8-1 К лекции 8 (4.10.2011)

Повтор (в теореме о $|AB| = |A|\,|B|$, мы использовали Лемму об окаймлении с углом нулей:

$$C = \left(\begin{array}{c|c} A & U \\ \hline O & B \end{array}\right), \quad |C| = |A| \cdot |B|$$

$A \in M_n(K)$, $B \in M_m(K)$

$U \in M_{m,n}(K)$, $O \in M_{m,n}(K)$.

Доказательство: Разл. по 1 столбцу

$$\begin{vmatrix} a_{11} & \cdots & \\ \vdots & & \\ a_{m1} & & \\ 0 & \cdots & \\ \vdots & & \\ 0 & \cdots & \end{vmatrix} = a_{11}C_{11} + \dots + a_{n1}C_{n1} =$$

$$C_{i1} = (-1)^{i+1} M_{i1} = (-1)^{i+1} M_{i1}(B)$$

$$M_{i1} = \left|\begin{array}{c|c} M'_{i1} & U' \\ \hline 0 \ \cdots \ 0 & B \end{array}\right| \overset{\text{по инд.}}{=}$$

$$\left(\sum_{i=1}^{n} a_{i1}(-1)^{i+1} M'_{i1}\right)|B| = |A|\,|B| \quad \blacksquare$$

8-2

Лекция N 8
(4 октября 2011)

§ 9. Линейные пространства

Вывод свойств линейного пространства из аксиом

Пусть K — поле (например, $K = \mathbb{R}$ — поле действительных чисел). Многочисленные конкретные примеры линейных пространств, с которыми мы уже столкнулись (линейные пространства строк K^n, столбцов $\hat{K}^n$, пространства прямоугольных и квадратных матриц $\mathrm{M}_{m,n}(K)$ и $\mathrm{M}_n(K)$, пространство многочленов $K[x]$, пространство непрерывных вещественных функций $C[0,1]$ на отрезке $[0,1]$ и т. д.) оправдывают введение и рассмотрение понятия *абстрактного линейного пространства* ${}_KV$ над полем K как множества V с операцией сложения ($V \times V \to V$, $(a,b) \mapsto a+b$) и операциями умножения на элементы $c \in K$ ($V \to V$, $v \mapsto cv$), удовлетворяющими следующим условиям:

I.1) ассоциативность сложения (т. е. $(u+v)+w = u+(v+w)$ для всех $u, v, w \in V$);

I.2) коммутативность сложения (т. е. $u+v = v+u$ для всех $u, v \in V$);

8-3

I.3) существование нейтрального элемента 0 для операции сложения (т. е. $v + 0 = v$ для всех $v \in V$);

I.4) существование противоположного элемента $-v$ для всякого $v \in V$ (т. е. $v + (-v) = 0$);

II.1) $1 \cdot v = v$ для всех $v \in V$;

II.2) $(rs)v = r(sv)$ для всех $r, s \in K$, $v \in V$;

III.1) $r(v_1 + v_2) = rv_1 + rv_2$ для всех $r \in K$, $v_1, v_2 \in V$;

III.2) $(r + s)v = rv + sv$ для всех $r, s \in K$, $v \in V$.

Приведём вывод ряда следствий из этих аксиом линейного пространства (хотя, конечно, в каждом конкретном случае они достаточно очевидны).

1) Уравнение $u + x = v$ для $u, v \in {}_KV$ имеет, причём единственное, решение $x = (-u) + v$.

Действительно, прибавляя $-u$ к левой и правой части, получаем, что $x = (-u) + v$. С другой стороны, $u + (-u) + v = v$.

2) Если $x + x = x$ для $x \in {}_KV$, то $x = 0$.

Действительно, прибавляя к левой и правой части противоположный элемент $-x$, получаем, что $x = (-x) + x + x = (-x) + x = 0$.

3) $0v = 0$ для любого $v \in {}_KV$.

Действительно, если $x = 0v$ (здесь $0 \in K$), то $x + x = 0v + 0v = (0 + 0)v = 0v = x$, и поэтому $x = 0 \in {}_KV$.

4) $r0 = 0$ для $r \in K$, $0 \in V$.

Действительно, если $x = r0$, то $x + x = r0 + r0 = r(0 + 0) = r0 = x$, и поэтому $x = 0$.

5) $(-1)v = -v$ для всех $v \in V$.

Действительно, $(-1)v + v = (-1 + 1)v = 0v = 0$, т. е. $(-1)v = -v$.

6) $rv = 0$ для $r \in K$, $v \in V$ тогда и только тогда, когда либо $r = 0$, либо $v = 0$.

Действительно, если $r \neq 0$, то в поле K существует элемент $r^{-1} \in K$, и поэтому $v = 1v = r^{-1}rv = r^{-1}0 = 0$.

7) $r(u - v) = ru - rv$ для всех $r \in K$, $u, v \in V$.

Действительно, $r(u - v) + rv = r(u - v + v) = ru$, т. е. $r(u - v) = ru - rv$.

8-4

8) $-(-v) = v$ для всех $v \in V$.
Действительно, $v + (-v) = 0$, и поэтому $-(-v) = v$.

Линейная зависимость в линейных пространствах

Пусть ${}_KV$ — линейное пространство над полем K. Если $v_1, \ldots, v_r \in V$, $k_1, \ldots, k_r \in K$, то элемент

$$k_1v_1 + \ldots + k_rv_r \in V$$

называется *линейной комбинацией* элементов $v_1, \ldots, v_r$ с коэффициентами $k_1, \ldots, k_r \in K$.

Систему элементов $v_1, \ldots, v_r \in {}_KV$ назовём *линейно зависимой*, если найдутся элементы $k_1, \ldots, k_r \in K$ такие, что

а) не все k_i равны нулю (т. е. хотя бы один элемент k_i отличен от нуля);

б) $k_1v_1 + k_2v_2 + \ldots + k_rv_r = 0$.

Для краткости в этой ситуации мы будем говорить, что *«нетривиальная»* линейная комбинация элементов $v_1, \ldots, v_r$ равна нулю (конечно, *тривиальная* линейная комбинация всегда равна нулю, $0v_1 + \ldots + 0v_r = 0$).

Система элементов $v_1, \ldots, v_r \in {}_KV$ называется *линейно независимой*, если она не является линейно зависимой, это означает, что из равенства

$$k_1v_1 + \ldots + k_rv_r = 0, \quad k_1, \ldots, k_r \in K,$$

следует, что

$$k_1 = k_2 = \ldots = k_r = 0.$$

Теорема 9.1. *Система элементов $v_1, \ldots, v_r \in {}_KV$ линейно зависима тогда и только тогда, когда для некоторого i, $1 \leqslant i \leqslant r$,*

$$v_i = \sum_{j \neq i} l_jv_j, \quad l_j \in K$$

(т. е. элемент v_i является линейной комбинацией остальных элементов системы $v_1, \ldots, v_r$).

8-5

Доказательство.

1) Пусть система $v_1, \ldots, v_r$ линейно зависима, т. е.

$$k_1 v_1 + \ldots + k_r v_r = 0, \quad k_i \neq 0.$$

Тогда

$$v_i = \sum_{j \neq i} \frac{(-k_j)}{k_i} v_j.$$

2) Если

$$v_i = \sum_{j \neq i} l_j v_j,$$

то

$$\sum_{j \neq i} l_j v_j + (-1) v_i = v_i + (-1) v_i = 0,$$

т. е. система $v_1, \ldots, v_r$ линейно зависима, поскольку $-1 \neq 0$. □

Пример 9.2. Если в системе элементов $v_1, \ldots, v_r \in {}_K V$ есть нулевой элемент, скажем, $v_i = 0$, то система $v_1 \ldots, v_r$ линейно зависима.

Действительно, $0v_1 + \ldots + 1v_i + \ldots + 0v_r = 0$, или, другим способом, $v_i = 0 = \sum\limits_{j \neq i} 0 v_j$.

Пример 9.3. Если $v_i = v_j$ для $i \neq j$, то система $v_1, \ldots, v_r \in {}_K V$ линейно зависима.

Действительно, $0v_1 + \ldots + 1v_i + \ldots + (-1)v_j + \ldots + 0v_r = 0$, или, иначе, $v_i = v_j + \sum\limits_{\substack{k \neq i \\ k \neq j}} 0 v_k$.

Пример 9.4. Система строк $\varepsilon_1, \ldots, \varepsilon_n \in {}_K K^n$, где

$$\begin{cases} \varepsilon_1 = (1, 0, \ldots, 0), \\ \varepsilon_2 = (0, 1, \ldots, 0), \\ \ldots \\ \varepsilon_n = (0, 0, \ldots, 1), \end{cases}$$

$(k_1, k_2 \ldots k_n) = (0, \ldots, 0)$

линейно независима. Кроме того, любая строка $\alpha = (k_1, \ldots, k_n) \in {}_K K^n$ является линейной комбинацией элементов $\varepsilon_1, \ldots, \varepsilon_n$, а именно, $\alpha = k_1 \varepsilon_1 + \ldots + k_n \varepsilon_n$.

$(k_1, \ldots, k_n) =$

8-6

Действительно,

$$k_1\varepsilon_1 + \ldots + k_n\varepsilon_n = (k_1, \ldots, k_n),$$

и поэтому если

$$k_1\varepsilon_1 + \ldots + k_n\varepsilon_n = (0, \ldots, 0),$$

то

$$k_1 = k_2 = \ldots = k_n = 0,$$

следовательно, система строк $\{\varepsilon_1, \ldots, \varepsilon_n\}$ линейно независима.

Пример 9.5. Пусть $v_1, v_2, v_3 \in {}_{\mathbb{R}}V$ — линейно независимая система в линейном пространстве ${}_{\mathbb{R}}V$. Тогда

$$u_1 = v_1 + v_2, \quad u_2 = v_1 + v_3, \quad u_3 = v_2 + v_3 -$$

также линейно независимая система.

Действительно, если

$$k_1u_1 + k_2u_2 + k_3u_3 = 0,$$

то

$$0 = k_1(v_1 + v_2) + k_2(v_1 + v_3) + k_3(v_2 + v_3) = \\ = (k_1 + k_2)v_1 + (k_1 + k_3)v_2 + (k_2 + k_3)v_3,$$

поэтому

$$\begin{cases} k_1 + k_2 = 0, \\ k_1 + k_3 = 0, \\ k_2 + k_3 = 0. \end{cases}$$

Следовательно, $k_1 = 0$, $k_2 = 0$, $k_3 = 0$, и система элементов u_1, u_2, u_3 линейно независима.

Упражнения 9.6.

1) Подсистема линейно независимой системы линейно независима.

2) Если подсистема линейно зависима, то линейно зависима и вся система.

8-7

Замечание 9.7. Для системы строк в K^n

$$\begin{array}{l} k_1 \\ \vdots \\ k_r \end{array} \left\{ \begin{array}{l} \alpha_1 = (a_{11}, \ldots, a_{1n}), \\ \ldots \\ \alpha_r = (a_{r1}, \ldots, a_{rn}) \end{array} \right.$$

вопрос о её линейной зависимости равносилен существованию ненулевого решения $(k_1, \ldots, k_r)$ следующей однородной системы линейных уравнений:

$$\begin{cases} a_{11}x_1 + \ldots + a_{r1}x_r = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}x_1 + \ldots + a_{rn}x_r = 0 \end{cases}$$

с транспонированной матрицей A^*, где

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rn} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{pmatrix}.$$

Таким образом, метод Гаусса даёт нам в этом случае алгоритмическое решение задачи о линейной зависимости строк.

Теорема 9.8. *Пусть $A = (a_{ij}) \in \mathrm{M}_n(K)$ — квадратная матрица. Тогда следующие условия равносильны:*

1) $|A| = 0$;

2) *система строк $A_1, \ldots, A_n$ матрицы A линейно зависима (в пространстве строк K^n);*

3) *система столбцов $\widehat{A_1}, \ldots, \widehat{A_n}$ матрицы A линейно зависима (в пространстве столбцов $\hat{K}^n$).*

Доказательство.

1) Если строки матрицы A линейно зависимы, скажем, i-я строка A_i является линейной комбинацией остальных, $A_i = \sum\limits_{j \neq i} l_j A_j$, то, как мы показали, $|A| = 0$, т. е. 2) $\Longrightarrow$ 1).

2) Пусть $|A| = 0$. Тогда

$$k_1 A_1 + \ldots + k_n A_n = 0$$

$k_1(a_{11}, \ldots, a_{1n})$
$+$
$+ k_n(a_{n1}, \ldots, a_{nn})$
$(0, \ldots, 0)$

8-8

в том и только в том случае, если $(k_1, \ldots, k_n)$ является решением однородной системы линейных уравнений с матрицей A^*. Так как $|A^*| = |A| = 0$, то существует ненулевое решение $(k_1, \ldots, k_n)$, т. е. система строк $A_1, \ldots, A_n$ матрицы A линейно зависима. Итак, 1) $\Longrightarrow$ 2).

3) Так как $|A^*| = |A|$, то 1) $\Longleftrightarrow$ 3). □

Задача 9.9. Пусть $A = (a_{ij}) \in \mathrm{M}_n(K)$, $B = (b_{ij}) \in \mathrm{M}_n(K)$, где $b_{ij} = A_{ji}$. Покажите, что если $|A| = 0$, то $|B| = 0$.

Теорема 9.10. *Любая система из m строк в K^n при $m > n$ линейно зависима.*

Доказательство. Если

$$\alpha_1 = (a_{11}, \ldots, a_{1n}),$$
$$\ldots$$
$$\alpha_m = (a_{m1}, \ldots, a_{mn}),$$

то равенство $k_1\alpha_1 + \ldots + k_m\alpha_m = 0$ равносильно тому, что $(k_1, \ldots, k_m)$ является решением следующей однородной системы линейных уравнений:

$$n < m \quad \begin{cases} a_{11}x_1 + \ldots + a_{m1}x_m = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}x_1 + \ldots + a_{mn}x_m = 0. \end{cases}$$

Так как число n уравнений меньше числа m переменных, то однородная система обладает ненулевым решением, т. е. система $\alpha_1, \ldots, \alpha_m$ линейно зависима. □

Следствие 9.11. *Если система $\alpha_1, \ldots, \alpha_r \in K^n$ линейно независима, то $r \leqslant n$.*

Лемма 9.12. *Если система элементов $\alpha_1, \ldots, \alpha_r \in {}_KV$ линейного пространства ${}_KV$ над полем K линейно независима, $\beta \in {}_KV$ и система $\alpha_1, \ldots, \alpha_r, \beta$ линейно зависима, то β является линейной комбинацией элементов $\alpha_1, \ldots, \alpha_r$.*

Доказательство. Пусть

$$k_1\alpha_1 + \ldots + k_r\alpha_r + k_{r+1}\beta = 0, \quad k_1, \ldots, k_{r+1} \in K,$$

8-9

где не все k_i, $1 \leqslant i \leqslant r+1$, равны нулю. Если бы $k_{r+1} = 0$, то нетривиальная линейная комбинация $k_1\alpha_1 + \ldots + k_r\alpha_r = 0$, равная нулю, означала бы, что система $\alpha_1, \ldots, \alpha_r$ линейно зависима, что противоречит предположению.

Итак, $k_{r+1} \neq 0$, и поэтому

$$\beta = \frac{-k_1}{k_{r+1}}\alpha_1 + \ldots + \frac{-k_r}{k_{r+1}}\alpha_r. \quad \square$$

Лемма 9.13 (единственность представления элемента линейного пространства $_KV$ в виде линейной комбинации линейно независимой системы элементов). *Пусть $\{\alpha_1, \ldots, \alpha_r\}$ — линейно независимая система элементов линейного пространства $_KV$ и*

$$\beta = k_1\alpha_1 + \ldots + k_r\alpha_r = k_1'\alpha_1 + \ldots + k_r'\alpha_r, \quad k_i, k_i' \in K.$$

Тогда $k_1 = k_1', \ldots, k_r = k_r'$.

Доказательство. Действительно,

$$(k_1 - k_1')\alpha_1 + \ldots + (k_r - k_r')\alpha_r = 0,$$

и поэтому $k_1 - k_1' = 0, \ldots, k_r - k_r' = 0$. $\square$

Максимальные линейно независимые подсистемы систем элементов линейных пространств, базис линейного пространства

Пусть $S \subseteq {}_KV$. Наиболее важные для нас случаи:

а) S — конечное подмножество элементов в $_KV$;

б) $S = {}_KV$.

Подсистема $v_1, \ldots, v_r \in S \subseteq {}_KV$ называется *максимальной линейно независимой подсистемой* в S, если:

1) $v_1, \ldots, v_r$ — линейно независимая система;

2) $v_1, \ldots, v_r, v$ — линейно зависимая система для всякого $v \in S$,

или, что эквивалентно,

8-10

2') любой элемент $v \in S$ является линейной комбинацией элементов $v_1, \ldots, v_r$.

Максимальная линейно независимая подсистема $v_1, \ldots, v_r$ в $S = {}_KV$ (если в ${}_KV$ существует такая *конечная* система) называется *базисом* линейного пространства ${}_KV$. Линейное пространство ${}_KV$ с конечным базисом $v_1, \ldots, v_r$ называется *конечномерным линейным пространством* (при этом ~~любая система $u_1, \ldots, u_s \in {}_KV$ при $s > r$ уже линейно зависима~~ будет показано, что любой другой базис линейного пространства содержит то же самое число элементов).

Пример 9.14. Как мы уже видели, система строк

$$\begin{aligned} \varepsilon_1 &= (1, 0, \ldots, 0), \\ \varepsilon_2 &= (0, 1, \ldots, 0), \\ &\ldots \\ \varepsilon_n &= (0, 0, \ldots, 1) \end{aligned}$$

является базисом линейного пространства строк K^n.

Лемма 9.15. *Любую линейно независимую подсистему $v_1, \ldots, v_r$ в $S \subseteq K^n$ можно дополнить до максимальной линейно независимой подсистемы в $S \subseteq K^n$.*

Доказательство. Если $v_1, \ldots, v_r$ — максимальная линейно независимая подсистема в $S \subseteq K^n$, то все доказано. Если нет, то найдётся элемент $v \in S$ такой, что $v_1, v_2, \ldots, v_r, v = v_{r+1}$ — линейно независимая подсистема в S. После конечного числа шагов процесс остановится, так как любые системы из $n+1$ элементов в линейном пространстве K^n оказываются линейно зависимыми. □

Следствие 9.16. *Любой ненулевой элемент $0 \neq v \in S \subseteq K^n$ дополняем до максимальной линейно независимой подсистемы в S.*

Следствие 9.17. *В $S = \mathbb{R}^n$ (или $S = K^n$ для бесконечного поля K) бесконечно много различных базисов. Если поле K конечно, $|K| = q$ (например, $K = \mathbb{Z}_2$), то число элементов в K^n равно q^n, и поэтому число базисов в K^n конечно. Найдите их число.*

Замечание 9.18. Пусть строки $a_1, \ldots, a_s \in K^n$ линейно независимы, $s < n$. Тогда существуют такие строки $a_{s+1}, \ldots, a_n \in K^n$,

что $\{a_1, \ldots, a_n\}$ — базис линейного пространства K^n. Практическое нахождение строк $a_{s+1}, \ldots, a_n$ можно осуществить следующим образом. Запишем строки $a_1, \ldots, a_s$ по столбцам и приведём полученную матрицу к ступенчатому виду: $\varphi(a_1^*, \ldots, a_s^*) = A_{\text{ступ}}$, где $(a_1^*, \ldots, a_s^*), A_{\text{ступ}} \in \mathrm{M}_{n,s}(K)$, φ — последовательность элементарных преобразований строк. Так как строки $a_1, \ldots, a_s$ линейно независимы, то в $A_{\text{ступ}}$ имеется ровно s ненулевых строк (первые s строк). Пусть $\hat{b}_{s+1}, \ldots, \hat{b}_n \in \hat{K}^n$ — столбцы, на i-м месте которых стоит 1, а остальные элементы равны 0, $i = s+1, \ldots, n$. Припишем эти столбцы справа к матрице $A_{\text{ступ}}$. Пусть $B \in \mathrm{M}_n(K)$ — полученная матрица. Применяя к матрице B последовательность элементарных преобразований строк, обратную к φ, приходим к матрице $\tilde{B}$. При этом $(\tilde{B})^*$ — матрица, в которой первые s строк — это $a_1, \ldots, a_s$, а последующие строки дополняют их до базиса линейного пространства K^n.

Замечание о линейной выражаемости конечных систем элементов в линейном пространстве

Пусть ${}_KV$ — линейное пространство, $S_1 \subseteq {}_KV$, $S_2 \subseteq {}_KV$. Будем говорить, что система S_2 элементов $u_1, \ldots, u_s$ *линейно выражается* через систему S_1 элементов $v_1, \ldots, v_r$, если каждый элемент $u_i \in S_2$, $1 \leqslant i \leqslant s$, является линейной комбинацией элементов $v_1, \ldots, v_r$ системы S_1,

$$u_i = \sum_{j=1}^{r} k_{ij} v_j, \quad k_{ij} \in K.$$

Если к тому же система S_3 элементов $w_1, \ldots, w_t$ линейно выражается через систему S_2,

$$w_k = \sum_{i=1}^{s} l_{ki} u_i, \quad l_{ki} \in K, \quad 1 \leqslant k \leqslant t,$$

то

$$w_k = \sum_{i=1}^{s} l_{ki} u_i = \sum_{i=1}^{s} \sum_{j=1}^{r} (l_{ki} k_{ij}) v_j = \sum_{j=1}^{r} \Big(\sum_{i=1}^{s} l_{ki} k_{ij} \Big) v_j,$$

т. е. система S_3 линейно выражается через систему S_1.

Системы S_1 и S_2 называются *эквивалентными*, если они линейно выражаются друг через друга (обозначение: $S_1 \sim S_2$).

8–12

Следствие 9.19. *Отношение «быть эквивалентными системами», $S_1 \sim S_2$, является отношением эквивалентности.*

Следствие 9.20. *Если элемент $v \in {}_KV$ является линейной комбинацией элементов $v_1, \ldots, v_r$ системы S_1, $S_1 \sim S_2$, где S_2 — система элементов $u_1, \ldots, u_s$, то элемент v является линейной комбинацией элементов $u_1, \ldots, u_s$ системы S_2.*

Следствие 9.21. *Любая (конечная) система элементов $S \subseteq {}_KV$ эквивалентна своей максимальной линейно независимой подсистеме.*

Следствие 9.22. *Любые две (конечные) максимально независимые подсистемы любой системы $S \subseteq {}_KV$ эквивалентны.*

Замечание 9.23. Если $A, B \in \mathrm{M}_{m,n}(K)$ и матрица B получена из матрицы A конечным числом элементарных преобразований 1-го, 2-го и 3-го типов, то каждая строка матрицы B является линейной комбинацией строк матрицы A (поскольку от матрицы B мы можем вернуться к матрице A с помощью элементарных преобразований строк 1-го, 2-го и 3-го типов, то каждая строка матрицы A является линейной комбинацией строк матрицы B). Таким образом, в линейном пространстве строк K^n системы строк $A_1, \ldots, A_m$ матрицы A и $B_1, \ldots, B_m$ матрицы B линейно выражаются друг через друга.

Теорема 9.24 (основная теорема о линейной зависимости). *Пусть в линейном пространстве ${}_KV$ линейно независимая система элементов $v_1, \ldots, v_r$ линейно выражается через другую систему элементов $u_1, \ldots, u_s$. Тогда $r \leqslant s$.*

Доказательство. Допустим противное: пусть $r > s$. В силу нашего предположения

$$\begin{cases} v_1 = a_{11}u_1 + \ldots + a_{1s}u_s, \\ \ldots \\ v_r = a_{r1}u_1 + \ldots + a_{rs}u_s, \quad a_{ij} \in K. \end{cases}$$

Так как $r > s$, то r строк

$$\begin{array}{ll} k_1 & (a_{11}, \ldots, a_{1s}), \\ & \ldots \\ k_r & (a_{r1}, \ldots, a_{rs}) \\ \hline & (0, \ldots 0) \end{array} \qquad K^s \qquad r > s$$

$k_i \neq 0$

8-13

в линейном пространстве строк K^s линейно зависимы: найдётся их линейная комбинация с коэффициентами $k_1, \ldots, k_r$, где $k_i \neq 0$ для некоторого i, равная нулевой строке $(0, \ldots, 0) \in K^s$. Но тогда и линейная комбинация элементов $v_1, \ldots, v_r$ с этими же коэффициентами $k_1, \ldots, k_r$, равна нулю, $k_1 v_1 + \ldots + k_r v_r = 0$. Таким образом, система элементов $v_1, \ldots, v_r$ линейно зависима, что приводит нас к противоречию. □

Следствие 9.25. *Две эквивалентные конечные линейно независимые системы в линейном пространстве ${}_KV$ содержат равное число элементов.*

Следствие 9.26. *Для системы $S \subseteq {}_KV$, где ${}_KV$ — конечномерное линейное пространство, любые две (конечные) максимальные линейно независимые подсистемы содержат одинаковое число элементов $\mathrm{r}(S)$, называемое рангом системы S.*

Следствие 9.27. *Если $S = {}_KV$ и ${}_KV$ — конечномерное линейное пространство, то любые два базиса в ${}_KV$ состоят из одного и того же числа элементов n, это число n называется размерностью линейного пространства ${}_KV$, обозначение: $\dim {}_KV = n$.*

${}_KV = K^n$

Как мы видели ранее, одним из базисов в линейном пространстве строк ${}_KK^n$ является система строк

$$\varepsilon_1 = (1, 0, \ldots, 0),$$
$$\ldots$$
$$\varepsilon_n = (0, 0, \ldots, 1),$$

и поэтому $\dim {}_KK^n = n$.

Следствие 9.28. *Если в конечномерном линейном пространстве ${}_KV$ одна система элементов S_1 линейно выражается через другую систему S_2, то $\mathrm{r}(S_1) \leqslant \mathrm{r}(S_2)$.*

Следствие 9.29. *Если в линейном пространстве ${}_KV$ система M из m элементов имеет ранг r, то любая её подсистема S из s элементов ($s \leqslant m$) имеет ранг не меньше чем $r + s - m$.*

8-14

Доказательство. Действительно, если R — максимальная линейно независимая подсистема в M, $|R| = r$, то $R \setminus (R \cap S) \subset M \setminus S$, и поэтому $|R \setminus (R \cap S)| \leqslant m - s$. Следовательно, $|R \cap S| \geqslant r - (m - s) = r + s - m$. □

Следствие 9.30. *Для системы строк $v_1, \ldots, v_r \in K^n$ следующие условия эквивалентны:*

1) *система строк $v_1, \ldots, v_r$ является базисом линейного пространства строк K^n (т. е. максимальной линейно независимой подсистемой строк в K^n; и тогда $r = n$);*

2) *каждая строка $v \in K^n$ единственным образом представляется в виде линейной комбинации*
$$v = \lambda_1 v_1 + \ldots + \lambda_r v_r, \quad \lambda_1, \ldots, \lambda_r \in K$$
(и тогда $r = n$);

3) *$r = n$ и система строк $v_1, \ldots, v_n$ линейно независима;*

4) *$r = n$ и каждая строка $v \in K^n$ представима в виде линейной комбинации*
$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n, \quad \lambda_1, \ldots, \lambda_n \in K.$$

Доказательство. Мы уже показали, что 1) $\Longrightarrow$ 2). Покажем, что 2) $\Longrightarrow$ 1). Если $v_1, \ldots, v_r$ — линейно зависимая система строк, $\lambda_1 v_1 + \ldots + \lambda_r v_r = 0$ с некоторым $\lambda_i \neq 0$, то нулевая строка имеет два различных представления
$$0 = 0 \cdot v_1 + \ldots + 0 \cdot v_r = \lambda_1 v_1 + \ldots + \lambda_r v_r, \quad \lambda_i \neq 0.$$
При этом $r = n$, так как любые базисы в K^n содержат n элементов.

Ясно, что 1) $\Longrightarrow$ 3). Покажем, что 3) $\Longrightarrow$ 1). Для любой строки $v \in K^n$ система строк $v_1, \ldots, v_n, v$ линейно зависима ($n + 1 > n$). Так как $v_1, \ldots, v_n$ — линейно независимая система, то $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$ для некоторых $\lambda_1, \ldots, \lambda_n \in K$.

Ясно, что 1) $\Longrightarrow$ 4). Покажем, что 4) $\Longrightarrow$ 1). Допустим, что $v_1, \ldots, v_n$ — линейно зависимая система. Тогда её максимально линейно независимая подсистема $v_{i_1}, \ldots, v_{i_r}$, $r < n$, является максимальной линейно независимой подсистемой в K^n, что противоречит $r = n$. □

8-15

12В

Единственность главного ступенчатого вида матрицы

Теорема 9.31. *Пусть $A, B, C \in \mathrm{M}_{m,n}(K)$, B и C — ступенчатые матрицы, полученные из ненулевой матрицы A конечным числом элементарных преобразований строк 1-го, 2-го и 3-го типов. Тогда:*

1) *системы строк $\{B_1, \ldots, B_m\}$ матрицы B и $\{C_1, \ldots, C_m\}$ матрицы C в линейном пространстве строк K^n линейно выражаются друг через друга (другими словами, линейные оболочки строк матриц A, B и C в K^n совпадают: $\langle A_1, \ldots, A_m\rangle = \langle B_1, \ldots, B_m\rangle = \langle C_1, \ldots, C_m\rangle$, см. с. 203);*

2) *числа r_1 и r_2 ненулевых строк в ступенчатых матрицах B и C соответственно совпадают (при этом $r = r_1 = r_2 = \dim_K\langle A_1, \ldots, A_m\rangle$; другие интерпретации числа $r = r(A)$ будут даны в теореме 9.58 о ранге матрицы);*

3) *лидеры строк ступенчатых матриц B и C располагаются в одних и тех же столбцах;*

4) *если B и C — главные ступенчатые виды ненулевой матрицы $A \in \mathrm{M}_{m,n}(K)$, то $B = C$.*

Доказательство.

1) В силу замечания 9.23, в линейном пространстве строк K^n системы строк $\{A_1, \ldots, A_m\}$ матрицы A и $\{B_1, \ldots, B_m\}$ матрицы B линейно выражаются друг через друга. Аналогично, системы строк $\{A_1, \ldots, A_m\}$ матрицы A и $\{C_1, \ldots, C_m\}$ матрицы C также линейно выражаются друг через друга. Принимая во внимание транзитивность линейной выражаемости систем строк (см. следствие 9.20), получаем, что системы строк $\{B_1, \ldots, B_m\}$ матрицы B и $\{C_1, \ldots, C_m\}$ матрицы C линейно выражаются друг через друга. Следовательно,

$$\langle A_1, \ldots, A_m\rangle = \langle B_1, \ldots, B_m\rangle = \langle C_1, \ldots, C_m\rangle.$$

2) Так как ненулевые строки ступенчатой матрицы образуют максимально независимую подсистему строк, то из 1) следует, что $r_1 = r_2$ (см. следствие 9.28), при этом

$$r = r_1 = r_2 = \dim\langle B_1, \ldots, B_m\rangle = \\ = \dim\langle C_1, \ldots, C_m\rangle = \dim\langle A_1, \ldots, A_m\rangle.$$

8-16

3) Пусть лидеры r ненулевых строк $B_1, B_2, \ldots, B_r$ ступенчатой матрицы B расположены в столбцах с номерами $k_1, k_2, \ldots, k_r$, $k_1 < k_2 < \ldots < k_r$, а лидеры r ненулевых строк $C_1, C_2, \ldots, C_r$ ступенчатой матрицы C расположены в столбцах с номерами $l_1, l_2, \ldots, l_r$, $l_1 < l_2 < \ldots < l_r$. Так как системы строк $\{B_1, B_2, \ldots, B_r\}$, $\{C_1, C_2, \ldots, C_r\}$ линейно выражаются друг через друга, то, в силу леммы 3.15 и следствия 3.16, $k_1 = l_1$ ($k_1 \geqslant \min\{l_i\} = l_1$; $l_1 \geqslant \min\{k_i\} = k_1$).

Если

$$B_2 = \sum_{j=1}^{r} \lambda_{2j} C_j, \quad C_2 = \sum_{j=1}^{r} \mu_{2j} B_j,$$

то $\lambda_{21} = 0 = \mu_{21}$. Применяя наше рассуждение для систем $\{B_2, \ldots, B_r\}$ и $\{C_2, \ldots, C_r\}$, которые линейно выражаются друг через друга, получаем, что $k_2 = l_2$.

Продолжая этот процесс, убеждаемся в том, что $k_3 = l_3, \ldots, k_r = l_r$.

