pi = \gamma_1 \cdots \gamma_s$. Порядок π равен наименьшему общему кратному длин циклов $\gamma_1, \dots, \gamma_s$.

Доказательство. Порядок цикла $\gamma = (i_1 \dots i_m)$ равен его длине, так как $\gamma^k(i_1) = i_{k+1}$ при $1 \leq k \leq m-1$ и $\gamma^k(i_1) = i_1$.

Пусть циклы $\gamma_1, \dots, \gamma_s$ имеют длины m_1, \dots, m_s и пусть $\pi^k = e$. Т.к. циклы γ_i попарно коммутируют, то $\pi^k = \gamma_1^k \cdots \gamma_s^k = e$. Так как перестановки $\gamma_1^k, \dots, \gamma_s^k$ независимы, то

$$\gamma_1^k = \cdots = \gamma_s^k = e \iff m_i \mid k \text{ для всех } i.$$

Поэтому наименьшее положительное k , для которого $\pi^k = e$, есть наименьшее общее кратное чисел m_1, \dots, m_s . \square

Предложение 6.23. Порядок любого элемента конечной группы является делителем порядка группы (как обычно, под порядком множества G понимается число его элементов, которое обозначается через $|G|$).

Другими словами, если G — группа конечного порядка n , то $a^n = e \forall a \in G$.

Доказательство. Пусть $|G| = n$ и a_1, \dots, a_n — ее элементы. Пусть порядок элемента $a \in G$ равен k . Рассмотрим перестановку π_a на множестве a_1, \dots, a_n : $\pi_a(a_i) = aa_i$. Это биективное отображение, так как если $aa_i = aa_j$, то $a_i = a_j$. Разложим π_a в произведение независимых циклов. Всякий цикл имеет вид $(a_i, aa_i, \dots, a^{k-1}a_i)$, так как $a^l a_i \neq a_i$ при $1 \leq l < k$ и $\pi_a(a^{k-1}a_i) = a^k a_i = a_i$. Таким образом, все независимые циклы этой перестановки имеют длину k и если их число равно m , то $km = n$. \square

6.4. Понятие подполугруппы и подгруппы. Циклические подгруппы. Циклические группы, их порождающие и их подгруппы.

Пусть (G, \cdot) — множество с бинарной операцией. Подмножество $H \subset G$ называется *устойчивым* (говорят также “замкнутым”) относительно операции \cdot , если $ab \in H \forall a, b \in H$. В этом случае операция \cdot определена и на H . Если (G, \cdot) — полугруппа и H — устойчивое подмножество в G , то (H, \cdot) также является полугруппой, и такая полугруппа называется *подполугруппой* в (G, \cdot) .

Определение 6.24. Подмножество H в группе (G, \cdot) называется *подгруппой*, если оно устойчиво относительно операции \cdot и (H, \cdot) является группой.

Легко видеть, что подмножество H в группе G является подгруппой, если и только если выполнимы следующие условия:

- 1) $ab \in H \quad \forall a, b \in H$;
- 2) $e \in H$;
- 3) $\forall a \in H \quad a^{-1} \in H$.

Заметим, что если $H \neq \emptyset$, то 2) следует из 1) и 3).

Всякая группа G содержит так называемые несобственные подгруппы: подгруппу, совпадающую с самой группой G , и подгруппу, состоящую только из единицы.

Задача 6.25. Показать, что всякая конечная подполугруппа в группе является подгруппой.

Задача 6.26. Пусть H — (непустая и отличная от нулевой) подполугруппа в полугруппе всех неотрицательных целых чисел по сложению и d — наибольший общий делитель чисел из H . Доказать, что H содержит все достаточно большие целые числа, делящиеся на d .

Примеры. В приведенных в п. 6.3 примерах групп группа $SL(n, \mathbb{R})$ является подгруппой в $GL(n, \mathbb{R})$, группа A_n — подгруппой в S_n , группа $(\mathbb{Z}, +)$ — подгруппой в $(\mathbb{Q}, +)$ и $(\mathbb{R}, +)$; в свою очередь, $(\mathbb{Q}, +)$ — подгруппа в $(\mathbb{R}, +)$; кроме того, (\mathbb{Q}_+, \cdot) —

подгруппа в (\mathbb{Q}^*, \cdot) , (\mathbb{R}_+, \cdot) и в (\mathbb{R}^*, \cdot) ; (\mathbb{Q}^*, \cdot) — подгруппа в (\mathbb{R}^*, \cdot) , а (\mathbb{R}_+, \cdot) — в (\mathbb{R}^*, \cdot) . Всякое линейное подпространство в \mathbb{R}^n является подгруппой в $(\mathbb{R}^n, +)$. В группе S_4 имеется подгруппа $V_4 = \{\varepsilon, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$, называемая *четверной группой Клейна*.

Циклические подгруппы и группы. Пусть G — группа и $a \in G$. Множество $\{a^n\}_{n \in \mathbb{Z}}$ всех степеней элемента a является подгруппой, которая называется *циклической подгруппой*, порожденной элементом a , и обозначается через $\langle a \rangle$. Из предложения 6.19 следует

Предложение 6.27. *Порядок циклической подгруппы, порожденной элементом a , равен порядку элемента a .*

Определение 6.28. Группа G , совпадающая с циклической подгруппой, порожденной каким-либо элементом $a \in G$, т.е. состоящая из степеней этого элемента, называется *циклической группой*; этот элемент a называется *порождающим* циклической группы G .

Примеры циклических групп.

- 1) Группа $(\mathbb{Z}, +)$. В качестве порождающих могут быть взяты числа 1 и -1 . Это бесконечная циклическая группа.
- 2) Множество поворотов евклидовой плоскости вокруг фиксированной точки на углы, кратные $2\pi/n$, является циклической группой порядка n с порождающим — поворотом на угол $2\pi/n$.

Очевидно, имеет место

Предложение 6.29. *Конечная группа порядка n является циклической, если и только если она содержит элемент порядка n ; всякий элемент порядка n служит ее порождающим.*

Следствие 6.30. *Всякая группа простого порядка является циклической.*

Доказательство. В силу предложения 6.23 всякий ее неединичный элемент имеет порядок, равный порядку группы. \square

Предложение 6.31. Пусть $G = \langle a \rangle$ — циклическая группа. Если G бесконечная, то в качестве порождающих могут быть взяты только элементы a и a^{-1} . Если $|G| = n$, то элемент a^k служит порождающим для G , если и только если k и n взаимно просты.

Доказательство. Первое утверждение очевидно. Второе следует из предложений 6.29 и 6.20. \square

Следствие 6.32. Число различных порождающих циклической группы порядка n равно $\varphi(n)$ (функция Эйлера, значение которой $\varphi(n)$ равно количеству положительных целых чисел, не превосходящих n и взаимно простых с n).

Задача 6.33. а) Пусть a и b — коммутирующие элементы группы, порядки которых взаимно просты. Доказать, что $O(ab) = O(a)O(b)$.

б) Пусть a и b — коммутирующие элементы группы G , имеющие конечные порядки. Тогда в G имеется элемент, порядок которого равен наименьшему общему кратному $O(a)$ и $O(b)$.

в) Число $d = \min\{k : a^k = e \ \forall a \in G\}$ называется показателем группы G . Если такое d существует, то оно равно наименьшему общему кратному порядков элементов G и, когда G конечна, является делителем $|G|$. Показать, что в конечной абелевой группе существует элемент, порядок которого равен показателю G . Верно ли это для конечной неабелевой группы?

г) Конечная абелева группа является циклической, если и только если ее показатель равен ее порядку. Обязана ли быть циклической при выполнении этого условия произвольная конечная группа?

Предложение 6.34. Пусть $G = \langle a \rangle$ — циклическая группа. Всякая подгруппа H в G циклическая и, если порядок группы G равен n , порождается элементом a^k , где $k > 0$ является делителем n .

Доказательство. Если H состоит только из единицы, то утверждение очевидно. Пусть $H \neq \{e\}$. Тогда существует $a^m \in H$ с $m \neq 0$. Если $m < 0$, то имеется элемент $a^{-m} \in H$ с положительным показателем. Пусть k — наименьшее среди положительных целых чисел m , для которых $a^m \in H$. Покажем, что тогда если $a^m \in H$, то $k \mid m$. Имеем: $m = qk + r$, $0 \leq r < k$, и $a^r = a^m a^{-qk} \in H$. В силу выбора k число $r = 0$. Таким образом, $H = \langle a^k \rangle$. Если $|G| = n$, то $a^n \in H$ и $k \mid n$. \square

Следствие 6.35. *Если $G = \langle a \rangle$ — бесконечная циклическая группа, то множество ее подгрупп находится в биективном соответствии с множеством неотрицательных целых чисел: $k \leftrightarrow \langle a^k \rangle$. Если $G = \langle a \rangle$ — циклическая группа порядка n , то множество ее подгрупп находится в биективном соответствии с множеством делителей числа n : для всякого делителя d числа n имеется единственная подгруппа $\langle a^{n/d} \rangle$ порядка d .*

Следствие 6.36. *Пусть $G = \langle a \rangle$ — циклическая группа порядка n . Для всякого делителя d числа n все элементы группы G порядка d содержатся в единственной циклической подгруппе порядка d и являются ее порождающими; их число равно $\varphi(d)$.*

6.5. Понятия гомоморфизма и изоморфизма. Классификация циклических групп с точностью до изоморфизма

Пусть (G, \cdot) и $(K, *)$ — два множества, на которых заданы бинарные операции.

Определение 6.37. *Отображение $f: (G, \cdot) \rightarrow (K, *)$ называется гомоморфизмом, если оно “сохраняет операцию”, т.е. $f(a \cdot b) = f(a) * f(b) \forall a, b \in G$.*

Если $f: (G, \cdot) \rightarrow (K, *)$ и $g: (K, *) \rightarrow (L, \star)$ — гомоморфизмы, то, очевидно, их композиция $g \circ f: (G, \cdot) \rightarrow (L, \star)$ — также гомоморфизм.

