Конспект лекций по Алгебре

Первый семестр

Власов Ярослав
Современное программирование, МКН СПбГУ
2025 г.

Предисловие

Этот конспект основан на конспекте по алгебре 2020 года ребят с МКН СПбГУ, LaTeX-код был обновлён и немного доработан, а также исправлены опечатки и некоторые неточности.

Оглавление

Первый семестр. Первая четверть

1 Множества и операции над ними

Определение. Множество — любая совокупность каких-либо объектов.

Множества обычно обозначаются заглавными буквами $A, B, \ldots$.
Элементы множеств — строчными буквами $a, b, \ldots$.

$$x \in A \quad — x \text{ принадлежит } A, \qquad x \notin A \quad — x \text{ не принадлежит } A.$$

Примеры.

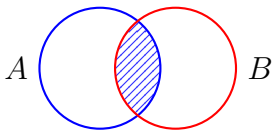
$$\mathbb{N} = \{1, 2, 3, \ldots\}, \qquad \mathbb{Z} = \{0, -1, 1, -2, 2, -3, 3, \ldots\},$$
$$\mathbb{Q} = \left\{\frac{m}{n} : m \in \mathbb{Z},\ n \in \mathbb{N}\right\},$$
$\mathbb{R}$ — множество вещественных чисел, $\mathbb{C}$ — множество комплексных чисел.

Определение. Множество S называется подмножеством множества T, если все элементы из S лежат в T. В этом случае пишут $S \subset T$.

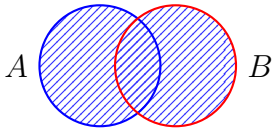
$$S = \{2, 6\}, \quad T = \{2, 4, 6\} : \quad S \subset T.$$

Определение. Операции над множествами.

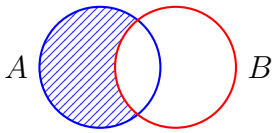
Пересечение: $A \cap B = \{x \mid x \in A \wedge x \in B\}$



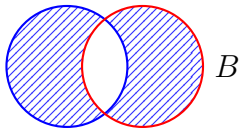
Объединение: $A \cup B = \{x \mid x \in A \vee x \in B\}$



Разность: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$



Симметрическая разность: $A \triangle B = (A \setminus B) \cup (B \setminus A)$



Предложение (Правила Де Моргана)**.** *Для произвольного семейства множеств* $\{B_\alpha\}_{\alpha \in I}$ *справедливы равенства:*

$$A \setminus \bigcup_{\alpha \in I} B_\alpha = \bigcap_{\alpha \in I} (A \setminus B_\alpha),$$

$$A \setminus \bigcap_{\alpha \in I} B_\alpha = \bigcup_{\alpha \in I} (A \setminus B_\alpha).$$

Доказательство. Докажем первое равенство (второе доказывается аналогично).
Пусть $x \in A \setminus \bigcup_{\alpha \in I} B_\alpha$. Это эквивалентно системе

$$\begin{cases} x \in A, \\ x \notin \bigcup_{\alpha \in I} B_\alpha. \end{cases}$$

Второе условие означает, что $x \notin B_\alpha$ для всех $\alpha \in I$. Значит,

$$x \in A \setminus B_\alpha \quad \text{для всех } \alpha \in I,$$

то есть

$$x \in \bigcap_{\alpha \in I} (A \setminus B_\alpha).$$

Обратное включение доказывается аналогично: если $x \in \bigcap_{\alpha \in I} (A \setminus B_\alpha)$, то $x \in A$ и $x \notin B_\alpha$ для всех $\alpha \in I$, а значит $x \notin \bigcup_{\alpha \in I} B_\alpha$ и, следовательно, $x \in A \setminus \bigcup_{\alpha \in I} B_\alpha$. ■

Замечание. Операции $\triangle$, $\cup$, $\cap$ являются коммутативными и ассоциативными.

Определение. Декартово произведение множеств A и B — это множество

$$A \times B = \{\langle a, b \rangle : a \in A,\ b \in B\}.$$

Пример.