4) В 2) и 3) доказано, что число ненулевых строк r и номера столбцов $l_1, \ldots, l_r$, $1 \leqslant l_1 < l_2 < \ldots < l_r \leqslant n$, в которых находятся главные неизвестные главных ступенчатых видов B и C, определены однозначно. Таким образом, разбиения на главные и свободные неизвестные, определяемые ступенчатыми видами B и C, совпадают. Поскольку главные неизвестные однозначно выражаются через свободные (в эквивалентных однородных системах линейных уравнений с главными ступенчатыми матрицами B и C), при этом главный ступенчатый вид определяется этим выражением однозначно (см. замечание 3.29), то $B = C$. □

Замечание 9.32 (матричное доказательство п. 4 теоремы о единственности главного ступенчатого вида). Для $A \in \mathrm{M}_{m,n}(K)$ существуют такие обратимые матрицы $F, G \in \mathrm{M}_m(K)$ (произведения матриц, соответствующих элементарным преобразованиям строк), что

$$A = F \cdot B = G \cdot C.$$

Следовательно,

$$B = D \cdot C, \quad \text{где} \quad D = F^{-1}G.$$

8-17

Используя определение главного ступенчатого вида и переставляя столбцы матриц B и C, имеем:

$$B \cdot Q = \left(\begin{array}{c|c} E_r & * \\ \hline 0 & 0 \end{array}\right) = D \cdot \left(\begin{array}{c|c} E_r & *' \\ \hline 0 & 0 \end{array}\right) = D \cdot C \cdot Q, \qquad (8)$$

где $Q \in \mathrm{M}_n(K)$ (матрица Q — обратимая матрица, соответствующая последовательности элементарных преобразований столбцов; мы уже доказали в п. 2 и 3, что числа r и столбцы $j_1, \ldots, j_r$, в которых стоят лидеры строк, одинаковы для ступенчатых матриц B и C, соответственно; нулевые блоки могут отсутствовать (если $k = r = m$)). Следовательно, матрица D имеет следующий блочный вид:

$$D = \left(\begin{array}{c|c} E_r & \tilde{*} \\ \hline 0 & \end{array}\right),$$

где матрица $\tilde{*} \in \mathrm{M}_{m,m-r}(K)$ (если $r < m$) состоит из произвольных элементов поля K. Поэтому, умножая D на

$$\left(\begin{array}{c|c} E_r & *' \\ \hline 0 & 0 \end{array}\right)$$

и приравнивая к

$$\left(\begin{array}{c|c} E_r & * \\ \hline 0 & 0 \end{array}\right),$$

получаем, что $* = *' \in \mathrm{M}_{m-r,n-r}(K)$. Умножая (8) справа на Q^{-1}, получаем $B = C$.

Изоморфизм линейных пространств

Пусть ${}_KU$, ${}_KV$ — линейные пространства над полем K. Биективное отображение

$$f\colon {}_KU \to {}_KV,$$

для которого

$$f(u_1 + u_2) = f(u_1) + f(u_2),$$
$$f(ku) = kf(u)$$

для всех $u_1, u_2, u \in {}_KU$, $k \in K$, называется *изоморфизмом* линейных пространств ${}_KU$ и ${}_KV$ (в этом случае будем говорить, что линейные пространства ${}_KU$ и ${}_KV$ *изоморфны*, обозначение: ${}_KU \cong {}_KV$).

8-18

$V \cong V$

$U \cong V \Rightarrow V \cong U$

$U \cong V$, $V \cong W \Rightarrow U \cong W$

Упражнение 9.33. Отношение ${}_KU \cong {}_KV$ является отношением эквивалентности.

Лемма 9.34. *Если $f\colon {}_KU \to {}_KV$ — изоморфизм линейных пространств, $\dim {}_KU = n$, $\{e_1, \ldots, e_n\}$ — базис в ${}_KU$, то $\{f(e_1), \ldots, f(e_n)\}$ — базис в ${}_KV$, и поэтому $\dim {}_KV = n = \dim {}_KU$.*

Доказательство.

1) Если $v \in {}_KV$, то $f(u) = v$ для некоторого $u \in {}_KU$. Пусть $u = k_1e_1 + \ldots + k_ne_n$, где $k_1, \ldots, k_n \in K$. Тогда

$$v = f(u) = k_1f(e_1) + \ldots + k_nf(e_n).$$

2) Пусть $k_1f(e_1) + \ldots + k_nf(e_n) = 0$ для $k_1, \ldots, k_n \in K$. Тогда

$$0 = k_1f(e_1) + \ldots + k_nf(e_n) = f(k_1e_1 + \ldots + k_ne_n),$$

и поэтому

$$k_1e_1 + \ldots + k_ne_n = 0,$$

следовательно, $k_1 = k_2 = \ldots = k_n = 0$.

Итак, в силу 1) и 2), $\{f(e_1), \ldots, f(e_n)\}$ — базис линейного пространства ${}_KV$. ▨

Лемма 9.35. *Если $\dim {}_KV = n$ и $\{e_1, \ldots, e_n\}$ — базис линейного пространства ${}_KV$, то, сопоставляя каждому элементу $v = k_1e_1 + \ldots + k_ne_n \in {}_KV$ однозначно определённую строчку его координат $(k_1, \ldots, k_n)$ в базисе $\{e_1, \ldots, e_n\}$, получаем изоморфизм линейных пространств ${}_KV \cong K^n$, таким образом, каждое n-мерное линейное пространство ${}_KV$ над полем K изоморфно линейному пространству строк K^n.*

Доказательство. Соответствие

$$\Delta\colon {}_KV \in v = k_1e_1 + \ldots + k_ne_n \mapsto (k_1, \ldots, k_n) \in K^n$$

является биекцией, для которой

$$\Delta(v + v') = \Delta((k_1e_1 + \ldots + k_ne_n) + (k'_1e_1 + \ldots + k'_ne_n)) =$$
$$= \Delta((k_1 + k'_1)e_1 + \ldots + (k_n + k'_n)e_n) =$$

8-19

$$= (k_1 + k_1', \ldots, k_n + k_n') = (k_1, \ldots, k_n) + (k_1', \ldots, k_n') =$$
$$= \Delta(v) + \Delta(v');$$
$$\Delta(kv) = \Delta(k(k_1e_1 + \ldots + k_ne_n)) = \Delta((kk_1)e_1 + \ldots + (kk_n)e_n) =$$
$$= (kk_1, \ldots, kk_n) = k(k_1, \ldots, k_n) = k\Delta(v). \quad \square$$

Теорема 9.36. *Конечномерные линейные пространства* ${}_KU$ *и* ${}_KV$ *изоморфны тогда и только тогда, когда* $\dim_K U = \dim_K V = n$, *и в этом случае* ${}_KU \cong K^n \cong {}_KV$.

Доказательство теоремы следует из лемм 9.34 и 9.35. $\square$

Упражнение 9.37. Покажите, что следующие линейные пространства являются бесконечномерными линейными пространствами (это означает, что в них нет базиса из конечного числа элементов):

1) ${}_{\mathbb{R}}C[0,1]$ — линейное пространство вещественных непрерывных функций на отрезке $[0,1]$;

2) ${}_KK[x]$ — линейное пространство многочленов от переменной x с коэффициентами из поля K;

3) ${}_KK^{\mathbb{N}}$ — линейное пространство всех счётных последовательностей $(k_1, k_2, \ldots, k_n, \ldots)$ элементов из поля K.

Упражнение 9.38. Докажите, что

а) $\dim_K \mathrm{M}_{m,n}(K) = mn$;

б) $\dim_{\mathbb{R}}\{A \in \mathrm{M}_n(\mathbb{R}) \mid A^* = A\} = \dfrac{n(n+1)}{2}$;

в) $\dim_{\mathbb{R}}\{A \in \mathrm{M}_n(\mathbb{R}) \mid A^* = -A\} = \dfrac{n(n-1)}{2}$.

Замена базиса линейного пространства

Пусть V — конечномерное линейное пространство над полем K, $\dim V = n < \infty$, $\{v_1, \ldots, v_n\}$ — базис в V, $\{v_1', \ldots, v_n'\}$ — другой базис в V,

$$v_j' = c_{1j}v_1 + c_{2j}v_2 + \ldots + c_{nj}v_n, \quad j = 1, \ldots, n, \quad c_{ij} \in K$$

8-20

(запись по столбцу!). $C = (c_{ij}) \in \mathrm{M}_n(K)$ — *матрица перехода* от первого базиса ко второму.

Замечание 9.39. Так как умножение в поле K коммутативно, то левое линейное пространство ${}_KV$ можно рассматривать и как правое линейное пространство V_K, полагая $v\lambda = \lambda v$ для всех $\lambda \in K$, $v \in V$. Тогда определение матрицы перехода может быть записано в матричном виде как

$$(v'_1, \ldots, v'_n) = (v_1, \ldots, v_n)C.$$

Ограничиваясь левыми линейными пространствами, мы можем использовать эквивалентную форму записи:

$$\begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = C^* \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

или, кратко, $\mathcal{E}' = C^*\mathcal{E}$, где

$$\mathcal{E} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \ \mathcal{E}' = \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} \in \mathrm{M}_{n,1}(V).$$

Если $V = K^n$, то $v_1, \ldots, v_n, v'_1, \ldots, v'_n \in K^n$, $\mathcal{E}, \mathcal{E}' \in \mathrm{M}_n(K)$ и $\mathcal{E}' = C^*\mathcal{E}$ означает равенство квадратных $(n \times n)$-матриц.

Обратимость матрицы перехода

1) Если $|C| = 0$, то $|C^*| = 0$ и строки матрицы C^* линейно зависимы. Поэтому из

$$\begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = C^* \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \quad \text{то есть} \quad \mathcal{E}' = C^*\mathcal{E},$$

следует, что $v'_1, \ldots, v'_n$ — линейно зависимая система в V, что приводит к противоречию с тем, что $v'_1, \ldots, v'_n$ — базис. Итак, мы показали, что $|C| \neq 0$ и существует обратная матрица C^{-1} (тогда $(C^*)^{-1} = (C^{-1})^*$).

§-21

2) Другое доказательство обратимости матрицы C даёт интерпретация матрицы $B = C^{-1}$ как матрицы перехода от второго базиса к первому.

Действительно, элементы $v_1, \ldots, v_n$ также выражаются как линейные комбинации элементов базиса $\{v'_1, \ldots, v'_n\}$:

$$v_i = b_{1i}v'_1 + \ldots + b_{ni}v'_n, \quad i = 1, \ldots, n, \quad b_{ij} \in K,$$

$B = (b_{ij}) \in \mathrm{M}_n(K)$. Тогда $\mathcal{E} = B^*\mathcal{E}'$. Так как $\mathcal{E}' = C^*\mathcal{E}$, то

$$\mathcal{E} = B^*(C^*\mathcal{E}) = (B^*C^*)\mathcal{E} = (CB)^*\mathcal{E}.$$

Так как $\{v_1, \ldots, v_n\}$ — базис в V, то $(CB)^* = E$, следовательно, $CB = E$, и поэтому $B = C^{-1}$. □

3) Для любой обратимой матрицы $C \in \mathrm{M}_n(K)$, $|C| \neq 0$, и любого базиса $\{v_1, \ldots, v_n\}$ конечномерного линейного пространства ${}_KV$, $\dim {}_KV = n$, элементы $v'_1, \ldots, v'_n \in {}_KV$, где

$$\begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = C^* \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

образуют базис линейного пространства ${}_KV$.

Действительно, в этом случае

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = (C^*)^{-1} \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix}, \quad (C^*)^{-1} = (C^{-1})^*,$$

т. е. n линейно независимых элементов $v_1, \ldots, v_n$ линейно выражаются через $v'_1, \ldots, v'_n$. По основной лемме о линейной зависимости элементы $v'_1, \ldots, v'_n$ линейно независимы. Так как $\dim {}_KV = n$, то $\{v'_1, \ldots, v'_n\}$ — базис линейного пространства ${}_KV$. □

Замена координат элемента линейного пространства при замене базиса

Пусть $\{v_1, \ldots, v_n\}$, $\{v'_1, \ldots, v'_n\}$ — два базиса линейного пространства ${}_KV$, $\dim {}_KV = n$, $C \in \mathrm{M}_n(K)$, $|C| \neq 0$, — матрица перехода от

8-22

первого базиса ко второму,

$$\begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix} = C^* \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

$x = x_1v_1 + \ldots + x_nv_n = x_1'v_1' + \ldots + x_n'v_n' \in {}_KV$. Так как

$$x = x_1v_1 + \ldots + x_nv_n = (x_1, \ldots, x_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} =$$

$$= (x_1, \ldots, x_n)(C^{-1})^* \begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix} = (x_1', \ldots, x_n') \begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix},$$

то

$$(x_1', \ldots, x_n') = (x_1, \ldots, x_n)(C^{-1})^*,$$

или

$$\begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix} = C^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

что эквивалентно

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = C \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix}. \quad \square$$

Пример 9.40. Пусть $V = \mathbb{R}^3$, $v_1 = (2, 1, -3)$, $v_2 = (3, 2, -5)$, $v_3 = (1, -1, 1)$. Необходимо выяснить, образуют ли элементы v_1, v_2, v_3 базис в $\mathbb{R}^3$, и если да, то найти координаты строки $x = (6, 2, -7)$ в базисе $\{v_1, v_2, v_3\}$.

Решение.

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = C^* \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix},$$

где $\{e_1, e_2, e_3\}$ — стандартный базис в $\mathbb{R}^3$,

$$C = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & -1 \\ -3 & -5 & 1 \end{pmatrix}.$$

8-23 –

Строки v_1, v_2, v_3 образуют базис в $\mathbb{R}^3$ тогда и только тогда, когда матрица C обратима. Если матрица C обратима, то столбец координат строки x в базисе $\{v_1, v_2, v_3\}$ равен

$$C^{-1}\begin{pmatrix} 6 \\ 2 \\ -7 \end{pmatrix}.$$

Для вычисления этого столбца применим алгоритм (с. [redacted]), в процессе работы которого проверяется, обратима ли матрица A = C!

$$\left(\begin{array}{ccc|c} 2 & 3 & 1 & 6 \\ 1 & 2 & -1 & 2 \\ -3 & -5 & 1 & -7 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 2 & 3 & 1 & 6 \\ -3 & -5 & 1 & -7 \end{array}\right) \to$$

$$\to \left(\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 0 & -1 & 3 & 2 \\ -3 & -5 & 1 & -7 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 0 & 1 & -3 & -2 \\ 0 & 1 & -2 & -1 \end{array}\right) \to$$

$$\to \left(\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 0 & 1 & -3 & -2 \\ 0 & 0 & 1 & 1 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \to$$

$$\to \left(\begin{array}{ccc|c} 1 & 2 & 0 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Таким образом, матрица C обратима, $(1, 1, 1)$ — координаты строки x в базисе $\{v_1, v_2, v_3\}$, $x = v_1 + v_2 + v_3$.

Этот же результат можно было получить, используя формулу $(6, 2, -7)(C^*)^{-1} = (1, 1, 1)$,

$$\left(\begin{array}{ccc} 2 & 1 & -3 \\ 3 & 2 & -5 \\ 1 & -1 & 1 \\ \hline 6 & 2 & -7 \end{array}\right) \to \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 1 & 1 \end{array}\right)$$

(здесь применяем элементарные преобразования столбцов).

Конец лекции №8

9-1

Лекция N 9
(11 октября 2011 г.)

Линейные подпространства линейных пространств

9.1

Пусть K — поле, ${}_KV$ — линейное пространство над полем K. Непустое подмножество $\varnothing \neq U \subseteq {}_KV$ называется *линейным подпространством* линейного пространства ${}_KV$, если:

9-2

1) $u_1 + u_2 \in U$ для всех $u_1, u_2 \in U$;

2) $ku \in U$ для всех $k \in K$, $u \in U$.

Ясно, что ${}_KU$ — линейное пространство относительно тех же операций сложения элементов и умножения на элементы из поля K, что и в линейном пространстве ${}_KV$.

КВ !

Если U — линейное подпространство в конечномерном линейном пространстве ${}_KV$, $n = \dim {}_KV < \infty$, то $\dim {}_KU \leqslant \dim {}_KV$. Действительно, если элементы $u_1, \ldots, u_s \in {}_KU$ линейно независимы в ${}_KU$, то эти элементы линейно независимы и в линейном пространстве ${}_KV$, $s \leqslant n$, поэтому $\dim {}_KU \leqslant \dim {}_KV$.

КВ !

Если ${}_KU$ — линейное подпространство линейного пространства ${}_KV$, ${}_KU \subseteq {}_KV$ и $\dim {}_KU = \dim {}_KV = n$, то ${}_KU = {}_KV$. Действительно, если $\{u_1, \ldots, u_n\}$ — базис линейного пространства ${}_KU \subseteq$ $\subseteq {}_KV$, то эти n элементов $u_1, \ldots, u_n$ линейно независимы в ${}_KV$ и $\dim {}_KV = n$, поэтому $\{u_1, \ldots, u_n\}$ — базис линейного пространства ${}_KV$. Итак, каждый элемент $v \in V$ имеет вид $v = k_1u_1 + \ldots +$ $+ k_nu_n \in {}_KU$, $k_i \in K$, т. е. ${}_KV = {}_KU$.

Пересечение линейных подпространств

Лемма 9.41. *Пересечение*

$$U = \bigcap_{i \in I} U_i$$

любого семейства линейных подпространств $\{U_i \subset {}_KV \mid i \in I\}$ *линейного пространства* ${}_KV$ *является линейным подпространством.*

Доказательство. Если $u, u_1, u_2 \in U = \bigcap_{i \in I} U_i$, $k \in K$, то $u, u_1, u_2 \in U_i$ для любого $i \in I$, поэтому $u_1 + u_2, ku \in U_i$ для любого $i \in I$, т. е. $u_1 + u_2, ku \in U = \bigcap_{i \in I} U_i$. □

Следствие 9.42. *Если* U_1 *и* U_2 *— линейные подпространства линейного пространства* ${}_KV$, *то* $U_1 \cap U_2$ *— линейное подпространство в* ${}_KV$ *(наибольшее подпространство среди подпространств, лежащих одновременно в* U_1 *и в* U_2*).*

9-3

Сумма линейных подпространств

Если U_1 и U_2 — линейные подпространства линейного пространства ${}_KV$, то *сумма линейных подпространств*

$$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1,\ u_2 \in U_2\}$$

также является линейным подпространством. Действительно, если $u_1 + u_2, u_1' + u_2' \in U_1 + U_2$, $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$, $k \in K$, то

$$(u_1 + u_2) + (u_1' + u_2') = (u_1 + u_1') + (u_2 + u_2') \in U_1 + U_2;$$
$$k(u_1 + u_2) = ku_1 + ku_2 \in U_1 + U_2. \quad \square$$

Замечание 9.43. $U_1 + U_2$ — наименьшее линейное подпространство среди линейных подпространств, содержащих одновременно U_1 и U_2. Более того,

$$U_1 + U_2 = \bigcap_{\substack{U \subseteq_K V \\ U_1 \subseteq U,\ U_2 \subseteq U}} U.$$

Замечание 9.44. Если U, U_1, U_2, U_3 — линейные подпространства в ${}_KV$, то

$$U \cap U = U, \quad U + U = U,$$
$$U_1 \cap U_2 = U_2 \cap U_1, \quad U_1 + U_2 = U_2 + U_1,$$
$$U_1 \cap (U_2 \cap U_3) = (U_1 \cap U_2) \cap U_3,$$
$$U_1 + (U_2 + U_3) = (U_1 + U_2) + U_3,$$
$$U_1 \cap (U_1 + U_2) = U_1, \quad U_1 + (U_1 \cap U_2) = U_1.$$

Линейная оболочка элементов линейного пространства

Пусть ${}_KV$ — линейное пространство, $v_1, \ldots, v_m \in {}_KV$. Рассмотрим

$$\langle v_1, \ldots, v_m \rangle = \{k_1 v_1 + \ldots + k_m v_m \mid k_1, \ldots, k_m \in K\} -$$

совокупность всех линейных комбинаций $k_1 v_1 + \ldots + k_m v_m$ элементов $v_1, \ldots, v_m$ с коэффициентами $k_1, \ldots, k_m \in K$, называемую *линейной*

9-4

оболочкой элементов $v_1, \ldots, v_m$. Линейная оболочка $\langle v_1, \ldots, v_m \rangle$ является наименьшим линейным подпространством, содержащим элементы $v_1, \ldots, v_m$. Действительно,

$$(k_1 v_1 + \ldots + k_m v_m) + (l_1 v_1 + \ldots + l_m v_m) = \\ = (k_1 + l_1) v_1 + \ldots + (k_m + l_m) v_m;$$

$$k(k_1 v_1 + \ldots + k_m v_m) = (k k_1) v_1 + \ldots + (k k_m) v_m;$$

если U — линейное подпространство в ${}_K V$, $v_1, \ldots, v_m \in U$, то $k_1 v_1 + \ldots + k_m v_m \in U$, следовательно, $\langle v_1, \ldots, v_m \rangle \subseteq U$. Более того,

$$\langle v_1, \ldots, v_m \rangle = \bigcap_{\substack{U \subseteq_K V \\ v_1, \ldots, v_m \in U}} U.$$

Замечание 9.45. Если $0 \neq v \in {}_K V$, то $\langle v \rangle = Kv = \{kv \mid k \in K\}$, $\dim \langle v \rangle = 1$; если $v = 0$, $\langle v \rangle = Kv = \{0\}$.

Замечание 9.46. $\langle v_1, \ldots, v_m \rangle = Kv_1 + \ldots + Kv_m$.

Замечание 9.47. $\dim_K \langle v_1, \ldots, v_m \rangle = \mathrm{r}\{v_1, \ldots, v_m\}$; любая максимальная линейно независимая подсистема в $\{v_1, \ldots, v_m\}$ является базисом линейного подпространства $\langle v_1, \ldots, v_m \rangle$.

Основная лемма о линейной зависимости может быть сформулирована в следующей эквивалентной форме.

Теорема 9.48 (о замене). *Пусть $v_1, \ldots, v_s \in {}_K V$ — линейно независимая система, $u_1, \ldots, u_r \in \langle v_1, \ldots, v_s \rangle$, $\{u_1, \ldots, u_r\}$ — линейно независимая система элементов. Тогда $r \leqslant s$ и*

$$\langle v_1, \ldots, v_s \rangle = \langle u_1, \ldots, u_r, v_{i_{r+1}}, \ldots, v_{i_s} \rangle,$$

где

$$1 \leqslant i_{r+1} < \ldots < i_s \leqslant s.$$

Доказательство. Так как $s = \dim_K \langle v_1, \ldots, v_s \rangle$, то $r \leqslant s$. Если $r = s$, то $\langle v_1, \ldots, v_s \rangle = \langle u_1, \ldots, u_r \rangle$. Если $r < s$, то найдётся $v_{i_{r+1}} \notin \langle u_1, \ldots, u_r \rangle$ (индекс i_{r+1} — минимальный с этим свойством). Продолжая этот процесс, построим базис $\{u_1, \ldots, u_r, v_{i_{r+1}}, \ldots, v_{i_s}\}$ в $\langle v_1, \ldots, v_s \rangle$. □

9-5

Следствие 9.49. *Пусть U, W — линейные подпространства в ${}_KV$ и $U \subseteq W$, $\dim_K U = l$, $\dim_K W = m$. Тогда $l \leqslant m$ и любой базис подпространства U можно дополнить $m - l$ элементами до базиса подпространства W. В частности, если $U \subseteq W$ и $l = m$, то $U = W$.*

Теорема 9.50 (формула размерности). *Пусть U, W — линейные подпространства в ${}_KV$, $\dim_K V = n < \infty$. Тогда*

$$\dim_K U + \dim_K W = \dim_K (U \cap W) + \dim_K (U + W),$$

или, что эквивалентно,

$$\dim_K (U + W) = \dim_K U + \dim_K W - \dim_K (U \cap W).$$

Доказательство. Пусть $\dim_K (U \cap W) = d$, $\dim_K U = s$, $\dim_K W = t$. Ясно, что $0 \leqslant d \leqslant s$, $d \leqslant t$. При $d = 0$ утверждение очевидно (объединение базисов в U и W даёт базис в $U + W$). Выберем базис $v_1, \ldots, v_d$ линейного пространства $U \cap W$ и дополним его до базиса $v_1, \ldots, v_d, u_1, \ldots, u_{s-d}$ линейного пространства U и до базиса $v_1, \ldots, v_d, w_1, \ldots, w_{t-d}$ линейного пространства W. Ясно, что

$$U + W = \langle v_1, \ldots, v_d, u_1, \ldots, u_{s-d}, w_1, \ldots, w_{t-d} \rangle.$$

Если

$$\lambda_1 v_1 + \ldots + \lambda_d v_d + \mu_1 u_1 + \ldots + \mu_{s-d} u_{s-d} + \gamma_1 w_1 + \ldots + \gamma_{t-d} w_{t-d} = 0,$$

то

$$\sum_{i=1}^{d} \lambda_i v_i + \sum_{j=1}^{s-d} \mu_j u_j = -\sum_{k=1}^{t-d} \gamma_k w_k \in U \cap W,$$

поэтому $\mu_1 = \ldots = \mu_{s-d} = 0$, $\gamma_1 = \ldots = \gamma_{t-d} = 0$. Следовательно, $\lambda_1 = \ldots = \lambda_d = 0$. Таким образом,

$$\{v_1, \ldots, v_d, u_1, \ldots, u_{s-d}, w_1, \ldots, w_{t-d}\} -$$

базис линейного подпространства $U + W$, откуда

$$s + t = d + (s - d) + d + (t - d) = d + (d + (s - d) + (t - d)),$$

поэтому

$$\dim_K U + \dim_K W = \dim_K U \cap W + \dim_K (U + W). \quad \boxtimes$$

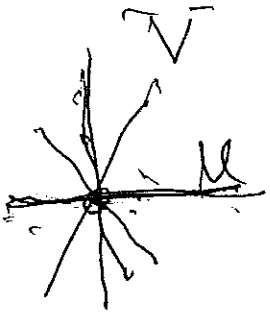
9-6

Теорема 9.51 (о существовании прямого дополнения подпространства). *Пусть* $\dim {}_KV = n < \infty$, U — *линейное подпространство в* ${}_KV$. *Тогда существует линейное подпространство* W *в* ${}_KV$ *такое, что*

$$U + W = V, \quad U \cap W = \{0\},$$

(*называемое прямым дополнением подпространства* U *в* ${}_KV$; *в этом случае также говорят, что линейное пространство* ${}_KV$ *является прямой суммой линейных подпространств* U *и* W, *обозначение:* ${}_KV = U \oplus W$).

Доказательство. Если $\dim {}_KU = r$ и $\{u_1, \ldots, u_r\}$ — базис в ${}_KU$, то дополним его до базиса линейного пространства ${}_KV$: $u_1, \ldots, u_r, v_1, \ldots, v_{n-r}$. Пусть $W = \langle v_1, \ldots, v_{n-r}\rangle$. Тогда ${}_KV = U + W$, $U \cap W = \{0\}$. □



Замечание 9.52. Конечно, прямое дополнение определено неоднозначно, однако все прямые дополнения линейного пространства изоморфны (а именно, все они имеют размерность $\dim {}_KV - \dim {}_KU$).

Замечание 9.53. Если ${}_KV = U \oplus W$, то представление элемента $v \in V$ в виде $v = u + w$, $u \in U$, $w \in W$, определено однозначно (действительно, если $v = u + w = u' + w'$, $u' \in U$, $w' \in W$, то $u - u' = w' - w \in U \cap W = \{0\}$, следовательно, $u = u'$, $w = w'$), и поэтому линейное пространство ${}_KV = U \oplus W$ изоморфно *внешней прямой* сумме $\{(u, w) \mid u \in U,\ w \in W\}$ линейных пространств ${}_KU$ и ${}_KW$ с естественными операциями сложения пар и их умножения на $c \in K$.

Пример 9.54 (прямого разложения). Пусть

$$V = \mathrm{M}_n(\mathbb{R}), \quad U = \{A \in \mathrm{M}_n(\mathbb{R}) \mid A^* = A\},$$
$$W = \{A \in \mathrm{M}_n(\mathbb{R}) \mid A^* = -A\}.$$

Тогда

$${}_{\mathbb{R}}V = U \oplus W.$$

Действительно, $A = \dfrac{A + A^*}{2} + \dfrac{A - A^*}{2}$. Если $A = A^* = -A$, то $A = 0 \in \mathrm{M}_n(\mathbb{R})$. □

$U' = \{(u, 0)\}$
$W' = \{(0, w)\}$

$U, W \Longrightarrow \{(u, w) \mid u \in U$ и $w \in W\}$
$U \oplus W$

9-7

Решётка подпространств линейного пространства

Рассмотрим частично упорядоченное множество всех линейных подпространств U линейного пространства ${}_KV$:

$$\mathcal{L}({}_KV) = \{U \mid U \subseteq {}_KV\},$$

где $U_1 \leqslant U_2$ означает $U_1 \subseteq U_2$. Для любых двух элементов $U_1, U_2 \in \mathcal{L}({}_KV)$ существует точная верхняя грань $U_1 \vee U_2 = U_1 + U_2$ и точная нижняя грань $U_1 \wedge U_2 = U_1 \cap U_2$, таким образом, частично упорядоченное множество $\mathcal{L}({}_KV)$ является *решёткой* (*решёткой линейных подпространств* линейного пространства ${}_KV$), при этом $\mathcal{L}({}_KV)$ — решётка с дополнениями (т. е. для всякого $U \in \mathcal{L}({}_KV)$ существует такой элемент $W \in \mathcal{L}({}_KV)$, что $U \vee W = V$, $U \wedge W = \{0\}$).

Теорема 9.55. *В решётке $\mathcal{L}({}_KV)$ выполнено следующее модулярное тождество Дедекинда: если $X, Y, Z \in \mathcal{L}({}_KV)$, $X \subseteq Z$, то*

$$X + (Y \cap Z) = (X + Y) \cap Z.$$

Доказательство.

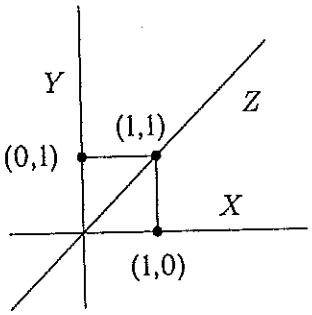
1) Пусть $x + a \in X + (Y \cap Z)$, где $x \in X$, $a \in Y \cap Z$, тогда $a \in Y$, и поэтому $x + a \in X + Y$; $x \in X \subseteq Z$, $a \in Y \cap Z \subseteq Z$, и следовательно, $x + a \in Z$; итак, $x + a \in (X + Y) \cap Z$.

2) Пусть $z \in (X + Y) \cap Z$, $z = x + y$, где $x \in X$, $y \in Y$. Тогда $y = z - x \in Y \cap Z$, поскольку $X \subseteq Z$, и поэтому $z = x + y \in X + (Y \cap Z)$. □

Замечание 9.56. Если $\dim {}_KV \geqslant 2$, то в $\mathcal{L}({}_KV)$ не выполняется тождество дистрибутивности

$$(X + Y) \cap Z = (X \cap Z) + (Y \cap Z).$$

Действительно, в ${}_KV = K^2$ имеем для



9-8

$$X + Y = {}_KV = K^2, \quad X \cap Z = \{0\}, \quad Y \cap Z = \{0\},$$
$$(X + Y) \cap Z = Z \neq \{0\} = (X \cap Z) + (Y \cap Z). \quad \square$$

Замечание 9.57. Итак, мы убедились в том, что решётка $\mathcal{L}({}_KV)$ всех линейных подпространств линейного пространства ${}_KV$ является модулярной (дедекиндовой) решёткой с дополнениями.

Замечание

Проективная размерность подпространств и проективная геометрия $\mathrm{PG}({}_KV)$

Если $\dim {}_KV = n$, $U \in \mathcal{L}({}_KV)$ — линейное подпространство в ${}_KV$, то определим *проективную размерность*

$$\mathrm{p.dim}\, U = \dim {}_KU - 1.$$

Таким образом, нулевое подпространство в ${}_KV$ имеет проективную размерность, равную -1; одномерные линейные подпространства имеют нулевую проективную размерность (их называют *точками* проективной геометрии); двумерные линейные подпространства имеют проективную размерность, равную 1 (их называют *прямыми* проективной геометрии); и т. д., $\mathrm{p.dim}\, V = n-1$. Обозначая через G_i совокупность всех $(i+1)$-мерных линейных подпространств в ${}_KV$, получаем $(n-1)$-*мерную проективную геометрию*

$$\mathrm{PG}({}_KV) = \{G_0, G_1, \ldots, G_{n-1}\},$$

где G_0 — множество точек, G_1 — множество прямых, G_2 — плоскостей, G_i — множество i-мерных плоскостей, с отношением инцидентности $U \prec W$ для $U \in G_i$, $W \in G_j$, где $0 \leqslant i \leqslant j \leqslant n-1$, означающим, что $U \subseteq W$.