Предложение 6.38. Пусть $f: (G, \cdot) \rightarrow (K, *)$ — гомоморфизм. Его образ $\text{Im } f$ устойчив относительно операции $*$. Если (H, \cdot) — полугруппа (группа), то $(\text{Im } f, *)$ — полугруппа (группа). Если (G, \cdot) и $(K, *)$ — группы, то $f(e)$ — единица группы K , $f(a^{-1}) = f(a)^{-1} \forall a \in G$ и $\text{Im } f$ является подгруппой в K .

Доказательство. Пусть $a', b', c' \in \text{Im } f$, т.е. $a' = f(a)$, $b' = f(b)$, $c' = f(c)$, $a, b, c \in G$. Тогда

$$a' * b' = f(a) * f(b) = f(ab) \in \text{Im } f.$$

Пусть G — полугруппа. Тогда

$$\begin{aligned} a' * (b' * c') &= f(a) * (f(b) * f(c)) = f(a) * f(bc) = \\ &= f(a(bc)) = f((ab)c) = f(ab) * f(c) = (a' * b') * c', \end{aligned}$$

т.е. $\text{Im } f$ — полугруппа.

Пусть G — группа и $e' = f(e)$. Тогда $e' * a' = f(e) * f(a) = f(ea) = a'$ и, аналогично, $a' * e' = a'$, т.е. $f(e)$ — единица в $\text{Im } f$. $f(a^{-1}) * a' = f(a^{-1}) * f(a) = f(a^{-1}a) = f(e) = e'$ и, аналогично, $a' * f(a^{-1}) = e'$, т.е. $f(a^{-1})$ — обратный для a' в $\text{Im } f$. Так как $e' * e' = e'$, то если K — группа, e' является единицей в K и $f(a^{-1})$ является обратным для $f(a)$ в K . \square

Замечание 6.39. Согласно предложению 6.38, при гомоморфизме групп единица переходит в единицу. Это не всегда так при гомоморфизме полугрупп. Например, пусть $M_n(\mathbb{R})$ обозначает полугруппу квадратных матриц порядка n с операцией умножения. При гомоморфизме $f: M_{n-1}(\mathbb{R}) \rightarrow M_n(\mathbb{R})$, при котором $f(A)$ получается из A окаймлением посредством нулевых строки и столбца, $f(E)$ не совпадает с единицей в $M_n(\mathbb{R})$.

Примеры гомоморфизмов.

- 1) Если H — устойчивое подмножество в (G, \cdot) , то имеется гомоморфизм вложения $i: (H, \cdot) \rightarrow (G, \cdot)$, при котором $i(x) = x \forall x \in H$.
- 2) Если G и K — любые группы, то имеется тривиальный гомоморфизм $f: G \rightarrow K$, при котором $f(a) = e \forall a \in G$.

- 3) Отображения $f: (\mathbb{R}^*, \cdot) \rightarrow (R_+, \cdot) : f(a) = |a|$ и $f: \text{GL}(n, \mathbb{R}) \rightarrow (\mathbb{R}^*, \cdot), f(A) = \det A$ являются гомоморфизмами.
- 4) Пусть (G, \cdot) — произвольная абелева группа и n — фиксированное целое число. Отображение $f(a) = a^n$ является гомоморфизмом (согласно предложению 6.13).

Предложение 6.40. Пусть $f: G \rightarrow K$ — гомоморфизм групп. Для всякого $a \in G$ порядок $f(a)$ является делителем порядка a .

Доказательство. Пусть $O(a) = n$. Тогда $f(e) = f(a^n) = f(a)^n = e$, а потому $O(f(a)) \mid n$. \square

Предложение 6.41. Пусть $G = \langle a \rangle$ — циклическая группа и (K, \cdot) — произвольная группа. Если G — бесконечная циклическая группа (циклическая группа порядка n), то для всякого элемента $b \in K$ (соответственно такого, что $b^n = e$) существует единственный гомоморфизм $f: G \rightarrow K$, при котором $f(a) = b$.

Доказательство. Так как при гомоморфизме $f: G \rightarrow K$ $f(a^k) = (f(a))^k$, то f однозначно задается своим значением $f(a)$. Если G — бесконечная циклическая группа, то поскольку представление элемента группы G в виде a^k однозначно, то для всякого $b \in K$ можно задать отображение $f(a^k) = b^k$, которое является гомоморфизмом и при котором $f(a) = b$. Пусть теперь G — циклическая группа порядка n . Согласно предложению 6.40, условие $b^n = e$ является необходимым для существования гомоморфизма $f: G \rightarrow K$, при котором $f(a) = b$. Покажем, что оно является и достаточным. Снова зададим $f(a^k) = b^k$. Но теперь запись элемента G в виде a^k не единственна, а потому нужно проверить корректность определения f , т.е. нужно показать, что если $a^k = a^l$, то $b^k = b^l$. Но $a^k = a^l \iff l - k \equiv 0 \pmod{n}$, т.е. $l = k + qn$. Поэтому $b^l = b^{k+qn} = (b^n)^q b^k = b^k$. Итак, f определено корректно и, очевидно, является гомоморфизмом. \square

Определение 6.42. Пусть (G, \cdot) и $(K, *)$ — множества с бинарными операциями. Отображение $f: G \rightarrow K$ называется *изоморфизмом*, если оно биективно и является гомоморфизмом.

Короче: изоморфизм это биективный гомоморфизм. Очевидно, композиция изоморфизмов является изоморфизмом.

Предложение 6.43. *Отображение, обратное к изоморфизму, также является изоморфизмом.*

Доказательство. Пусть $f: (G, \cdot) \rightarrow (K, *)$ — изоморфизм. Если $a', b' \in K$, то $a' = f(a)$, $b' = f(b)$, $a, b \in G$ и

$$\begin{aligned} f^{-1}(a' * b') &= f^{-1}(f(a) * f(b)) = \\ &= f^{-1}(f(ab)) = ab = f^{-1}(a') \cdot f^{-1}(b'). \end{aligned}$$

Таким образом, f^{-1} — изоморфизм. □

Предложение 6.43 показывает, что существование изоморфизма $(G, \cdot) \rightarrow (K, *)$ равносильно существованию изоморфизма $(K, *) \rightarrow (G, \cdot)$. Это позволяет говорить об изоморфизме между (G, \cdot) и $(K, *)$, не уточняя направление отображения.

Определение 6.44. Два множества с бинарными операциями (G, \cdot) и $(K, *)$ называются *изоморфными*, если между ними существует изоморфизм. Обозначается: $(G, \cdot) \cong (K, *)$.

Важность этого понятия состоит в том, что задание изоморфизма позволяет отождествить множества и заданные на них операции, и тем самым свойства этих операций оказываются полностью идентичными. В частности, изоморфные множества (G, \cdot) и $(K, *)$ имеют одинаковые порядки; если одно из них является полугруппой (группой), то и другое является полугруппой (группой); если одно из них — абелева (циклическая) группа, то и другое — абелева (циклическая) группа. Соответствующие друг другу при изоморфизме элементы имеют одинаковые порядки.

Пример изоморфизма: для всякого положительного действительного числа $a \neq 1$ функции

$$x \mapsto a^x : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+, \cdot); \quad x \mapsto \log_a x : (\mathbb{R}_+, \cdot) \rightarrow (\mathbb{R}, +)$$

являются взаимно обратными изоморфизмами.

Задача 6.45. Показать, что группы $(\mathbb{Q}, +)$ и (\mathbb{Q}_+, \cdot) не только не являются изоморфными, но даже всякий гомоморфизм $f: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}_+, \cdot)$ тривиален. В то же время существует бесконечно много различных, в том числе сюръективных, гомоморфизмов $f: (\mathbb{Q}_+, \cdot) \rightarrow (\mathbb{Q}, +)$.

К числу наиболее важных задач относятся задачи классификации алгебраических объектов какого-либо типа с точностью до изоморфизма. Они состоят в том, чтобы в данном классе объектов выбрать такой набор попарно неизоморфных между собой объектов, что всякий объект из рассматриваемого класса был изоморфен одному из выбранных. Следующее предложение и его следствие решают такую задачу в простейших случаях циклических групп и групп простого порядка.

Предложение 6.46. *Две циклические группы гомоморфны в том и только том случае, если они имеют одинаковые порядки.*

Доказательство. Действительно, если циклические группы $G = \langle a \rangle$ и $K = \langle b \rangle$ имеют одинаковые порядки, то согласно предложению 6.41 существует гомоморфизм $f: G \rightarrow K$, при котором $f(a) = b$ и который, очевидно, биективен. \square

Следствие 6.47. *Любые две группы одного и того же простого порядка изоморфны между собой.*

Доказательство. Действительно, согласно следствию 6.31 любая группа простого порядка является циклической. \square

6.6. Задание конечной группы таблицей Кейли. Теорема Кейли

Пусть G — конечное множество порядка n и $\{a_1, \dots, a_m\}$ — его элементы. Операцию на G можно задать таблицей умножения (называемой таблицей Кейли), в которой на пересечении

i -ой строки и j -го столбца стоит произведение $a_i a_j$:

	a_1	a_2	a_j	a_n
a_1	$a_1 a_1$	$a_1 a_2$	$a_1 a_j$	$a_1 a_n$
a_2	$a_2 a_1$	$a_2 a_2$	$a_2 a_j$	$a_2 a_n$
a_i	$a_i a_1$	$a_i a_2$	$a_i a_j$	$a_i a_n$
a_n	$a_n a_1$	$a_n a_2$	$a_n a_j$	$a_n a_n$

Каким условиям должна удовлетворять эта таблица, чтобы она задавала группу? Однозначная разрешимость уравнений $ax = b$ и $ya = b$ равносильна тому, что в каждой строке и каждом столбце таблицы стоят все элементы G в некотором порядке. Чтобы, скажем, элемент a_1 был единицей, в первой строке и первом столбце элементы группы должны быть записаны в исходном порядке. Наиболее трудоемкой является проверка того, что операция, задаваемая таблицей, ассоциативна. Это будет заведомо так, если установить изоморфизм множества с операцией, заданной таблицей, и некоторой уже известной группой. Коммутативность операции равносильна тому, что таблица симметрична относительно главной диагонали.