$A = \{1, 2\}, B = \{x, y\}$

$A \times B = \{\langle 1, x \rangle \langle 1, y \rangle \langle 2, x \rangle \langle 2, y \rangle\}$
$B \times A = \{\langle x, 1 \rangle \langle y, 1 \rangle \langle x, 2 \rangle \langle y, 2 \rangle\}$

Предложение. *Для произвольного семейства множеств* $\{B_\alpha\}_{\alpha \in I}$ *справедливы равенства:*

$$A \cap \bigcup_{\alpha \in I} B_\alpha = \bigcup_{\alpha \in I} (A \cap B_\alpha),$$

$$A \cup \bigcap_{\alpha \in I} B_\alpha = \bigcap_{\alpha \in I} (A \cup B_\alpha).$$

Доказательство. Докажем первое равенство (второе доказывается аналогично).
Пусть $x \in A \cap \bigcup_{\alpha\in I} B_\alpha$. Это эквивалентно системе

$$\begin{cases} x \in A, \\ x \in \bigcup_{\alpha\in I} B_\alpha. \end{cases}$$

Второе условие означает, что $x \in B_\alpha$ для некоторого $\alpha \in I$. Тогда

$$x \in A \cap B_\alpha \quad \text{для некоторого } \alpha \in I,$$

а значит

$$x \in \bigcup_{\alpha\in I} (A \cap B_\alpha).$$

Обратное включение доказывается аналогично. ■

Определение. Упорядоченная пара $\langle a, b\rangle$ — это пара «пронумерованных» элементов.

Две упорядоченные пары равны, если равны соответствующие элементы:

$$\langle a, b\rangle = \langle c, d\rangle \quad \Longleftrightarrow \quad (a = c) \text{ и } (b = d).$$

2 Отображения. Инъективность. Сюръективность. Биективность

Определение. Отображением называется сопоставление

$$f : A \to B,$$

при котором каждому элементу $a \in A$ сопоставлен единственный элемент $f(a) \in B$. $\forall a \in A\ \exists! b \in B : f(a) = b$ элемент $f(a)$ называется образом элемента a.

Определение. Отображение $f : M \to N$ называется инъективным, если

$$\forall m_1, m_2 \in M\ \big(m_1 \neq m_2 \Rightarrow f(m_1) \neq f(m_2)\big).$$

Определение. Отображение $f : M \to N$ называется сюръективным, если

$$\forall n \in N\ \exists m \in M : f(m) = n.$$

Определение. Отображение $f : M \to N$ называется биективным, если оно инъективно и сюръективно.

Определение. Пусть $n \in N$ и $f : M \to N$. Тогда

$$f^{-1}(n) = \{m \in M \mid f(m) = n\}$$

называется полным прообразом элемента n.

f инъективно $\Leftrightarrow \forall n \in N : |f^{-1}(n)| \leq 1$.

f сюръективно $\Leftrightarrow \forall n \in N : |f^{-1}(n)| \geq 1$.

f биективно $\Leftrightarrow \forall n \in N : |f^{-1}(n)| = 1$.

3 Алгебраические операции, их свойства

Определение. Бинарной операцией на множестве M называется отображение

$$* : M \times M \to M.$$

Примеры бинарных операций:

$M = \mathbb{Z}:$ сложение, умножение, вычитание; $M = \mathbb{N}:$ сложение, умножение, возведение в степень.

Определение. Композицией отображений $f : M \to N$ и $g : N \to P$ называется отображение

$$g \circ f : M \to P,$$

задаваемое формулой

$$(g \circ f)(m) = g(f(m)).$$

Предложение. *Пусть $f : X \to Y$. Тогда:*

1. *f — инъекция $\Leftrightarrow$ f обратима слева, то есть $\exists\, g : Y \to X \mid g \circ f = \mathrm{id}_X$.*
2. *f — сюръекция $\Leftrightarrow$ f обратима справа, то есть $\exists\, g : Y \to X \mid f \circ g = \mathrm{id}_Y$.*

Доказательство.

1. «$\Longleftarrow$».
   Пусть $g : Y \to X$ — левая обратная к f, то есть $g \circ f = \mathrm{id}_X$. Возьмём $x, x' \in X$ и предположим, что $f(x) = f(x')$. Тогда

   $$x = \mathrm{id}_X(x) = g(f(x)) = g(f(x')) = \mathrm{id}_X(x') = x'.$$

   Таким образом, из $f(x) = f(x')$ следует $x = x'$, а значит, f — инъекция.