Теорема о ранге матрицы

Пусть $A = (a_{ij}) \in \mathrm{M}_{m,n}(K)$ — прямоугольная $(m \times n)$-матрица с элементами a_{ij} из поля K. Определитель $M_{i_1,\ldots,i_k;j_1,\ldots,j_k}$ квадратной $(k \times k)$-матрицы, состоящей из элементов на пересечении k строк с номерами $i_1, \ldots, i_k$ и k столбцов с номерами $j_1, \ldots, j_k$, называется *минором k-го порядка* матрицы A. Наивысший порядок *ненулевого* минора матрицы A обозначим через $\mathrm{r}(A)$.

r(A)

9-9

Теорема 9.58 (о ранге матрицы). *Следующие четыре числовые характеристики матрицы* $A = (a_{ij}) \in \mathrm{M}_{m,n}(K)$ *совпадают:*

1) $\mathrm{r}(A_1, \ldots, A_m)$ *(ранг системы строк, в* K^n*);*

2) $\mathrm{r}(\widehat{A}_1, \ldots, \widehat{A}_n)$ *(ранг системы столбцов, в* $\widehat{K}^n$*);*

3) $\mathrm{r}(A)$ *(наивысший порядок ненулевого минора);*

4) *число ненулевых строк* r *в ступенчатом виде* $\overline{A}$ *матрицы* A.

(Это совпадающее число называется рангом матрицы A *и будет обозначаться через* $\mathrm{r}(A)$*).*

Доказательство разобьём на четыре леммы.

Лемма 9.59. *Пусть матрица* $\widetilde{A}$ *получена из матрицы* A *элементарным преобразованием строк (столбцов) 1-го или 2-го типа, тогда* $\mathrm{r}(A) = \mathrm{r}(\widetilde{A})$. *Если* $\overline{A}$ *— ступенчатая форма, к которой приводится матрица* A, *то* $\mathrm{r}(A) = \mathrm{r}(\overline{A})$.

Доказательство проведём для преобразований строк (для столбцов всё аналогично).

Случай 1. $A'_i = A_i + cA_j$, $c \in K$, $i \neq j$. Для $k > \mathrm{r}(A)$ рассмотрим минор $M = \widetilde{M}_{i_1,\ldots,i_k;j_1,\ldots,j_k}$ в $\widetilde{A}$.

а) Если $i \notin \{i_1, \ldots, i_k\}$, то $\widetilde{M} = M_{i_1,\ldots,i_k;j_1,\ldots,j_k} = 0$.

б) Если $i, j \in \{i_1, \ldots, i_k\}$, то $\widetilde{M} = M_{i_1,\ldots,i_k;j_1,\ldots,j_k} = 0$.

в) Если $i \in \{i_1, \ldots, i_k\} \not\ni j$, то разложим определитель $\widetilde{M}$ по i-й строке $A'_i = A_i + cA_j$ в сумму двух определителей: $\widetilde{M} = M + c\tilde{\Delta} = 0$, так как $M = M_{i_1,\ldots,i_k;j_1,\ldots,j_k} = 0$, поскольку $k > \mathrm{r}(A)$, определитель $\tilde{\Delta}$ в качестве i-й строчки имеет часть строки A_j, но $j \notin \{i_1, \ldots, i_k\}$, и поэтому $\tilde{\Delta}$ отличается от минора матрицы порядка k перестановкой двух строк, и поэтому $\tilde{\Delta} = 0$. Итак, $\mathrm{r}(\widetilde{A}) \leqslant \mathrm{r}(A)$. Поскольку от A к $\widetilde{A}$ можно вернуться элементарным преобразованием строк, то $\mathrm{r}(A) \leqslant \mathrm{r}(\tilde{A})$.

Случай 2. $A_i \leftrightarrow A_j$ разбирается аналогично ($i, j \in \{i_1, \ldots, i_k\}$; $i, j \notin \{i_1, \ldots, i_k\}$; $i \in \{i_1, \ldots, i_k\} \not\ni j$). □

Лемма 9.60 (о сохранении линейных соотношений между столбцами при элементарных преобразованиях строк). *Пусть от матрицы* A *к матрице* A' *мы перешли элементарными преобразова-*

9-10

ниями строк, тогда столбцы матриц A и A' имеют одни и те же линейные соотношения, а именно, $k_1\widehat{A}_1 + \ldots + k_n\widehat{A}_n = 0$ тогда и только тогда, когда $k_1\widehat{A}'_1 + \ldots + k_n\widehat{A}'_n = 0$.

Доказательство. Ясно, что элементарные преобразования 1-го и 2-го типа для строк сохраняют линейное соотношение для столбцов и эти преобразования обратимы. □

Следствие 9.61. *Система столбцов $\widehat{A}_{j_1}, \ldots, \widehat{A}_{j_r}$ матрицы A линейно зависима (соответственно, линейно независима или является максимальной линейно независимой подсистемой в $\widehat{A}_1, \ldots, \widehat{A}_n \in \widehat{K}^m$) тогда и только тогда, когда соответствующая система столбцов (с теми же номерами) $\widehat{A}'_{j_1}, \ldots, \widehat{A}'_{j_r}$ матрицы A' линейно зависима (соответственно линейно независима или является максимальной линейно независимой подсистемой в $\widehat{A}'_1, \ldots, \widehat{A}'_n \in \widehat{K}^m$).*

Следствие 9.62. $\mathrm{r}\{\hat{A}_1, \ldots, \hat{A}_n\} = \mathrm{r}\{\hat{A}'_1, \ldots, \hat{A}'_n\}$.

Лемма 9.63. *Если $\overleftarrow{A}$ — ступенчатая матрица, то наивысший порядок ненулевого минора $\mathrm{r}(\overleftarrow{A})$ совпадает с числом r ненулевых строк.*

Доказательство.

1) Минор r-го порядка на пересечении r ненулевых строк и столбцов, проходящих через уголки ступенек, является определителем треугольной матрицы с ненулевыми элементами на главной диагонали, и поэтому отличен от нуля.

2) Все миноры, порядок которых больше r, нулевые, так как имеют нулевую строку. □

Лемма 9.64. *В ступенчатой матрице $\overleftarrow{A}$ ранг системы столбцов совпадает с числом r ненулевых строк (а именно, столбцы, проходящие через уголки ступенек, образуют максимальную линейно независимую подсистему столбцов).*

Доказательство.

1) Указанные столбцы линейно независимы, так как проходят через $(r \times r)$-матрицу с ненулевым определителем.

2) Любой столбец ступенчатой матрицы является линейной комбинацией указанных. □

9-11

Следствие 9.65 (алгоритм нахождения максимальной линейно независимой подсистемы в системе столбцов прямоугольной матрицы). *От матрицы A перейдём к ступенчатой матрице $\bar{A}$ с помощью элементарных преобразований строк 1-го и 2-го типов, запомним номера столбцов $j_1, \ldots, j_r$, проходящих через уголки ступенек в $\bar{A}$, в матрице A возьмём столбцы с этими номерами $\widehat{A}_{j_1}, \ldots, \widehat{A}_{j_r}$.*

КВ

Пример 9.66. Найти какую-либо максимальную линейно независимую подсистему строк в системе $a_1, a_2, a_3, a_4 \in \mathbb{R}^4$,

$$a_1 = (-1, 4, -3, -2), \quad a_2 = (3, -7, 5, 3),$$
$$a_3 = (3, -2, 1, 0), \quad a_4 = (-4, 1, 0, 1),$$

а остальные строки выразить как линейные комбинации строк этой подсистемы.

Решение. Записываем строки a_1, a_2, a_3, a_4 как столбцы и приводим полученную матрицу к ~~главному~~ ступенчатому виду с помощью элементарных преобразований строк:

$$\begin{array}{c} \begin{pmatrix} -1 & 3 & 3 & -4 \\ 4 & -7 & -2 & 1 \\ -3 & 5 & 1 & 0 \\ -2 & 3 & 0 & 1 \end{pmatrix} \\ a_1 \quad a_2 \quad a_3 \quad a_4 \end{array} \to \begin{pmatrix} -1 & 3 & 3 & -4 \\ 0 & 5 & 10 & -15 \\ 0 & -4 & -8 & 12 \\ 0 & -3 & -6 & 9 \end{pmatrix} \to$$

$$\to \begin{pmatrix} -1 & 3 & 3 & -4 \\ 0 & 1 & 2 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \left(\begin{pmatrix} 1 & 0 & 3 & -5 \\ 0 & 1 & 2 & -3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right).$$

Записываем номера столбцов в ступенчатом виде, проходящие через уголки ступенек: 1, 2. Поэтому $\{a_1, a_2\}$ — максимальная линейно независимая подсистема, $a_3 = 3a_1 + 2a_2$, $a_4 = -5a_1 - 3a_2$; ранг системы строк a_1, a_2, a_3, a_4 равен 2.

Завершение доказательства теоремы о ранге:

$$\mathrm{r}(\widehat{A}_1, \ldots, \widehat{A}_n) \overset{\text{лемма 9.60}}{=} \mathrm{r}(\widehat{\bar{A}}_1, \ldots, \widehat{\bar{A}}_n) \text{ (ранг столбцов ступенчатой матрицы } \bar{A}) \overset{\text{лемма 9.64}}{=} r \overset{\text{лемма 9.63}}{=}$$
$$= \mathrm{r}(\bar{A}) \overset{\text{лемма 9.59}}{=} \mathrm{r}(A) = \mathrm{r}(A^*) \overset{\cancel{\text{лемма 9.60}}}{=} \mathrm{r}(A_1, \ldots, A_m). \quad \square$$

(столбцы в A^*)

9-12

$c_{ij} = a_{i1}b_{1j} + \dots$

$C_i = a_{i1}B_1 + \dots$

$\widehat{C}_j = \widehat{A}_1 b_{1j} + \dots$

равенства одно под другим

Теорема 9.67. *Пусть* $A = (a_{ij}) \in \mathrm{M}_{m,n}(K)$, $B = (b_{ij}) \in \mathrm{M}_{n,r}(K)$. *Тогда*

$$\mathrm{r}(AB) \leqslant \mathrm{r}(A), \quad \mathrm{r}(AB) \leqslant \mathrm{r}(B).$$

Доказательство. Пусть $C = (c_{ij}) = AB$. Тогда $c_{ij} = a_{i1}b_{1j} + \ldots + a_{in}b_{nj}$, ~~и поэтому~~

$c_{ij} = a_{i1}b_{1j} + \dots + a_{in}b_{nj}$,

$$C_i = a_{i1}B_1 + \ldots + a_{in}B_n,$$
$$\widehat{C}_j = \widehat{A}_1 b_{1j} + \ldots + \widehat{A}_n b_{nj},$$

т. е. строки матрицы C линейно выражаются через строки матрицы B, столбцы матрицы C линейно выражаются через столбцы матрицы A. Поэтому $\mathrm{r}(C) \leqslant \mathrm{r}(B)$ и $\mathrm{r}(C) \leqslant \mathrm{r}(A)$. □

Следствие 9.68. *При умножении на квадратную матрицу* A *с* $|A| \neq 0$ *ранг не меняется.*

Доказательство. Так как $|A| \neq 0$, то существует обратная матрица A^{-1}. Поэтому

$$(BA)A^{-1} = B = A^{-1}(AB),$$

и следовательно,

$$\mathrm{r}(B) \leqslant \mathrm{r}(BA), \quad \mathrm{r}(B) \leqslant \mathrm{r}(AB).$$

Ранее мы доказали, что

$$\mathrm{r}(B) \geqslant \mathrm{r}(BA), \quad \mathrm{r}(B) \geqslant \mathrm{r}(AB).$$

Поэтому

$$\mathrm{r}(B) = \mathrm{r}(BA), \quad \mathrm{r}(B) = \mathrm{r}(AB). \quad \square$$

Задачи 9.69.

1) В условиях теоремы:

$$\mathrm{r}(A) + \mathrm{r}(B) - n \leqslant \mathrm{r}(AB).$$

2) Если $A, B, C \in \mathrm{M}_n(K)$ и $ABC = 0$, то

$$\mathrm{r}(A) + \mathrm{r}(B) + \mathrm{r}(C) \leqslant 2n.$$

(9-13)

3) Пусть $A \in \mathrm{M}_{m,n}(K)$, $B \in \mathrm{M}_{n,m}(K)$ и $m > n$. Покажите, что $\det(AB) = 0$.

Доказательство. Так как $AB \in \mathrm{M}_m(K)$, то $\mathrm{r}(AB) \leqslant \mathrm{r}(B) \leqslant \leqslant n < m$. □

4) Если $A^2 = A \in \mathrm{M}_n(K)$, то

$$\mathrm{r}(A) + \mathrm{r}(E - A) = n.$$

5) Если $A, B \in \mathrm{M}_n(K)$ и $A^2 = A$, $AB = 0 = BA$, то

$$\mathrm{r}(A + B) = \mathrm{r}(A) + \mathrm{r}(B).$$

6) Если $A, B \in \mathrm{M}_n(K)$, $AB = BA$, $\mathrm{r}(A^2) = \mathrm{r}(A)$ и $\mathrm{r}(B^2) = \mathrm{r}(B)$, то

$$\mathrm{r}((AB)^2) = \mathrm{r}(AB).$$

7) Если $A_1, \ldots, A_k \in \mathrm{M}_n(K)$, $k \geqslant 2$, то

$$\mathrm{r}(A_1 \ldots A_k) \geqslant \mathrm{r}(A_1) + \ldots + \mathrm{r}(A_k) - n(k-1).$$

КВ*

Упр.

Теорема 9.70 (о факториальном ранге). *Пусть $m, n \in \mathbb{N}$, $A \in \mathrm{M}_{m,n}(K)$. Ранг матрицы $\mathrm{r}(A)$ равен наименьшему числу k такому, что*

$$A = B \cdot C, \quad \text{где} \quad B \in \mathrm{M}_{m,k}(K), \quad C \in \mathrm{M}_{k,n}(K)$$

(это число k называется факториальным рангом матрицы A).

Доказательство. Допустим, что $A = B \cdot C$, где $B \in \mathrm{M}_{m,n}(K)$, $C \in \mathrm{M}_{k,n}(K)$. Тогда система столбцов матрицы A линейно выражается через систему столбцов матрицы B (их k штук). Поэтому $\mathrm{r}(A) \leqslant k$. Т-ма 9.67

Пусть $k = \mathrm{r}(A)$. Выберем строки $A_{i_1}, \ldots, A_{i_k}$, образующие максимальную линейно независимую подсистему строк $A_1, \ldots, A_m$ матрицы A,

$$A_i = \beta_{i1} A_{i_1} + \ldots + \beta_{ik} A_{i_k}, \quad \beta_{ij} \in K, \quad 1 \leqslant i \leqslant m.$$

Рассмотрим матрицы $B \in \mathrm{M}_{m,k}(K)$, $B = (\beta_{ij})$, и $C \in \mathrm{M}_{k,n}(K)$, для которой j-я строка $C_j = A_{i_j}$, $j = 1, \ldots, k$. Тогда $A = B \cdot C$. □

9-14

Теорема 9.71 (теорема Кронекера—Капелли: критерий совместности и определённости системы линейных уравнений в терминах рангов матриц). *Пусть* $(a_{ij} \mid b_i)$ *— система* m *линейных уравнений с* n *неизвестными,* $A = (a_{ij}) \in \mathrm{M}_{m,n}(K)$ *— матрица коэффициентов,*

$$A' = \left(A \left| \begin{matrix} b_1 \\ \vdots \\ b_m \end{matrix} \right. \right) \in \mathrm{M}_{m,n+1}(K) -$$

расширенная матрица системы линейных уравнений.

а) *Система линейных уравнений совместна тогда и только тогда, когда ранг матрицы коэффициентов* A *равен рангу расширенной матрицы* $A' = (A, \hat{b})$, т.е. $r(A) = r(A')$.

б) *Система линейных уравнений определённая тогда и только тогда, когда* $\mathrm{r}(A) = \mathrm{r}(A') = n$.

Доказательство.

1) Используя определение ранга матрицы с помощью столбцов, видим, что всегда $\mathrm{r}(A) \leqslant \mathrm{r}(A')$.

2) Если $(k_1, \ldots, k_n)$ — решение, то

$$k_1\hat{A}_1 + \ldots + k_n\hat{A}_n = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

т. е. столбцы матрицы A' линейно выражаются через столбцы матрицы A, следовательно, $\mathrm{r}(A') \leqslant \mathrm{r}(A)$, и поэтому $\mathrm{r}(A') = \mathrm{r}(A)$.

3) Пусть $\mathrm{r}(A') = \mathrm{r}(A) = r$. Тогда максимальная линейно независимая система столбцов матрицы A содержит r столбцов, и поэтому она является и максимальной линейно независимой системой столбцов матрицы A'. Таким образом, столбец

$$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

9-15

линейно выражается через эту систему столбцов матрицы A, а поэтому и через *все* столбцы матрицы A,

$$k_1\hat{A}_1 + \ldots + k_n\hat{A}_n = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

Итак, существует решение $(k_1, \ldots, k_n)$ системы линейных уравнений. □

4) *Второе доказательство.* Элементарными преобразованиями приведём систему линейных уравнений к ступенчатому виду (ранги матриц не меняются при этом). Совпадение рангов означает отсутствие «экзотических» уравнений в ступенчатом виде, т. е. совместность системы линейных уравнений. □

5) *Доказательство критерия определённости (в терминах рангов).* Если система ~~определена~~ совместна, т. е. $\mathrm{r}(A) = \mathrm{r}(A')$, то она определена тогда и только тогда, когда в ступенчатом виде нет свободных неизвестных, т. е. $\mathrm{r}(A) = \mathrm{r}(A') = n$. □

4)

Размерность пространства решений однородной системы линейных уравнений

Как мы отметили ранее, совокупность решений $X_{\text{одн}}$ однородной системы линейных уравнений с матрицей $A = (a_{ij}) \in \mathrm{M}_{m,n}(K)$ является линейным пространством, подпространством в K^n.

Теорема 9.72. *Если $r = \mathrm{r}(A) < n$, то $\dim X_{\text{одн}} = n - r$ (т. е. размерность пространства решений равна числу свободных неизвестных). (Если $\mathrm{r}(A) = n$, то система линейных уравнений имеет лишь нулевое решение.)*

Доказательство. Для удобства записи переупорядочим неизвестные, если это необходимо, так, чтобы

$$\underbrace{x_1, \ldots, x_r}_{r \text{ главных неизвестных}} \text{ и } \underbrace{x_{r+1}, \ldots, x_n}_{n-r \text{ свободных неизвестных}}.$$

Пусть $E = E_{n-r} \in \mathrm{M}_{n-r}(K)$ — единичная матрица размера $(n-r) \times (n-r)$. Возьмём её строки в качестве наборов значений

9-16

для свободных неизвестных и дополним их (единственно возможным способом) до решений нашей системы линейных уравнений

$$\begin{aligned} \alpha_1 &= (c_{11}, \ldots, c_{1r}, 1, 0, \ldots, 0), \\ &\vdots \\ \alpha_{n-r} &= (c_{(n-r)1}, \ldots, c_{(n-r)r}, 0, 0, \ldots, 1). \end{aligned}$$

n-r

Эта система $n - r$ строк-решений линейно независима (поскольку строки единичной матрицы, конечно, линейно независимы). Если

$$\beta = (\beta_1, \ldots, \beta_{n-r}, \beta_{n-r+1}, \ldots, \beta_n) \in X_{\text{одн}} -$$

произвольное решение, то

$$\gamma = \beta - \beta_{n-r+1}\alpha_1 - \ldots - \beta_n\alpha_{n-r} = (\gamma_1, \ldots, \gamma_{n-r}, 0, \ldots, 0) \in X_{\text{одн}}.$$

Однако, конечно,

$$(0, \ldots, 0, 0, \ldots, 0) \in X_{\text{одн}},$$

при этом γ и нулевое решение имеют одинаковый набор значений для свободных неизвестных. Так как значения главных неизвестных однозначно определяются по свободным, то $\gamma = 0$, следовательно,

$$\beta = \beta_{n-r+1}\alpha_1 + \ldots + \beta_n\alpha_{n-r}.$$

Итак, мы построили базис $\{\alpha_1, \ldots, \alpha_{n-r}\}$ линейного пространства решений $X_{\text{одн}}$, поэтому $\dim X_{\text{одн}} = n - r$. ∎

Замечание 9.73. Если вместо строк единичной матрицы E_{n-r} для свободных неизвестных брать строки всевозможных матриц $C \in \mathrm{GL}_{n-r}(K)$ (т. е. $C \in \mathrm{M}_n(K)$, $|C| \neq 0$), то этот алгоритм позволяет построить все базисы в $X_{\text{одн}}$.

Замечание 9.74. Любой базис линейного пространства решений $X_{\text{одн}}$ однородной системы линейных уравнений называется в ряде алгебраических текстов «фундаментальной системой решений однородной системы линейных уравнений».

Конец лекции №9

10-07 Лекция N 10 (14 октября 2011г.)

Задание любого подпространства в ${}_KV = K^n$ как пространства решений однородной системы линейных уравнений

Пусть K — поле, $u_1, \ldots, u_m \in {}_KV = K^n$, $U = \langle u_1, \ldots, u_m \rangle$ — подпространство в K^n, являющееся линейной оболочкой строк $u_1, \ldots, u_m$, т. е. множеством всех линейных комбинаций строк $u_1, \ldots, u_m$. Мы найдём такую матрицу $A \in \mathrm{M}_{s,n}(K)$, что множество решений однородной системы линейных уравнений

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

совпадает с U.

Если U — нулевое подпространство, то в качестве A мы можем взять любую матрицу $n \times n$ с ненулевым определителем (например, $A = E$). Если $U = K^n$ (это эквивалентно тому, что $\dim U = n$), то в качестве A мы можем взять нулевую матрицу из $\mathrm{M}_{s,n}$, $s \geqslant 1$. Если же $1 \leqslant \dim U = \mathrm{r}(u_1, \ldots, u_m) < n$, то пусть $u_i = (u_{i1}, u_{i2}, \ldots, u_{in})$, $1 \leqslant i \leqslant m$, $u_{ij} \in K$. $U = \langle u_1, \ldots, u_m \rangle$

Рассмотрим матрицу $B \in \mathrm{M}_{m,n}(K)$, $B = (b_{ij})$, $b_{ij} = u_{ij}$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, и однородную систему линейных уравнений

$$B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \left.\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\right\} m. \qquad (9)$$

Ясно, что $r = \mathrm{r}(B) = \dim U$, поэтому $1 \leqslant r < n$. Размерность s пространства решений этой системы равна $n - r$, и так как $1 \leqslant r < n$, то $1 \leqslant s < n$. $X_{одн}$

Пусть строки $v_1, \ldots, v_s \in K^n$ образуют фундаментальную систему решений системы (9), $v_i = (v_{i1}, \ldots, v_{in})$, $1 \leqslant i \leqslant s$, $v_{ij} \in K$. Пусть $A \in \mathrm{M}_{s,n}(K)$, $A = (a_{ij})$, $a_{ij} = v_{ij}$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant n$. Покажем, что A — искомая матрица.

Действительно, по построению матрицы A любая строка из U (как линейная комбинация строк $u_1, \ldots, u_m$) является решением од-

нородной системы уравнений

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{10}$$

т. е. $U \subseteq X_{\text{одн}}$. С другой стороны,

$$\dim X_{\text{одн}} = n - \mathrm{r}(A) = n - s = n - (n - r) = r = \dim U.$$

Следовательно, $U = X_{\text{одн}}$. □

В заключение отметим, что матрица A определена неоднозначно. Например, другая матрица A' может быть получена с помощью другой фундаментальной системы решений системы (9).

Полученное задание линейных подпространств оказывается полезным при решении ряда практических задач. Например, пусть $u_1, \ldots, u_m \in \mathbb{R}^n$ — линейно независимые строки, $m < n$. Требуется найти такие строки $u_{m+1}, \ldots, u_n$, что $\{u_1, \ldots, u_n\}$ — базис линейного пространства $\mathbb{R}^n$. Как и выше, пусть $v_1, \ldots, v_s$ — какая-нибудь фундаментальная система решений системы (9) (в нашем случае $\mathrm{r}(B) = m$, $s = n - m$). Положим $u_{m+1} = v_1, \ldots, u_n = v_{n-m}$. Покажем, что $\{u_1, \ldots, u_n\}$ — базис в $\mathbb{R}^n$. Достаточно показать, что строки $u_1, \ldots, u_n$ линейно независимы над $\mathbb{R}$. Пусть $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ и $\alpha_1 u_1 + \ldots + \alpha_n u_n = 0 \in \mathbb{R}^n$. Тогда для строки

$$z = \alpha_1 u_1 + \ldots + \alpha_m u_m = -\alpha_{m+1} u_{m+1} - \ldots - \alpha_n u_n$$

имеем $z \in U \cap V$, где $V = \langle u_{m+1}, \ldots, u_n \rangle$. Если $z = (z_1, \ldots, z_n)$, $z_i \in \mathbb{R}$, $1 \leqslant i \leqslant n$, то по построению подпространств U и V (см. (9), (10)) имеем

$$(z_1, \ldots, z_n)\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = 0,$$

$z_1^2 + \ldots + z_n^2 = 0$, следовательно, $z_1 = \ldots = z_n = 0$, и $z = 0 \in \mathbb{R}^n$. Значит,

$$\alpha_1 u_1 + \ldots + \alpha_m u_m = 0 (\in \mathbb{R}^n) = \alpha_{m+1} u_{m+1} + \ldots + \alpha_n u_n.$$

Но $u_1, \ldots, u_m$ — линейно независимые строки, поэтому $\alpha_1 = \ldots = \alpha_m = 0$. Строки $u_{m+1}, \ldots, u_n$ также линейно независимы, следовательно, $\alpha_{m+1} = \ldots = \alpha_n = 0$. Итак, $\alpha_1 = \ldots = \alpha_n = 0$, и строки $u_1, \ldots, u_n$ линейно независимы.

Таким образом, мы рассмотрели два способа задания линейных подпространств в ${}_KV = K^n$:

1) как множество решений $X_{\text{одн}}$ однородной системы линейных уравнений;

2) как линейную оболочку $\langle u_1, \ldots, u_m \rangle$ строк $u_1, \ldots, u_m \in {}_KV = K^n$.

При этом мы научились переходить от первого задания ко второму (фундаментальная система решений) и от второго задания к первому. Первый способ задания удобен для задания пересечения $U \cap W$ подпространств (надо к первой однородной системе уравнений приписать вторую). Второй способ задания удобен для задания суммы подпространств:

$$\langle u_1, \ldots, u_m \rangle + \langle w_1, \ldots, w_t \rangle = \langle u_1, \ldots, u_m, w_1, \ldots, w_t \rangle.$$

В следующем примере мы увидим комбинацию этих приёмов.

Пример 9.75. Пусть $V_1 = \langle u_1, u_2, u_3 \rangle \subseteq \mathbb{R}^4$ (линейная оболочка строк $u_1 = (1,1,0,0)$, $u_2 = (0,1,1,0)$, $u_3 = (0,0,1,1)$), $V_2 = \langle v_1, v_2, v_3 \rangle \subseteq \mathbb{R}^4$ (линейная оболочка строк $v_1 = (1,0,1,0)$, $v_2 = (0,2,1,1)$, $v_3 = (1,2,1,2)$). Необходимо найти базисы линейных пространств $V_1 + V_2$ и $V_1 \cap V_2$, при этом строки u_1, u_2, u_3, v_1, v_2, v_3 выразить через базис пространства $V_1 + V_2$.

Решение. Запишем строки u_1, u_2, u_3, v_1, v_2, v_3 по столбцам и приведём полученную матрицу к ступенчатому виду с помощью элементарных преобразований строк:

$$\begin{array}{c} \begin{array}{cccccc} u_1 & u_2 & u_3 & v_1 & v_2 & v_3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 2 & 2 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{pmatrix} \end{array} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{pmatrix} \to$$

10-04

$$\to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 2 & 1 \\ 0 & 0 & 1 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{pmatrix} \to \begin{array}{c} \begin{matrix} u_1' & u_2' & u_3' & v_1' & v_2' & v_3' \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 2 & 1 \\ 0 & 0 & 1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & -1 \end{pmatrix} \end{array}.$$

Поскольку $V_1 + V_2 = \langle u_1, u_2, u_3, v_1, v_2, v_3 \rangle$ и элементарные преобразования строк матрицы не меняют линейных соотношений между столбцами, то $\{u_1, u_2, u_3, v_1\}$ — базис в $V_1 + V_2$ (и так как $\dim(V_1 + V_2) = 4$, то $V_1 + V_2 = \mathbb{R}^4$). Из ступенчатого вида мы вычисляем v_2' и v_3' через u_1', u_2', u_3', v_1':

$$v_2' + v_1' = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = u_1' + u_2' + u_3'.$$

Поэтому $v_2' = u_1' + u_2' + u_3' - v_1'$ и, следовательно, $v_2 = u_1 + u_2 + u_3 - v_1$. Для v_3' мы видим, что $v_3' + v_1' = (2, 0, 2, 0)^* = 2u_1' + 2u_3'$, поэтому $v_3 = 2u_1 + 2u_3 - v_1$. Проведённые вычисления равносильны завершению приведения матрицы к главному ступенчатому виду:

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

Рассмотрим теперь $V_1 \cap V_2$. Для этого найдём однородные системы линейных уравнений, чьи множества решений совпадают с V_1 и V_2 соответственно.

Для V_1:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

система уже имеет ступенчатый вид, x_1, x_2, x_3 — главные неизвестные, x_4 — свободная. Фундаментальная система решений состоит из одной строки $(-1, 1, -1, 1)$. Итак, подпространство V_1 совпадает

с пространством решений однородной системы линейных уравнений

$$(-1,1,-1,1)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=0. \tag{11}$$

Для V_2:

$$\begin{pmatrix}1&0&1&0\\0&2&1&1\\1&2&1&2\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\to\begin{pmatrix}1&0&1&0\\0&2&1&1\\0&2&0&2\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\to$$

$$\to\begin{pmatrix}1&0&1&0\\0&2&1&1\\0&1&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\to\begin{pmatrix}1&0&1&0\\0&1&0&1\\0&2&1&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}\to$$

$$\to\begin{pmatrix}1&0&1&0\\0&1&0&1\\0&0&1&-1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix},$$

и мы приходим к ступенчатому виду, при этом x_1, x_2, x_3 — главные неизвестные, а x_4 — свободная. Фундаментальная система решений состоит из одной строки $(-1,-1,1,1)$. Значит, однородная система линейных уравнений

$$(-1,-1,1,1)\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=0 \tag{12}$$

задаёт подпространство V_2.

Ясно, что система

$$\begin{pmatrix}-1&1&-1&1\\-1&-1&1&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$

10-06

задаёт подпространство $V_1 \cap V_2$. Решим эту систему:

$$\begin{pmatrix} -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & -1 & 1 & -1 \\ 0 & -2 & 2 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

x_1, x_2 — главные неизвестные, x_3, x_4 — свободные неизвестные. Фундаментальная система решений состоит из двух строк

$$u = (0, 1, 1, 0),$$
$$v = (1, 0, 0, 1).$$

Следовательно, $\{u, v\}$ — базис линейного подпространства $V_1 \cap V_2$.

Проверить КВ

Собственные числа и собственные векторы матрицы

Пусть K — поле, $A \in \mathrm{M}_n(K)$, $0 \neq \hat{X} \in \hat{K}^n = \mathrm{M}_{n,1}(K)$, $\lambda \in K$. Если $A \cdot \hat{X} = \lambda \cdot \hat{X}$, то λ называется *собственным числом* матрицы A, а $\hat{X}$ — *собственным вектором* матрицы A, отвечающим собственному числу λ.

Условие $A \cdot \hat{X} = \lambda \cdot \hat{X}$ эквивалентно условию

$$(A - \lambda E)\hat{X} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \hat{K}^n,$$

где $E \in \mathrm{M}_n(K)$ — единичная матрица. При фиксированном λ это условие превращается в однородную систему линейных уравнений

10-07

относительно неизвестных $x_1, \ldots, x_n$,

$$\hat{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Матрица $A - \lambda E$ этой системы — квадратная матрица размера n. Поэтому наличие ненулевого решения этой системы равносильно тому, что $|A - \lambda E| = 0$. Пусть t — переменная,

$$P(t) = |A - tE| = p_n t^n + p_{n-1} t^{n-1} + \ldots + p_0 \in K[t] -$$

многочлен степени n от переменной t (называемый характеристическим многочленом матрицы A), при этом:

$$p_n = (-1)^n,$$

$$p_{n-1} = (-1)^{n-1} \sum_{i=1}^{n} a_{ii} = (-1)^{n-1} \operatorname{Tr} A, \quad p_0 = |A|.$$

Мы показали, что собственные числа и только они являются корнями характеристического многочлена из поля K.