Задача 6.48. С помощью построения таблиц Кейли классифицировать с точностью до изоморфизма группы порядка ≤ 7 .

Теорема 6.49 (теорема Кейли). *Всякая группа порядка n изоморфна некоторой подгруппе симметрической группы S_n .*

Доказательство. Пусть $G = \{a_1, \dots, a_n\}$ — группа порядка n . Составим для группы G таблицу Кейли и сопоставим каждому элементу $a_i \in G$ перестановку на множестве G , задаваемую i -ой строкой таблицы Кейли, т.е. рассмотрим отображение $f: G \rightarrow S_n$, при котором для всякого $a \in G$ $f(a) = \pi_a \in S_n$, где $\pi_a(a_j) = aa_j$. Разным элементам группы G соответствуют разные перестановки, так как в каждом столбце таблицы Кейли нет одинаковых элементов (для инъективности f достаточно того, что это так хотя бы в одном столбце). Таким образом, отображение $G \rightarrow \text{Im } f$ биективно. Докажем, что оно является гомоморфизмом. Нужно показать, что $\pi_{ab} = \pi_a \circ \pi_b \forall a, b \in G$. Для

всякого $a_j \in G$ имеем $\pi_{ab}(a_j) = (ab)a_j = a(ba_j) = \pi_a(\pi_b(a_j))$. Поскольку f — гомоморфизм, $\text{Im } f$ есть подгруппа в S_n . \square

Замечание 6.50. Эта теорема не дает классификации групп порядка n , так как у нас нет способа перечислить все с точностью до изоморфизма подгруппы в S_n .

6.7. Разложение группы на смежные классы. Теорема Лагранжа

Пусть (G, \cdot) — группа. Для двух подмножеств $K, L \subset G$ определим их произведение $KL = \{ab \mid a \in K, b \in L\}$. Для множества K пусть $K^{-1} = \{a^{-1} \mid a \in K\}$.

Определение 6.51. Пусть H — подгруппа в G . Множества вида $gH = \{gh \mid h \in H\}$ (при фиксированном $g \in G$) называются *левыми смежными классами* группы G по подгруппе H . Аналогично, множества вида $Hg = \{hg \mid h \in H\}$ называются *правыми смежными классами* по подгруппе H .

Отметим, что одним из смежных классов по H , как левым, так и правым, является сама подгруппа $H = eH = He$.

Следующее предложение описывает основные свойства левых смежных классов. Правые смежные классы обладают аналогичными свойствами.

Предложение 6.52. *Каждый левый смежный класс определяется любым своим элементом, т.е. если $g' \in gH$, то $g'H = gH$. Два левых смежных класса либо не пересекаются, либо совпадают. Объединение всех левых смежных классов равно G . отображение $H \rightarrow gH$, при котором $h \mapsto gh$, биективно (в частности, все смежные классы являются множествами одного и того же порядка).*

Доказательство. Пусть $g' \in gH$, т.е. $g' = gh$, $h \in H$. Тогда $g'H = ghH \subseteq gH$; так как $g = g'h^{-1}$, то $g \in g'H$ и $gH \subseteq g'H$; таким образом, $gH = g'H$. Если два смежных класса g_1H и g_2H пересекаются: $\exists g \in g_1H \cap g_2H$, то, по предыдущему, $g_1H = gH = g_2H$. Так как $g \in gH \forall g \in G$, то $\cup_{g \in G} gH = G$. отображение $H \rightarrow gH$ сюръективно по определению смежного класса, и оно инъективно, так как $gh_1 = gh_2 \implies h_1 = h_2$. \square

Как известно, задание разбиения множества G на попарно непересекающиеся классы равносильно заданию на множестве G отношения эквивалентности: если задано разбиение, то эквивалентными считаются элементы, попавшие в один класс разбиения, а если задано отношение эквивалентности, то каждый класс составляется из множества всех элементов, эквивалентных некоторому фиксированному. Отношения эквивалентности, соответствующие разбиениям группы G на левые или правые смежные классы по подгруппе H , описываются следующим предложением.

Предложение 6.53. *Два элемента $g_1, g_2 \in G$ принадлежат одному левому (соответственно, правому) смежному классу по подгруппе H , если и только если $g_1^{-1}g_2 \in H$ (соответственно, $g_2g_1^{-1} \in H$).*

Доказательство. $g_2 \in g_1H \iff g_2 = g_1h$ для некоторого $h \in H \iff g_1^{-1}g_2 \in H$. Аналогично для правых смежных классов. \square

Предложение 6.54. *Отображение $x \mapsto x^{-1}$ группы G на себя задает биективное соответствие между множествами левых смежных классов и правых смежных классов группы G по подгруппе H .*

Доказательство.

$$\begin{aligned} gH)^{-1} &= \{(gh)^{-1} \mid h \in H\} = \\ &= \{h^{-1}g^{-1} \mid h \in H\} = \{hg^{-1} \mid h \in H\} = Hg^{-1}. \end{aligned}$$

\square

Определение 6.55. Число (левых или правых) смежных классов группы G по подгруппе H равно числу правых смежных классов по H называется *индексом подгруппы H в G* и обозначается через $(G : H)$.

Из разложения группы на левые (или правые) смежные классы по подгруппе в силу предложения 6.52 получаем:

Теорема 6.56 (теорема Лагранжа). *Пусть G — конечная группа и H — ее подгруппа. Тогда $|H| \cdot (G : H) = |G|$.*

Следствие 6.57. *Порядок подгруппы и индекс подгруппы являются делителями порядка группы.*

Применяя это следствие к циклической подгруппе, порожденной элементом a , получаем уже ранее доказанное (см. предложение 6.23) утверждение о том, что порядок любого элемента конечной группы является делителем порядка группы.

Примеры. 1) $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$ — подгруппа, состоящая из чисел, кратных фиксированному натуральному числу n . Смежный класс $a + n\mathbb{Z}$ ($a \in \mathbb{Z}$) состоит из чисел, имеющих при делении на n такой же остаток, что и a , т.е. два числа $a, b \in \mathbb{Z}$ лежат в одном смежном классе, если и только если $n \mid b - a$, что записывается также в виде $a \equiv b \pmod{n}$. Смежные классы по подгруппе $n\mathbb{Z}$ называются *классами вычетов* по модулю n . Индекс $(\mathbb{Z} : n\mathbb{Z}) = n$.

2) $G = (\mathbb{R}, +)$, $H = 2\pi\mathbb{Z}$ — множество чисел, являющихся целыми кратными числа 2π . Смежные классы $\alpha + 2\pi\mathbb{Z}$ находятся в биективном соответствии с углами, которые образуют векторы на плоскости с положительным направлением оси абсцисс.

3) $G = (\mathbb{R}^n, +)$, H — линейное подпространство. Смежные классы $x + H$, ($x \in \mathbb{R}^n$) — это линейные многообразия (плоскости) в \mathbb{R}^n , получаемые параллельным переносом из H . Разбиение на смежные классы — это разбиение на плоскости, параллельные H .

4) $G = \text{GL}(n, \mathbb{R})$, $H = \text{SL}(n, \mathbb{R})$. Смежные классы, как левые $A \cdot \text{SL}(n, \mathbb{R})$, так и правые $\text{SL}(n, \mathbb{R}) \cdot A$ ($A \in \text{GL}(n, \mathbb{R})$) — это множества матриц, имеющих фиксированный определитель, равный $\det(A)$.

5) $G = S_n$, $H = A_n$. Разбиение на смежные классы (левые и правые) — это разбиение S_n на множества четных и нечетных перестановок. Индекс $(S_n : A_n) = 2$.

6) $G = S_n$, $H = \{\pi \in S_n : \pi(n) = n\}$ (H можно естественным образом отождествить с S_{n-1}). Левый смежный класс τS_{n-1} ($\tau \in S_n$) — это множество таких перестановок $\pi \in S_n$, что $\pi(n) = i$, где $i = \tau(n)$. Правый смежный

класс $S_{n-1}\tau$ ($\tau \in S_n$) состоит из таких перестановок π , что $\pi^{-1}(n) = i$, где $i = \tau^{-1}(n)$. В отличие от предыдущих примеров здесь разбиения на левые и правые смежные классы различны. Индекс $(S_n : S_{n-1}) = n$.

6.8. Нормальные подгруппы. Структура гомоморфизмов. Факторгруппы

Определение 6.58. Подгруппа H группы G называется *нормальной*, если разбиения G на левые и правые смежные классы по H совпадают, т.е. $gH = Hg$ для всякого $g \in G$. То, что H — нормальная подгруппа в G , обозначают так: $H \triangleleft G$.

Предложение 6.59. Следующие условия для подгруппы H группы G эквивалентны:

- 1) H нормальна в G ;
- 2) $gHg^{-1} = H \forall g \in G$;
- 3) $gHg^{-1} \subseteq H \forall g \in G$.

Доказательство. 1) \Rightarrow 2) $gH = Hg \Rightarrow gHg^{-1} = Hgg^{-1} \Rightarrow gHg^{-1} = H$ для всех $g \in G$.

2) \Rightarrow 3) очевидно.

3) \Rightarrow 1) $gHg^{-1} \subseteq H \Rightarrow gHg^{-1}g \subseteq Hg \Rightarrow gH \subseteq Hg$. Меняем 3) для g^{-1} : $g^{-1}Hg \subseteq H \Rightarrow Hg \subseteq gH$. Итак, $gH = Hg$ для всех $g \in G$. \square

Примеры. 1) В абелевой группе всякая подгруппа нормальна.