   «$\Longrightarrow$».
   Пусть f — инъекция. Зафиксируем некоторый элемент $x' \in X$. Определим отображение $g : Y \to X$ следующим образом:

   $$g(y) = \begin{cases} x, & \text{если } y = f(x) \text{ для некоторого } x \in X, \\ x', & \text{если } y \notin \mathrm{range}(f). \end{cases}$$

   Тогда для любого $x \in X$ имеем

   $$(g \circ f)(x) = g(f(x)) = x,$$

   следовательно, $g \circ f = \mathrm{id}_X$, и g является левой обратной к f.

2. «$\Longleftarrow$».
   Пусть $g : Y \to X$ — правая обратная к f, то есть $f \circ g = \mathrm{id}_Y$. Возьмём произвольный $y \in Y$. Тогда

   $$y = \mathrm{id}_Y(y) = f(g(y)),$$

то есть любой элемент $y \in Y$ является образом некоторого $x = g(y)$. Следовательно, f — сюръекция.

«$\Longrightarrow$».
Пусть f — сюръекция, то есть $\mathrm{range}(f) = Y$. Определим отображение $g : Y \to X$, выбрав для каждого $y \in Y$ некоторый элемент $x \in X$, удовлетворяющий $f(x) = y$, и положив

$$g(y) = x.$$

Тогда для любого $y \in Y$ выполняется

$$y = f(g(y)) = \mathrm{id}_Y(y),$$

то есть $f \circ g = \mathrm{id}_Y$, и g — правая обратная к f.

■

Определение. Операция $*$ (или $\cdot$) на M называется коммутативной, если

$$\forall m_1, m_2 \in M : \quad m_1 \cdot m_2 = m_2 \cdot m_1.$$

Определение. Операция $\cdot$ на M называется ассоциативной, если

$$\forall m_1, m_2, m_3 \in M : \quad (m_1 \cdot m_2) \cdot m_3 = m_1 \cdot (m_2 \cdot m_3).$$

Предложение. *Общая ассоциативность. Если операция ассоциативна, то значение произведения не зависит от расстановки скобок.*

Доказательство. Докажем по индукции по числу сомножителей k.

База: $k = 3$ — это обычная ассоциативность.

Переход: пусть утверждение верно для всех произведений из $k-1$ элементов. Рассмотрим произведение из k элементов $a_1 a_2 \dots a_k$. Любую расстановку скобок можно представить как

$$B = (\text{произведение } a_1, \dots, a_l) \cdot (\text{произведение } a_{l+1}, \dots, a_k).$$

По предположению индукции каждое из скобочных произведений не зависит от расстановки скобок, то есть

$$B = (a_1 a_2 \dots a_l)\,(a_{l+1} \dots a_k).$$

Применяя ассоциативность к последнему множителю, можно последовательно перенести скобки, получая

$$B = a_1 a_2 \dots a_k.$$

Следовательно, результат не зависит от расстановки скобок. ■

Определение. Пусть $g \in M$ и $n \in \mathbb{N}$. Тогда

$$g^n = \overbrace{g * g * \cdots * g}^{n \text{ раз}}.$$

Определение. Элемент $e \in M$ называется левым нейтральным, если

$$\forall m \in M : \ e \cdot m = m,$$

правым нейтральным, если

$$\forall m \in M : \ m \cdot e = m,$$

и нейтральным (двусторонним), если он одновременно левый и правый нейтральный.

Предложение. *Нейтральный элемент, если существует, единственен.*

Доказательство. Пусть e' и e'' — нейтральные элементы в M. Тогда

$$e' = e' \cdot e'' = e'',$$

значит, $e' = e''$. ■

Определение. Пусть $a \in M$. Элемент $b \in M$ называется обратным к a, если

$$ab = ba = e,$$

где e — нейтральный элемент. Обратный элемент обычно обозначают как $a^{-1} = b$.