Если $\lambda \in K$ и $P(\lambda) = 0$, то все собственные векторы матрицы A относительно собственного числа λ — это все ненулевые решения системы

$$(A - \lambda E)\hat{X} = (0) \in \hat{K}^n.$$

Отметим, что множество всех собственных векторов матрицы A относительно собственного числа λ не образует линейного подпространства в $\hat{K}^n$, так как все эти векторы ненулевые. Но если к этому множеству добавить нулевой вектор, то получится линейное подпространство всех решений системы

$$(A - \lambda E)\hat{X} = (0).$$

Таким образом, если $P(\lambda) = |A - \lambda E| = 0$, $r = \mathrm{r}(A - \lambda E)$, ~~то~~ $0 \leqslant r < n$, то размерность пространства решений этой системы равна $s = n - r$, поэтому $1 \leqslant s \leqslant n$. Если $\{X_1, \ldots, X_s\}$ — какая-либо фундаментальная система решений системы $(A - \lambda E)\hat{X} = (0)$, то все собственные векторы матрицы A, отвечающие собственному числу λ, — это все нетривиальные линейные комбинации элементов $\hat{X}_1, \ldots, \hat{X}_s$ с коэффициентами из поля K.

10-08

Пример 9.76.

$$A = \begin{pmatrix} 10 & 3 \\ -5 & 2 \end{pmatrix}, \quad K = \mathbb{R},$$

$$|A - \lambda E| = \begin{vmatrix} 10-\lambda & 3 \\ -5 & 2-\lambda \end{vmatrix} = \lambda^2 - 12\lambda + 35.$$

Корни: $\lambda_1 = 7$, $\lambda_2 = 5$, $\lambda_1, \lambda_2 \in \mathbb{R}$ (собственные числа матрицы A).

Собственные векторы для $\lambda_1 = 7$:

$$A - 7E = \begin{pmatrix} 3 & 3 \\ -5 & -5 \end{pmatrix}, \quad \begin{pmatrix} 3 & 3 \\ -5 & -5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

ненулевые решения:

$$\left\{ \begin{pmatrix} s \\ -s \end{pmatrix} \middle| \, s \in \mathbb{R}, \ s \neq 0 \right\}.$$

Собственные векторы для $\lambda_2 = 5$:

$$A - 5E = \begin{pmatrix} 5 & 3 \\ -5 & -3 \end{pmatrix}, \quad \begin{pmatrix} 5 & 3 \\ -5 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

ненулевые решения:

$$\left\{ \begin{pmatrix} -3t \\ 5t \end{pmatrix} \middle| \, t \in \mathbb{R}, \ t \neq 0 \right\}.$$

Пример 9.77.

$$K = \mathbb{C}, \quad A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

$$P(\lambda) = |A - \lambda E| = \begin{vmatrix} -\lambda & 1 & 0 \\ 0 & -\lambda & 2 \\ 0 & 0 & -\lambda \end{vmatrix} = -\lambda^3.$$

Имеется лишь одно собственное число: $\lambda = 0$. Собственные векторы относительно $\lambda = 0$ задаются системой линейных уравнений

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

10-09

Система уже имеет ступенчатый вид, x_2, x_3 — главные неизвестные, x_1 — свободная переменная, множество собственных векторов относительно $\lambda = 0$:

$$\left\{ \begin{pmatrix} s \\ 0 \\ 0 \end{pmatrix} \middle| \, s \in \mathbb{C}, \ s \neq 0 \right\}.$$

Пример 9.78. Если

$$A = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix} -$$

диагональная матрица, то $\alpha_1, \ldots, \alpha_n$ — все корни характеристического многочлена матрицы A (и следовательно, собственные числа).

Пример 9.79.

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

$$P(\lambda) = |A - \lambda E| = \begin{vmatrix} -\lambda & 1 \\ -1 & -\lambda \end{vmatrix} = \lambda^2 + 1.$$

а) $K = \mathbb{R}$: нет действительных корней многочлена $P(\lambda) = \lambda^2 + 1$, поэтому для матрицы A нет действительных собственных чисел (и собственных векторов).

б) $K = \mathbb{C}$: многочлен $P(\lambda)$ имеет корни $\lambda_1 = i \in \mathbb{C}$, $\lambda_2 = -i \in \mathbb{C}$ (собственные числа матрицы A).

Собственные векторы для $\lambda = i$:

$$\begin{pmatrix} -i & 1 \\ -1 & -i \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

ненулевые решения:

$$\left\{ c \cdot \begin{pmatrix} -i \\ 1 \end{pmatrix} \middle| \, c \in \mathbb{C}, \ c \neq 0 \right\}.$$

Собственные векторы для $\lambda = -i$:

$$\begin{pmatrix} i & 1 \\ -1 & i \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

10-10

ненулевые решения

$$\left\{ c \cdot \begin{pmatrix} i \\ 1 \end{pmatrix} \middle| \, c \in \mathbb{C},\ c \neq 0 \right\}.$$

Пример 9.80.

$$K = \mathbb{R}, \quad A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix},$$

$$P(\lambda) = |A - \lambda E| = -\lambda^3 + 12\lambda + 16.$$

Корни многочлена $P(\lambda)$: $\lambda_1 = -2$, $\lambda_2 = -2$, $\lambda_3 = 4$ (собственные числа).

Собственные векторы для $\lambda = -2$:

$$(A + 2E) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

ненулевые решения

$$\left\{ \begin{pmatrix} s - t \\ s \\ t \end{pmatrix} \middle| \, s, t \in \mathbb{R},\ s^2 + t^2 \neq 0 \right\}.$$

Собственные векторы для $\lambda = 4$:

$$(A - 4E) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

ненулевые решения

$$\left\{ \begin{pmatrix} s \\ s \\ 2s \end{pmatrix} \middle| \, s \in \mathbb{R},\ s \neq 0 \right\}.$$

Задача 9.81 (уравнение Сильвестера). Пусть $A \in \mathrm{M}_n(\mathbb{C})$, $B \in \mathrm{M}_m(\mathbb{C})$, $C \in \mathrm{M}_{n,m}(\mathbb{C})$ и матрицы A и B не имеют общих собственных чисел. Тогда матричное уравнение Сильвестера $AX - XB = C$ имеет единственное решение $X \in \mathrm{M}_{n,m}(\mathbb{C})$.

10-11

Задача 9.82. Пусть $A, B \in \mathrm{M}_n(\mathbb{C})$, $AB = BA$. Покажите, что для матриц A и B существует общий собственный вектор.

Трудная задача 9.83. Пусть $A, B \in \mathrm{M}_n(\mathbb{C})$ и $\mathrm{r}(AB - BA) = 1$. Тогда для матриц A и B существует общий собственный вектор.

Теорема 9.84. *Пусть $A \in \mathrm{M}_n(K)$, $0 \neq \hat{X}_1, \ldots, \hat{X}_l \in \hat{K}_n$, $\lambda_1, \ldots, \lambda_l \in K$, $\lambda_i \neq \lambda_j$ при $1 \leqslant i \neq j \leqslant l$, $A \cdot \hat{X}_i = \lambda_i \cdot \hat{X}_i$, $i = 1, \ldots, l$. Тогда столбцы $\hat{X}_1, \ldots, \hat{X}_l$ линейно независимы, т. е. собственные векторы, отвечающие различным собственным значениям, линейно независимы.*

Доказательство. Доказательство проведём индукцией по l. Основание индукции: $l = 1$, $A \cdot \hat{X}_1 = \lambda_1 \cdot \hat{X}_1$, $0 \neq \hat{X}_1$, $\{\hat{X}_1\}$ — линейно независимая система векторов.

Пусть теперь $l \geqslant 2$ и наше утверждение доказано для всех l', $1 \leqslant l' < l$. Допустим, что

$$\alpha_1 \hat{X}_1 + \ldots + \alpha_l \hat{X}_l = 0 \in \hat{K}^n, \quad \alpha_i \in K, \quad i = 1, \ldots, l. \tag{13}$$

Умножая слева на матрицу A обе части равенства, получаем, что

$$\alpha_1 \cdot A \cdot \hat{X}_1 + \ldots + \alpha_l \cdot A \cdot \hat{X}_l = A \cdot 0 = 0 \in \hat{K}^n,$$

и поэтому

$$\alpha_1 \lambda_1 \hat{X}_1 + \ldots + \alpha_l \lambda_l \hat{X}_l = 0. \tag{14}$$

Умножая (13) на λ_l, имеем

$$\alpha_1 \lambda_l \hat{X}_1 + \ldots + \alpha_l \lambda_l \hat{X}_l = 0. \tag{15}$$

Вычитаем (15) из (14):

$$\alpha_1 (\lambda_1 - \lambda_l) \hat{X}_1 + \ldots + \alpha_{l-1} (\lambda_{l-1} - \lambda_l) \hat{X}_{l-1} = 0 \in \hat{K}^n.$$

Применяя предположение индукции, получаем, что

$$\alpha_1 (\lambda_1 - \lambda_l) = \ldots = \alpha_{l-1} (\lambda_{l-1} - \lambda_l) = 0.$$

Поскольку $\lambda_1 \neq \lambda_l, \ldots, \lambda_{l-1} \neq \lambda_l$, отсюда следует, что $\alpha_1 = \ldots = \alpha_{l-1} = 0$. Следовательно, из (13) следует, что $\alpha_l \hat{X}_l = 0 \in \hat{K}^n$. Так как $\hat{X}_l \neq 0$, то $\alpha_l = 0$. Таким образом, $\alpha_1 = \ldots = \alpha_l = 0$, и поэтому собственные векторы $\hat{X}_1, \ldots, \hat{X}_l$ линейно независимы. □

Следствие. Если $A \in M_n(K)$, характеристический многочлен $p(t) = |A - tE|$ имеет n различных корней $\lambda_1, \ldots, \lambda_n$ в поле K, то матрица A подобна диагональной матрице: $C^{-1}AC = d(\lambda_1, \ldots, \lambda_n)$, где $C \in GL_n(K)$.

10-12

Теорема 9.85. *Матрица $A \in \mathrm{M}_n(\mathbb{C})$ нильпотентна (т. е. $A^m = 0 \in \mathrm{M}_n(K)$ для некоторого $m \in \mathbb{N}$) тогда и только тогда, когда собственные числа $\lambda_1, \ldots, \lambda_n$ равны нулю.*

Доказательство. а) Если $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$, то $|A - \lambda E| = (-1)^n \lambda^n$. По теореме Гамильтона—Кэли $A^n = (0) \in \mathrm{M}_n(\mathbb{C})$.

б) Если $A^m = (0) \in \mathrm{M}_n(\mathbb{C})$ и $A\hat{X} = \lambda\hat{X}$, где $\lambda \in \mathbb{C}$, $0 \neq \hat{X} \in \hat{\mathbb{C}}^n$, то $\hat{\mathbb{C}}^n \ni 0 = A^m\hat{X} = \lambda^n\hat{X}$, следовательно, $\lambda^n = 0$ и $\lambda = 0$. □

Замечание 9.86. Одним из фундаментальных результатов об алгебре матриц $\mathrm{M}_n(\mathbb{C})$ над полем комплексных чисел $\mathbb{C}$ (и о строении отдельно взятого линейного оператора конечномерного линейного пространства ${}_{\mathbb{C}}V$) является теорема о *жордановой нормальной форме*:

1) для каждой матрицы $A \in \mathrm{M}_n(\mathbb{C})$ найдётся такая обратимая матрица $C \in \mathrm{GL}_n(\mathbb{C})$, что

$$C^{-1}AC = J_A = \left(\begin{array}{c|c|c|c} J_1 & 0 & \ldots & 0 \\ \hline 0 & J_2 & \ldots & 0 \\ \hline & & \vdots & \\ \hline 0 & 0 & & J_k \end{array}\right) -$$

жорданова матрица (т. е. $J_1, \ldots, J_k$ — жордановы клетки);

2) нормальная жорданова форма J_A матрицы A определена однозначно (с точностью до порядка жордановых клеток).

см. упражнение 8.37

Эта теорема обычно является одним из центральных результатов курса линейной алгебры. Она также доказывается в более общем виде в разделе о строении конечнопорождённых модулей над кольцами главных идеалов.

Конечно, теорема Гамильтона—Кэли над полем $\mathbb{C}$ является следствием теоремы о жордановой нормальной форме. В то же время имеются элегантные доказательства теоремы о жордановой нормальной форме, использующие теорему Гамильтона—Кэли.

Мы оставляем этот сюжет для следующих частей наших «начал алгебры» (или его можно рассматривать как достаточно трудную задачу).

10-13

Определение 1.147. Пусть $f(x) \in K[x]$, $c \in K$, и c — корень многочлена $f(x)$, т. е. $f(c) = 0$. По теореме Безу многочлен $f(x)$ делится на $x - c$. Возможно, многочлен $f(x)$ делится на более высокие степени многочлена $x - c$. Пусть $k \in \mathbb{N}$ — такое натуральное число, что $f(x)$ делится на $(x - c)^k$, но не делится на $(x - c)^{k+1}$, поэтому

$$f(x) = (x - c)^k \varphi(x),$$

многочлен $\varphi(x) \in K[x]$ уже не делится на $x - c$ (это равносильно тому, что $\varphi(c) \neq 0$). В этом случае число k назовём *кратностью* корня c многочлена $f(x)$, а сам корень c — k-кратным корнем многочлена $f(x)$. Если $k = 1$, то корень c называется *простым корнем* многочлена $f(x)$.

Замечание 1.148. Понятие *абстрактного линейного пространства* мы детально рассмотрим в § 9, после того как изучим ряд конкретных линейных пространств.

Понятие *алгебры над полем* (как кольца, являющегося к тому же и линейным пространством) будет рассмотрено в § 8.

§ 2. Поле $\mathbb{C}$ комплексных чисел

Понятие числа является одним из основных понятий в математических теориях. К основным числовым системам принадлежат:

- натуральные числа $\mathbb{N}$ (полукольцо);
- натуральные числа с нулём $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ (полукольцо с нулём);
- целые числа $\mathbb{Z}$ (кольцо);
- рациональные числа $\mathbb{Q}$ (поле);
- действительные числа $\mathbb{R}$ (поле).

При этом

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Отметим, что рациональные числа $\mathbb{Q}$ и действительные числа $\mathbb{R}$ с операциями сложения и умножения являются *полями*. Напомним, что множество K с операциями сложения и умножения, $(K, +, \cdot)$, называется полем, если:

Поле

10 - 14

1) операция сложения

коммутативна ($a + b = b + a \quad \forall a, b \in K$);

ассоциативна ($(a + b) + c = a + (b + c) \quad \forall a, b, c \in K$);

существует нейтральный элемент 0 ($0 + a = a \quad \forall a \in K$);

$\forall a \in K$ существует противоположный элемент $-a$ ($a + (-a) = 0$)

(кратко, $(K, +)$ — *коммутативная группа*);

2) операция умножения

коммутативна ($ab = ba \quad \forall a, b \in K$);

ассоциативна ($(ab)c = a(bc) \quad \forall a, b, c \in K$);

существует нейтральный элемент 1 ($1a = a \quad \forall a \in K$), $1 \neq 0$

(кратко, $(K, \cdot)$ — *коммутативный моноид*);

3) имеет место дистрибутивность, связывающая операции сложения и умножения ($(a + b)c = ac + bc \quad \forall a, b, c \in K$).

Условия 1), 2), 3) определяют *коммутативное кольцо*.

4) Имеет место обратимость ненулевых элементов ($\forall a \in K, \ a \neq 0, \ \exists b \in K \quad ab = 1$).

Поле действительных чисел $\mathbb{R}$, при всех его достоинствах, не является *алгебраически замкнутым полем* (т. е. многочлены с действительными коэффициентами могут не иметь действительных корней: например, многочлен $x^2 + 1$ не имеет действительного корня). Нашей целью является построение расширения $\mathbb{C}$ поля действительных чисел $\mathbb{R}$, $\mathbb{R} \subset \mathbb{C}$, в котором есть такой элемент $i \in \mathbb{C}$, что $i^2 = -1$ (уравнение $x^2 + 1 = 0$ имеет решение), при этом в некотором смысле это минимальное расширение с этим свойством. Построенное поле $\mathbb{C}$ окажется алгебраически замкнутым (*алгебраическим замыканием* поля $\mathbb{R}$).

$\mathbb{R} \subseteq \mathbb{C}$

10-15

Анализ ситуации

Допустим, что существует поле K, содержащее в качестве подполя поле действительных чисел, $\mathbb{R} \subset K$, и элемент $i \in K$ такой, что $i^2 = -1$. Тогда:

1) для $a, b, c, d \in \mathbb{R}$ равенство $a + bi = c + di$ выполнено тогда и только тогда, когда $a = c$, $b = d$.

$a = c$
$b = d$

Доказательство. Если $a + bi = c + di$, то $a - c = (d - b)i$, поэтому $(a - c)^2 = -(d - b)^2$, следовательно, $(a - c)^2 = 0 = (d - b)^2$, т. е. $a = c$, $b = d$. □

2) подмножество D всех элементов $a + bi$, $a, b \in \mathbb{R}$, замкнуто относительно операции сложения

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$0 = 0 + 0i \in D$ является в D нейтральным элементом, $-(a+bi) = (-a)+(-b)i$ — противоположный элемент для $a+bi$. Итак, D относительно сложения — коммутативная группа. □

3) подмножество D замкнуто относительно умножения

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i. \quad \square$$

4) $(a + bi)(a - bi) = a^2 + b^2$. □

5) если $a + bi \neq 0$, то $a^2 + b^2 > 0$, и

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

следовательно,

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

для $a + bi \neq 0$. Итак, D является подполем поля K, $\mathbb{R} \subset D$, $i \in D$, D — наименьшее подполе в K, содержащее $\mathbb{R}$ и i. □

10-16

Построение поля комплексных чисел

На основе проведённого анализа положим

$$\mathbb{C} = \mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\} -$$

совокупность упорядоченных пар действительных чисел.

Рассмотрим следующие операции сложения и умножения:

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

Тогда:

1) $\mathbb{C} = (\mathbb{R}^2, +)$ — абелева группа (сложение ассоциативно и коммутативно; $(0, 0)$ — нейтральный элемент; $(-a, -b)$ — противоположный элемент для (a, b));

2) умножение: ассоциативно

$$\begin{aligned}((a, b)(c, d))(e, f) &= (ac - bd, ad + bc)(e, f) = \\ &= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e) = \\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce) = \\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf) = \\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df)) = \\ &= (a, b)(ce - df, cf + de) = (a, b)((c, d)(e, f));\end{aligned}$$

коммутативно

$$(a, b)(c, d) = (ac - bd, ad + bc) = (ca - db, cb + da) = (c, d)(a, b);$$

$(1, 0)$ — нейтральный элемент, $(a, b)(1, 0) = (a, b)$, $(1, 0) \neq (0, 0)$;

3) выполнено свойство дистрибутивности:

$$\begin{aligned}(a, b)((c, d) + (e, f)) &= (a, b)((c + e, d + f)) = \\ &= (a(c + e) - b(d + f), a(d + f) + b(c + e)) = \\ &= (ac + ae - bd - bf, ad + af + bc + be) = \\ &= (ac - bd + ae - bf, ad + bc + af + be) = \\ &= (ac - bd, ad + bc) + (ae - bf, af + be) = \\ &= (a, b)(c, d) + (a, b)(e, f).\end{aligned}$$

10-17

Итак, $\mathbb{C} = \mathbb{R}^2$ с этими операциями сложения и умножения является коммутативным кольцом с единицей $(1, 0)$.

Если $(a, b) \neq (0, 0)$, $a, b \in \mathbb{R}$, то $a^2 + b^2 > 0$ и

$$(a, b)\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, 0\right) = (1, 0),$$

таким образом, каждый элемент $(0, 0) \neq (a, b) \in \mathbb{C} = \mathbb{R}^2$ имеет обратный.

Итак, $\mathbb{C} = \mathbb{R}^2$ с этими операциями сложения и умножения — поле.

$\mathbb{R} \subseteq \mathbb{C}$

Осуществим вложение поля действительных чисел $\mathbb{R}$ в построенное поле $\mathbb{C} = \mathbb{R}^2$, сопоставляя любому элементу $a \in \mathbb{R}$ пару $(a, 0) \in \mathbb{C} = \mathbb{R}^2$. Так как для $a, b \in \mathbb{R}$ имеем

$$(a + b, 0) = (a, 0) + (b, 0),$$
$$(ab, 0) = (a, 0)(b, 0),$$

то это отображение является изоморфизмом поля $\mathbb{R}$ на подполе $\{(a, 0) \mid a \in \mathbb{R}\}$ поля $\mathbb{C} = \mathbb{R}^2$. В дальнейшем мы будем отождествлять a и $(a, 0)$, полагая $a = (a, 0)$, в частности $1 = (1, 0)$.

i

Если $i = (0, 1)$, то

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1,$$

(элемент $i = (0, 1)$ в построенном расширении $\mathbb{C} = \mathbb{R}^2$ поля $\mathbb{R}$ является корнем уравнения $x^2 + 1 = 0$).

Для любых $a, b \in \mathbb{R}$ имеем

$a+bi$

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi,$$

при этом это представление единственно (как из «анализа задачи», так и непосредственно: если $a+bi = c+di$, то $(a, b) = a+bi = c+di = (c, d)$, следовательно, $a = c$, $b = d$).

Элементы построенного поля $\mathbb{C} = \mathbb{R}^2$ называются комплексными числами. Форма записи комплексного числа в виде $a + bi$, $a, b \in \mathbb{R}$, называется алгебраической формой записи, в которой:

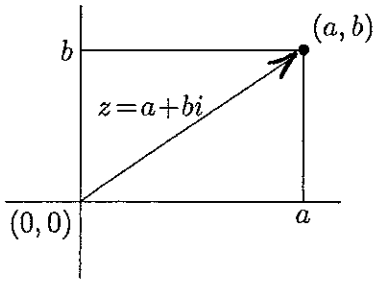
алг. форма

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

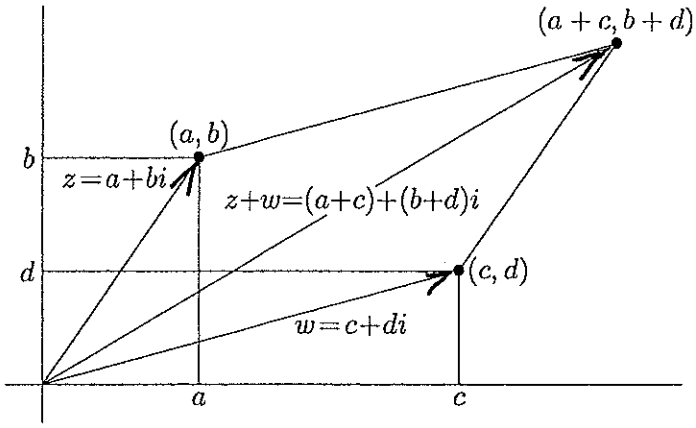
10-18

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \quad \text{для} \quad a+bi \neq 0.$$

В геометрической интерпретации комплексное число $z = a + bi$ изображается вектором в прямоугольной системе координат, выходящим из точки $(0,0)$ в точку (a,b).



Сложение комплексных чисел соответствует сложению векторов:



Геометрическая интерпретация умножения и перехода к обратному элементу будет дана позже.

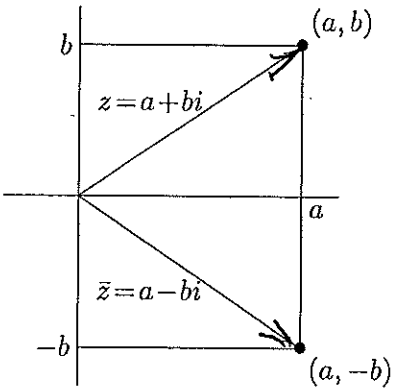
Для комплексного числа $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, $a = \operatorname{Re} z$ называется его вещественной частью, $b = \operatorname{Im} z$ — его мнимой частью.

Замечание 2.1. В построенном поле $\mathbb{C}$ уравнение $x^2+1=0$ имеет лишь два решения: $x = i$, $x = -i$. Действительно, если $(a+bi)^2 = -1$, то $a^2 - b^2 = -1$, $2ab = 0$. Так как $b \neq 0$ (иначе $a^2 = -1$), то $a = 0$ и $b^2 = 1$, поэтому $b = \pm 1$.

10-19

Сопряжение комплексных чисел

Каждому комплексному числу $z = x + iy \in \mathbb{C}$ сопоставим комплексное число $\bar{z} = x - iy \in \mathbb{C}$, называемое *комплексно сопряжённым*. Геометрическая интерпретация перехода от $z = a + bi$ к сопряжённому комплексному числу $\bar{z} = a - bi$ прозрачна: это отражение относительно вещественной оси:



Теорема 2.2.

1) *Операция комплексного сопряжения $z \to \bar{z}$ является автоморфизмом поля $\mathbb{C}$ комплексных чисел (т. е. биекцией, для которой $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$ для $z, w \in \mathbb{C}$ и, как следствие, $\overline{\left(\frac{w}{z}\right)} = \frac{\bar{w}}{\bar{z}}$ для $z \neq 0$), оставляющим все действительные числа и только их на месте ($\bar{a} = a$ для $a \in \mathbb{R} \subseteq \mathbb{C}$; если $\bar{z} = z$, то $z \in \mathbb{R}$).*

$\mathbb{R} \subset \mathbb{C}$

2) *Квадрат комплексного сопряжения равен тождественному отображению ($\bar{\bar{z}} = z$).*

3) *Если $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, то $z + \bar{z} = 2a \in \mathbb{R}$, $z - \bar{z} = 2bi \in \mathbb{R}i$, $N(z) = z\bar{z} = a^2 + b^2 \in \mathbb{R}$, при этом $N(wz) = N(w)N(z)$ для $w, z \in \mathbb{C}$.*

4) *Если $f\colon \mathbb{C} \to \mathbb{C}$ — такой автоморфизм поля $\mathbb{C}$ комплексных чисел, что $f(a) = a$ для всех $a \in \mathbb{R} \subseteq \mathbb{C}$, то либо $f = 1_{\mathbb{C}}$, либо $f(z) = \bar{z}$ для $z \in \mathbb{C}$ (тем самым показано, что группа Галуа расширения $\mathbb{R} \subset \mathbb{C}$ состоит из двух элементов).*

10–20

Доказательство.

1) Ясно, что соответствие

$$z = a + bi = (a, b) \to \bar{z} = a - bi = (a, -b)$$

является биекцией.

Если $z = a + bi$, $w = c + di$, то

$$\overline{z + w} = \overline{(a + b) + (c + d)i} = (a + b) - (c + d)i = \\ = (a - ci) + (b - di) = \bar{z} + \bar{w};$$

$$\overline{-z} = \overline{-a - bi} = -a + bi = -(a - bi) = -(\bar{z});$$

$$\overline{z - w} = \bar{z} + \overline{(-w)} = \bar{z} - \bar{w};$$

$$\overline{zw} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = \\ = (a - bi)(c - di) = \bar{z}\bar{w}.$$

Если $z \neq 0$, то $1 = \overline{z \cdot z^{-1}} = \bar{z} \cdot \overline{z^{-1}}$, т. е. $\overline{z^{-1}} = (\bar{z})^{-1}$. Поэтому

$$\overline{\left(\frac{w}{z}\right)} = \overline{wz^{-1}} = \bar{w}\overline{(z^{-1})} = \bar{w}(\bar{z})^{-1} = \frac{\bar{w}}{\bar{z}}.$$

Если $z = a \in \mathbb{R}$, то $\bar{z} = a$. Если $z = a + bi$, то $\bar{z} = z$ означает, что $z = a + bi = a - bi = \bar{z}$, т. е. $b = -b$, поэтому $b = 0$ и $z = a \in \mathbb{R}$. Итак, $z = \bar{z}$ тогда и только тогда, когда $z \in \mathbb{R}$.

2) $\bar{z} = a - bi = a + bi = z$. $\bar{\bar{z}} = z$

3) Если $z = a + bi$, то

$$z + \bar{z} = (a + bi) + (a - bi) = 2a \in \mathbb{R},$$
$$z - \bar{z} = (a + bi) - (a - bi) = 2bi \in \mathbb{R}i,$$
$$z \cdot \bar{z} = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{R}.$$

Далее,

$$N(wz) = wz\overline{wz} = wz\bar{w}\bar{z} = w\bar{w}z\bar{z} = N(w)N(z).$$

4) Так как $i^2 = -1$, то $f(i)^2 = f(-1) = -1$, поэтому

либо $f(i) = i$, и тогда $f(a + bi) = f(a) + f(b)f(i) = a + bi$,
либо $f(i) = -i$, и тогда $f(a + bi) = f(a) + f(b)f(i) = a - bi$. $\square$

$\mathbb{R} \subset \mathbb{C}$ $\quad Gal(\mathbb{C}, \mathbb{R}) = \{1_{\mathbb{C}}, z \to \bar{z}\}$

10-21

Замечание 2.3.

1) Если комплексное число α получено как выражение из комплексных чисел $\alpha_1, \ldots, \alpha_n$ с помощью операций сложения, вычитания, умножения и деления, то то же выражение из комплексных чисел $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ даёт $\bar{\alpha}$.

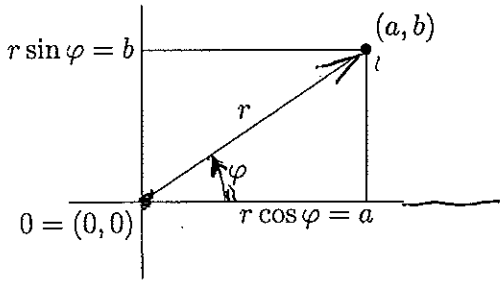
2) Правило деления комплексного числа $w = c + di$ на ненулевое комплексное число $0 \neq z = a+bi \in \mathbb{C}$ (в алгебраической форме):

$$\frac{w}{z} = \frac{c+di}{a+bi} = \frac{(c+di)(a-bi)}{(a+bi)(a-bi)} = \left(\frac{ca+db}{a^2+b^2}\right) + \left(\frac{-cb+da}{a^2+b^2}\right) i.$$

Полярные координаты точек плоскости (отличных от начала координат)

$z \neq (0,0)$
$\parallel$
(a,b)

Точка плоскости (a, b), отличная от начала координат $(0,0)$, однозначно задаётся своими *полярными координатами* r, φ, где r — расстояние от данной точки до начала координат, φ — угол между положительной полуосью абсцисс и радиусом-вектором точки (a, b), отсчитываемый против часовой стрелки (определённый с точностью до $2\pi k$, $k \in \mathbb{Z}$, и называемый *аргументом точки* (a, b)).



Аргумент точки $0 = (0, 0)$ не определён.

Формулы перехода от декартовых координат a и b точки (a, b) к полярным координатам и обратно:

$$r = \sqrt{a^2 + b^2},$$

$$\sin\varphi = \frac{b}{\sqrt{a^2+b^2}}, \quad \cos\varphi = \frac{a}{\sqrt{a^2+b^2}};$$

$$a = r\cos\varphi, \quad b = r\sin\varphi.$$

10-22

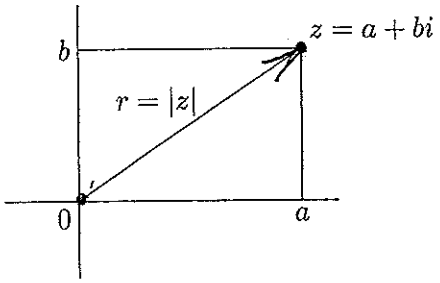
Свойства модуля комплексных чисел

Для комплексного числа $z = a+bi \in \mathbb{C}$ определим его *модуль* как

$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2}$$

(в геометрической интерпретации на плоскости $\mathbb{C} = \mathbb{R}^2$ модуль комплексного числа $r = |z| = \sqrt{a^2+b^2}$ — это расстояние от точки $(0,0)$ до точки (a,b), т. е. длина вектора z).

$r = \rho(z, 0)$



Пример 2.4.

1) Если $z = a \in \mathbb{R}$, то $|z| = \sqrt{a^2} = |a|$, т. е. функция модуль комплексного числа $|\ |: \mathbb{C} \to \mathbb{R}^+$ является продолжением функции модуль действительного числа $|\ |: \mathbb{R} \to \mathbb{R}^+ = \{r \in \mathbb{R},\ r \geqslant 0\}$.

2) $|i| = 1$, $|1+i| = \sqrt{2}$.

3) $|z| = \sqrt{a^2+b^2} = |\bar{z}|$ для $z = a+bi \in \mathbb{C}$.

4) $|a| = \sqrt{a^2} \leqslant \sqrt{a^2+b^2} = |z|$ для $z = a+bi \in \mathbb{C}$.

Лемма 2.5. *$|wz| = |w|\,|z|$ для $w, z \in \mathbb{C}$.*

Доказательство.

$$|wz| = \sqrt{(wz)\overline{(wz)}} = \sqrt{(w\bar{w})(z\bar{z})} = \sqrt{w\bar{w}}\sqrt{z\bar{z}} = |w|\,|z|. \quad \square$$

Другое доказательство этого факта следует из свойств тригонометрической формы.

10 – 23

Следствие 2.6.

1) *Если* $w = z^{-1}$ *для* $0 \neq z \in \mathbb{C}$, *то* $1 = |1| = |z^{-1}z| = |z^{-1}|\,|z|$, *поэтому*

$$|w| = \left|\frac{1}{z}\right| = \frac{1}{|z|}, \quad \text{или} \quad |z^{-1}| = |z|^{-1}.$$

2) *Для* $w, z \in \mathbb{C}$, $z \neq 0$:

$$\left|\frac{w}{z}\right| = |wz^{-1}| = |w|\,|z^{-1}| = |w|\,|z^{-1}| = \frac{|w|}{|z|}.$$

Лемма 2.7. $|w + z| \leqslant |w| + |z|$ *для* $w, z \in \mathbb{C}$.