2) Всякая подгруппа индекса 2 нормальна, т.к. второй смежный класс (левый и правый) — дополнение к подгруппе. Обязана ли подгруппа индекса 3 быть нормальной?

3) $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$, но S_{n-1} не является нормальной в S_n (см. примеры в п. 6.7).

Произвольное отображение множеств $f: X \rightarrow Y$ определяет отношение эквивалентности на X (обозначим его через R_f): $x_1 \overset{R_f}{\sim} x_2 \iff f(x_1) = f(x_2)$. Соответствующее разбиение X на классы — это разбиение X на полные прообразы $f^{-1}(y)$ элементов $y \in \text{Im } f$: $f^{-1}(y) = \{x \in X: f(x) = y\}$. Пусть задано произвольное отношение эквивалентности R на X . Оно определяет разбиение множества X на классы R -эквивалентных между собой элементов. Класс элементов, эквивалентных элементу $a \in X$, обозначаем через $[a]$. Имеем: $[a] = [b] \iff a \sim b$. Множество этих классов называется *фактормножеством* X по R и обозначается через X/R . Имеется каноническое отображение $\pi: X \rightarrow X/R$, при котором для $x \in X$ $\pi(x)$ есть класс эквивалентности $[x]$, в котором лежит x . Вернемся к отображению $f: X \rightarrow Y$. Рассмотрим каноническое отображение $\pi_f: X \rightarrow X/R_f$ и определим отображение $\bar{f}: X/R_f \rightarrow Y$, при котором класс $f^{-1}(y)$ отображается в y ; \bar{f} инъективно и оно биективно отображает X/R_f на $\text{Im } f$. Исходное отображение f является композицией $f = \bar{f} \circ \pi_f$ сюръективного отображения π_f и инъективного отображения \bar{f} . Эту факторизацию отображения f можно изобразить в виде диаграммы

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \pi_f \searrow & & \nearrow \bar{f} \\ & X/R_f & \end{array},$$

о которой говорят, что она коммутативна, поскольку два пути по ней f и $\bar{f} \circ \pi_f$ из X в Y совпадают.

Отметим, что при заданных f и π_f отображение \bar{f} является единственным отображением $X/R_f \rightarrow Y$, для которого диаграмма коммутативна.

Пусть теперь $f: (G, \cdot) \rightarrow (K, *)$ — гомоморфизм множеств с бинарными операциями. Отношение эквивалентности R_f на G , соответствующее гомоморфизму f , обладает следующим свойством: если $a_1 \overset{R_f}{\sim} a_2$ и $b_1 \overset{R_f}{\sim} b_2$, то $a_1 b_1 \overset{R_f}{\sim} a_2 b_2$. Действительно, $f(a_1) = f(a_2)$, $f(b_1) = f(b_2)$ и $f(a_1 b_1) = f(a_1) * f(b_1) = f(a_2) * f(b_2) = f(a_2 b_2) \implies a_1 b_1 \overset{R_f}{\sim} a_2 b_2$.

Определение 6.60. Отношение эквивалентности R на (G, \cdot) называется *отношением конгруэнтности*, или *конгру-*

эцией, если

$$a_1 \overset{R}{\sim} a_2 \text{ и } b_1 \overset{R}{\sim} b_2 \implies a_1 b_1 \overset{R}{\sim} a_2 b_2. \quad (6.4)$$

Если на (G, \cdot) задана конгруэнция R , то на фактормножестве G/R можно ввести операцию \bullet :

$$[a] \bullet [b] = [ab]$$

(как и выше, через $[a]$ обозначается класс эквивалентности элемента a). В силу 6.4 это определение корректно (не зависит от выбора элементов a и b в классах $[a]$ и $[b]$) и каноническое отображение $\pi: G \rightarrow G/R$, при котором $\pi(a) = [a]$, является гомоморфизмом. Соответствующая этому гомоморфизму конгруэнция совпадает с исходной. Таким образом, доказано

Предложение 6.61. *Отношение эквивалентности на множестве с бинарной операцией соответствует гомоморфизму, если и только если оно является конгруэнцией.*

Теорема 6.62 (о гомоморфизме для множеств с бинарной операцией). *Пусть $f: (G, \cdot) \rightarrow (K, *)$ — гомоморфизм множеств с бинарной операцией, R_f — соответствующая конгруэнция на G , $\pi_f: (G, \cdot) \rightarrow (G/R_f, \cdot)$ — канонический гомоморфизм и $\bar{f}: G/R_f \rightarrow K$ — отображение, при котором $\bar{f}([a]) = f(a)$. Тогда $f = \bar{f} \circ \pi_f$ и \bar{f} является изоморфизмом $(G/R_f, \cdot)$ на $(\text{Im } f, *)$.*

Остается только проверить, что \bar{f} — гомоморфизм. Но это очевидно:

$$\bar{f}([a] \cdot [b]) = \bar{f}([ab]) = f(ab) = f(a) * f(b) = \bar{f}([a]) * \bar{f}([b]).$$

Рассмотрим теперь случай, когда (G, \cdot) — группа. Отличие от общего случая состоит в том, что для групп имеется очень простое описание конгруэнций.

Определение 6.63. Пусть $f: (G, \cdot) \rightarrow (K, *)$ — гомоморфизм группы (G, \cdot) в множество с бинарной операцией $(K, *)$. Тогда $(\text{Im } f, *)$ — группа и пусть e' — единица группы $\text{Im } f$. *Ядром f (обозначается $\text{Ker } f$) называется $f^{-1}(e')$, т.е. $\text{Ker } f = \{a \in G: f(a) = e'\}$.*

Предложение 6.64. $\text{Ker } f$ — нормальная подгруппа в G . Разбиение G , соответствующее гомоморфизму f , — это разбиение на смежные классы по подгруппе $\text{Ker } f$.

Доказательство. Покажем, что $\text{Ker } f$ — подгруппа. Если $a, b \in \text{Ker } f$, то $f(ab) = f(a)f(b) = e'$, т.е. $ab \in \text{Ker } f$. Так как $f(e) = e'$, то $e \in \text{Ker } f$. Если $a \in \text{Ker } f$, то $f(a^{-1}) = f(a)^{-1} = e'$, т.е. $a^{-1} \in \text{Ker } f$. Пусть теперь $a \in \text{Ker } f$ и $g \in G$. Тогда $f(gag^{-1}) = f(g)e'f(g)^{-1} = e'$, т.е. $gag^{-1} \in \text{Ker } f$. Следовательно, $\text{Ker } f \triangleleft G$.

Пусть $a' \in \text{Im } f$, $a' = f(a)$; тогда $f^{-1}(a')$ есть один из классов разбиения, соответствующего f . Покажем, что $f^{-1}(a') = a \text{Ker } f$. Так как $f(a \text{Ker } f) = f(a) = a'$, то $a \text{Ker } f \subseteq f^{-1}(a')$. Обратно, пусть $b \in f^{-1}(a')$, тогда $f(b) = a'$, $f(a^{-1}b) = f(a)^{-1}f(b) = e'$, т.е. $a^{-1}b \in \text{Ker } f$, $b \in a \text{Ker } f$. Таким образом, $f^{-1}(a') = a \text{Ker } f$. \square

Теорема 6.65. Отношение эквивалентности на группе G является конгруэнцией, если и только если оно соответствует разбиению группы G на смежные классы по некоторой нормальной подгруппе.

Доказательство. Пусть R — конгруэнция на G . Тогда на фактормножестве G/R вводится операция и имеется канонический гомоморфизм $\pi: G \rightarrow G/R$. Ему соответствует разбиение G на классы эквивалентности относительно R и, согласно предложению 6.64, оно совпадает с разбиением на смежные классы по нормальной подгруппе $\text{Ker } \pi$ (которая, очевидно, совпадает с классом элементов, R -эквивалентных единице группы).

Обратно, пусть задана произвольная нормальная подгруппа H . Покажем, что отношение эквивалентности, соответствующее разбиению на смежные классы по H , является конгруэнцией. В этом случае класс эквивалентности $[a] = aH$. Надо показать, что если $a_1 \sim a_2$, $b_1 \sim b_2$, т.е. $a_2 \in a_1H$, $b_2 \in b_1H$, то $a_1b_1 \sim a_2b_2$. Имеем: $a_2 = a_1h$, $b_2 = b_1h'$, $a_2b_2 = (a_1h)(a_2h') = (a_1b_1)(b_1^{-1}hb_1)h'$. Так как H нормальна, то $b_1^{-1}hb_1 \in H$, откуда $a_2b_2 \in a_1b_1H$, т.е. $a_1b_1 \sim a_2b_2$. \square

Множество смежных классов группы G по нормальной подгруппе H обозначается через G/H . Согласно данной выше общей конструкции на этом множестве корректно определяется

операция

$$aN \cdot bN = abN$$

(корректность этого определения следует также из того, что класс abN является произведением $aN \cdot bN$ как подмножеств в G , а потому не зависит от выбора представителей a и b в классах aN и bN). Имеем канонический гомоморфизм $\pi: G \rightarrow G/H$. Так как образ группы при гомоморфизме является группой, то G/H с введенной операцией есть группа. Она называется *факторгруппой* группы G по H . Единицей группы G/H служит $\pi(e) = H$, обратный к aN есть $a^{-1}N$.

Применение общей теоремы о гомоморфизме (теоремы 6.62) к случаю гомоморфизмов групп дает следующую теорему.

Теорема 6.66 (о гомоморфизме для групп). Пусть $f: (G, \cdot) \rightarrow (K, *)$ — гомоморфизм групп, $H = \text{Ker } f$, $\pi_f: (G, \cdot) \rightarrow (G/H, \cdot)$ — канонический гомоморфизм и $\bar{f}: G/H \rightarrow K$ — отображение, при котором $\bar{f}(aN) = f(a)$. Тогда $f = \bar{f} \circ \pi_f$ и \bar{f} является изоморфизмом $(G/H, \cdot)$ на $(\text{Im } f, *)$.