Определение. Пусть $m \in M$, $n \in \mathbb{Z}$. Тогда

$$m^n = \begin{cases} \underbrace{m \cdot m \cdot \dots \cdot m}_{n \text{ раз}}, & n > 0, \\ e, & n = 0, \\ \underbrace{m^{-1} \cdot \dots \cdot m^{-1}}_{|n| \text{ раз}}, & n < 0. \end{cases}$$

4 Группы. Подгруппы. Сокращение в группе

Определение. Группа — это множество G с заданной на нём бинарной операцией $\cdot$, такой что выполняются следующие свойства:

1. Операция $\cdot$ ассоциативна:

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

2. Существует нейтральный элемент $e \in G$, то есть

$$\forall a \in G : \ e \cdot a = a \cdot e = a.$$

3. У каждого элемента $a \in G$ существует обратный элемент $a^{-1} \in G$, для которого

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

В предыдущем билете содержится доказательство данного предложения.

Предложение.

Если $f : M \to N$ имеет левое обратное отображение $g : N \to M$, то есть $g \circ f = \mathrm{id}_M$, то и только тогда f является инъективным.

Если $f : M \to N$ имеет правое обратное отображение $g : N \to M$, то есть $f \circ g = \mathrm{id}_N$, то и только тогда f является сюръективным.

Определение. S_n — симметрическая группа степени n, то есть группа всех перестановок множества $\{1, \ldots, n\}$.

Определение. Группа $(G, \cdot)$ называется абелевой, если операция $\cdot$ коммутативна:

$$\forall a, b \in G : \ a \cdot b = b \cdot a.$$

Подгруппами группы являются, в частности, следующие более общие конструкции.

- Если операция на множестве только ассоциативна, то множество с этой операцией называется полугруппой. Например, $(\mathbb{N}, +)$.
- Если операция ассоциативна и существует нейтральный элемент, то множество с этой операцией называется моноидом. Например, $(\mathbb{N} \cup \{0\}, +)$.

Определение. Пусть $(G, \cdot)$ — группа. Подмножество $H \subset G$ называется подгруппой, если выполняются следующие условия:

1. Замкнутость относительно операции:

$$H \cdot H \subset H, \text{ то есть } \forall a, b \in H : \ a \cdot b \in H.$$

2. Наличие нейтрального элемента группы в H:

$$e \in H.$$

3. Замкнутость относительно взятия обратных:

$$H^{-1} \subset H, \text{ то есть } \forall a \in H : \ a^{-1} \in H.$$

5 Примеры групп. Произведение групп. Изоморфизм групп

Примеры групп:

1. $(\mathbb{Z}, +)$ — абелева группа по сложению.
2. Пусть операция на $\mathbb{Z}$ задана правилом

$$m * n = m + n + 1.$$

Тогда $(\mathbb{Z}, *)$ образует группу; нейтральным элементом является число 1, а обратный к n элемент равен $n^{-1} = 1 - n$.

3. $(\mathbb{Z}, \cdot)$ не является группой, так как у большинства элементов нет обратного по умножению в $\mathbb{Z}$.

4. $(\{\pm 1\}, \cdot)$ — группа по умножению.

Пример: G — группа перемещений плоскости.

$$G = \{f : P \to P \mid \forall A, B \in P : \ \rho(f(A), f(B)) = \rho(A, B)\},$$

где P — множество точек плоскости, а ρ — расстояние между точками.

Для фиксированного множества Φ вводят подгруппу

$$\Sigma(\Phi) = \{g \in G \mid g(\Phi) = \Phi\},$$

то есть множество всех движений, сохраняющих Φ.

Определение. Пусть $(G_1, *), (G_2, \diamond)$ — группы. Их прямым произведением называется группа

$$(G_1 \times G_2, \cdot),$$

в которой операция определяется по формуле

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 * g_1', \ g_2 \diamond g_2'),$$

где $*, \diamond, \cdot$ — соответствующие групповые бинарные операции.

Определение. Изоморфизмом групп G и G' называется отображение $\varphi : G \to G'$, для которого выполняются условия:

1. φ — биекция.
2. Для всех $g_1, g_2 \in G$
$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2).$$

6 Кольцо. Примеры. Группа обратимых элементов

Определение. Кольцом называется множество A, на котором заданы две бинарные операции $+$ и $\cdot$ (называемые сложением и умножением), для которых выполняются:

1. $(A, +)$ — абелева группа.
2. Для всех $a, b, c \in A$ выполнена дистрибутивность:
$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Замечание Ассоциативность умножения часто включают в определение кольца, но здесь она выделяется как дополнительное свойство.