Первое доказательство. Длина $|w+z|$ стороны треугольника не превосходит суммы длин $|w| + |z|$ двух других сторон. □

Второе доказательство. Если $w = 0$ или $z = 0$, то утверждение очевидно.

Пусть теперь $w \neq 0$ и $z \neq 0$. Так как для $z = a + bi$ имеем $|a| = \sqrt{a^2} \leqslant \sqrt{a^2 + b^2} = |z|$, то

$$|1 + z|^2 = (1 + z)(1 + \bar{z}) = 1 + (z + \bar{z}) + z\bar{z} =$$
$$= 1 + 2a + |z|^2 \leqslant 1 + 2|z| + |z|^2 = (1 + |z|)^2,$$

и поэтому, поскольку $|1 + z| \geqslant 0$, $1 + |z| \geqslant 0$,

$$|1 + z| \leqslant 1 + |z|.$$

Далее,

$$|w + z| = |w(1 + w^{-1}z)| = |w| \cdot |1 + w^{-1}z| \leqslant$$
$$\leqslant |w|(1 + |w^{-1}z|) = |w|(1 + |w^{-1}|\,|z|) =$$
$$= |w| + |ww^{-1}|\,|z| = |w| + |z|. \quad ☒$$

Следствие 2.8. $|w| - |z| \leqslant |w \pm z| \leqslant |w| + |z|$ *для* $w, z \in \mathbb{C}$.

Доказательство.
1) $|w - z| \leqslant |w| + |-z| = |w| + |z|$.
2) Так как $|w| = |(w - z) + z| \leqslant |w - z| + |z|$, то $|w| - |z| \leqslant |w - z|$.
3) $|w| - |z| = |w| - |-z| \leqslant |w + z|$. □

10 - 24

Тригонометрическая форма ненулевого комплексного числа

Используя полярные координаты, модуль $r = \sqrt{a^2 + b^2}$ и аргумент $\varphi = \arg z$, для комплексного числа $z = a + bi$ и принимая во внимание, что $a = r\cos\varphi$, $b = r\sin\varphi$, получаем *тригонометрическую форму*:

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

Примеры 2.9.

1) $1 = 1(\cos 0 + i\sin 0)$;

2) $i = 1\left(\cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2}\right)$;

3) $z = -1 + \sqrt{3}i$, $r = |z| = \sqrt{1+3} = 2$, $\cos\varphi = -\dfrac{1}{2}$, $\sin\varphi = \dfrac{\sqrt{3}}{2}$, $\varphi = \dfrac{2\pi}{3}$, поэтому

$$z = -1 + \sqrt{3}i = 2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right);$$

4) $\cos\varphi - i\sin\varphi = \cos(-\varphi) + i\sin(-\varphi)$.

Теорема 2.10 (о единственности тригонометрической формы). *Если* $0 \neq z = a + bi \in \mathbb{C}$ *и*

$$z = r_1(\cos\varphi_1 + i\sin\varphi_1) = r_2(\cos\varphi_2 + i\sin\varphi_2),$$

где $\mathbb{R} \ni r_1 > 0$, $\mathbb{R} \ni r_2 > 0$, *то*

$$r_1 = r_2 \quad \text{и} \quad \varphi_1 - \varphi_2 = 2\pi k, \quad k \in \mathbb{Z}.$$

Доказательство. Из единственности алгебраической формы имеем

$$a = r_1\cos\varphi_1 = r_2\cos\varphi_2, \quad b = r_1\sin\varphi_1 = r_2\sin\varphi_2.$$

Возводя в квадрат и складывая, получаем

$$r_1^2 = r_1^2(\cos^2\varphi_1 + \sin^2\varphi_1) = r_2^2(\cos^2\varphi_2 + \sin^2\varphi_2) = r_2^2.$$

Так как $r_1 > 0$, $r_2 > 0$, то $r_1 = r_2$. Поэтому $\cos\varphi_1 = \cos\varphi_2$, $\sin\varphi_1 = \sin\varphi_2$, следовательно, $\varphi_1 - \varphi_2 = 2\pi k$, $k \in \mathbb{Z}$. ∎

10-25

Следствие 2.11. *Если*

$$0 \neq z = a + bi \in \mathbb{C}, \quad z = r(\cos\varphi + i\sin\varphi), \quad \mathbb{R} \ni r > 0,$$

то

$$r = |z| = \sqrt{a^2 + b^2}, \quad \varphi = \arg z$$

(*т. е.* $\arg z = \varphi + 2\pi k$, $k \in \mathbb{Z}$).

Упражнение 2.12. Если $z = r(\cos\varphi + i\sin\varphi)$, $r > 0$, то

$$-z = r(\cos(\varphi + \pi) + i\sin(\varphi + \pi)),$$
$$\bar{z} = r(\cos(-\varphi) + i\sin(-\varphi)).$$

Умножение комплексных чисел в тригонометрической форме

Алгебраическая форма записи комплексных чисел удобна для операций сложения и разности. Как мы сейчас убедимся, тригонометрическая форма записи ненулевых комплексных чисел удобна для операции умножения (и как следствие — для деления, возведения в степень, извлечения корней).

Теорема 2.13. *Если*

$$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2),$$

$r_1 > 0$, $r_2 > 0$, $r_1, r_2 \in \mathbb{R}$, *то*

$$z_1 z_2 = (r_1 r_2)(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)),$$

т. е. $|z_1 z_2| = |z_1|\,|z_2|$, $\arg z_1 z_2 = (\varphi_1 + \varphi_2) + 2\pi k$ *(аргумент произведения равен сумме аргументов).*

Множ. функция

Доказательство.

$$z_1 z_2 = (r_1 r_2)((\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)) = (r_1 r_2)(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)),$$

$r_1 r_2 > 0$. Итак, это тригонометрическая форма для $z_1 z_2$, поэтому

$$|z_1 z_2| = r_1 r_2 = |z_1|\,|z_2|, \quad \arg z_1 z_2 = (\varphi_1 + \varphi_2) + 2\pi k. \quad \boxtimes$$

(обмысл. тригон. формы)

10-26

Следствие 2.14. $\left|\dfrac{z_1}{z_2}\right| = \dfrac{|z_1|}{|z_2|}$ *для* $z_1, z_2 \in \mathbb{C}$, $z_2 \neq 0$, $\arg\left(\dfrac{z_1}{z_2}\right) = \arg z_1 - \arg z_2$. *В частности,* $|z^{-1}| = |z|^{-1}$, $\arg z^{-1} = -\arg z$.

Доказательство. Если $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $|z_1| = r_1$, $\arg z_1 = \varphi_1 + 2\pi k$, $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, $|z_2| = r_2$, $\arg z_2 = \varphi_2 + 2\pi k$, то

$$r_2(\cos\varphi_2 + i\sin\varphi_2)\cdot\frac{r_1}{r_2}(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)) = \\ = r_1(\cos\varphi_1 + i\sin\varphi_1),$$

следовательно,

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)), \quad \frac{r_1}{r_2} > 0,$$

поэтому

$$\left|\frac{z_1}{z_2}\right| = \frac{r_1}{r_2} = \frac{|z_1|}{|z_2|}, \quad \arg\frac{z_1}{z_2} = (\varphi_1-\varphi_2) + 2\pi k, \quad k \in \mathbb{Z}.$$

Если

$$z = r(\cos\varphi + i\sin\varphi), \quad r > 0,$$

то

$$z^{-1} = \frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi)),$$

и поэтому

$$|z^{-1}| = \frac{1}{r} = |z|^{-1}, \quad \arg z^{-1} = -\varphi + 2\pi k, \quad k \in \mathbb{Z}. \quad \square$$

Следствие 2.15. *Умножение комплексного числа* z *на комплексное число* $r(\cos\varphi + i\sin\varphi)$, $r > 0$, *означает «растяжение» вектора* z *в* r *раз и поворот полученного вектора на угол* φ *(т. е. умножение модуля* $|z|$ *на* r, *а затем прибавление* φ *к* $\arg z$*).*

В частности, умножение комплексного числа на $\cos\varphi + i\sin\varphi$ *равносильно повороту на* φ *(умножение на* $i = \cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2}$ *означает поворот плоскости вокруг начала координат на* $\dfrac{\pi}{2}$*).*

110-27

Упражнение 2.16 (экспоненциальная форма Эйлера записи комплексного числа). Рассмотрим последовательность

$$c_n = a_n + ib_n \in \mathbb{C},$$

где $a_n, b_n \in \mathbb{R}$. Если существуют

$$\lim_{n\to\infty} a_n = a \in \mathbb{R}, \quad \lim_{n\to\infty} b_n = b \in \mathbb{R},$$

то существует

$$\lim_{n\to\infty} (a_n + ib_n) = a + ib \in \mathbb{C}$$

(в метрике на $\mathbb{C} = \mathbb{R}^2$, определяемой $|z|$ для $z \in \mathbb{C}$).

Покажите, что

$$\lim_{n\to\infty} \left(1 + \frac{a+bi}{n}\right)^n = e^a(\cos b + i \sin b).$$

Это даёт основание (Эйлер) ввести обозначение

$$e^{a+bi} = e^a e^{bi},$$

где

$$e^{bi} = \cos b + i \sin b.$$

Если $z, w \in \mathbb{C}$, то $e^z \cdot e^w = e^{z+w}$.

Геометрическая интерпретация обратного элемента z^{-1} для $z = a + bi \in \mathbb{C}$

Если $0 \neq z = a + bi \in \mathbb{C}$, то, как мы видели, $z\bar{z} = N(z) = |z|^2 = a^2 + b^2$,

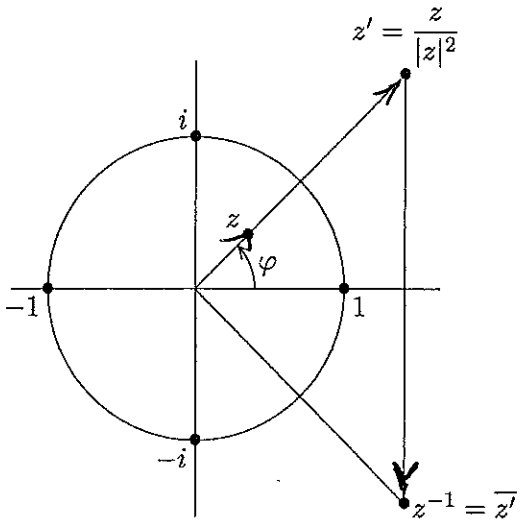
$$z^{-1} = \frac{\bar{z}}{|z|^2} = \overline{\left(\frac{z}{|z|^2}\right)}.$$

Таким образом, геометрическое построение комплексного числа z^{-1} можно провести двумя последовательными процедурами:

а) инверсия $z \to z' = \dfrac{z}{|z|^2}$ относительно окружности единичного радиуса ($|z'| = \dfrac{1}{|z|}$);

б) сопряжение $z' \to \overline{z'} = z^{-1}$.

10-28



Задача 2.17. Найти геометрическое множество точек z^{-1}, где z пробегает прямую $\{1 + bi \mid b \in \mathbb{R}\}$.

Упражнение 2.18.

а) Для $w \in \mathbb{C}$, $w \neq 0$, имеем

$$\left|\frac{w}{\bar{w}}\right| = \frac{|w|}{|\bar{w}|} = \frac{|w|}{|w|} = 1,$$

таким образом,

$$\frac{w}{\bar{w}} \in T = \{z \in \mathbb{C} \mid |z| = 1\}.$$

б) Если $z \in T$, т. е. $|z| = 1$, $z = \cos\varphi + i\sin\varphi$, то $z = \dfrac{w}{\bar{w}}$ для некоторого $0 \neq w \in \mathbb{C}$. Таким образом,

$$\left\{z = \frac{1+it}{1-it} \,\middle|\, t \in \mathbb{R}\right\} = T.$$

Действительно, если $w = \cos\theta + i\sin\theta$, то $\bar{w} = \cos(-\theta) + i\sin(-\theta)$ и

$$\frac{w}{\bar{w}} = \cos 2\theta + i\sin 2\theta = \cos\varphi + i\sin\varphi.$$

10-29

Таким образом, если $2\theta = \varphi$, т. е. $\theta = \dfrac{\varphi}{2}$, то $w = \cos\dfrac{\varphi}{2} + i\sin\dfrac{\varphi}{2}$ является одним из решений этой задачи.

Упражнение 2.19.

1) Единичная окружность $T = \{z \in \mathbb{C} \mid |z| = 1\}$ с операцией умножения является группой (подгруппой мультипликативной группы $(\mathbb{C}^* = \mathbb{C} \setminus \{0\}, \cdot)$ поля $\mathbb{C}$ комплексных чисел).

2) $\{r \in \mathbb{R} \mid r < 0\} = \{z \in \mathbb{C} \mid \arg z = \pi + 2\pi k\}$.

3) Найти все $z \in \mathbb{C}$, для которых $\left|\dfrac{z-i}{z+i}\right| = 1$.

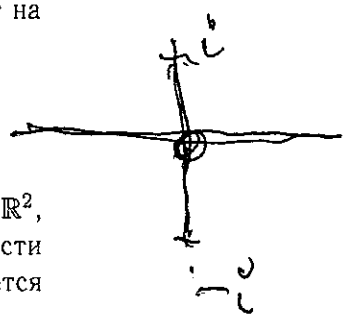
z

$\rho(z, i) = \rho(z, -i)$

4) Найти все $z \in \mathbb{C}$, для которых $|z+i| + |z-i| = 2$.

5) Три различных комплексных числа $z_1, z_2, z_3 \in \mathbb{C} \in \mathbb{R}^2$ лежат на одной прямой в $\mathbb{R}^2$ тогда и только тогда, когда

$$\frac{z_1 - z_3}{z_2 - z_3} \in \mathbb{R}.$$



6) Четыре различных комплексных числа $z_1, z_2, z_3, z_4 \in \mathbb{C} = \mathbb{R}^2$, не лежащие на одной прямой в $\mathbb{R}^2$, лежат на одной окружности тогда и только тогда, когда их *двойное отношение* является вещественным числом:

$$\frac{z_1 - z_3}{z_2 - z_3} : \frac{z_1 - z_4}{z_2 - z_4} \in \mathbb{R}.$$

7) Рассмотрим отображение *инфлексии* $\mathbb{C} \to \mathbb{C}$,

$$z = x + yi \mapsto y + xi = \underline{z}, \quad x, y \in \mathbb{R}.$$

Показать, что:

(a) отображение $z \to \underline{z}$ является биекцией, при этом $\underline{(z_1 + z_2)} = \underline{z_1} + \underline{z_2}$, $|\underline{z}| = |z| = \sqrt{x^2 + y^2}$;

(b) $\underline{zw} = \dfrac{1}{i}\underline{z} \cdot \underline{w}$ для $z, w \in \mathbb{C}$;

(c) $|\underline{zw}| = |\underline{z} \cdot \underline{w}| = |\underline{z}|\,|\underline{w}|$, в частности $|z\underline{z}| = |z|^2$ для $z \in \mathbb{C}$.

10-30

Теорема 2.20 (формула Муавра о возведении в степень комплексного числа в тригонометрической форме). *Пусть* $0 \neq z \in \mathbb{C}$, $z = r(\cos\varphi + i\sin\varphi)$, $r > 0$, $n \in \mathbb{Z}$. *Тогда*

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

Доказательство. Утверждение теоремы — частный случай теоремы 2.13. □

Упражнение 2.21. Так как для $n \in \mathbb{N}$

$$(\cos n\varphi + i\sin n\varphi) = (\cos\varphi + i\sin\varphi)^n,$$

то, выражая правую часть с помощью формулы бинома Ньютона, получаем, приравнивая действительные и мнимые части:

$$\cos n\varphi = \cos^n\varphi - C_n^2\cos^{n-2}\varphi\sin^2\varphi + C_n^4\cos^{n-4}\varphi\sin^4\varphi - \ldots,$$
$$\sin n\varphi = n\cos^{n-1}\varphi\sin\varphi - C_n^3\cos^{n-3}\varphi\sin^3\varphi + C_n^5\cos^{n-5}\varphi\sin^5\varphi - \ldots.$$

Например:

$$\begin{aligned}
\cos 2\varphi &= \cos^2\varphi - \sin^2\varphi,\\
\cos 3\varphi &= \cos^3\varphi - 3\cos\varphi\sin^2\varphi,\\
\cos 4\varphi &= \cos^4\varphi - 6\cos^2\varphi\sin^2\varphi + \sin^4\varphi,\\
\sin 2\varphi &= 2\cos\varphi\sin\varphi,\\
\sin 3\varphi &= 3\cos^2\varphi\sin\varphi - \sin^3\varphi,\\
\sin 4\varphi &= 4\cos^3\varphi\sin\varphi - 4\cos\varphi\sin^3\varphi.
\end{aligned}$$

Упражнение 2.22. Если

$$u = \cos\varphi + i\sin\varphi, \quad v = \bar{u} = \cos\varphi - i\sin\varphi,$$

то

$$u + v = 2\cos\varphi, \quad u - v = 2i\sin\varphi, \quad uv = 1,$$
$$u^m = \cos m\varphi + i\sin m\varphi,$$
$$v^m = (\bar{u})^m = \overline{(u^m)} = \cos m\varphi - i\sin m\varphi,$$

(10-31)

$$2^n \cos^n \varphi = (u+v)^n = \sum_{k=0}^{n} C_n^k u^{n-k} v^k =$$
$$= (u^n + v^n) + nuv(u^{n-2} + v^{n-2}) + C_n^2 u^2 v^2 (u^{n-4} + v^{n-4}) + \ldots.$$

Если $n = 2k$, то

$$(-1)^{n/2} 2^n \sin^n \varphi = (u-v)^n =$$
$$= (u^n + v^n) - nuv(u^{n-2} + v^{n-2}) + C_n^2 u^2 v^2 (u^{n-4} + v^{n-4}) - \ldots.$$

Если $n = 2k+1$, то

$$(-1)^{(n-1)/2} i 2^n \sin^n \varphi = (u-v)^n =$$
$$= (u^n - v^n) - nuv(u^{n-2} - v^{n-2}) + C_n^2 u^2 v^2 (u^{n-4} - v^{n-4}) - \ldots.$$

Отсюда: если $n = 2k$, то

$$2^n \cos^n \varphi =$$
$$= 2\cos n\varphi + 2n\cos(n-2)\varphi + 2C_n^2 \cos(n-4)\varphi + \ldots + C_n^{n/2},$$
$$(-1)^{n/2} 2^n \sin^n \varphi =$$
$$= 2\cos n\varphi - 2n\cos(n-2)\varphi + 2C_n^2 \cos(n-4)\varphi - \ldots + (-1)^{n/2} C_n^{n/2};$$

если $n = 2k+1$, то

$$2^n \cos^n \varphi =$$
$$= 2\cos n\varphi + 2n\cos(n-2)\varphi + 2C_n^2 \cos(n-4)\varphi + \ldots +$$
$$+ 2C_n^{(n-1)/2} \cos\varphi,$$
$$(-1)^{(n-1)/2} 2^n \sin^n \varphi =$$
$$= 2\sin n\varphi - 2n\sin(n-2)\varphi + 2C_n^2 \sin(n-4)\varphi - \ldots +$$
$$+ (-1)^{(n-1)/2} 2C_n^{(n-1)/2} \sin\varphi.$$

Упражнение 2.23. Если $u = \cos\varphi + i\sin\varphi$, $\varphi \neq 2\pi k$, то

$$u + \ldots + u^n = u\frac{u^n - 1}{u - 1}.$$

№ -32

Приравнивая вещественные и мнимые части, получаем:

$$\sum_{k=1}^{n} \cos k\varphi = \frac{\sin\dfrac{n\varphi}{2}\cos\dfrac{(n+1)\varphi}{2}}{\sin\dfrac{\varphi}{2}};$$

$$\sum_{k=1}^{n} \sin k\varphi = \frac{\sin\dfrac{n\varphi}{2}\sin\dfrac{(n+1)\varphi}{2}}{\sin\dfrac{\varphi}{2}}.$$

Теорема 2.24 (извлечение корней n-й степени из комплексных чисел). *Пусть $n \geqslant 1$, $0 \neq z \in \mathbb{C}$, $z = r(\cos\varphi + i\sin\varphi)$, $r > 0$. Тогда существует ровно n различных корней n-й степени из z (таких $w \in \mathbb{C}$, что $w^n = z$):*

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

Они все лежат на окружности радиуса $\rho = \sqrt[n]{r}$, образуя вершины правильного n-угольника с аргументами

$$\frac{\varphi}{n}, \frac{\varphi+2\pi}{n} = \frac{\varphi}{n} + \frac{2\pi}{n}, \ldots, \frac{\varphi+2\pi(n-1)}{n} = \frac{\varphi}{n} + \frac{2\pi}{n}(n-1).$$

Доказательство. Будем искать решения w уравнения $w^n = z$ в тригонометрической форме:

$$w = \rho(\cos\theta + i\sin\theta), \quad \rho > 0.$$

Тогда по формуле Муавра

$$w^n = \rho^n(\cos n\theta + i\sin n\theta) = r(\cos\varphi + i\sin\varphi) = z,$$

т. е. $\rho^n = r$, и поэтому $\rho = \sqrt[n]{r}$, $n\theta = \varphi + 2\pi k$, $k \in \mathbb{Z}$. Различных корней будет ровно n при $k = 0, 1, 2, \ldots, n-1$:

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

Упражнение 2.25. Найдём корни уравнения

$$x^2 - (2+i)x + (-1+7i) = 0$$

10-33

(в алгебраической форме):

$$x_{1,2} = \frac{(2+i) \pm \sqrt{(2+i)^2 - 4(-1+7i)}}{2} = \frac{(2+i) \pm \sqrt{7-24i}}{2};$$

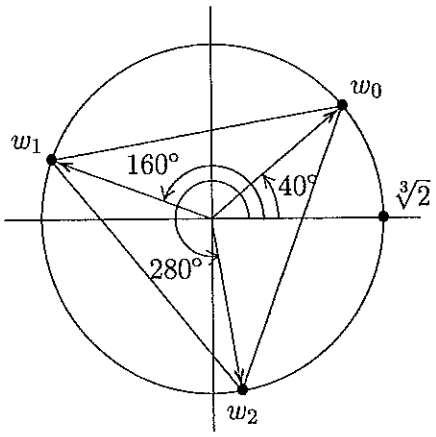
$\sqrt{7-24i} = 5\sqrt{\frac{7}{25} - \frac{24}{25}i}$, $z = \frac{7}{25} - \frac{24}{25}i = \cos\varphi + i\sin\varphi$, где $\cos\varphi = \frac{7}{25}$, $\sin\varphi = -\frac{24}{25}$, $\sqrt{z} = \pm\left(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}\right)$. Так как $\sin\varphi < 0$, $\cos\varphi > 0$, то $\frac{3\pi}{2} < \varphi < 2\pi$, и поэтому $\frac{3\pi}{4} < \frac{\varphi}{2} < \pi$, т. е. $\cos\frac{\varphi}{2} < 0$, $\sin\frac{\varphi}{2} > 0$, следовательно, $\cos\frac{\varphi}{2} = -\sqrt{\frac{1+\cos\varphi}{2}} = -\frac{4}{5}$, $\sin\frac{\varphi}{2} = +\frac{1-\cos\varphi}{2} = \frac{3}{5}$, $\sqrt{z} = \pm\left(-\frac{4}{5} + \frac{3}{5}i\right)$. Итак, $x_{1,2} = \frac{(2+i) \pm (-4+3i)}{2}$, $x_1 = -1+2i$, $x_2 = 3-i$.

Упражнение 2.26. Найти все корни третьей степени из $-1+\sqrt{3}i = 2\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$. По формуле из теоремы все три корня из $-1+\sqrt{3}i$ имеют следующий вид:

$$w_0 = \sqrt[3]{2}\left(\cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}\right);$$

$$w_1 = \sqrt[3]{2}\left(\cos\frac{8\pi}{9} + i\sin\frac{8\pi}{9}\right); \quad w_2 = \sqrt[3]{2}\left(\cos\frac{14\pi}{9} + i\sin\frac{14\pi}{9}\right).$$

На картинке:

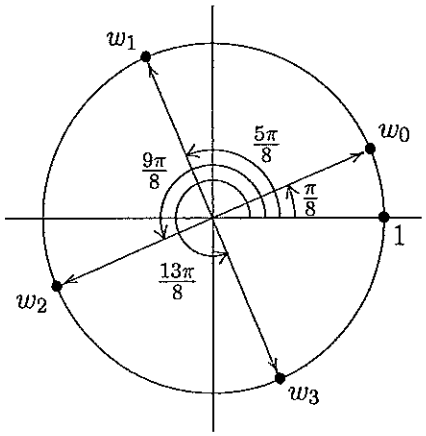


(10-34)

Упражнение 2.27. Найти все корни четвёртой степени из i. Так как $i = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$, по формуле из теоремы все четыре корня из i имеют следующий вид:

$$w_0 = \cos\frac{\pi}{8} + i\sin\frac{\pi}{8}; \quad w_1 = \cos\frac{5\pi}{8} + i\sin\frac{5\pi}{8};$$
$$w_2 = \cos\frac{9\pi}{8} + i\sin\frac{9\pi}{8}; \quad w_3 = \cos\frac{13\pi}{8} + i\sin\frac{13\pi}{8}.$$

На картинке:



Упражнение 2.28. Извлеките все корни

$$\sqrt[6]{\frac{1-i}{\sqrt{3}+i}}.$$

Упражнение 2.29. Покажите, что

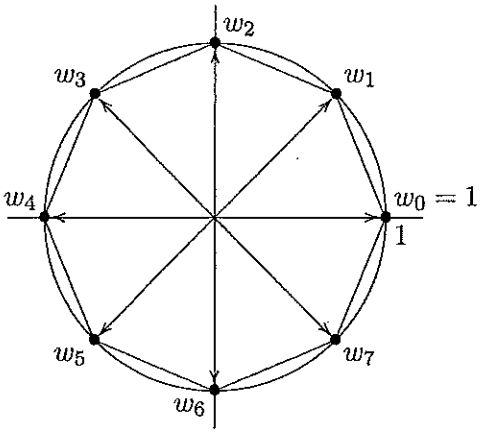
$$\sqrt[4]{-\frac{18}{1+i\sqrt{3}}} = \left\{\pm\left(\frac{3}{2} + i\frac{\sqrt{3}}{2}\right), \pm\left(\frac{\sqrt{3}}{2} - \frac{3}{2}i\right)\right\}.$$

Комплексные корни n-й степени из единицы

Так как $1 = 1(\cos 0 + i\sin 0)$, $r = 1$, $\varphi = 0$, то формула для корней n-й степени из 1 принимает вид

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

Точки w_k являются вершинами правильного n-угольника, вписанного в окружность единичного радиуса с центром в начале координат, при этом одной из вершин этого многоугольника является 1. Например, при $n = 8$



Теорема 2.30. *Совокупность $T_n = \{w \in \mathbb{C} \mid w^n = 1\}$ всех n корней n-й степени из 1 с операцией умножения является коммутативной группой (подгруппой в $T = \{z \mid |z| = 1\} \subset \mathbb{C}^* = \mathbb{C} \setminus \{0\}$).*

Доказательство.

1) Если $w, z \in T_n$, т. е. $w^n = 1$, $z^n = 1$, то $(wz)^n = w^n z^n = 1 \cdot 1 = 1$, поэтому $wz \in T_n$. Таким образом, на T_n определена операция умножения (очевидно, коммутативная и ассоциативная).

2) Ясно, что $1^n = 1$, т. е. $1 \in T_n$, и 1 — нейтральный элемент в T_n.

3) Если $w \in T_n$, то $w^n = 1$,

$$\left(\frac{1}{w}\right)^n = \frac{1}{w^n} = \frac{1}{1} = 1,$$

и поэтому $w^{-1} \in T_n$. □

Замечание 2.31. Группа T_n является циклической, т. е. все её элементы являются степенями одного элемента, называемого циклическим образующим (в качестве одного из циклических образующих можно взять $w_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, так как $w_k = (w_1)^k$ для $0 \leqslant k \leqslant n-1$, т. е. все элементы w_k группы T_n являются степенями корня w_1, такие корни называются *первообразными*). Покажите,

10-36

что $w_k = \cos\dfrac{2\pi k}{n} + i\sin\dfrac{2\pi k}{n}$ является первообразным корнем тогда и только тогда, когда наибольший общий делитель чисел k и n равен 1.

Упражнение 2.32. Доказать, что сумма всех k-х степеней корней уравнения $x^n = 1$ равна

$$\begin{aligned} &n, \text{ если } k \text{ делится на } n;\\ &0, \text{ если } k \text{ не делится на } n. \end{aligned}$$

Задача 2.33. Если $z = \dfrac{2+i}{2-i}$, то $|z| = 1$, но z не является корнем из единицы (т. е. $z \in T \setminus T_n$ для любого $n \in \mathbb{N}$).

Задача 2.34. Доказать, что

а) $\sin\left(\dfrac{\pi}{2n}\right)\sin\left(\dfrac{2\pi}{2n}\right)\ldots\sin\left(\dfrac{(n-1)\pi}{2n}\right) = \dfrac{\sqrt{n}}{2^{n-1}}$;

б) $\prod\limits_{k=1}^{n}\sin\dfrac{\pi k}{2n+1} = \dfrac{\sqrt{2n+1}}{2^n}$.

Указание. Пусть

$$x_s = \varepsilon_s = \cos\frac{\pi s}{n} + i\sin\frac{\pi s}{n}, \quad s = 1, 2, \ldots, 2n$$

(все корни степени $2n$ из 1). Тогда

$$x^{2n} - 1 = \prod_{s=1}^{2n}(x - x_s) = \prod_{s=1}^{n-1}(x - x_s)\prod_{s=n+1}^{2n-1}(x - x_s)(x^2 - 1)$$

(так как $x_n = -1$, $x_{2n} = 1$). Но $x_{2n-s} = \bar{x}_s$, поэтому

$$\begin{aligned} x^{2n} - 1 &= (x^2 - 1)\prod_{s=1}^{n-1}(x - x_s)(x - \bar{x}_s) = \\ &= (x^2 - 1)\prod_{s=1}^{n-1}\left(x^2 - 2x\cos\frac{\pi s}{n} + 1\right). \end{aligned}$$

Следовательно,

$$\frac{x^{2n}-1}{x^2-1} = x^{2(n-1)} + x^{2(n-2)} + \ldots + x^2 + 1 = \prod_{s=1}^{n-1}\left(x^2 - 2x\cos\frac{\pi s}{n} + 1\right).$$

10-37

Полагая $x = 1$, имеем

$$n = \prod_{s=1}^{n-1}\left(2 - 2\cos\left(\frac{\pi s}{n}\right)\right) = \prod_{s=1}^{n-1} 4\sin^2\left(\frac{\pi s}{2n}\right) =$$
$$= 2^{2(n-1)}\sin^2\left(\frac{\pi}{2n}\right)\sin^2\left(\frac{2\pi}{2n}\right)\ldots\sin^2\left(\frac{\pi(n-1)}{2n}\right).$$

Пункт б) доказывается аналогично.

Решение уравнений третьей и четвёртой степени

Любое уравнение

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{C},$$

с помощью замены

$$x = y - \frac{a_{n-1}}{n}$$

(если $a_{n-1} \neq 0$) сводится к уравнению

$$y^n + b_{n-2}y^{n-2} + \ldots + b_1 y + b_0 = 0, \quad b_i \in \mathbb{C}.$$

Упражнение 2.35 (решение уравнений третьей степени, формула Кардано). Покажите, что для $n = 3$ все решения кубического уравнения $x^3 + px + q = 0$ ($p, q \in \mathbb{C}$) имеют вид $u + v$, где $uv = -\frac{p}{3}$, u^3 и v^3 — корни квадратного уравнения $z^2 + qz - \frac{p^3}{27} = 0$. Таким образом, для всех трёх решений имеем формулу Кардано

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

где кубические корни u и v связаны соотношением $uv = -\frac{p}{3}$.

Если u_1 и v_1 — какие-либо значения корней

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad \text{и} \quad \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Ю-38

соответственно и $u_1v_1 = -\frac{p}{3}$, то корни находятся по правилу

$$x_1 = u_1 + v_1, \quad x_2 = u_1\omega + v_1\omega^2, \quad x_3 = u_1\omega^2 + v_1\omega,$$

где $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = \sqrt[3]{1}$.

Величина $D = -27q^2 - 4p^3$ называется *дискриминантом* многочлена $x^3 + px + q$. Условие $D = 0$ равносильно существованию кратного корня (при $D = 0$ и $p \neq 0$ имеем $x_1 = \frac{3q}{p}$, $x_2 = x_3 = -\frac{3q}{2p}$, при этом, если $\frac{3q}{p} = -\frac{3q}{2p}$, то имеется корень кратности 3; если $D = 0$ и $p = 0$, то $q = 0$, а уравнение принимает вид $x^3 = 0$).