§7. Понятия кольца и поля

7.1. Определение кольца. Общие и специальные свойства, примеры

Определение 7.1. Множество R , на котором заданы две бинарные операции: $+$ (сложение) и \cdot (умножение) называется *кольцом*, если выполняются следующие условия:

- 1) $(R, +)$ — абелева группа;
- 2) выполняются законы дистрибутивности:

$$a(b+c) = ab+ac, \quad (a+b)c = ac+bc \quad \forall a, b, c \in R.$$

Следующее предложение показывает, что элемент $0 \in R$ и операция вычитания $a-b = a+(-b)$ в произвольном кольце обладают обычными свойствами.

Предложение 7.2. Пусть R — кольцо. $\forall a, b, c \in R$

$$a \cdot 0 = 0 \cdot a = 0, \quad a(-b) = -ab = (-a)b,$$

$$a(b-c) = ab-ac, \quad (a-b)c = ac-bc.$$

Доказательство. Имеем:

$$a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0 \implies a \cdot 0 = 0;$$

$$a(-b) + ab = a(-b+b) = a \cdot 0 = 0 \implies a(-b) = -ab;$$

$$a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-ac) = ab - ac.$$

Остальные равенства доказываются аналогично. □

Заметим, что в общем определении кольца не требуется, чтобы операция умножения была ассоциативной. Важным примером кольца с неассоциативным умножением является множество трехмерных векторов с обычной операцией сложения и векторным умножением.

Определение 7.3. Кольцо R называется *ассоциативным*, если оно удовлетворяет также условию

3) (G, \cdot) — полугруппа.

Поскольку в дальнейшем мы будем рассматривать только ассоциативные кольца, то под названием “кольцо” мы всегда будем понимать “ассоциативное кольцо”.

Абелеву группу $(R, +)$ называют *аддитивной группой кольца*, а полугруппу (R, \cdot) — его *мультипликативной полугруппой*.

Определение 7.4. Кольцо R называется *кольцом с единицей*, если выполняется условие

4) существует нейтральный элемент относительно операции умножения.

Такой элемент, как мы знаем, может быть только один; он называется *единицей кольца* и обозначается через 1. Заметим, что если $1 = 0$, то кольцо состоит только из одного элемента 0. Такое кольцо называется тривиальным (или нулевым). В кольце с 1 можно говорить об обратных элементах относительно операции умножения и об обратимых элементах. Множество $U(R)$ всех обратимых элементов кольца с единицей устойчиво относительно операции умножения и является группой. Ее также называют *группой единиц* кольца R .

Определение 7.5. Элемент a кольца R называется левым (правым) делителем нуля в R , если в R существует такой элемент $b \neq 0$, что $ab = 0$ (соответственно, $ba = 0$).

Элемент 0 в любом кольце, согласно этому определению, является (тривиальным) делителем нуля.

Определение 7.6. Кольцо R называется *кольцом без делителей нуля*, если оно не содержит нетривиальных делителей нуля, т.е. удовлетворяет условию

5) если для $a, b \in R$ имеет место $ab = 0$, то $a = 0$ или $b = 0$.

Очевидно, это равносильно тому, что множество $R^* = R \setminus \{0\}$ устойчиво относительно умножения.

Предложение 7.7. *В кольце R можно сокращать слева (справа) на элемент $a \in R$, если и только если a не является левым (соответственно, правым) делителем нуля. В кольце с единицей обратимые элементы не являются делителями нуля.*

Доказательство. Действительно, если на a возможно сокращение слева, то из $ab = 0 = a \cdot 0$ следует, что $b = 0$. Обратное, если a не является левым делителем нуля и $ab = ac$, то $ab - ac = a(b - c) = 0 \implies b - c = 0$, т.е. $b = c$. Если a обратим и $ab = 0$, то $b = a^{-1} \cdot 0 = 0$. \square

Определение 7.8. Кольцо R называется *коммутативным*, если выполняется условие

6) операция умножения в R коммутативна.

Определение 7.9. Кольцо R называется *телом* (или *кольцом с делением*), если

7) R содержит $1 \neq 0$, и всякий ненулевой элемент из R обратим.

Из предложения 7.7 следует, что в теле нет делителей нуля. Если R — тело, то $U(R) = R^* = R \setminus \{0\}$. R^* называется *мультипликативной группой тела*.

Определение 7.10. *Полем* называется коммутативное кольцо с $1 \neq 0$, в котором всякий ненулевой элемент обратим.

Другими словами, полем называется коммутативное тело. В поле выполняются все условия 1)–7). Важность понятия поля связана с тем, что все изложенные ранее в курсе высшей алгебры результаты, касающиеся систем линейных уравнений, определителей, линейной зависимости векторов, понятий ранга, размерности, базиса, подпространства, теории матриц, полностью сохраняются, если в них заменить действительные числа элементами произвольного фиксированного поля.

Примеры. Во всех примерах, когда операции не указаны, имеются в виду обычные сложение и умножение.

- 1) \mathbb{Z} — коммутативное кольцо с 1 без делителей нуля, не являющееся полем; $U(\mathbb{Z}) = \{\pm 1\}$.
- 2) \mathbb{Q}, \mathbb{R} — поля.
- 3) Если n — целое число > 1 , то $n\mathbb{Z}$ — коммутативное кольцо без делителей нуля, не имеющее единицы.
- 4) $M_n(\mathbb{R})$ при $n \geq 2$ — некоммутативное кольцо с единицей. $U(M_n(\mathbb{R})) = GL(n, \mathbb{R})$. Это кольцо содержит делители нуля.

Задача 7.11. Показать, что в $M_n(\mathbb{R})$ все вырожденные матрицы (и только они) являются делителями нуля.

Можно рассматривать матрицы с элементами из произвольного данного кольца R . Для них обычным образом определяются сложение и умножение. Множество $M_n(R)$ квадратных матриц порядка n с элементами из R является кольцом (с 1, если R — кольцо с 1). Если R — коммутативное кольцо, то для матриц из $M_n(R)$ обычным способом вводится понятие определителя, который обладает обычными свойствами (разложение по строке или столбцу, определитель произведения).

Задача 7.12. Пусть R — коммутативное кольцо с 1.

- а) Показать, что $U(M_n(R)) = \{A \in M_n(R) \mid \det A \in U(R)\}$.
- б) Показать, что матрица $A \in M_n(R)$ является делителем нуля, если и только если $\det A$ — делитель нуля в R .
- в) Пусть A — $m \times n$ -матрица над R . Показать, что столбцы матрицы A линейно зависимы над R (в обычном смысле), если и только если существует такой элемент $a \in R$, $a \neq 0$, что $a\Delta = 0$ для всех $n \times n$ -миноров матрицы A .

- 5) Пусть R — любое из следующих множеств функций, принимающих вещественные значения, с данной областью определения (некоторым интервалом) на числовой прямой: все функции; непрерывные функции; функции, обладающие производными до некоторого порядка $k \leq \infty$. Каждое из этих множеств образует коммутативное кольцо с единицей, имеющее делители нуля. $U(R)$ — множество функций, не обращающихся в области определения в нуль. Когда R — множество всех функций, все необратимые функции являются делителями нуля; в остальных случаях делителями нуля являются функции, обращающиеся в нуль на некотором интервале.
- 6) Пусть M — непустое множество и R — множество всех подмножеств в M . Введем на R операции:

$$\begin{aligned} a + b &= (a \cup b) \setminus (a \cap b) && \text{(симметрическая разность),} \\ a \cdot b &= a \cap b. \end{aligned}$$

R — кольцо с 1, в котором $a + a = 0$ и всякий элемент идемпотентен (т.е. $a^2 = a$). Кольца с этими свойствами называются булевыми.

Задача 7.13. Показать, что булево кольцо R коммутативно; если $|R| > 2$, то в нем есть делители нуля, а когда $|R| = 2$, то это поле.

Задача 7.14. Доказать, что конечное кольцо (содержащее более одного элемента) без делителей нуля является телом (на самом деле — полем, но это более трудная задача).

7.2. Кольца и поля классов вычетов

Построение кольца вычетов по модулю n . Пусть n — натуральное число > 1 . Два целых числа a, b называются сравнимыми по модулю n (обозначается $a \equiv b \pmod{n}$), если $n \mid b - a$

(n делит $b - a$). Это есть отношение эквивалентности на множестве целых чисел, и классы эквивалентности относительно этого отношения называются классами вычетов (остатков) по модулю n , поскольку каждый такой класс состоит из всех целых чисел, имеющих один и тот же остаток при делении на n . Имеется точно n таких классов, и множество этих классов обозначается через \mathbb{Z}/n . Класс вычетов целого числа a обозначается через $[a]$ (или, при необходимости, через $[a]_n$), и $[a] = [b] \iff n \mid b - a$. Определим на множестве \mathbb{Z}/n операции сложения и умножения:

$$[a] + [b] = [a + b];$$

$$[a][b] = [ab].$$

Чтобы эти операции были корректными, нужно проверить, что результат операций зависит только от заданных классов вычетов, а не от выбора в них целых чисел a и b . Приведем проверку для случая умножения (для сложения аналогично). Пусть $[a] = [a']$, $[b] = [b']$, т.е. \exists такие целые числа k, l , что $a' = a + kn$, $b' = b + ln$. Тогда $a'b' = ab + (kb + al + kln)n$, т.е. $[a'b'] = [ab]$. Легко видеть, что $(\mathbb{Z}/n, +)$ есть абелева группа. Нулем служит класс $[0]$, состоящий из чисел, кратных n , и $-[a] = [-a]$. Легко также видеть, что $(\mathbb{Z}/n, +, \cdot)$ удовлетворяет аксиомам кольца. Вот, например, проверка дистрибутивности:

$$\begin{aligned} [a]([b] + [c]) &= [a][b + c] = [a(b + c)] = [ab + ac] = \\ &= [ab] + [ac] = [a][b] + [a][c]. \end{aligned}$$

Заметим, что построение $(\mathbb{Z}/n, +)$ есть частный случай конструкции факторгруппы (см. п. 6.8). \mathbb{Z}/n — коммутативное кольцо с единицей (единицей служит класс $[1]$). Его аддитивная группа — циклическая группа порядка n с порождающим элементом $[1]$. Если числа k и n не взаимно просты, т.е. $k = k'd$, $n = n'd$, $d > 1$, то класс $[k]$ является делителем 0: $[k][n'] = [kn'] = [k'n] = [0]$. Если k и n взаимно просты, то класс $[k]$ не является делителем 0. Действительно, если класс $[l] \neq 0$, т.е. l не делится на n , то kl не делится на n , а потому $[k][l] = [kl] \neq 0$. На самом деле, если $[k]$ и $[n]$ взаимно просты, то класс $[k]$ обратим в \mathbb{Z}/n . Это следует из следующей леммы.