Если $p, q \in \mathbb{R}$, то: при $D > 0$ имеется три различных действительных корня; при $D < 0$ имеется один действительный и два мнимых сопряжённых корня; при $D = 0$ все корни действительные, из них хотя бы два совпадают.

Примеры 2.36.

1) $x^3 + 5x^2 + 2x - 8 = 0$, $x_1 = 1$, $x_2 = -2$, $x_3 = -4$.

2) $x^3 - 6ix + 4(1 - i) = 0$, $x_1 = -1 - i$, $x_2 = -1 - i$, $x_3 = 2 + 2i$.

3) $x^3 + 9x^2 + 18x + 28 = 0$, $x_1 = -7$, $x_2 = -1 - i\sqrt{3}$, $x_3 = -1 + i\sqrt{3}$.

Упражнение 2.37 (решение уравнений четвёртой степени; Феррари, Эйлер). Для решения уравнения

$$x^4 + px^2 + qx + r = 0 \quad (p, q, r \in \mathbb{C})$$

рассматривается соответствующее кубическое уравнение

$$y^3 + 2py^2 + (p^2 - 4r)y - q^2 = 0.$$

Если y_1, y_2, y_3 — корни этого уравнения, то все корни исходного уравнения находятся по правилу

$$x = \frac{1}{2}\left(\sqrt{y_1} + \sqrt{y_2} + \sqrt{y_3}\right),$$

где выбор квадратных корней подчинён условию

$$\sqrt{y_1}\sqrt{y_2}\sqrt{y_3} = -q.$$

10-39

Конец лекции N10

Лекция N12

Задача 2.38. Решить уравнения

а) $x^4 + 2x^3 + x^2 - 1 = 0$,

Ответ: $-\frac{1}{2}(1 \pm \sqrt{5})$, $-\frac{1}{2}(1 \pm i\sqrt{3})$;

б) $x^4 + 2x^3 + 2x^2 + x - 7 = 0$,

Ответ: $-\frac{1}{2}\left(1 \pm i\sqrt{2\sqrt{29}+1}\right)$, $-\frac{1}{2}\left(1 \pm \sqrt{2\sqrt{29}-1}\right)$.

Замечание 2.39. Отметим, что общее уравнение пятой степени неразрешимо в радикалах, при этом существует критерий разрешимости в радикалах уравнения любой степени (Абель, Галуа).

Основная теорема алгебры комплексных чисел (теорема Гаусса, 1799 г.)

(теорема Гаусса)

Теорема 2.40. *Если $f(x) \in \mathbb{C}[x]$, $\deg f(x) \geqslant 1$, то существует корень $c \in \mathbb{C}$ многочлена $f(x)$, т. е. $f(c) = 0$.*

Доказательство.

$|f(x)|$!

Шаг 1 (существование абсолютного минимума вещественнозначной функции $|f(x)|$ на комплексных числах $\mathbb{C}$). Напомним, что

$$|z_1 z_2| = |z_1|\,|z_2|$$

и

$$|z_1| - |z_2| \leqslant |z_1 + z_2| \leqslant |z_1| + |z_2|$$

для $z_1, z_2 \in \mathbb{C}$.

Лемма 2.41. *Если $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_i \in \mathbb{C}$, $n \geqslant 1$, то найдётся радиус $0 < A \in \mathbb{R}$ такой, что*

$$|f(z)| > |f(0)| \ (= |a_0|) \quad \text{для всех } z \in \mathbb{C}, \quad |z| > A$$

(это означает, что вне круга радиуса A с центром в 0 значение функции $|f(x)|$ превосходит $|f(0)| = |a_0|$).

11-1 Лекция N 11 (18 октября 2011 г.)

Задача 2.38. Решить уравнения

а) $x^4 + 2x^3 + x^2 - 1 = 0$,

Ответ: $-\frac{1}{2}(1 \pm \sqrt{5})$, $-\frac{1}{2}(1 \pm i\sqrt{3})$;

б) $x^4 + 2x^3 + 2x^2 + x - 7 = 0$,

Ответ: $-\frac{1}{2}\left(1 \pm i\sqrt{2\sqrt{29}+1}\right)$, $-\frac{1}{2}\left(1 \pm \sqrt{2\sqrt{29}-1}\right)$.

Замечание 2.39. Отметим, что общее уравнение пятой степени неразрешимо в радикалах, при этом существует критерий разрешимости в радикалах уравнения любой степени (Абель, Галуа).

Основная теорема алгебры комплексных чисел (теорема Гаусса, 1799 г.)

(теорема Гаусса)

Теорема 2.40. *Если $f(x) \in \mathbb{C}[x]$, $\deg f(x) \geqslant 1$, то существует корень $c \in \mathbb{C}$ многочлена $f(x)$, т. е. $f(c) = 0$.*

$|f(x)|$!

Доказательство.

Шаг 1 (существование абсолютного минимума вещественнозначной функции $|f(x)|$ на комплексных числах $\mathbb{C}$). Напомним, что

$$|z_1 z_2| = |z_1|\,|z_2|$$

и

$$|z_1| - |z_2| \leqslant |z_1 + z_2| \leqslant |z_1| + |z_2|$$

для $z_1, z_2 \in \mathbb{C}$.

Лемма 2.41. *Если $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_i \in \mathbb{C}$, $n \geqslant 1$, то найдётся радиус $0 < A \in \mathbb{R}$ такой, что*

$$|f(z)| > |f(0)| \ (= |a_0|) \quad \text{для всех } z \in \mathbb{C}, \quad |z| > A$$

(это означает, что вне круга радиуса A с центром в 0 значение функции $|f(x)|$ превосходит $|f(0)| = |a_0|$).

11-2

Доказательство. Пусть $0 \neq z \in \mathbb{C}$. Тогда

$$f(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = z^n\left(1 + \frac{a_{n-1}}{z} + \ldots + \frac{a_0}{z^n}\right),$$

и поэтому

$$\begin{aligned} |f(z)| &= |z|^n \left|1 + \left(\frac{a_{n-1}}{z} + \ldots + \frac{a_0}{z^n}\right)\right| \geqslant \\ &\geqslant |z|^n \left(1 - \left|\frac{a_{n-1}}{z} + \ldots + \frac{a_0}{z^n}\right|\right) \geqslant \\ &\geqslant |z|^n \left(1 - \frac{|a_{n-1}|}{|z|} - \ldots - \frac{|a_0|}{|z|^n}\right) = \varphi(|z|), \end{aligned}$$

где

$$\varphi(t) = t^n \left(1 - \frac{|a_{n-1}|}{t} - \ldots - \frac{|a_0|}{t^n}\right) \quad \text{для} \quad t \in \mathbb{R}.$$

Ясно, что $\lim\limits_{t \to +\infty} \varphi(t) = +\infty$, и поэтому для любого C (например, для $C = |f(0)| = |a_0|$) найдётся $\mathbb{R} \ni A > 0$ такое, что для $t > A$ имеем $\varphi(t) > C$. Итак, если $|z| = t > A$, то

$$|f(z)| \geqslant \varphi(|z|) = \varphi(t) > C = |f(0)| = |a_0|. \quad \boxtimes$$

Так как функция $|f(z)|: \mathbb{C} \to \mathbb{R}$ непрерывна как композиция двух непрерывных функций $\mathbb{C} \to \mathbb{C}$, $z \mapsto f(z)$, $\mathbb{C} \to \mathbb{R}$, $w \mapsto |w|$ (или, если $z = u + vi$, $(u, v) \in \mathbb{R}^2$, то $f(z) = \psi_1(u, v) + \psi_2(u, v)i$, где $\psi_1(u, v)$ и $\psi_2(u, v)$ — многочлены с действительными коэффициентами от u, v, и поэтому $|f(z)| = \sqrt{\psi_1(u, v)^2 + \psi_2(u, v)^2}$ — непрерывная функция от (u, v)), то на замкнутом ограниченном множестве (компакте)

$$K = \{z \in \mathbb{C} \mid |z| \leqslant A\}$$

непрерывная функция $|f(z)|$ достигает своего минимума в точке $z_0 \in K$. В частности, $|f(z_0)| \leqslant |f(0)| = |a_0|$. Если $z \in \mathbb{C} \setminus K$, т. е. $|z| > A$, то, как мы видели,

$$|f(z_0)| \leqslant |f(0)| \leqslant |f(z)|.$$

Таким образом, в точке z_0 достигается абсолютный минимум функции $|f(z)|$ на $\mathbb{C}$.

Шаг 2. Мы покажем, что $f(z_0) = 0$, т. е. $c = z_0$ является корнем многочлена $f(x)$. Действительно, если $f(z_0) \neq 0$, то $|f(z_0)| > 0$ и, как показывает следующая лемма Даламбера, это допущение противоречит тому, что z_0 — абсолютный минимум функции $|f(x)|$.

11-3

Лемма 2.42 (лемма Даламбера). *Пусть $f(x) \in \mathbb{C}[x]$, $\deg f(x) \geqslant 1$, $f(z_0) \neq 0$ для $z_0 \in \mathbb{C}$. Тогда для любого $\varepsilon > 0$ найдётся такой элемент $y \in \mathbb{C}$, что $|y| < \varepsilon$ и $|f(z_0 + y)| < |f(z_0)|$.*

Доказательство. Если $z = z_0 + y$, т. е. $y = z - z_0$, то

$$f(z) = a_0 + a_1 z + \ldots + a_{n-1} z^{n-1} + z^n =$$
$$= c_0 + c_1 y + \ldots + c_{n-1} y^{n-1} + c_n y^n,$$

$c_i \in \mathbb{C}$

где $c_0 = f(z_0) \neq 0$ (при $y = 0$ имеем $z = z_0$), $c_n = 1$ (как коэффициент при y^n в $(z_0 + y)^n$).

Пусть $k > 0$ — наименьший номер слагаемого, для которого $c_k \neq 0$. Итак,

$$f(z) = c_0 + c_k y^k + c_{k+1} y^{k+1} + \ldots + c_n y^n.$$

Основное соображение заключается в том, что в окрестности точки z_0 (т. е. $y = 0$) поведение многочлена определяется первыми двумя членами $c_0 + c_k y^k$.

Сначала пусть y_0 — одно из решений уравнения $c_0 + c_k y^k = 0$ (т. е. $y_0^k = -\dfrac{c_0}{c_k}$, y_0 — один из k корней из комплексного числа $-\dfrac{c_0}{c_k}$). Если, далее, $t \in (0,1) \subseteq \mathbb{R}$, то $c_k y_0^k = -c_0$, и поэтому

$$f(z_0 + t y_0) = c_0 + c_k t^k y_0^k + c_{k+1} t^{k+1} y_0^{k+1} + \ldots + c_n t^n y_0^n =$$
$$= c_0(1 - t^k) + (c_{k+1} y_0^{k+1} + \ldots + c_n t^{n-(k+1)}) t^{k+1}.$$

Пропущено

Если $|c_{k+1}|\,|y_0|^{k+1} + \ldots + |c_n| = M$, то $|y_0|^n$ y_0^n

$$|f(z_0 + t y_0)| \leqslant |c_0|(1 - t^k) + M t^{k+1} = |c_0| \left(1 - t^k \left(1 - \frac{Mt}{|c_0|}\right)\right).$$

Выберем $t \in (0,1)$ достаточно малым, так, что $Mt < |c_0|$, $t|y_0| = |t y_0| < \varepsilon$. Тогда $0 < 1 - \dfrac{Mt}{|c_0|} < 1$, и поэтому

$$|f(z_0 + t y_0)| < |c_0| = |f(z_0)|, \quad |t y_0| < \varepsilon.$$

Таким образом, $y = t y_0$ удовлетворяет утверждению леммы. □

11-4

Теорема 2.43 (о разложении многочлена с комплексными коэффициентами в произведение линейных множителей). *Пусть* $f(x) \in \mathbb{C}[x]$, $\deg f(x) = n \geqslant 1$. *Тогда*

$$f(x) = a(x-\alpha_1)\dots(x-\alpha_n), \quad a, \alpha_1, \dots, \alpha_n \in \mathbb{C},$$

при этом это разложение единственное (с точностью до порядка сомножителей).

Доказательство. В силу теоремы Гаусса найдётся такое $c \in \mathbb{C}$, что $f(c) = 0$. По теореме Безу $(f(x) = (x-c)q(x) + f(c))$:

$$f(x) = (x-c)q(x), \quad q(x) \in \mathbb{C}[x], \quad \deg q(x) = n-1.$$

Применим далее теорему Гаусса к $q(x)$, если $n-1 \geqslant 1$. Продолжая этот процесс, убеждаемся в существовании разложения на линейные множители.

Пусть теперь

$$f(x) = a(x-\alpha_1)\dots(x-\alpha_n) = \\ = b(x-\beta_1)\dots(x-\beta_n), \quad a, b, \alpha_i, \beta_i \in \mathbb{C}, \ a \neq 0, \ b \neq 0.$$

Ясно, что $a = b$. Если $\alpha_i \neq \beta_j$ для всех $j = 1, \dots, n$, то

$$f(\alpha_i) = 0 = b(\alpha_i - \beta_1)\dots(\alpha_i - \beta_j) \neq 0.$$

Поэтому в оба разложения входит одинаковое множество различных корней. Убедимся в совпадении кратностей вхождения каждого корня в оба разложения. Действительно, если

$$f(x) = (x-\alpha)^r q_1(x) = (x-\alpha)^s q_2(x), \quad q_1(\alpha) \neq 0, \quad q_2(\alpha) \neq 0, \quad r < s,$$

то, сокращая в $\mathbb{C}[x]$ на $(x-\alpha)^r$, получаем $q_1(x) = (x-\alpha)^{s-r} q_2(x)$, и поэтому $q_1(\alpha) = 0$, что противоречит $q_1(\alpha) \neq 0$. □

$\mathbb{C}[x]$ без делителей нуля (ст. коэфф. произв.)

Следствие 2.44. *Если* $\alpha_1, \dots, \alpha_r$ — *различные корни многочлена* $f(x) \in \mathbb{C}[x]$, $k_1, \dots, k_r$ — *их кратности*, $n = \deg f(x)$, *то* $n = k_1 + \dots + k_n$ *(таким образом, многочлен степени* $n = \deg f$ *имеет ровно* n *корней с учётом их кратности).*

11-5

Замечание 2.45 (о неприводимых многочленах над полем комплексных чисел). По аналогии с определением простых чисел в кольце целых чисел $\mathbb{Z}$ многочлен $f(x) \in K[x]$, $\deg f(x) \geqslant 1$, называется *неприводимым*, если $f(x)$ нельзя представить в виде $f(x) = \varphi(x)\psi(x)$, $\deg\varphi(x) \geqslant 1$, $\deg\psi(x) \geqslant 1$. (иными словами, если $\varphi(x)$ — делитель многочлена $f(x)$, $\deg\varphi(x) \geqslant 1$, то $\deg\varphi(x) = n = \deg f(x)$).

Таким образом, мы установили, что *неприводимые многочлены над полем $\mathbb{C}$ комплексных чисел — это в точности многочлены первой степени*. Из единственности разложения на линейные множители над $\mathbb{C}$ получаем существование и единственность разложения на неприводимые многочлены над $\mathbb{C}$.

Лемма 2.46. *Если K — поле, $f(x), g(x) \in K[x]$, $\deg f(x) \leqslant n$, $\deg g(x) \leqslant n$, $f(x)$ и $g(x)$ совпадает в $(n+1)$-й различных точках $\alpha_1, \ldots, \alpha_{n+1} \in K$, то $f(x) = g(x)$.*

Доказательство. Пусть $h(x) = f(x) - g(x)$. Тогда если $h(x) \neq 0$, то $\deg h(x) \leqslant n$ и $h(\alpha_i) = f(\alpha_i) - g(\alpha_i) = 0$ для $i = 1, \ldots, n+1$. Но это противоречит тому, что число различных корней не превосходит степени многочлена. □

Следствие 2.47. *Если $|K| = \infty$ (в частности, для $K = \mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$), то формальное и функциональное определение равенства многочленов совпадают.*

Замечание 2.48. Для конечного поля $\mathbb{Z}_2$ разные многочлены x и x^2 в точках 0 и 1 принимают одинаковые значения, т. е. равны как функции их $\mathbb{Z}_2$ в $\mathbb{Z}_2$.

Теорема 2.49 (формулы Виета). *Если K — поле, $\alpha_1, \ldots, \alpha_n \in K$,*

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = (x - \alpha_1)\ldots(x - \alpha_n),$$

то

$$\begin{aligned}
&a_{n-1} = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n),\\
&a_{n-2} = \alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n,\\
&\ldots\\
&a_1 = (-1)^{n-1}(\alpha_1\alpha_2\ldots\alpha_{n-1} + \ldots + \alpha_2\alpha_3\ldots\alpha_n),\\
&a_0 = (-1)^n\alpha_1\alpha_2\ldots\alpha_n.
\end{aligned}$$

11-6 Лекция VII (18 октября 2011 г.)
(2-ой час)

Глава 1

Элементы теории групп

1.1. Начала теории групп

Определение 1.1.1. Непустое множество G с бинарной операцией $*\colon G \times G \to G$, $(a, b) \to a * b \in G$ для $a, b \in G$, называется *группой*, если:

1) операция ассоциативна (т. е. $(a * b) * c = a * (b * c)$ для всех $a, b, c \in G$);

2) существует нейтральный элемент $e \in G$ (т. е. $g * e = g = e * g$ для всех $g \in G$);

3) для каждого элемента $g \in G$ существует обратный элемент $g^{-1} \in G$ (т. е. $g * g^{-1} = e = g^{-1} * g$).

повтор

Замечание 1.1.2. Напомним, что нейтральный элемент (при мультипликативной записи называемый *единицей группы*) единственный. Действительно, если e и e' — два нейтральных элемента в группе G, то $eg = g = ge$, $e'g = g = ge'$ для всех $g \in G$. Но тогда

$$e' = ee' = e.$$

повтор

Замечание 1.1.3. Обратный элемент g^{-1} для элемента $g \in G$ определён однозначно. Действительно, если $f, h \in G$ — два обратных элемента для g, т. е. $fg = e = gf$, $hg = e = gh$, то $f = fe = f(gh) = (fg)h = eh = h$.

Лемма 1.1.4. *Если G — группа, $a, b, c \in G$, то*

1) *уравнение $ax = b$ имеет, и только одно, решение $x = a^{-1}b$;*

2) *уравнение $ya = b$ имеет, и только одно, решение $y = ba^{-1}$;*

3) *если $ab = ac$, то $b = c$; если $ba = ca$, то $b = c$;*

4) *уравнение $axb = c$ имеет единственное решение $x = a^{-1}cb^{-1}$;*

5) *если $x^2 = x$, то $x = e$;*

6) $(ab)^{-1} = b^{-1}a^{-1}$; $(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$; $(a^{-1})^{-1} = a$.

повтор

Доказательство.
1) Ясно, что $a(a^{-1}b) = b$. Если же $ax = b$ для $x \in G$, то $x = a^{-1}ax = a^{-1}b$.
2) Ясно, что $(ba^{-1})a = b$. Если же $ya = b$ для $y \in G$, то $y = (ya)a^{-1} = ba^{-1}$.
3), 4) и 5) следуют из 1) и 2).
6) проверяется непосредственно. □

11-7

1.2. Изоморфизм групп (первое появление на сцене)

Хотя изоморфизм групп (как частный случай гомоморфизмов групп) будет детально исследован позднее, в то же время на начальном этапе рассмотрения групп крайне необходимо понимать, какие группы надо считать «одинаковыми».

Определение 1.2.1. Пусть G и G' — группы. Отображение

$$\alpha\colon G \to G'$$

называется *изоморфизмом*, если:

1) $\alpha\colon G \to G'$ — биекция;

2) $\alpha(xy) = \alpha(x)\alpha(y)$ для всех элементов $x, y \in G$ (здесь: в левой части $xy \in G$ с операцией произведения группы G; в правой части $\alpha(x)\alpha(y) \in G'$ с операцией произведения группы G').

При этом говорят, что условие 2) означает, что биекция $\alpha\colon G \to G'$ согласована с операциями групп G и G'.

Символ $G_1 \cong G_2$ будет означать, что существует хотя бы один изоморфизм $\alpha\colon G_1 \to G_2$ между группами G_1 и G_2, при этом будем говорить, что группы G_1 и G_2 *изоморфны*, обозначение $G_1 \cong G_2$.

Замечание 1.2.2. Отношение $G_1 \cong G_2$ на классе групп является отношением эквивалентности:

1) $G \cong G$, поскольку тождественное отображение $1_G\colon G \to G$ — изоморфизм;

2) если $G_1 \cong G_2$ и $\alpha\colon G_1 \to G_2$ — изоморфизм, то $\alpha^{-1}\colon G_2 \to G_1$ — изоморфизм (действительно, для любых $u = \alpha(x)$, $v = \alpha(y) \in G_2$, $x, y \in G_1$:

$$\alpha^{-1}(uv) = \alpha^{-1}\big(\alpha(x)\alpha(y)\big) = \alpha^{-1}\big(\alpha(xy)\big) = xy = \alpha^{-1}(u)\alpha^{-1}(v)),$$

и поэтому $G_2 \cong G_1$;

3) если $G_1 \cong G_2$, $\alpha\colon G_1 \to G_2$ — изоморфизм, и $G_2 \cong G_3$, $\beta\colon G_2 \to G_3$ — изоморфизм, то $\beta\alpha\colon G_1 \to G_3$ — биекция, при этом для любых $x, y \in G_1$ имеем

$$(\beta\alpha)(xy) = \beta\big(\alpha(xy)\big) = \beta\big(\alpha(x)\alpha(y)\big) = \beta\big(\alpha(x)\big)\beta\big(\alpha(y)\big) = (\beta\alpha)(x)\beta\alpha(y),$$

и поэтому $\beta\alpha\colon G_1 \to G_3$ — изоморфизм групп, и следовательно, $G_1 \cong G_3$. ∎

Из определения изоморфизма групп ясно, что любое свойство группы G, выраженное в её мощности и её групповой операции, также выполнено во всех группах G', изоморфных $G' \cong G$ группе G. Например, если $G \cong G'$, $\alpha\colon G \to G'$ — изоморфизм, то:

Примеры

1) если G — конечная группа, то G' — конечная группа;

2) если G — p-группа, т. е. $|G| = p^k$, где p — простое число, то G' — p-группа;

3) если G — коммутативная группа, то G' — коммутативная группа (если $u = \alpha(x)$, $v = \alpha(y) \in G'$, $x, y \in G$, то $uv = \alpha(x)\alpha(y) = \alpha(xy) = \alpha(yx) = \alpha(y)\alpha(x) = vu$).

11-8

Упражнение 1.2.3.

1) Докажите, что следующие две группы G и G' изоморфны:

$$G = \{-1, 1\} = (\mathrm{U}(\mathbb{Z}), \cdot), \qquad \begin{array}{c|c|c} & -1 & 1 \\ \hline -1 & 1 & -1 \\ \hline 1 & -1 & 1 \end{array};$$

$$G' = \{0, 1\} = (\mathbb{Z}_2, +), \qquad \begin{array}{c|c|c} & 0 & 1 \\ \hline 0 & 0 & 1 \\ \hline 1 & 1 & 0 \end{array}.$$

Действительно, пусть $f\colon G \to G'$ — биекция, где $f(1) = 0$, $f(-1) = 1$. Так как

$$\begin{aligned}
&f(1 \cdot 1) = f(1) = 0 = 0 + 0 = f(1) + f(1),\\
&f\big((-1) \cdot 1\big) = f(-1) = 1 = 1 + 0 = f(-1) + f(1),\\
&f\big((-1) \cdot (-1)\big) = f(1) = 0 = 1 + 1 = f(-1) + f(-1),\\
&f\big(1 \cdot (-1)\big) = f(-1) = 1 = 0 + 1 = f(1) + f(-1),
\end{aligned}$$

то

$$f(x \cdot y) = f(x) + f(y)$$

для всех $x, y \in G$, таким образом, f — изоморфизм групп G и G'. □

Заметим, что в этом примере выбор для биекции $f\colon G \to G'$ был не велик: так как изоморфизм переводит нейтральный элемент в нейтральный, то мы обязаны положить $f(1) = 0$; но тогда $f(-1)$ обязано быть равным 1.

2) Если X и Y — два непустых множества и $\varphi\colon X \to Y$ — биекция, то группы подстановок $\mathrm{S}(X)$ и $\mathrm{S}(Y)$ изоморфны. В частности, если $|X| = n$, то $\mathrm{S}(X) \cong \mathrm{S}_n = \mathrm{S}(\{1, 2, \ldots, n\})$.

Действительно, если $\sigma \in \mathrm{S}(X)$, то $\varphi\sigma\varphi^{-1} \in \mathrm{S}(Y)$,

$$\begin{tikzcd}
X \arrow[r, "\sigma"] & X \arrow[d, "\varphi"] \\
Y \arrow[u, "\varphi^{-1}"] \arrow[r, "\varphi\sigma\varphi^{-1}"] & Y
\end{tikzcd}.$$

Соответствие $\sigma \mapsto \varphi\sigma\varphi^{-1}$ является биекцией $\mathrm{S}(X) \to \mathrm{S}(Y)$, поскольку:

а) если $\varphi\sigma_1\varphi^{-1} = \varphi\sigma_2\varphi^{-1}$ для $\sigma_1, \sigma_2 \in \mathrm{S}(X)$, то $\sigma_1 = \varphi^{-1}(\varphi\sigma_1\varphi^{-1})\varphi = \varphi^{-1}(\varphi\sigma_2\varphi^{-1})\varphi = \sigma_2$;

б) если $\sigma \in \mathrm{S}(Y)$, то $\sigma = \varphi(\varphi^{-1}\sigma\varphi)\varphi^{-1}$, где $\varphi^{-1}\sigma\varphi \in \mathrm{S}(X)$. Так как $\varphi(\sigma_1\sigma_2)\varphi^{-1} = (\varphi\sigma_1\varphi^{-1})(\varphi\sigma_2\varphi^{-1})$, то это соответствие является изоморфизмом групп $\mathrm{S}(X)$ и $\mathrm{S}(Y)$. ■

11-9

Примеры групп

1. Целые числа $\mathbb{Z}$, рациональные числа $\mathbb{Q}$, действительные числа $\mathbb{R}$, комплексные числа $\mathbb{C}$ с операцией сложения, при этом никакие две из групп $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ не являются изоморфными, хотя $(\mathbb{R},+) \cong (\mathbb{C},+)$ (поскольку $\dim_{\mathbb{Q}} \mathbb{R} = \dim_{\mathbb{Q}} \mathbb{C}$).

Заметим, что: а) натуральные числа $\mathbb{N}$ с операцией сложения группой не являются (отсутствует нейтральный элемент); б) натуральные числа с нулём $\mathbb{N}_0$ также не являются группой (обратный элемент (в аддитивной записи обычно называемый противоположным элементом) существует только для 0; таким образом, например, 1 уже не имеет обратного элемента).

2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ ($K^* = K \setminus \{0\}$ для любого поля K) относительно умножения являются группами (называемыми *мультипликативными группами* соответствующих *полей*).

3. $\mathbb{Q}_+ = \{q \in \mathbb{Q} \mid q > 0\}$, $\mathbb{R}_+ = \{r \in \mathbb{R} \mid r > 0\}$ с операциями умножения являются группами.

4. $\mathrm{U}(\mathbb{Z}) = \{1, -1\}$ — группа обратимых элементов в кольце целых чисел $\mathbb{Z}$ с операцией умножения. Более общим образом, если R — ассоциативное кольцо с 1, то обратимые элементы $\mathrm{U}(R)$ кольца R являются группой с операцией умножения.

5. Линейная группа $\mathrm{GL}_n(K)$ обратимых $(n \times n)$-матриц над полем K ($\mathrm{GL}_n(K) = \mathrm{U}(\mathrm{M}_n(K))$, где $\mathrm{M}_n(K)$ — кольцо $(n \times n)$-матриц над полем K). Специальная линейная группа $\mathrm{SL}_n(K)$ матриц $A \in \mathrm{M}_n(K)$ таких, что $|A| = 1$. Ортогональная группа $\mathrm{O}_n(K) = \{A \in \mathrm{M}_n(K) \mid |A| \neq 0,\ A^{-1} = A^*\}$.

6. Группа комплексных чисел $z \in \mathbb{C}$ таких, что $|z| = 1$, с операцией умножения. Группа $\{z \in \mathbb{C} \mid z^n = 1\}$ комплексных корней n-й степени из 1, $n \in \mathbb{N}$.

7. Группа подстановок S_n, $n \geqslant 1$; группа чётных подстановок A_n. Для произвольного непустого множества M группа $\mathrm{S}(M)$ всех *биекций* $f\colon M \to M$ с операцией умножения.

Замечание 1.2.4. Множество $\mathrm{T}(M)$ всех отображений $f\colon M \to M$ с операцией умножения (т. е. композицией) является *полугруппой* (т. е. множеством с ассоциативной бинарной операцией), но не является группой при $|M| > 1$ (существуют отображения $f\colon M \to M$, не являющиеся биекций и, следовательно, не имеющие обратного отображения).

Замечание 1.2.5. Полугруппа $\mathrm{T}(M)$ коммутативна тогда и только тогда, когда $|M| = 1$. Действительно, если $|M| \geqslant 2$, то для $a, b \in M$, $a \neq b$, имеем

$$f_a f_b = f_a \neq f_b = f_b f_a,$$

где $f_c(x) = c$ для всех $x \in M$, $c \in M$.

Замечание 1.2.6. Группа S_n коммутативна тогда и только тогда, когда $n \leqslant 2$ (в частности, группы S_n при $n \geqslant 3$ уже некоммутативны). Действительно, при $n \geqslant 3$ для циклов $(1\,2)$, $(1\,3)$:

$$(1\,3)(1\,2) \neq (1\,2)(1\,3).$$

Замечание 1.2.7. Линейная группа $\mathrm{GL}_n(R) = \mathrm{U}(\mathrm{M}_n(R))$, где $\mathrm{M}_n(R)$ — кольцо $(n \times n)$-матриц над кольцом R, коммутативна тогда и только тогда, когда $n = 1$ и группа $\mathrm{U}(R)$ обратимых элементов кольца R коммутативна.

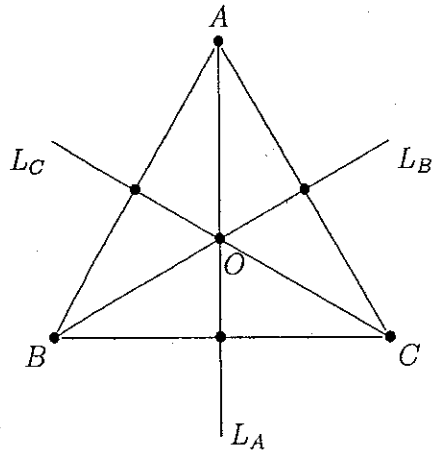
Действительно, если $\mathrm{GL}_n(R)$ — коммутативная группа, то $n = 1$ (при $n \geqslant 2$: $E+E_{12}, E+E_{21} \in \mathrm{GL}_n(R)$, но $(E+E_{12})(E+E_{21}) = E+E_{12}+E_{21}+E_{11} \neq E+E_{12}+E_{21}+E_{22} = (E+E_{21})(E+E_{12})$) и $\mathrm{U}(R) = \mathrm{GL}_1(R)$ — коммутативная группа.

11-10

8. Группа симметрий. Пусть V — евклидово аффинное пространство $\mathbb{R}^2$ или $\mathbb{R}^3$. Под *изометрией* пространства V понимается биекция $\alpha\colon V \to V$, сохраняющая расстояние (примеры: переносы; вращения; отражения). Если $\varnothing \neq X \subset V$, то будем говорить, что изометрия α является *симметрией* множества X, если $X = \alpha(X)$ $(= \{\alpha(x) \mid x \in X\})$, при этом возможно, что $x \neq \alpha(x)$. Совокупность $\mathrm{Sym}(X)$ всех симметрий α множества $\varnothing \neq X \subseteq V$ образует группу (*группа симметрий* $\mathrm{Sym}(X)$, подгруппа группы $\mathrm{S}(X)$).

!!

а) Пусть T — правильный треугольник с вершинами A, B и C, с высотами-медианами L_A, L_B и L_C, с центром описанной окружности O:



Рассмотрим совокупность D_3 симметрий правильного треугольника T (т. е. все сохраняющие расстояние отображения $f\colon P \to P$ плоскости $P = \mathbb{R}^2$ такие, что $f(T) = T$). С операцией композиции D_3 — группа. Рассмотрим её элементы:

- $e = 1_P$, $1_P(x) = x$ для всех $x \in P$;
- φ_1, φ_2 — два вращения плоскости P против часовой стрелки, соответственно на углы 120° и 240°;
- θ_1, θ_2, θ_3 — три зеркальных отображения плоскости P, соответственно относительно прямых L_A, L_B, L_C.

Как результат, получаем таблицу умножения для группы D_3:

	e	φ_1	φ_2	θ_1	θ_2	θ_3
e	e	φ_1	φ_2	θ_1	θ_2	θ_3
φ_1	φ_1	φ_2	e	θ_3	θ_1	θ_2
φ_2	φ_2	e	φ_1	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	e	φ_1	φ_2
θ_2	θ_2	θ_3	θ_1	φ_2	e	φ_1
θ_3	θ_3	θ_1	θ_2	φ_1	φ_2	e

(из которой также видно, что D_3 — группа).

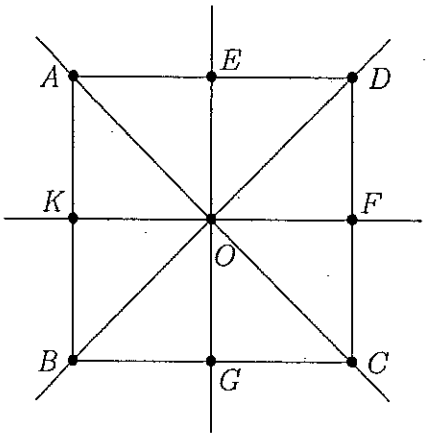
11–11

Если $S = \{1 = A,\ 2 = B,\ 3 = C\}$ — множество вершин правильного треугольника T, то каждому элементу группы D_3 поставим в соответствие подстановку вершин треугольника T:

$$e \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \varphi_1 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \varphi_2 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\theta_1 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \theta_2 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \theta_3 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Проверьте, что данная биекция осуществляет изоморфизм группы симметрий треугольника D_3 и группы подстановок S_3.

б) Пусть в данном примере T — квадрат в плоскости $P = \mathbb{R}^2$ с вершинами A, B, C, D, центром O, с серединами рёбер E, F, G, K:



Рассмотрим группу симметрий D_4 квадрата $ABCD$. Она состоит: из четырёх вращений на 0°, 90°, 180°, 270°; из четырёх отражений относительно прямых L_{AC}, L_{BD}, L_{EG}, L_{KF}. Выпишите для группы D_4, $|\mathrm{D}_4| = 8$, таблицу умножения.

Каждому элементу из D_4 поставим в соответствие подстановку множества вершин $\{A = 1,\ B = 2,\ C = 3,\ D = 4\}$. Например, повороту на 90° соответствует подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Эта биекция осуществляет вложение (≡ инъективный гомоморфизм) группы D_4 в группу подстановок S_4. Отметим, что $|\mathrm{D}_4| = 8$, $|\mathrm{S}_4| = 24$, поэтому не все подстановки из S_4 лежат в образе этой биекции. Например, подстановка

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

не является результатом никакой симметрии квадрата.

9. Группа симметрий правильного n-угольника (диэдральная группа $\mathrm{Dih}(2n)$ порядка $2n$) состоит: из n поворотов правильного n-угольника против часовой стрелки вокруг его центра (включая тождественное отображение); из n отражений относительно оси симметрии (если n нечётное, то ось отражения определяется вершиной и серединой противоположного ребра; если n чётное, то имеется два типа отражений, определяемых

11–12

парой противоположных вершин и определяемых серединами противоположных рёбер, $(1/2)\,n + (1/2)\,n = n$). При $n \geqslant 4$ имеем $2n < n!$, и поэтому $\mathrm{Dih}(2n)$ — собственная подгруппа в S_n.

10. Группы строк K^n, группы прямоугольных матриц $\mathrm{M}_{m,n}(K)$ над полем K с операциями сложения.

11. Пусть

$$G = \{A = (a_{ij}) \in \mathrm{M}_2(\mathbb{R}) \mid a_{ij} \geqslant 0\}.$$

Тогда $(G, +)$ — моноид, не являющийся группой.

12. Пусть X — непустое множество, $\mathrm{P}(X)$ — совокупность всех его подмножеств (включая пустое), $S * T = (S \cup T) - (S \cap T)$ для $S, T \in \mathrm{P}(X)$. Тогда $(\mathrm{P}(X), *)$ — коммутативная группа.

13. Группа Дирака. В квантовой теории поля операторы рождения и уничтожения $\gamma_1, \ldots, \gamma_n$ $(n = 2m)$ удовлетворяют соотношениям антикоммутативности

$$\gamma_i\gamma_j + \gamma_j\gamma_i = 2\delta_{ij} \quad (1 \leqslant i, j \leqslant n).$$

Поэтому операторы

$$\pm\gamma_1^{i_1}\gamma_2^{i_2}\ldots\gamma_n^{i_n} \quad (i_j = 1 \text{ или } 2)$$

образуют группу $\mathrm{G}(n)$ порядка $g(n) = 2^{n+1}$. В случае, когда $n = 4$, группа $\mathrm{G}(4)$ называется *группой Дирака*, $|\mathrm{G}(4)| = 32$.

14. Пусть $C([0,1])$, $C(\mathbb{R})$ — множества всех непрерывных вещественнозначных функций на отрезке $[0,1]$ и на вещественной прямой $\mathbb{R}$ соответственно, пусть $D\big((0,1)\big)$ и $D(\mathbb{R})$ — множества всех дифференцируемых вещественнозначных функций на интервале $(0,1)$ и на вещественной прямой $\mathbb{R}$ соответственно. Тогда $(C([0,1]), +)$, $(C(\mathbb{R}), +)$, $\big(D\big((0,1)\big), +\big)$, $(D(\mathbb{R}), +)$ — абелевы группы.

15. Пусть $G = (G, \cdot)$ — группа, $a \in G$. Тогда $G = (G, *)$, $x * y = xay$ для $x, y \in G$, также является группой, при этом $(G, \cdot) \cong (G, *)$.

Действительно, для $x, y, z \in G$ имеем

$$(x * y) * z = (xay)az = xa(yaz) = x * (y * z),$$

поэтому операция $*$ ассоциативна.

Так как для всех $x \in G$ имеем

$$a^{-1} * x = a^{-1}ax = x = xaa^{-1} = x * a^{-1},$$

то a^{-1} является нейтральным элементов в $(G, *)$.

Если $x \in G$, то

$$x * (a^{-1}x^{-1}a^{-1}) = xaa^{-1}x^{-1}a^{-1} = a^{-1},$$
$$(a^{-1}x^{-1}a^{-1}) * x = a^{-1}x^{-1}a^{-1}ax = a^{-1},$$

и поэтому $a^{-1}x^{-1}a^{-1}$ является обратным для элемента x относительно операции $*$.

Итак, $(G, *)$ — группа.

Рассмотрим биективное отображение

$$f\colon (G, \cdot) \to (G, *), \quad f(x) = xa^{-1} \quad \text{для} \quad x \in G.$$

Так как для $x, y \in G$

$$f(xy) = xya^{-1} = xa^{-1}aya^{-1} = (xa^{-1})a(ya^{-1}) = f(x) * f(y),$$

то f — изоморфизм, $(G, \cdot) \cong (G, *)$. ☒

11–13

Упражнение 1.2.8. $|\mathrm{SL}_2(\mathbb{Z}_p)| = p(p^2-1)$.

Упражнение 1.2.9.

1) Пусть $c \in \mathbb{R}$, $c > 0$, $G = \{r \in \mathbb{R} \mid -c < r < c\}$ $(= (-c, c))$. Показать, что $(G, *)$ — группа, где

$$a * b = \frac{a+b}{1+\dfrac{ab}{c^2}}$$

(сложение скоростей в специальной теории относительности).

2) Если G — группа, в которой $x^2 = 1$ для всех $x \in G$, то G — абелева группа.

3) а) Докажите, что если в группе G $(xy)^2 = x^2y^2$ для всех $x, y \in G$, то группа G коммутативна.

б) Если для любых элементов x, y группы G найдётся число n такое, что $(xy)^i = x^iy^i$ для $i = n, n+1, n+2$, то группа G коммутативна.

4) Если G — конечная группа порядка $n = |G|$, $g_1, g_2, \ldots, g_n$ — её элементы, то рассмотрим *таблицу умножения*

$$M = (m_{ij} = g_ig_j) \in \mathrm{M}_n(G).$$

В частности, i-я строка этой матрицы имеет вид

$$(g_ig_1, g_ig_2, \ldots, g_ig_n).$$

Все элементы в этой строке различны: из $g_ig_j = g_ig_k$ следует, что $g_j = g_k$, т. е. $j = k$. Это же верно и для столбцов.

Таким образом, каждый элемент группы появляется в точности один раз в каждой строке и в каждом столбце матрицы M (т. е. M является *латинским квадратом*).

5) Таблица умножения группы Клейна. Пусть

$$G = \{e,\ a = (1\,2)(3\,4),\ b = (1\,3)(2\,4),\ c = (1\,4)(2\,3)\} \subseteq \mathrm{S}_n,\ n \geqslant 4, \text{ —}$$

группа Клейна V_4 (*четверная группа*). Её таблица умножения:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Матричная реализация группы Клейна V_4 состоит из четырёх (2×2)-матриц в $\mathrm{M}_2(\mathbb{R})$:

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\quad a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\quad b = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},\quad c = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

11–14

6) Группа кватернионов $\mathbb{Q}_8$ состоит из восьми матриц из $\mathrm{M}_4(\mathbb{R})$: $\pm E$, $\pm i$, $\pm j$, $\pm k$, где

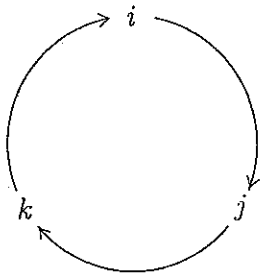
$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

с операцией умножения матриц. Отметим, что:

$$i^2 = j^2 = k^2 = -E, \quad ij = k$$

(остальные произведения вычисляются через эти равенства, например: $ijk = k^2 = -E$, $-i = i(ijk) = i^2jk = -jk$, отсюда $jk = i$; $jki = i^2 = -E$, $-j = j(jki) = j^2ki = -ki$, отсюда $ki = j$; $ji = (ki)i = k(ii) = -k$; $kj = (ij)j = i(jj) = -i$; $ik = (jk)k = j(kk) = -j$). Итак:



$$\begin{aligned} ij &= k, & & ji = -k, \\ jk &= i, & \text{но} \quad & kj = -i, \\ ki &= j, & & ik = -j. \end{aligned}$$

7) Матрицы

$$\pm E = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm I = \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \pm J = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm K = \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

относительно операции умножения в группе $\mathrm{GL}_2(\mathbb{C})$ образуют подгруппу, изоморфную группе кватернионов $\mathbb{Q}_8$.

8) **Таблица умножения для группы S_3 и её подгруппы A_3.**

а) Выпишем элементы группы S_3, $|\mathrm{S}_3| = 6$, например, в следующем порядке:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2), \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3),$$

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3), \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2).$$

11-15

Тогда

	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_2	τ_3	τ_1
σ_2	σ_2	e	σ_1	τ_3	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	e	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	e	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_1	e

(так как $\sigma_1\tau_1 = \tau_2 \neq \tau_3 = \tau_1\sigma_1$, то S_3 — некоммутативная группа).

б) В этих обозначениях

$$A_3 = \{e,\ \sigma_1,\ \sigma_2\} = \langle\sigma_1\rangle = \langle\sigma_2\rangle, \quad |A_3| = 3;$$

	e	σ_1	σ_2
e	e	σ_1	σ_2
σ_1	σ_1	σ_2	e
σ_2	σ_2	e	σ_1

Условия, при которых моноид оказывается группой

Моноид $(M, \cdot, e)$ называется

сократимым слева, если из $ab = ac$ следует, что $b = c$;

сократимым справа, если из $ba = ca$ следует, что $b = c$.

Моноид $(\mathbb{N}, \cdot, 1)$ сократим, но группой не является.

Лемма 1.2.10. *Если подмножество M группы G является моноидом относительно операции в группе G (т. е.: $m_1m_2 \in M$ для всех $m_1, m_2 \in M$; $e \in M$), то M — сократимый моноид.*

Лемма 1.2.11. *Пусть S — полугруппа, в которой:*

1) *существует правая единица (правый нейтральный элемент) e, т. е. $se = s$ для всех $s \in S$;*

2) *каждый элемент $x \in S$ обладает правым обратным $y \in S$ (относительно правой единицы e), т. е. $xy = e$.*

Тогда S является группой:

а) $yx = e$;

б) $ex = x$.

При этом:

11-16

в) *e — единственный левый единичный (левый нейтральный) элемент в S, а также e — единственный правый единичный (правый нейтральный) элемент в S;*

г) *y — единственный левый обратный для x, а также y — единственный правый обратный для x.*

Доказательство.

а) Пусть $x \in S$, $xy = e$. Рассмотрим $z = yx$. Тогда

$$zz = (yx)(yx) = y(xy)x = (ye)x = yx = z.$$

Если $zw = e$, то

$$e = zw = (zz)w = z(zw) = ze = z.$$

Итак, $yx = z = e$, следовательно, y — двусторонний обратный элемент для x.

б) В силу а):

$$x = xe = x(yx) = (xy)x = ex.$$

Итак, e — двусторонний единичный (нейтральный) элемент полугруппы S.

Из а) и б) следует, что S — группа.

в) В силу б) любая правая единица e является левой единицей. Пусть e' — некоторая левая единица, тогда $e' = e'e = e$.

г) В силу а) любой правый обратный y для x является левым обратным для x. Пусть t — некоторый левый обратный для x, тогда

$$t = te = t(xy) = (tx)y = ey = y. \qquad \square$$

l_m r_m

Пусть M — моноид, $m \in M$. Через $l_m\colon M \to M$, $l_m(k) = mk$ для всех $k \in M$, обозначим *отображение левого умножения* на элемент m (аналогично определяется $r_m\colon M \to M$, $r_m(k) = km$, — *отображение правого умножения* на элемент m).

Лемма 1.2.12. *Если M — моноид, $m \in M$, тогда:*

1) *отображение $l_m\colon M \to M$ инъективно тогда и только тогда, когда $mk \neq ml$ для всех $k, l \in M$, $k \neq l$;*

2) *отображение $l_m\colon M \to M$ сюръективно тогда и только тогда, когда элемент m обратим справа.*

Доказательство.

1) Записано определение инъективности для отображения l_m.

2) Если l_m — сюръективное отображение и $e = l_m(k) = mk$ для некоторого $k \in M$, то m обратим справа.

Так как $mk = e$, то $l = mkl = l_m(kl)$ для всех l. Итак, l_m — сюръекция. $\square$

!

l

Следствие 1.2.13. *Если G — группа, то для любого элемента $g \in G$ отображения*

$$l_g\colon G \to G, \quad l_g(x) = gx,$$
$$r_g\colon G \to G, \quad r_g(x) = xg,$$

являются биекциями. $\square$

11-17

Теорема 1.2.14. *Любой конечный моноид с сокращением (справа) является группой.*

Доказательство. Так как M — моноид с сокращением справа, то для всех $m \in M$ отображения l_m инъективны. Поэтому, поскольку $|M| < \infty$, все отображения l_m сюръективны, т. е. каждый элемент $m \in M$ обратим справа. В силу леммы 1.2.11 M — группа. □

Следствие 1.2.15. *Любой конечный подмоноид M группы G является группой (подгруппой группы G).*

Доказательство. Подмоноид группы сократим. Если он конечен, то он является группой. □

Задача 1.2.16. Любая конечная подполугруппа группы является группой (подгруппой группы G).

Следствие 1.2.17 (о группе Эйлера). *Пусть $\mathbb{Z}_m$ — кольцо вычетов по модулю m. Тогда*

$$\mathrm{Eu}(m) \equiv \mathrm{U}(\mathbb{Z}_m) = \{k \in \mathbb{N} \mid 1 \leqslant k < m,\ (k,m) = 1\}.$$

Доказательство. Пусть $G = \{k \in \mathbb{N} \mid 1 \leqslant k < m,\ (k,m) = 1\}$.

1) Если $k_1, k_2 \in G$, т. е. $(k_1, m) = 1$ и $(k_2, m) = 1$, то $(k_1k_2, m) = 1$, т. е. $k_1k_2 \in G$.

Если $k, l, n \in G$ и $kl = kn$ в $\mathbb{Z}_m$, то

$$kl - kn = k(l - n) = mq, \quad q \in \mathbb{Z},$$

поэтому, поскольку $(k, m) = 1$, m делит $l - n$, т. е. $l = n$ в $\mathbb{Z}_m$.

Итак, G — конечный моноид с сокращением. Следовательно, G — группа, и поэтому $G \subseteq \mathrm{U}(\mathbb{Z}_m)$.

2) Пусть $k \in \mathrm{U}(\mathbb{Z}_m)$, $kl = 1$ для $l \in \mathbb{Z}_m$, тогда $(k, m) = 1$, поскольку если $d \in \mathbb{N}$ — общий делитель чисел k и m, то $k = dq_1$, $m = dq_2$, то для $q \in \mathbb{Z}$ имеем

$$1 = kl + mq = dq_1l + dq_2q = d(q_1l + q_2q).$$

Итак, $d = 1$. □

Следствие 1.2.18. *Для любого простого числа p кольцо вычетов $\mathbb{Z}_p$ является полем.*

Доказательство. $\mathrm{U}(\mathbb{Z}_p) = \{1, 2, \ldots, p-1\} = \mathbb{Z}_p \setminus \{0\}$, итак, $\mathbb{Z}_p$ — поле. □

Следствие 1.2.19. *Если p — простое число, $i, t \in \mathbb{Z}$, $t \not\equiv 0 \pmod p$, то*

$$\{i, i+t, \ldots, i+(p-1)t\} -$$

различные элементы по $\mathrm{mod}\, p$ (т. е. $\bar{i}, \bar{i}+\bar{t}, \ldots, \bar{i}+\overline{(p-1)t}$, где $\bar{i} = i + \mathbb{Z}p$, $\bar{t} = t + \mathbb{Z}p \in \mathbb{Z}_p$, — различные элементы поля вычетов $\mathbb{Z}_p$).

Доказательство. Так как $\bar{t} \in \mathrm{Eu}(p) \equiv \mathrm{U}(\mathbb{Z}_p)$ и элементы

$$\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$$

различны в $\mathbb{Z}_p$, то все элементы

$$\{\bar{0}, \bar{t}, \overline{2t}, \ldots, \overline{(p-1)t}\}$$

различны в поле $\mathbb{Z}_p$, и поэтому различны в поле $\mathbb{Z}_p$ элементы

$$\{\bar{i}, \overline{i+t}, \ldots, \overline{i+(p-1)t}\},$$

получаемые сдвигом на элемент i в группе $(\mathbb{Z}_p, +)$. □

11–18

Следствие 1.2.20 (ранее мы получили это утверждение как следствие теоремы Евклида). *Если $m, n \in \mathbb{Z}$ и $(m, n) = 1$, то найдутся $u, v \in \mathbb{Z}$ такие, что $mu + nv = 1$.*

Доказательство. Так как $(m, n) = 1$, то $\bar{n} \in \mathrm{Eu}(m) \equiv \mathrm{U}(\mathbb{Z}_m)$, пусть $\bar{k} = \bar{n}^{-1} \in \mathrm{Eu}(m)$. Тогда $1 - kn = mq$ для некоторого $q \in \mathbb{Z}$. Итак, $mq + kn = 1$ (можно взять $u = q$, $v = k$). □

Обратимые элементы моноида

Лемма 1.2.21. *Совокупность*

$$\mathrm{U}(M) = \{m \in M \mid \exists m^{-1} \in M\}$$

обратимых элементов моноида $(M, \cdot)$ является группой ($\mathrm{U}(M)$ — наибольшая подгруппа в M, т. е. подгруппа $\mathrm{U}(M)$ содержит каждую подгруппу моноида M).

Доказательство.

1) Если $a, b \in \mathrm{U}(M)$, то $(ab)^{-1} = b^{-1}a^{-1}$, поэтому $ab \in \mathrm{U}(M)$. Таким образом, подмножество $\mathrm{U}(M)$ замкнуто относительно операции моноида M.

2) Ассоциативность операции $(\mathrm{U}(M), \cdot)$, очевидно, следует из ассоциативности операции $(M, \cdot)$.

3) Если e — нейтральный элемент моноида M, то $e^{-1} = e$, поэтому $e \in \mathrm{U}(M)$. Ясно, что e — нейтральный элемент в $\mathrm{U}(M)$.

4) Если $m \in \mathrm{U}(M)$, то существует $m^{-1} \in M$. Так как $(m^{-1})^{-1} = m$, то $m^{-1} \in \mathrm{U}(M)$ и является обратным элементом в $(\mathrm{U}(M), \cdot)$ для m.

Итак, мы проверили, что $(\mathrm{U}(M), \cdot)$ — группа. Из определения подгруппы $\mathrm{U}(M)$ в M ясно, что это наибольшая подгруппа в M. □

Это простое соображение даёт много интересных примеров групп.

а) Как мы видели, если в качестве моноида M рассмотреть моноид $M = T(X) = \{f \colon X \to X\}$ преобразований множества X с операцией композиция отображений, то

$$\mathrm{U}(T(X)) = \mathrm{S}(X) = \{f \colon X \to X,\ f \text{ — биекция}\} \text{ —}$$

группа подстановок на множестве X.

б) Если $(R, +, \cdot, 1)$ — кольцо с единицей, то, конечно, $(R, \cdot, 1)$ — моноид, и поэтому

$$\mathrm{U}(R) = \mathrm{U}((R, \cdot, 1)) = \{r \in R \mid \exists s = r^{-1} \in R,\ rs = 1 = sr\} \text{ —}$$

группа, называемая *группой обратимых элементов кольца R*.

в) Если $R = \mathrm{M}_n(K)$ — кольцо $(n \times n)$-матриц над полем K, то

$$\mathrm{U}(R) = \mathrm{GL}_n(K) = \{A \in \mathrm{M}_n(K) \mid |A| \neq 0\} \text{ —}$$

линейная группа (группа обратимых матриц, она изоморфна группе обратимых линейных отображений n-мерного линейного пространства над полем K).

г) Ясно, что $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}$.

д) Если $R = \mathbb{Z}_m$ — кольцо вычетов по модулю m, $m \in \mathbb{N}$, то

$$\mathrm{U}(R) = \mathrm{Eu}(m) = \{k \in \mathbb{Z}_m \mid 1 \leqslant m < n,\ (k, m) = 1\} \text{ —}$$

11-19

группа Эйлера обратимых элементов кольца вычетов $\mathbb{Z}_m$. Например $\mathrm{Eu}(2) = \{1\}$, $\mathrm{Eu}(3) = \{1,2\}$, $\mathrm{Eu}(4) = \{1,3\}$, $\mathrm{Eu}(5) = \{1,2,3,4\}$, $\mathrm{Eu}(6) = \{1,5\}$, $\mathrm{Eu}(7) = \{1,2,3,4,5,6\}$, $\mathrm{Eu}(8) = \{1,3,5,7\}$. Ясно, что $\mathrm{Eu}(p) = \{1,\dots,p-1\}$ для простого числа p.

Число элементов $\varphi(m) = |\mathrm{Eu}(m)|$ называется *числом Эйлера*. Из этих примеров: $\varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$, $\varphi(5) = \varphi(8) = 4$, $\varphi(7) = 6$, $\varphi(p) = p-1$ для простого числа p.

e) Если K — поле, то $\mathrm{U}(K) = K^* = K \setminus \{0\}$ — *мультипликативная группа* поля K.

Условие Дедекинда для моноида

Представляет интерес следующее *условие Дедекинда* для моноида: «$ab = 1 \implies ba = 1$».

Ясно, что в любой группе G для $a, b \in G$ из $ab = e$ следует, что $b = a^{-1}$, и поэтому $ba = a^{-1}a = e$. Итак, в любой группе выполнено условие Дедекинда.

Лемма 1.2.22. *Если $(M, \cdot, e)$ — конечный моноид, то для любых элементов $a, b \in M$ из $ab = e$ следует $ba = e$, т. е. в конечном моноиде выполнено условие Дедекинда.*

Доказательство. Если $ab = e$, то для $m \in M$ имеем:

$$(l_a l_b)(m) = l_a(l_b(m)) = l_a(bm) = abm = l_{ab}(m);$$
$$l_{ab}(m) = abm = em = 1_m.$$

Итак, $l_a l_b = l_{ab} = 1_M$. Поэтому $l_a\colon M \to M$ — сюръекция.

Так как M — конечное множество, то $l_a\colon M \to M$ — биекция и, следовательно, существует $(l_a)^{-1} \in \mathrm{T}(M)$. Тогда

$$(l_a)^{-1} = (l_a)^{-1} 1_M = l_a^{-1} l_a l_b = l_b,$$

поэтому

$$l_{ba} = l_b l_a = l_b (l_a)^{-1} = 1_M,$$
$$ba = bae = l_{ba}(e) = 1_M(e) = e. \qquad \square$$

Замечание 1.2.23.

1) Условие конечности моноида в этом утверждении существенно. Например, если $M = \mathrm{T}(\mathbb{N}) = \{f\colon \mathbb{N} \to \mathbb{N}\}$, $f \in \mathrm{T}(\mathbb{N})$, $f(1) = 1$, $f(m) = m-1$ для $m > 1$, $g \in \mathrm{T}(\mathbb{N})$, $g(n) = n+1$ для $n \in \mathbb{N}$, то $fg = 1_{\mathbb{N}}$, поскольку для всех $n \in \mathbb{N}$ имеем

$$(fg)(n) = f(g(n)) = f(n+1) = n = 1_{\mathbb{N}}(n).$$

Однако $gf \neq 1_{\mathbb{N}}$, поскольку

$$(gf)(1) = g(f(1)) = g(1) = 2 \neq 1 = 1_{\mathbb{N}}(1).$$

2) Напомним (см. ??), что в моноиде по умножению $(n \times n)$-матриц $(\mathrm{M}_n(K), \cdot)$ над полем K для любых $A, B \in \mathrm{M}_n(K)$ из $AB = E$ следует, что $BA = E$. Действительно, если $AB = E$, то $|A||B| = |AB| = |E| = 1$, поэтому $|A| \neq 0$ и существует обратная матрица A^{-1}. Следовательно, $B = A^{-1}AB = A^{-1}E = A^{-1}$, и поэтому $BA = A^{-1}A = E$. Итак, в моноиде $(\mathrm{M}_n(K), \cdot)$ выполнено условие Дедекинда.

повтор

11-20

1.3. Степень элемента группы

Определение 1.3.1. Пусть G — группа, $a \in G$, $n \in \mathbb{Z}$ — целое число. Положим

$$a^n = \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}, & \text{если } n > 0, \\ e, & \text{если } n = 0, \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{m=-n}, & \text{если } n < 0, \text{ где } m = -n > 0, \end{cases}$$

(или рекурсивно для $n \geqslant 0$: $a^0 = e$; $a^{n+1} = a^n a$; $a^{-n} = (a^n)^{-1}$).

Замечание 1.3.2. Если $m > 0$, то $(a^{-1})^m = (a^m)^{-1}$. Действительно,

$$(\underbrace{a \ldots a}_{m})(\underbrace{a^{-1} \ldots a^{-1}}_{m}) = e = (\underbrace{a^{-1} \ldots a^{-1}}_{m})(\underbrace{a \ldots a}_{m}).$$

Теорема 1.3.3. *Пусть G — группа, $a \in G$, $m, n \in \mathbb{Z}$ — целые числа. Тогда:*

1) $a^m \cdot a^n = a^{m+n}$;

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

Доказательство.

1) Формально, мы должны рассмотреть $3 \times 3 = 9$ случаев.

Случай 1. $m > 0$, $n > 0$ (следовательно, $m + n > 0$). Тогда

$$a^m \cdot a^n = (\underbrace{a \ldots a}_{m}) \cdot (\underbrace{a \ldots a}_{n}) = \underbrace{a \ldots a}_{m+n} = a^{m+n}.$$

Случай 2. $m > 0$, $n < 0$ (поэтому $n' = -n > 0$). Тогда

$$a^m \cdot a^n = (\underbrace{a \ldots a}_{m}) \cdot (\underbrace{a^{-1} \ldots a^{-1}}_{n'=-n}) =$$

$$= \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{m-n'=m+n}, & \text{если } m > n' = -n \text{ (т. е. } m + n > 0), \\ e, & \text{если } m = n' = -n \text{ (т. е. } m + n = 0), \\ \underbrace{a^{-1} \ldots a^{-1}}_{n'-m=-n-m}, & \text{если } m < n' = -n \text{ (т. е. } m + n < 0) \end{cases} =$$

$$= a^{m+n}.$$

Аналогично разбираются остальные случаи: 3) $m < 0$, $n > 0$; 4) $m < 0$, $n < 0$; 5) $m = 0$, $n > 0$; 6) $m = 0$, $n = 0$; 7) $m = 0$, $n < 0$; 8) $m > 0$, $n = 0$; 9) $m < 0$, $n = 0$.

Второе доказательство для 1). Сначала покажем, что $a^r a^s = a^{r+s}$ для всех $r, s \geqslant 0$, проводя индукцию по s. Начало индукции: $s = 0$. Пусть утверждение верно для s. Тогда

$$a^r a^{s+1} = a^r a^s a = a^{r+s} a = a^{r+s+1},$$

что завершает шаг индукции.

11-21

Из $a^r a^s = a^{r+s}$ следует, что $a^{-r}a^{r+s} = a^s$ и $a^{-r-s}a^r = a^{-s}$. Это показывает, что $a^{-r}a^s = a^{s-r}$ для всех $r, s \geqslant 0$. Аналогично $a^r a^{-s} = a^{r-s}$ для всех $r, s \geqslant 0$. Переходя к обратному в $a^s a^r = a^{r+s}$ при $r, s \geqslant 0$, получаем $a^{-r}a^{-s} = a^{-r-s}$.

Таким образом, все случаи оказываются рассмотренными.

2) При $n \geqslant 0$ проведём индукцию по n. Начало индукции: $n = 0$. Пусть утверждение верно для n. Тогда, используя 1):

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

Далее,

$$(a^m)^{-n} = \left((a^m)^n\right)^{-1} = (a^{mn})^{-1} = a^{-mn},$$

что завершает рассмотрение в том случае, когда вторая степень отрицательна. □

Замечание 1.3.4 (другое доказательство теоремы о целых степенях элемента группы). Пусть G — группа, $a \in G$, $n \in \mathbb{Z}$ — целое число. Определим n-ю степень a^n элемента a рекурсивно:

1) $a^0 = e$, $a^1 = a$, a^{-1} — обратный элемент для a;

2) $a^{n+1} = a^n a$, если $n > 0$;

3) $a^n = (a^{-n})^{-1}$, если $n < 0$.

Теорема 1.3.3′. *Пусть G — группа, $a \in G$, $m, n \in \mathbb{Z}$ — целые числа. Тогда:*

1) $a^m a^n = a^{m+n} = a^n a^m$;

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

Доказательство. 1) Пусть $m \geqslant 0$, $n \geqslant 0$. Проводя индукцию по n получаем, что $a^m a^n = a^{m+n} = a^n a^m$. Отсюда:

$$\begin{aligned}
&a^{-m}a^{m+n} = a^{-m}a^m a^n = a^n;\\
&a^{m+n}a^{-n} = a^m a^n a^{-n} = a^m;\\
&a^{-n}a^{-m} = (a^m a^n)^{-1} = (a^{m+n})^{-1} = a^{-(m+n)} = a^{(-m)+(-n)}.
\end{aligned}$$

2) Если $n \geqslant 0$, то из 1) следует, что $(a^m)^n = a^{mn}$. Пусть $n < 0$, тогда:

$$(a^m)^n = \left((a^m)^{-n}\right)^{-1} = (a^{-mn})^{-1} = a^{mn},$$

поскольку $a^{-mn}a^{mn} = e$. □

Упражнение 1.3.5. Пусть G — группа, $a, b \in G$.

1) Если $a^2 = e$ и $a^{-1}b^2a = b^3$, то $b^5 = e$.

2) Если $a^{-1}b^2a = b^3$, $b^{-1}a^2b = a^3$, то $a = e = b$.

11-22

Доказательство.
1) Имеем $b^2a = ab^3$, $b^3 = ab^2a$, $b^2 = ab^3a$. Поэтому

$$b^9 = b^3 \cdot b^3 \cdot b^3 = ab^2a \cdot ab^2a \cdot ab^2a = ab^6a = ab^3a \cdot ab^3a = b^2 \cdot b^2 = b^4,$$

следовательно, $b^5 = e$.

2) Имеем $b^2a = ab^3$, $a^2b = ba^3$, поэтому $a = b^{-2}ab^3$, $b = a^{-2}ba^3$. Следовательно,

$$b^{-1}a^2b = a^3 = (b^{-2}ab^3)(b^{-2}ab^3)(b^{-2}ab^3) = b^{-2}ababab^3,$$

отсюда (умножая слева на b^2, справа на b^{-1}) $ba^2 = ababab^2$. Аналогично, $b^2a = bababa^2$. Поэтому $bababab^2 = b^2a^2 = bababa^3$. Итак, $b^2 = a^2$, следовательно, $a = b^{-2}ab^3 = a^{-2}ab^3 = a^{-1}b^3$, $b^2 = a^2 = b^3$, $b = 3$. Аналогично, $a = e$. □

1.4. Порядок элемента группы

Рассмотрим целые степени элемента a группы G

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots$$

Возможны два случая.