Лемма 7.15. В конечном коммутативном кольце R с единицей всякий неделитель нуля обратим.

Доказательство. Действительно, если a — неделитель 0 , то все элементы ax , $x \in R$, различны, а потому один из них равен 1 . \square

Таким образом, доказано

Предложение 7.16. Группа $U(\mathbb{Z}/n)$ обратимых элементов кольца \mathbb{Z}/n состоит из классов вычетов чисел, взаимно простых с n . Кольцо \mathbb{Z}/n является полем, если и только если n — простое число. В случае непростого n кольцо \mathbb{Z}/n содержит делители нуля.

Следствие 7.17. Группа $U(\mathbb{Z}/n)$ имеет порядок $\varphi(n)$, где φ — функция Эйлера.

Следствие 7.18 (обобщенная малая теорема Ферма). Если целое число k взаимно просто с n , то

$$k^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказательство. Действительно, в группе $U(\mathbb{Z}/n)$ имеем: $[k]^{\varphi(n)} = [1]$. \square

В частном случае, когда $n = p$ — простое число, имеем $\varphi(p) = p - 1$ и получаем

Следствие 7.19 (малая теорема Ферма). Если целое число k не делится на простое число p , то

$$k^{p-1} \equiv 1 \pmod{p}.$$

7.3. Подкольца и подполя. Гомоморфизмы и изоморфизмы колец. Группа автоморфизмов

Определение 7.20. Подкольцом кольца называется подгруппа его аддитивной группы, устойчивая относительно умножения.

Очевидно, что подкольцо коммутативного кольца коммутативно, а подкольцо кольца без делителей нуля также не имеет делителей нуля. В то же время подкольцо кольца с 1 может не иметь единицы (например, подкольцо четных чисел в кольце целых чисел), но даже если оно имеет единицу, то его единица может не совпадать с единицей кольца (например, подкольцо в $M_n(\mathbb{R})$, состоящее из всех матриц с нулевой последней строкой и последним столбцом). Однако, имеет место

Предложение 7.21. *Всякое ненулевое подкольцо в поле, имеющее единицу (в частности, всякое подполе) содержит единицу поля.*

Доказательство. Действительно, в поле имеется только один элемент, отличный от нуля, а именно единица, удовлетворяющий уравнению $x^2 = x$. \square

В предложении 7.21 можно вместо поля, более общо, рассматривать любое кольцо с 1 без делителей нуля.

Примерами подколец и подполей могут служить $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ и (если отождествить числа с соответствующими скалярными матрицами) $\mathbb{R} \subset M_n(\mathbb{R})$.

Пусть $\mathbb{Q}(\sqrt{2})$ обозначает множество тех действительных чисел, которые можно представить в виде $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. Это множество устойчиво относительно сложения и умножения и является подполем в \mathbb{R} .

В любом кольце с 1 множество $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ является подкольцом.

Определение 7.22. Отображение колец $f : R \rightarrow S$ называется *гомоморфизмом*, если

$$f(a + b) = f(a) + f(b) \quad \text{и}$$

$$f(ab) = f(a)f(b) \quad \forall a, b \in R,$$

т.е. если это отображение является одновременно гомоморфизмом для аддитивных групп и мультипликативных полугрупп этих колец.

Для любых двух колец R, S всегда существует нулевой гомоморфизм $R \rightarrow S$ (все элементы отображаются в нуль). Очевидно, что образ $\text{Im } f$ гомоморфизма $f : R \rightarrow S$ является подкольцом в S .

Предложение 7.23. *Если R — поле, то всякий гомоморфизм $f : R \rightarrow S$ либо нулевой, либо инъективен.*

Доказательство. Пусть для двух элементов $a_1, a_2 \in R$, $a_1 \neq a_2$, $f(a_1) = f(a_2)$. Тогда $f(a_2 - a_1) = 0$ и, так как существует $(a_2 - a_1)^{-1}$, $f(1) = f((a_2 - a_1)^{-1}(a_2 - a_1)) = 0$, а тогда $f(a) = f(a \cdot 1) = 0 \forall a \in R$. \square

Для всякого подкольца $R \subset S$ имеется гомоморфизм вложения $i : R \rightarrow S$.

Примеры гомоморфизмов. 1. Канонический гомоморфизм $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n$, при котором $\pi(k) = [k]$ для всех $k \in \mathbb{Z}$.

2. Если $m \mid n$, то имеется гомоморфизм $\pi_{n,m} : \mathbb{Z}/n \rightarrow \mathbb{Z}/m$, при котором $\pi_{n,m}([a]_n) = [a]_m$ (определение корректно, так как все числа из $[a]_n$ лежат в одном и том же классе вычетов по модулю m).

Эти примеры показывают, что свойство кольца быть или не быть кольцом без делителей 0 может не сохраняться при гомоморфизме.

3. Если R — кольцо с 1, то отображение $f : \mathbb{Z} \rightarrow R$, при котором $f(n) = n \cdot 1$, является гомоморфизмом.

При гомоморфизмах колец единица не обязана переходить в единицу, однако если $f : R \rightarrow S$ — сюръективный гомоморфизм, и R — кольцо с 1, то $f(1)$ есть единица кольца S . При сюръективном гомоморфизме $f : R \rightarrow S$ из коммутативности R , очевидно, следует коммутативность S .

Определение 7.24. Пусть R и S — кольца. Отображение $f : R \rightarrow S$ называется *изоморфизмом*, если оно биективно и является гомоморфизмом. Кольца R и S называются *изоморфными*, если между ними существует изоморфизм.

Определение 7.25. Изоморфизм кольца R (группы, полугруппы и др.) на себя называется *автоморфизмом*. Множество автоморфизмов R образует группу относительно композиции (согласно предложению 6.43), которая обозначается через $\text{Aut}(R)$. Единицей этой группы служит тождественный автоморфизм.

Задача 7.26. Найти группу автоморфизмов для всякой циклической группы.

Задача 7.27. а) Показать, что кольца \mathbb{Z} , \mathbb{Z}/n , поля \mathbb{Q} , \mathbb{R} обладают только тождественными автоморфизмами.

б) Найти все автоморфизмы поля $\mathbb{Q}(\sqrt{2})$.

7.4. Характеристика поля

Предложение 7.28. *Все ненулевые элементы поля имеют одинаковый порядок в его аддитивной группе. Этот порядок либо бесконечен, либо является простым числом.*

Доказательство. Докажем это утверждение в более общем случае — для любого кольца R с единицей без делителей нуля. Пусть $a \in R$, $a \neq 0$; покажем, что $O(a) = O(1)$. Для этого надо показать, что для целого положительного числа n $na = 0 \iff n \cdot 1 = 0$. Имеем:

$$na = \underbrace{a + \dots + a}_n = \underbrace{(1 + \dots + 1)}_n \cdot a = (n \cdot 1) \cdot a.$$

Поэтому $n \cdot 1 = 0 \implies na = 0$, а обратное следует из того, что $a \neq 0$ и в кольце нет делителей нуля. Пусть теперь этот порядок равен n ; покажем, что n — простое число. В противном случае $n = kl$, $0 < k < n$, $0 < l < n$, и

$$n \cdot 1 = \underbrace{(1 + \dots + 1)}_k \underbrace{(1 + \dots + 1)}_l = (k \cdot 1)(l \cdot 1) = 0,$$

но $k \cdot 1 \neq 0$ и $l \cdot 1 \neq 0$. □

Определение 7.29. Пусть K — поле. Если общий порядок ненулевых элементов поля K равен простому числу p , то говорят, что поле K имеет характеристику p . Если этот порядок бесконечный, то говорят, что поле K имеет характеристику нуль. Характеристика поля K обозначается через $\text{char } K$.

Примеры. Все поля, составленные из чисел, имеют характеристику 0. Поле \mathbb{Z}/p имеет характеристику p . Если K — подполе поля L , то поля K и L имеют одинаковую характеристику. Как показывает пример кольца \mathbb{Z}/n при составном n , в кольце с делителями нуля ненулевые элементы могут иметь разные порядки в аддитивной группе. Однако в кольце с 1 порядок любого элемента является делителем $O(1)$.

Теорема 7.30. Пусть K — поле. Если K имеет характеристику 0, то существует единственный инъективный гомоморфизм $f : \mathbb{Q} \rightarrow K$. Если K имеет характеристику p , то существует единственный инъективный гомоморфизм $f : \mathbb{Z}/p \rightarrow K$. В обоих случаях $\text{Im } f$ является единственным минимальным подполем поля K (т.е. содержится в любом его подполе).