Случай 1. Все элементы в этом ряду различны (т. е. $a^k \neq a^l$ для всех целых чисел $k \neq l$). В этом случае будем говорить, что *порядок элемента бесконечный* (обозначение: $\mathrm{O}(a) = \infty$).

Случай 2. В этом ряду $a^k = a^l$ для некоторых $k \neq l$. Пусть $k > l$. Тогда $a^{k-l} = e$, где $k - l > 0$, т. е. встретилась и натуральная степень элемента a, равная e. Рассмотрим множество $T = \{t \in \mathbb{Z} \mid t > 0,\ a^t = e\}$. Это непустое подмножество натуральных чисел. Следовательно, в T существует наименьший элемент n, который мы назовём *порядком элемента* a и обозначим через $\mathrm{O}(a)$.

Таким образом:

1) $a^n = e$, $n > 0$;

2) если $a^k = e$, $k > 0$, то $k \geqslant n$.

Ясно, что если группа G конечна, то $\mathrm{O}(g) < \infty$ для всех $g \in G$.

Пример 1.4.1. Если $0 \neq n \in (\mathbb{Z}, +)$, то $\mathrm{O}(n) = \infty$.

Пример 1.4.2. $G = (\{1, -1\}, \cdot)$, $a = -1$. Тогда $a^1 = -1$, $a^2 = 1$, т. е. $\mathrm{O}(a) = 2$.

Пример 1.4.3. $G = \mathrm{S}_3$,

$$a = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 1, & 3 \end{pmatrix} = (1\ 2), \quad b = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \end{pmatrix} = (1\ 2\ 3).$$

Тогда $a^1 = a$, $a^2 = e$, т. е. $\mathrm{O}(a) = 2$; $b^1 = b \neq e$, $b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq e$, $b^3 = e$, т. е. $\mathrm{O}(b) = 3$.

11-23

Пример 1.4.4.

1) Пусть $G = \{z \in \mathbb{C} \mid z^3 = 1\}$ — группа корней третьей степени из 1. Тогда $\mathrm{O}\left(\frac{-1+\sqrt{-3}}{2}\right) = 3$.

2) Пусть $G = \{1, i, -1, -i\}$ — группа корней четвёртой степени из 1. Тогда $\mathrm{O}(1) = 1$, $\mathrm{O}(i) = 4$, $\mathrm{O}(-1) = 2$, $\mathrm{O}(-i) = 4$.

Пример 1.4.5. Если

$$G = \{e,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\} \subseteq \mathrm{S}_4 -$$

группа Клейна, то $\mathrm{O}(g) = 2$ для всех $e \neq g \in G$.

Пример 1.4.6.

1) Пусть $G = \{z \in \mathbb{C} \mid z^k = 1$ для некоторого $k \in \mathbb{N}\}$ — группа все комплексных корней из 1. Тогда группа G бесконечна, но каждый элемент $g \in G$ имеет конечный порядок, $\mathrm{O}(g) < \infty$. □

2) Пусть $G = (\mathbb{Z}_2^{\mathbb{N}}, +) = \{(a_1, a_2, a_3, \ldots) \mid a_i \in \mathbb{Z}_2\}$ — группа счётных строк с элементами из $\mathbb{Z}_2$ с покомпонентной операцией сложения. Тогда G — бесконечная группа, в которой $\mathrm{O}(g) = 2$ для всех $0 \neq g \in G$. □

Лемма 1.4.7. *Если $\mathrm{O}(a) = n < \infty$, то:*

1) *все элементы $e = a^0, a, a^2, \ldots, a^{n-1}$ различны;*

2) *для любого $k \in \mathbb{Z}$ элемент a^k совпадает с одним из $e, a, a^2, \ldots, a^{n-1}$, а именно, если $k = nq + r$, где $0 \leqslant r < n$, то $a^k = a^r$.*

Доказательство.
1) Следует из определения порядка элемента $\mathrm{O}(a)$.
2) Пусть $k \in \mathbb{Z}$. Тогда $k = nq + r$, где $0 \leqslant r < n$. Следовательно, $a^k = (a^n)^q a^r = ea^r = a^r$. ☒

Лемма 1.4.8. *Пусть $\mathrm{O}(a) = n < \infty$. Тогда $a^k = e$ тогда и только тогда, когда $k = nq$.*

Доказательство.
1) Если $k = nq$, то $a^k = (a^n)^q = e^q = e$.
2) Допустим противное, т. е. что $k = nq + r$, где $0 < r < n$. Тогда $a^k = (a^n)^q a^r = a^r \neq e$ (по лемме 1.4.7). Получили противоречие. ☒

Лемма 1.4.9. *Пусть G — конечная группа. Тогда найдётся число $n \in \mathbb{N}$ такое, что $x^n = e$ для всех $x \in G$.*

Доказательство. Пусть

$$n = \prod_{g \in G} \mathrm{O}(g).$$

Тогда для любого $g \in G$ число n делится на $\mathrm{O}(g)$, $n = \mathrm{O}(g)q$, и поэтому $g^n = e$. □

11-24

Замечание 1.4.10.

1) Несколько позже (см. 1.9.2) мы покажем, что если $|G| < \infty$, то $g^{|G|} = e$ для всех $g \in G$.

2) Если $|G| < \infty$ и $\exp(G) = \text{НОК}\{\text{O}(g) \mid g \in G\}$ — экспонента конечной группы G (см. 1.9.27), то $\exp(G)$ — наименьшее натуральное число m, такое что $g^m = e$ для всех $g \in G$.

3) Если G — конечная неабелева группа, то в G существует элемент $g \in G$, для которого $\text{O}(g) \geqslant 3$.

Лемма 1.4.11. *Пусть $G = (a)$ — конечная циклическая группа порядка n, $a \in G$, $\text{O}(a) = n < \infty$. Если $b = a^k \in G = (a)$, $k \in \mathbb{Z}$, то $\text{O}(b) = \dfrac{n}{d}$, где d — наибольший общий делитель чисел n и k.*

Доказательство. Пусть $d = \text{НОД}(n, k)$, т. е. $n = dn_1$, $k = dk_1$, n_1 и k_1 взаимно просты. Тогда $\dfrac{n}{d} = n_1$ и

$$b^{n_1} = (a^k)^{n_1} = a^{dk_1n_1} = (a^n)^{k_1} = e^{k_1} = e.$$

Если же $b^t = e$ и $t > 0$, то $a^{kt} = e$, и следовательно, $kt = nq$, поскольку $n = \text{O}(a)$, т. е. $dk_1t = dn_1q$. Сокращая на d, получаем $k_1t = n_1q$. Поскольку правая часть n_1q делится на n_1, а числа n_1 и k_1 взаимно просты, то t делится на число n_1, т. е. $t \geqslant n_1$. Итак, $\text{O}(b) = n_1 = \dfrac{n}{d}$. □

Лемма 1.4.12 (порядок подстановки). *Пусть $\pi \in \text{S}_n$.*

1) *Если $\pi = (i_1, i_2, \ldots, i_r)$ — цикл длины r, то $\text{O}(\pi) = r$.*

2) *Если $\pi = \pi_1\pi_2 \ldots \pi_k$, где π_i — циклы с непересекающимися орбитами длины l_i, то $\text{O}(\pi) = \text{НОК}\{l_1, l_2, \ldots, l_k\}$.*

Доказательство.

1) Если $1 \leqslant k < r$, то $\pi^k = (i_k, i_{k+1}, \ldots)$ и

$$\pi^r = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \\ i_1 & i_2 & \ldots & i_r \end{pmatrix} = e.$$

Итак, $\text{O}(\pi) = r$.

2) Так как $\pi_i\pi_j = \pi_j\pi_i$ для всех π_i, π_j, то $\pi^m = \pi_1^m\pi_2^m \ldots \pi_k^m$ для всех $m > 0$. Поэтому $\pi^m = e$ тогда и только тогда, когда $\pi_1^m = \pi_2^m = \ldots = \pi_k^m = e$. Итак, $\text{O}(\pi) = \text{НОК}\{l_1, \ldots, l_k\}$. □

Упражнение 1.4.13.

1) Найдите наибольший из возможных порядков элементов в группе S_8.

Указание. Если $\pi \in \text{S}_8$, $\pi = \pi_1 \ldots \pi_k$, π_i — циклы с непересекающимися орбитами длины l_i. Тогда $\sum\limits_{i=1}^{k} l_i = 8$ и $\text{O}(\pi) = \text{НОК}\{l_1, \ldots, l_k\}$. Отсюда максимальное значение для $\text{O}(\pi)$ равно 15 и достигается при $l_1 = 3$, $l_2 = 5$ на подстановке $\pi = (1\,2\,3)(4\,5\,6\,7\,8)$.

11-95

2) Найдите все элементы наибольшего порядка в S_{10}, S_{11}, S_{12} и в A_{10}.

3) Найти порядки элементов 2, 3 и 7 в мультипликативной группе $\mathbb{Z}_{11}^* = \mathbb{Z}_{11} \setminus \{0\}$ поля вычетов $\mathbb{Z}_{11}$.

Теорема 1.4.14. *Пусть G — конечная абелева группа. Тогда:*

1) *произведение всех элементов группы G, порядки которых отличны от 2, равно единичному элементу;*

2) *если группа G содержит элемент порядка 2, то произведение всех элементов группы G равно произведению всех элементов порядка 2 группы G.*

Доказательство. Если $e \neq x \in G$, то $O(x) = 2$ тогда и только тогда, когда $x = x^{-1}$. Если $O(x) > 2$, то $O(x^{-1}) = O(x) > 2$, и $x \neq x^{-1}$. Так как G — абелева группа, то:

$$\prod_{\substack{g \in G \\ O(g) \neq 2}} g = \prod_{\substack{\{x, x^{-1}\} \\ O(x) \neq 2}} x \cdot x^{-1} = e;$$

$$\prod_{g \in G} g = \left(\prod_{\substack{x \in G \\ O(x) = 2}} x \right) \cdot \left(\prod_{\substack{y \in G \\ O(y) \neq 2}} y \right) = \prod_{\substack{x \in G \\ O(x) = 2}} x. \qquad \square$$

Теорема 1.4.15 (теорема Вилсона). *Если $p \in \mathbb{N}$, то p — простое число тогда и только тогда, когда:*

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство.

1) Пусть $G = (\mathbb{Z}_p \setminus \{0\}, \cdot) = \mathbb{Z}_p^*$ — мультипликативная группа поля вычетов $\mathbb{Z}_p$. Если $a \in \mathbb{Z}_p^*$ и $O(a) = 2$, то $a^2 \equiv 1 \pmod{p}$, следовательно, $a^2 - 1 = (a-1)(a+1)$ делится на p, поэтому или $a \equiv 1 \pmod{p}$, или $a \equiv -1 \pmod{p}$. В силу теоремы 1.4.14 в $\mathbb{Z}_p$

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

2) Если $p = k \cdot l$, $k, l \in \mathbb{N}$, $1 < k < p$, $1 < l < p$, то $(p-1)! \equiv 0 \pmod{k}$. Если $(p-1)! \equiv -1 \pmod{p}$, то $(p-1)! + 1 = p \cdot q = k \cdot l \cdot q$, что приводит к противоречию. $\square$

Теорема 1.4.16. *Пусть G — группа, $|G| = 2k$. Тогда G содержит элемент g порядка $O(g) = 2$.*

Доказательство. Пусть для всех $e \neq g \in G$ имеем $O(g) > 2$. Тогда $g \neq g^{-1}$, $O(g^{-1}) = O(g)$, поэтому число неединичных элементов группы G чётно, а $|G|$ — нечётное число. Получили противоречие. $\square$

Замечание 1.4.17. В дальнейшем мы рассмотрим глубокое развитие этого утверждения: случаи, когда верно обращение теоремы Лагранжа, а именно теоремы Коши и Силова.

КВ

11-26

Замечания о порядке произведения двух элементов группы

Пусть G — группа, $a, b, c \in G$ и $a = bc$. В общем случае (без дополнительных предположений) мало что можно сказать о порядке $\mathrm{O}(a)$ элемента a, зная порядки $\mathrm{O}(b)$ и $\mathrm{O}(c)$. Приведём несколько утверждений и примеров.

Лемма 1.4.18. *Пусть G — группа, $a, b, c, a_1, a_2, \ldots, a_k \in G$. Тогда:*

1) $\mathrm{O}(a^{-1}) = \mathrm{O}(a)$,

2) $\mathrm{O}(b) = \mathrm{O}(a^{-1}ba)$,

3) $\mathrm{O}(ab) = \mathrm{O}(ba)$, $\mathrm{O}(abc) = \mathrm{O}(bca) = \mathrm{O}(cab)$ *и, более того,*

$$\mathrm{O}(a_1a_2\ldots a_k) = \mathrm{O}(a_2a_3\ldots a_ka_1) = \ldots = \mathrm{O}(a_ka_1\ldots a_{k-1}).$$

Доказательство.

1) Для любого $k \in \mathbb{Z}$ $a^k = e$ тогда и только тогда, когда $(a^{-1})^k = a^{-k} = e$, поэтому $\mathrm{O}(a^{-1}) = \mathrm{O}(a)$.

2) Так как $a^{-1}b^ka = (a^{-1}ba)^k$, то $b^k = e$ тогда и только тогда, когда $a^{-1}b^ka = e$, поэтому $\mathrm{O}(a^{-1}ba) = \mathrm{O}(b)$.

3) Так как $a^{-1}(ab)a = ba$, то в силу 2) $\mathrm{O}(ab) = ba$. Аналогично $a^{-1}(abc)a = bca$, $b^{-1}(bca)b = cab$, и поэтому $\mathrm{O}(abc) = \mathrm{O}(bca) = \mathrm{O}(cab)$. И более того,

$$\begin{gathered} a_1^{-1}(a_1a_2\ldots a_k)a_1 = a_2\ldots a_ka_1, \\ a_2^{-1}(a_2a_3\ldots a_ka_1)a_2 = a_3\ldots a_ka_1a_2, \\ \ldots \\ a_{k-1}^{-1}(a_{k-1}a_ka_1\ldots a_{k-2})a_{k-1} = a_ka_1\ldots a_{k-1}. \end{gathered}$$

Отсюда следует совпадение порядков этих сопряжённых между собой элементов. □

Упражнение 1.4.19. Пусть G — группа, $a \in G$. Тогда если a — единственный элемент группы G, имеющий порядок 2, $\mathrm{O}(a) = 2$, то $ax = xa$ для всех $x \in G$ (другими словами, $a \in \mathrm{Z}(G)$, где $\mathrm{Z}(G)$ — центр группы G). *Действительно,* так как $\mathrm{O}(xax^{-1}) = \mathrm{O}(a) = 2$, то $xax^{-1} = a$, и поэтому $xa = ax$. □

Примеры 1.4.20.

1) В группе $G = \mathrm{GL}_2(\mathbb{Q})$ произведение двух элементов конечного порядка может не быть элементов конечного порядка (таким образом, совокупность $T(G)$ всех элементов конечного порядка неабелевой группы G не является подгруппой). *Действительно,* пусть

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathrm{O}(a) = 4, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad \mathrm{O}(b) = 3,$$

поскольку

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a^3 = -a, \quad a^4 = E; \quad b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad b^3 = E.$$

В то же время

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (ab)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad \text{для} \quad k \in \mathbb{Z},$$

11-27

поэтому $\mathrm{O}(ab) = \infty$. □

2) В группе $G = \mathbb{Z}_2 \oplus \mathbb{Z}$ существуют два элемента a, b бесконечного порядка, сумма $a + b$ которых имеет конечный порядок. *Действительно*:

$$a = (0,1), \quad \mathrm{O}(a) = \infty; \quad b = (1,-1), \quad \mathrm{O}(b) = \infty;$$
$$a + b = (1,0), \quad \mathrm{O}(a+b) = 2.$$ □

~~3) Если в конечной группе G $c = b^{-1}$ для $e \neq b \in G$, то $\mathrm{O}(c) = \mathrm{O}(b) > 1$, $e = a = bc$,~~ $bc = e = cb$, но $\mathrm{O}(a) = 1$ для $a = bc$. □

Кое-что иногда можно сказать в том случае, когда элементы b и c перестановочны, $bc = cb$ (это объясняется тем, что в этом случае подгруппа $H = \langle a, b\rangle$, порождённая элементами a и b, является абелевой).

Лемма 1.4.21. *Пусть G — группа, $a, b, c \in G$, $a = bc$, $bc = cb$, $\mathrm{O}(b) = r < \infty$, $\mathrm{O}(c) = s < \infty$, $m = \mathrm{HOK}(r, s)$. Тогда:*

1) $\mathrm{O}(a)$ — *делитель числа* $m = \mathrm{HOK}(r, s)$, $m = \mathrm{O}(a)q$, $q \in \mathbb{N}$;

2) *если* $\langle b\rangle \cap \langle c\rangle = e$, *то* $\mathrm{O}(a) = \mathrm{HOK}\big(\mathrm{O}(b), \mathrm{O}(c)\big)$;

3) *если* $(r, s) = 1$, *то* $\mathrm{O}(a) = rs$;

4) *если* $G = K \times H$ $(K \lhd G,\ H \lhd G,\ G = KH,\ K \cap H = e)$, $b \in K$, $c \in H$, *то* $\mathrm{O}(a) = \mathrm{HOK}\big(\mathrm{O}(b), \mathrm{O}(c)\big)$.

Доказательство.

1) Так как $bc = cb$, то $a^k = b^k c^k$ для $k \in \mathbb{Z}$. Так как

$$m = \mathrm{HOK}(r, s) = rq_1 = sq_2, \quad q_1, q_2 \in \mathbb{N},$$

то

$$a^m = b^{rq_1} c^{sq_2} = (b^r)^{q_1} (c^s)^{q_2} = e \cdot e = e,$$

и поэтому $\mathrm{O}(a)$ — делитель числа $m = \mathrm{HOK}\big(\mathrm{O}(b), \mathrm{O}(c)\big)$.

2а) В силу 1) $m = \mathrm{O}(a)q$, поэтому $a^m = \big(a^{\mathrm{O}(a)}\big)^q = e$.

2б) Если $t > 0$, то из $e = a^t = b^t c^t$ следует, что

$$b^t = c^{-t} \in \langle b\rangle \cap \langle c\rangle = e.$$

Поэтому $b^t = e = c^t$, и следовательно, $t = rq = s\tilde{q}$. Поэтому $t = \mathrm{HOK}(r, s) \cdot q'$, в частности, $t \geqslant m = \mathrm{HOK}(r, s)$.

3) Если $(r, s) = 1$, то $\langle b\rangle \cap \langle c\rangle = e$, поэтому в силу 2) $\mathrm{O}(a) = \mathrm{HOK}(r, s) = rs$.

Второе (прямое) *доказательство*: $a^{rs} = (b^r)^s (c^s)^r = e \cdot e = e$; если $a^t = e$, $t > 0$, то $e = a^t = b^t c^t$, поэтому

$$b^t = c^{-t} \in \langle b\rangle \cap \langle c\rangle = e.$$

Таким образом, $b^t = e$, $c^t = e$, и следовательно, $t = rq = s\tilde{q}$, поэтому $t = rsq' \geqslant rs$.

4) Так как

$$\langle b\rangle \cap \langle c\rangle \subseteq K \cap H = e,$$

то это утверждение также следует из 2). □

11-28

Замечание 1.4.22 (к п. 1) леммы). Порядок $\mathrm{O}(a)$ элемента $a = bc = cb$ может быть собственным делителем числа $m = \mathrm{НОК}\big(\mathrm{O}(b), \mathrm{O}(c)\big)$ (отличным от m). Например, если, как в примере 3), $c = b^{-1}$, $a = bc = e$, то $\mathrm{O}(a) = 1$, $\mathrm{O}(b) = \mathrm{O}(c) = r > 1$, $m = \mathrm{НОК}\big(\mathrm{O}(b), \mathrm{O}(c)\big) = r$.

Теорема 1.4.23. *Пусть G — группа, $a \in G$, $\mathrm{O}(a) = n = rs < \infty$, $(r, s) = 1 = ur + vs$, $u, v \in \mathbb{Z}$. Тогда:*

1) a) $\mathrm{O}(a^s) = r$, $\mathrm{O}(a^r) = s$;

b) $a = bc$, *где* $b = a^{sv} \in \langle a^s \rangle$, $c = a^{ru} \in \langle a^r \rangle$;

c) $bc = cb$;

d) $\mathrm{O}(b) = r$, $\mathrm{O}(c) = s$;

2) *если*

$$a = bc = b_1c_1, \quad bc = cb, \quad b_1c_1 = c_1b_1,$$
$$\mathrm{O}(b) = \mathrm{O}(b_1) = r, \quad \mathrm{O}(c) = \mathrm{O}(c_1) = s,$$

то $b = b_1$, $c = c_1$ (*другими словами, представление* $a = bc = cb$ *для разложения* $\mathrm{O}(a) = n = rs$, $(r, s) = 1$, *где* $\mathrm{O}(b) = r$, $\mathrm{O}(c) = s$, *единственно*).

Доказательство.
1a) Действительно,

$$\mathrm{O}(a^s) = \frac{n}{(s, n)} = \frac{rs}{s} = r, \quad \mathrm{O}(a^r) = \frac{n}{(r, n)} = \frac{rs}{r} = s.$$

1b) Так как $1 = ur + vs$, то $a = a^{ur+vs} = a^{sv}a^{ru} = bc$, $b = (a^s)^v \in \langle a^s \rangle$, $c = (a^r)^u \in \langle a^r \rangle$.
1c) Ясно, что $\langle a \rangle$ — коммутативная группа, и поэтому из $b, c \in \langle a \rangle$ следует, что $bc = cb$.
1d) Так как $1 = ur + vs$, то $(v, r) = 1$ и $(u, s) = 1$, поэтому

$$\mathrm{O}\big((a^s)^v\big) = \frac{r}{(v, r)} = \frac{r}{1} = r, \quad \mathrm{O}\big((a^r)^u\big) = \frac{s}{(u, s)} = \frac{s}{1} = s.$$

2) Так как $a = b_1c_1$, $b_1c_1 = c_1b_1$, $\mathrm{O}(c_1) = s$, то $a^s = b_1^s c_1^s = b_1^s$. Следовательно, поскольку $\mathrm{O}(b_1) = r$,

$$b_1 = b_1^{ur+vs} = (b_1^s)^v = (a^s)^v = a^{sv} = b.$$

Аналогично $c_1 = a^{ru} = c$. □

Следствие 1.4.24. *Пусть в группе G: $a = bc = b'c'$, $bc = cb$, $b'c' = c'b'$, $\mathrm{O}(b) = p^k$, $k > 1$, $\mathrm{O}(b') = p^l$, $l > 1$, $\big(p, \mathrm{O}(c)\big) = 1 = \big(p, \mathrm{O}(c')\big)$, где p — простое число. Тогда $b = b'$, $c = c'$.*

Доказательство. Так как $\mathrm{O}(b) = p^k$, $\big(p, \mathrm{O}(c)\big) = 1$, $\mathrm{O}(b') = p^l$, $\big(p, \mathrm{O}(c')\big) = 1$, то

$$\big(\mathrm{O}(b), \mathrm{O}(c)\big) = 1 = \big(\mathrm{O}(b'), \mathrm{O}(c')\big).$$

Поэтому из $a = bc = b'c'$ по лемме ?? имеем:

$$p^k\mathrm{O}(c) = \mathrm{O}(b)\mathrm{O}(c) = \mathrm{O}(a) = \mathrm{O}(b')\mathrm{O}(c') = p^l\mathrm{O}(c').$$

Следовательно, $p^k = p^l$, $\mathrm{O}(c) = \mathrm{O}(c')$. В силу нашей теоремы для $r = p^k = p^l$, $s = \mathrm{O}(c) = \mathrm{O}(c')$, $n = rs = \mathrm{O}(a)$ имеем: $b = b'$; $c = c'$. □

11-29

Следствие 1.4.25. *Если G — группа, $a \in G$, $\mathrm{O}(a) = n < \infty$, $n = \prod\limits_p p^{m(p)}$, $n_p = n/p^{m(p)}$, то:*

1) $\mathrm{O}(a^{n_p}) = p^{m(p)}$;

2) *существуют $x_p \in \mathbb{Z}$, для которых $a = \prod\limits_p a^{n_p x_p}$;*

3) *элементы $\{a^{n_p x_p}\}$ перестановочны друг с другом;*

4) $\mathrm{O}(a^{n_p x_p}) = p^{m(p)}$;

5) *это представление $a = \prod\limits_p a^{n_p x_p}$ единственно.*

Доказательство.
1) Так как $n = p^{m(p)} n_p$ и $(n_p, n) = n_p$, то

$$\mathrm{O}(a^{n_p}) = \frac{n}{(n_p, n)} = \frac{p^{m(p)} \cdot n_p}{n_p} = p^{m(p)}.$$

2) Так как числа $\{n_p = n/p^{m(p)}\}$ в совокупности взаимно просты, то найдутся числа $x_p \in \mathbb{Z}$ такие, что $1 = \sum\limits_p n_p x_p$. Поэтому

$$a = a^{\sum\limits_p n_p x_p} = \prod_p a^{n_p x_p}.$$

3) Элементы $\{a^{n_p x_p}\}$ принадлежат коммутативной подгруппе $\langle a \rangle$, и поэтому они попарно перестановочны.
4) Так как

$$1 = \sum_p x_p n_p = \sum_p \frac{x_p n}{p^{m(p)}},$$

то x_p не делится на p, и поэтому $(x_p, p^{m(p)}) = 1$. Следовательно,

$$\mathrm{O}\big((a^{n_p})^{x_p}\big) = \frac{p^{m(p)}}{(x_p, p^{m(p)})} = \frac{p^{m(p)}}{1} = p^{m(p)}.$$

5) Рассмотрим прямое разложение абелевой подгруппы $H = \langle a \rangle = \prod\limits_p H_p$ в примарные компоненты $\{H_p\}$, при этом

$$a = \prod_p a^{n_p x_p}, \quad \mathrm{O}(a^{n_p x_p}) = p^{m(p)}, \quad a^{n_p x_p} \in H_p.$$

Из единственности примарного разложения $H = \prod\limits_p H_p$ следует единственность представления $a = \prod\limits_p a^{n_p x_p}$, $\mathrm{O}(a^{n_p x_p}) = p^{m(p)} \in H_p$. □

11-30

Замечание 1.4.26. Для различных разложений

$$n = \mathrm{O}(a) = rs = r's', \quad (r,s) = 1 = (r',s'),$$

канонические представления

$$a = bc = b'c', \quad bc = cb, \quad b'c' = c'b',$$
$$\mathrm{O}(b) = r, \ \mathrm{O}(c) = s, \ \mathrm{O}(b') = r', \ \mathrm{O}(c') = s',$$

различны. *Действительно,* для

$$\mathrm{O}(a) = 30 = (2\cdot 3)\cdot 5 = 2\cdot(3\cdot 5),$$
$$r = 2\cdot 3, \quad s = 5, \quad (r,s) = 1, \quad r' = 2, \quad s' = 3\cdot 5, \quad (r',s') = 1,$$

имеем для $b = a^5$, $c = a^{24}$, $b' = a^{15}$, $c' = a^{28}$: $n = rs = r's'$, $a = bc = b'c'$, $bc = cb$, $b'c' = c'b'$, $\mathrm{O}(b) = r = 6$, $\mathrm{O}(c) = s = 5$, $\mathrm{O}(b') = r' = 2$, $\mathrm{O}(c') = s' = 15$. □

Упражнение 1.4.27. Пусть G — группа, $a, b \in G$, $ab = ba$, $\mathrm{O}(a) = m$, $\mathrm{O}(b) = n$. Тогда группа G содержит такой элемент c, что $\mathrm{O}(c) = \mathrm{НОК}(m,n)$. *Действительно,* $H = \langle a, b\rangle$ — конечная абелева группа. Пусть $H = \bigoplus\limits_p H_p$ — разложение конечной абелевой группы в прямую сумму конечного числа p-примарных компонент, p — простое число. Если

$$a = \sum_p a_p, \quad a_p \in H_p, \quad \mathrm{O}(a_p) = p^{i_p},$$
$$b = \sum_p b_p, \quad b_p \in H_p, \quad \mathrm{O}(b_p) = p^{j_p}.$$

Так как

$$\big(\mathrm{O}(a_p), \mathrm{O}(a_q)\big) = 1 = \big(\mathrm{O}(b_p), \mathrm{O}(b_q)\big)$$

для различных простых чисел p и q, то

$$m = \mathrm{O}(a) = \prod_p p^{i_p}, \quad n = \mathrm{O}(b) = \prod_p p^{j_p}.$$

Тогда

$$\mathrm{НОК}(m,n) = \prod_p p^{\max(i_p, j_p)}.$$

Выберем

$$c_p = \begin{cases} a_p, & \text{если } i_p \geqslant j_p, \\ b_p, & \text{если } j_p > i_p. \end{cases}$$

Тогда $c_p \in H_p$ и $\mathrm{O}(c_p) = p^{\max(i_p, j_p)}$. Если $c = \sum\limits_p c_p \in \bigoplus\limits_p H_p = H \subset G$, $\mathrm{O}(c) = \prod\limits_p p^{\max(i_p, j_p)} = \mathrm{НОК}(m,n)$. □

Теорема 1.4.28. *В любой коммутативной группе G совокупность всех элементов конечного порядка*

$$T(G) = \{g \in G \mid \mathrm{O}(g) < \infty\}$$

образует подгруппу, называемую периодической частью *$T(G)$ абелевой группы G.*

11-31

Доказательство.

1) Если $a, b \in T(G)$, $\mathrm{O}(a) = k < \infty$, $\mathrm{O}(b) = l < \infty$, то

$$(ab)^{kl} = a^{kl}b^{kl} = (a^k)^l(b^l)^k = e \cdot e = e.$$

Поэтому $\mathrm{O}(ab) < \infty$, и следовательно, $ab \in T(G)$.

2) Так как $\mathrm{O}(a^{-1}) = \mathrm{O}(a) < \infty$ для $a \in T(G)$, то $a^{-1} \in T(G)$. □

Замечание 1.4.29. Как мы видели в примере 1.4.20 1) совокупность элементов конечного порядка $T(G)$ некоммутативной группы G может не быть подгруппой группы G.

Замечание 1.4.30. Важным инвариантом конечной группы G является её *спектр*

$$\omega(G) = \{n \in \mathbb{N} \mid \exists x \in G,\ \mathrm{O}(x) = n\},$$

другими словами, множество порядков её элементов.

Конечная группа G называется *распознаваемой по спектру*, если любая конечная группа H с условием равенства спектров $\omega(H) = \omega(G)$ изоморфна группе G. В задаче о характеризации распознаваемых по спектру конечных групп одна из интересных проблем заключается в выяснении распознаваемости по спектру конечных простых групп.

Группа G называется *периодической*, если каждый элемент g группы G имеет конечный порядок $\mathrm{O}(g) < \infty$, и *группой без кручения*, если каждый элемент $e \neq g \in G$ имеет бесконечный порядок, $\mathrm{O}(g) = \infty$.

1.5. Подгруппы группы

Конец лекции 11

Лемма 1.5.1. *Для непустого подмножества H группы G следующие условия эквивалентны:*

1) *H является группой относительно исходной операции в группе G;*

2) *подмножество H удовлетворяет следующим двум условиям:*

   а) *если $h_1, h_2 \in H$, то $h_1h_2 \in H$;*

   б) *если $h \in H$, то $h^{-1} \in H$.*

Непустое подмножество H группы G удовлетворяющее эквивалентным условиям 1) и 2), называется *подгруппой группы G*.

Доказательство.

1) $\Longrightarrow$ 2). Если $h_1, h_2 \in H$, то, поскольку операция определена на H (т. е. не выводит из H), имеем $h_1h_2 \in H$, т. е. 2а).

Если e' — нейтральный элемент группы H, то $e' \cdot e' = e'$. Умножая в группе обе стороны этого равенства на $(e')^{-1}$, получаем $e' = e$ (здесь e — нейтральный элемент группы G).

Если $\underset{\sim}{h}^{-1}$ — обратный элемент для элемента $h \in H$ в группе H, то $\underset{\sim}{h}^{-1} \cdot h = e' = e = h \cdot \underset{\sim}{h}^{-1}$, т. е. $h^{-1} = \underset{\sim}{h}^{-1} \in H$ (условие 2б)).

2) $\Longrightarrow$ 1). Условие 2а) показывает, что операция определена на множестве H. Конечно, она ассоциативна. Далее, для $h \in H$ в силу 2б) $h^{-1} \in H$, и поэтому в силу 2а) $e = h \cdot h^{-1} \in H$. Ясно, что e — нейтральный элемент в H, а h^{-1} — обратный элемент для h в H. Итак, H — группа относительно операции, индуцированной операцией группы G. □