Доказательство. Пусть $\text{char } K = 0$. Тогда все элементы $n \cdot 1 \neq 0$ ($n \in \mathbb{Z}, n \neq 0$). Зададим отображение $f : \mathbb{Q} \rightarrow K$, положив $f(m/n) = m \cdot 1 \cdot (n \cdot 1)^{-1}$ ($n \neq 0$). Так как запись рационального числа в виде дроби неоднозначна, необходимо проверить корректность этого задания. Пусть $m/n = r/s$, т.е. $sm = nr$. Тогда в поле K $(s1)(m1) = (n1)(r1)$, откуда $(m1)(n1)^{-1} = (r1)(s1)^{-1}$. Это отображение является гомоморфизмом:

$$\begin{aligned} f(m_1/n + m_2/n) &= f((m_1 + m_2)/n) = (m_1 + m_2)1 \cdot (n1)^{-1} = \\ &= m_1 1 \cdot (n1)^{-1} + m_2 1 \cdot (n1)^{-1} = f(m_1/n) + f(m_2/n); \end{aligned}$$

$$\begin{aligned} f(m/n \cdot r/s) &= f(mr/ns) = \\ &= (mr)1 \cdot (ns1)^{-1} = (m1)(r1) \cdot (n1)^{-1}(s1)^{-1} = \\ &= [(m1)(n1)^{-1}] \cdot [(r1)(s1)^{-1}] = f(m/n) \cdot f(r/s). \end{aligned}$$

Поскольку f — ненулевой гомоморфизм поля, f инъективен. Так как при любом ненулевом гомоморфизме $1 \in \mathbb{Q}$ переходит в $1 \in K$, то f определен однозначно.

Пусть теперь $\text{char } K = p$. Зададим отображение $f: \mathbb{Z}/p \rightarrow K$, при котором $f([k]_p) = k1$. Так как $O(1) = p$ в K , то $k1 = l1 \iff k \equiv l \pmod{p}$ и отображение f определено корректно. Оно, очевидно, является гомоморфизмом, который инъективен и определен однозначно.

В обоих случаях подполе $\text{Im } f$ содержится в любом подполе L поля K , так как $1 \in L$, а потому все элементы $n1 \in L$, $n \in \mathbb{Z}$, и $(n1)(n1)^{-1} \in L$ ($n1 \neq 0$). \square

Отождествляя соответственно \mathbb{Q} или \mathbb{Z}/p посредством f с $\text{Im } f$, получаем

Следствие 7.31. *Всякое поле K содержит в качестве единственного минимального подполя либо поле \mathbb{Q} (если $\text{char } K = 0$), либо \mathbb{Z}/p (если $\text{char } K = p$). Это подполе называется простым подполем в K .*

Предложение 7.32. *Пусть K — поле характеристики p . Для любых $a, b \in K$ и любого целого $n \geq 1$*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Доказательство. Для $n = 1$ имеем:

$$(a + b)^p = \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k = a^p + b^p,$$

так как при $1 \leq k \leq p - 1$ биномиальные коэффициенты $\binom{p}{k}$ делятся на p . Для произвольного n утверждение получается индукцией. \square

§8. Комплексные числа

8.1. Построение поля комплексных чисел

Задача состоит в построении поля \mathbb{C} , которое обладает следующими свойствами:

- 1) $\mathbb{C} \supset \mathbb{R}$ (как подполе);
- 2) \mathbb{C} содержит элемент i , такой что $i^2 = -1$ (тогда \mathbb{C} содержит точно два корня из -1 : это i и $-i$, так как если в поле $a^2 = b^2$, то $a^2 - b^2 = (a - b)(a + b) = 0$ и либо $a = b$, либо $a = -b$);
- 3) \mathbb{C} минимально относительно свойств 1) и 2), т.е. если некоторое подполе L в \mathbb{C} содержит \mathbb{R} и i , то $L = \mathbb{C}$.

Мы построим три изоморфных между собой реализации такого поля. Рассматриваем три множества:

- 1) Множество всех точек (векторов) на евклидовой плоскости с фиксированной прямоугольной декартовой системой координат.
- 2) Множество $\{(a, b) \mid a, b \in \mathbb{R}\}$ всех пар действительных чисел.
- 3) Множество всех матриц вида

$$\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Отождествим эти три множества между собой. Первые два множества отождествляются посредством сопоставления каждой точке ее декартовых координат. Второе и третье отождествляем посредством соответствия

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

С учетом этого отождествления все три множества будем обозначать одним и тем же символом \mathbb{C} . Введем на \mathbb{C} операции сложения и умножения. На каждом из указанных множеств уже имеется известная операция сложения: соответственно сложение векторов, сложение векторов-строк (длины 2), сложение матриц. При сделанном отождествлении эти операции переходят друг в друга, так что на \mathbb{C} имеем операцию сложения и $(\mathbb{C}, +)$ является абелевой группой.

Рассматриваемое множество матриц устойчиво относительно умножения:

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

Умножение матриц ассоциативно и связано со сложением законами дистрибутивности. Кроме того, из формулы для произведения непосредственно видно, что в случае матриц рассматриваемого вида умножение коммутативно. Эта операция умножения переносится на соответствующие пары действительных чисел и для них записывается в виде:

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Так как $\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 \neq 0$ для ненулевых матриц, то ненулевые матрицы рассматриваемого множества имеют обратную и обратная лежит в том же множестве:

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

Таким образом, множество \mathbb{C} с введенными операциями сложения и умножения является полем.

Отождествим действительное число a с соответствующей точкой на оси абсцисс (вещественная ось), соответственно с парой $(a, 0)$ и скалярной матрицей $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Это отождествление позволяет считать, что \mathbb{R} есть подмножество в \mathbb{C} . При этом для элементов из \mathbb{R} введенные операции совпадают с обычным сложением и умножением действительных чисел, так что \mathbb{R} — подполе в \mathbb{C} . Обозначим через i матрицу $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (соответственно пару $(0, 1)$ и соответствующую ей точку на оси ординат). Тогда

$i^2 = -1$. В терминах введенных операций всякий элемент $z \in \mathbb{C}$, представляемый парой (a, b) или матрицей $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, однозначно записывается в виде $z = a + bi$ и, следовательно, содержится в любом подполе поля \mathbb{C} , содержащем \mathbb{R} и i . Таким образом, построенное поле \mathbb{C} удовлетворяет всем трем сформулированным выше условиям.

Элементы поля \mathbb{C} называются *комплексными числами*. Запись в виде $z = a + bi$ называют иногда алгебраической формой комплексного числа z . Комплексные числа с $b = 0$ мы отождествили с действительными числами; числа вида bi ($a = 0$) называются чисто мнимыми, им соответствуют точки на оси ординат (мнимая ось). Если $z = a + bi$, то a и bi называются соответственно действительной и мнимой частями комплексного числа и обозначаются $\operatorname{Re}(z)$ и $\operatorname{Im}(z)$.

Лемма 8.1. Пусть K — поле, содержащее \mathbb{R} и такой элемент j , что $j^2 = -1$. Тогда отображение $f : \mathbb{C} \rightarrow K$, при котором $f(a + bi) = a + bj$, является (инъективным) гомоморфизмом, и это единственный гомоморфизм, при котором поле \mathbb{R} отображается тождественно, а i переходит в j .

Доказательство. То, что $f(z_1 + z_2) = f(z_1) + f(z_2)$, очевидно. Проверим, что $f(z_1 z_2) = f(z_1)f(z_2)$. Пусть $z_1 = a + bi$, $z_2 = c + di$. Имеем:

$$\begin{aligned} f(z_1)f(z_2) &= (a + bj)(c + dj) = ac + adj + bcj + bjdj = \\ &= (ac - bd) + (ad + bc)j = f((ac - bd) + (ad + bc)i) = \\ &= f((a + bi)(c + di)) = f(z_1 z_2). \end{aligned}$$

Единственность очевидна. □

Следствие 8.2 (теорема единственности поля комплексных чисел). Всякое поле, удовлетворяющее сформулированным выше условиям 1)–3), изоморфно полю комплексных чисел, причем существует изоморфизм, тождественный на поле действительных чисел.

Следствие 8.3. Поле \mathbb{C} имеет точно два автоморфизма, тождественных на \mathbb{R} . Один из них тождественный, а второй отображает i в $-i$.

Доказательство. Действительно, при таком автоморфизме f имеем $f(i)^2 = f(i^2) = -1$, а потому $f(i) = i$ или $-i$. \square

Второй из указанных автоморфизмов поля \mathbb{C} называется *комплексным сопряжением* и обозначается чертой сверху: $z \mapsto \bar{z}$. Если $z = a + bi$, то $\bar{z} = a - bi$. В геометрической реализации поля \mathbb{C} ему соответствует отражение относительно действительной оси, а матричной — транспонирование (показать, что это дает другое доказательство того, что комплексное сопряжение — автоморфизм).

Предложение 8.4. *Операция комплексного сопряжения обладает следующими свойствами:*

- 1) $\overline{\bar{z}} = z$;
- 2) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;
- 3) $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$;
- 4) если $z = a + bi$, то $z\bar{z} = a^2 + b^2$;
- 5) если $z = a + bi \neq 0$, то $z^{-1} = \bar{z}/(a^2 + b^2)$;
- 6) $\bar{z} = z \iff z \in \mathbb{R}$; $\bar{z} = -z \iff z$ — чисто мнимое.

Все эти свойства либо установлены выше, либо проверяются непосредственно.

Задача 8.5. Рассмотрим два следующих множества матриц:

$$H_1 = \left\{ \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\},$$

$$H_2 = \left\{ \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}.$$

Показать, что каждое из этих множеств устойчиво относительно сложения и умножения и является телом. Показать, что эти тела изоморфны.

8.2. Тригонометрическая форма комплексного числа. Формула Муавра. Извлечение корней из комплексных чисел

Рассматриваем комплексное число как соответствующий вектор на плоскости. Пусть $z = a + bi$. Длина вектора z обозначается через $|z|$ и называется *модулем* комплексного числа z . Имеем: $|z| = \sqrt{a^2 + b^2}$. Так как $z\bar{z} = a^2 + b^2$, то $z\bar{z} = |z|^2$. В случае $z \neq 0$ угол, образованный вектором z с положительным направлением действительной оси называется аргументом комплексного числа z и обозначается через $\text{Arg}(z)$. $\text{Arg}(z)$ — это класс действительных чисел, отличающихся на целое кратное 2π , который задается любым своим представителем α : $\text{Arg}(z) = \alpha + 2\pi k, k \in \mathbb{Z}$. Имеем: $a = |z| \cos \alpha$, $b = |z| \sin \alpha$ и $z = |z|(\cos \alpha + i \sin \alpha)$.

Представление комплексного числа в таком виде называется его тригонометрической формой. Тригонометрическая форма комплексного числа единственна: если

$$z = |z|(\cos \alpha + i \sin \alpha) = r(\cos \beta + i \sin \beta),$$

где $r > 0$ — вещественное, то $r = |z|$ и $\beta - \alpha \in 2\pi\mathbb{Z}$.

Пусть $z, w \in \mathbb{C}$ и отличны от 0, $z = |z|(\cos \alpha + i \sin \alpha)$, $w = |w|(\cos \beta + i \sin \beta)$; тогда

$$\begin{aligned} zw &= |z||w|(\cos \alpha \cos \beta - \sin \alpha \sin \beta) + i(\cos \alpha \sin \beta + \sin \alpha \cos \beta) = \\ &= |z||w|(\cos(\alpha + \beta) + i \sin(\alpha + \beta)). \end{aligned}$$

Из этого получаем

Предложение 8.6.

$$|zw| = |z||w|, \quad \text{Arg}(zw) = \text{Arg}(z) + \text{Arg}(w).$$

Замечание 8.7. Рассмотрим отображения $\varphi: \mathbb{C}^* \rightarrow \mathbb{R}_+$ и $\psi: \mathbb{C}^* \rightarrow \mathbb{R}/2\pi\mathbb{Z}$, где $\varphi(z) = |z|$ и $\psi(z) = \text{Arg}(z)$. Предложение 8.6 утверждает, что φ и ψ — гомоморфизмы групп. $\text{Ker } \varphi$ — единичная окружность, $\text{Ker } \psi = \mathbb{R}_+$.

Следствие 8.8. $w^{-1} = \frac{1}{|w|}(\cos(-\beta) + i \sin(-\beta))$ и

$$|zw^{-1}| = |z|/|w|, \quad \text{Arg}(zw^{-1}) = \text{Arg } z - \text{Arg } w.$$

Следствие 8.9 (формула Муавра).

$$(|z|(\cos \alpha + i \sin \alpha))^n = |z|^n(\cos n\alpha + i \sin n\alpha).$$

Следствие 8.10. Пусть z_0 — фиксированное комплексное число. Отображение плоскости на себя, при котором $z \mapsto z_0 z$ представляет собой композицию поворота на угол $\text{Arg}(z_0)$ и растяжения (сжатия) с коэффициентом $|z_0|$.

Определение 8.11. Пусть $z \in \mathbb{C}$ и n — целое число ≥ 1 . Тогда $\sqrt[n]{z} = \{w \in \mathbb{C} \mid w^n = z\}$ называется множеством корней n -й степени из z .

Предложение 8.12. Пусть $z \neq 0$, $z = |z|(\cos \alpha + i \sin \alpha)$. Тогда

$$\sqrt[n]{z} = \left\{ |z|^{1/n} \left(\cos \frac{\alpha + 2\pi k}{n} + i \sin \frac{\alpha + 2\pi k}{n} \right) \mid k = 0, \dots, n-1 \right\}.$$

В частности, имеется точно n различных корней n -й степени из z , все они расположены на окружности радиуса $|z|^{1/n}$ с центром в 0 и служат вершинами некоторого правильного n -угольника.

Доказательство. Действительно, пусть $w = |w|(\cos \beta + i \sin \beta)$ и $w^n = z$. В силу формулы Муавра

$$|w|^n(\cos n\beta + i \sin n\beta) = |z|(\cos \alpha + i \sin \alpha),$$

откуда $|w|^n = |z|$, $n\beta = \alpha + 2\pi k$, $k \in \mathbb{Z}$ и

$$w = |z|^{1/n} \left(\cos \frac{\alpha + 2\pi k}{n} + i \sin \frac{\alpha + 2\pi k}{n} \right), \quad k \in \mathbb{Z}.$$

Обозначим это число через w_k . При любом k $w_k^n = z$, причем $w_k = w_l \iff k \equiv l \pmod{n}$. Поэтому все различные корни получаются при $k = 0, \dots, n-1$. \square

Задача 8.13. Пусть $d \neq 1$ — бесквадратное целое число (т.е. не делящееся на квадрат простого числа), \sqrt{d} — одно из значений квадратного корня из d и

$$\mathbb{Q}(\sqrt{d}) = \{z = a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}.$$

- а) Показать, что $\mathbb{Q}(\sqrt{d})$ — поле.
- б) Пусть w_1, w_2 — фиксированные ненулевые числа из $\mathbb{Q}(\sqrt{d})$, такие что множество $R = \{aw_1 + bw_2 \mid a, b \in \mathbb{Z}\}$ является кольцом (например, $w_1 = 1, w_2 = \sqrt{d}$). Показать, что среди колец такого вида имеется одно максимальное (т.е. содержащее все такие кольца) и найти его.

8.3. Корни из единицы

Обозначим через μ_n множество корней n -й степени из 1 в поле \mathbb{C} . Имеем: $|\mu_n| = n$.

Предложение 8.14. μ_n — группа по умножению.

Доказательство. Действительно, если $z_1^n = 1$ и $z_2^n = 1$, то $(z_1 z_2)^n = z_1^n z_2^n = 1$, $1 \in \mu_n$ и если $z^n = 1$, то $(z^{-1})^n = (z^n)^{-1} = 1$. \square

Введем следующее обозначение для элементов из μ_n :

$$\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, \quad k = 0, 1, \dots, n-1.$$

Определение 8.15. Корень n -й степени из 1 называется *первообразным*, если он не является корнем из 1 меньшей степени, чем n .

Замечание 8.16. На языке теории групп условие, что $z \in \mathbb{C}^*$ является первообразным корнем n -й степени из 1, означает, что порядок z в группе (\mathbb{C}^*, \cdot) равен n .

Предложение 8.17. Для элемента $\zeta \in \mu_n$ следующие условия эквивалентны:

- 1) ζ — первообразный корень степени n из 1;

2) всякий корень степени n из 1 представляется как ζ^k для некоторого $k \in \mathbb{Z}$.

Доказательство. 1) \implies 2). Если ζ — первообразный, то числа $\zeta^0 = 1, \zeta, \dots, \zeta^{n-1}$ различны, т.к. если $\zeta^k = \zeta^l$ при $0 \leq k < l \leq n-1$, то $\zeta^{l-k} = 1$. Поэтому эти числа образуют все множество μ_n .

2) \implies 1). От противного: если бы $\zeta^k = 1$ для некоторого k , $0 < k < n$, то среди степеней ζ^k элемента ζ было бы не более чем l различных. \square

Замечание 8.18. Условие 2) на языке теории групп означает, что группа μ_n циклическая и ζ является ее порождающим.

Предложение 8.19. *Первообразные корни степени n существуют (равносильно: группа μ_n — циклическая).*

Доказательство. Действительно, например, ε_1 — первообразный, так как $\varepsilon_k = \varepsilon_1^k$ для всех k . \square

Предложение 8.20. *Число $\varepsilon_k \in \mu_n$ является первообразным корнем степени n из 1, если и только если k и n взаимно просты.*

Доказательство. Если наибольший общий делитель $(k, n) = d > 1$, то $\varepsilon_k^{n/d} = \cos \frac{2\pi kn}{nd} + i \sin \frac{2\pi kn}{nd} = 1$. Если $(k, n) = 1$ и $0 < m < n$, то $\varepsilon_k^m = \cos \frac{2\pi km}{n} + i \sin \frac{2\pi km}{n} \neq 1$, т.к. km/n не является целым числом. \square

Следствие 8.21. *Число первообразных корней n -й степени из 1 равно $\varphi(n)$ (функция Эйлера).*

Следствие 8.22. *Пусть $(k, n) = d$. Число $\varepsilon_k \in \mu_n$ является первообразным корнем степени n/d из 1.*

Доказательство. Действительно,

$$\varepsilon_k = \cos \frac{2\pi(k/d)}{n/d} + i \sin \frac{2\pi(k/d)}{n/d}$$

и числа $k/d, n/d$ взаимно простые. \square

Замечание 8.23. Предложение 8.20 в других терминах выражает то же самое, что и предложение 6.31, а следствие 8.22 — то же самое, что и предложение 6.20.

Задача 8.24. а) Пусть числа m и n взаимно простые.

Показать, что всякое число $\zeta \in \mu_{mn}$ однозначно представляется в виде $\zeta = \zeta' \zeta''$, где $\zeta' \in \mu_m$, $\zeta'' \in \mu_n$.

б) Показать, что $\zeta \in \mu_{mn}$ является первообразным корнем степени mn из 1, если и только если ζ' и ζ'' являются первообразными корнями соответственно степени m и n .

в) Показать, что если числа n_1, \dots, n_s попарно взаимно просты, то $\varphi(n_1 \cdot \dots \cdot n_s) = \varphi(n_1) \cdot \dots \cdot \varphi(n_s)$.

г) Если $n = p_1^{k_1} \dots p_s^{k_s}$, где p_1, \dots, p_s — различные простые числа, то $\varphi(n) = \prod_{i=1}^s (p_i - 1) p_i^{k_i - 1}$.

д) Показать, что $\sum_{d|n} \varphi(d) = n$.

Голод Евгений Соломонович

Курс лекций по алгебре

М., Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 112 стр.

Оригинал-макет изготовлен издательской группой механико-математического факультета МГУ

Подписано в печать 15.12.2004.

Формат 60×90 1/16. Объем 7 п.л.

Заказ 27. Тираж 100 экз.

Издательство ЦПИ при механико-математическом факультете МГУ,

г. Москва, Воробьевы горы.

Лицензия на издательскую деятельность ИД № 04059 от 20.02.2001.

Отпечатано на типографском оборудовании механико-математического факультета.