Множество A называется:

- *ассоциативным кольцом*, если умножение ассоциативно;
- *коммутативным кольцом*, если умножение коммутативно;

- *кольцом с* 1, если в A существует нейтральный элемент относительно умножения (обозначаемый 1), причём $1 \neq 0$, где 0 — нейтральный элемент по сложению.

Примеры.

1. $(\mathbb{Z}, +, \cdot)$ — коммутативное ассоциативное кольцо с 1.
2. $(2\mathbb{Z}, +, \cdot)$ — коммутативное ассоциативное кольцо без 1.
3. $(\mathbb{R}^3, +, \times)$, где $\times$ — векторное произведение, — некоммутативное и неассоциативное кольцо без 1 (если считать умножением только векторное произведение).
4. Пусть M — множество. Тогда $(2^M, \triangle, \cap)$ — коммутативное ассоциативное кольцо с 1, где

$$A \triangle B = B \triangle A, \quad (A \triangle B) \triangle C = A \triangle (B \triangle C),$$

$$0 = \varnothing, \quad A \triangle A = \varnothing,$$

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C),$$

$$A \cap B = B \cap A, \quad A \cap (B \cap C) = (A \cap B) \cap C,$$

$$1 = M.$$

Предложение (Лемма)**.** *Пусть A — кольцо. Тогда для любого $a \in A$*

$$0 \cdot a = 0.$$

Доказательство. Имеем

$$0 + 0 = 0.$$

Умножим равенство слева на a:

$$(0 + 0) \cdot a = 0 \cdot a.$$

По дистрибутивности

$$0 \cdot a + 0 \cdot a = 0 \cdot a.$$

Переносим $0 \cdot a$ влево (используя существование противоположного):

$$0 \cdot a = 0.$$

■

Определение. Пусть $(A, +, \cdot)$ — кольцо. Подмножество $B \subset A$ называется подкольцом кольца A, если выполнены условия:

- B замкнуто относительно умножения:

$$\forall b_1, b_2 \in B : \ b_1 \cdot b_2 \in B;$$

- B является аддитивной подгруппой $(A, +)$.

Определение. Подмножество $I \subset A$ называется идеалом кольца A, если

- A — коммутативное ассоциативное кольцо с 1;

- I — аддитивная подгруппа $(A, +)$;
- для любых $a \in A$, $b \in I$ выполнено
$$a \cdot b \in I.$$

Например, $2\mathbb{Z}$ — идеал кольца $\mathbb{Z}$.

Замечание Множество $\{0\}$ всегда является идеалом в A.
Само A всегда является идеалом в A.

Определение. Пусть A — коммутативное ассоциативное кольцо с 1. Идеал I называется главным идеалом кольца A, если
$$\exists\, a \in A: \quad I = aA = \{a \cdot x \mid x \in A\}.$$

Определение. Пусть A — ассоциативное кольцо с 1. Множество A^* всех обратимых элементов кольца A называется множеством (или группой) обратимых элементов:
$$A^* = \{a \in A \mid \exists\, a^{-1} \in A:\ aa^{-1} = a^{-1}a = 1\}.$$

Например,
$$\mathbb{Z}^* = \{\pm 1\}, \qquad \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}.$$

Предложение. $(A^*, \cdot)$ — *группа обратимых элементов кольца* A.

Доказательство.
- Ассоциативность операции в A^* наследуется от ассоциативности умножения в A.
- Нейтральный элемент 1 принадлежит A^*, так как $1 \cdot 1 = 1$.
- По определению все элементы A^* обратимы.
- Докажем замкнутость относительно умножения. Пусть $a, b \in A^*$. Тогда
$$\exists\, a' \in A:\ aa' = a'a = 1, \qquad \exists\, b' \in A:\ bb' = b'b = 1.$$
Рассмотрим элемент $b'a'$. Тогда
$$(ab)(b'a') = a(bb')a' = a \cdot 1 \cdot a' = aa' = 1,$$
а также
$$(b'a')(ab) = b'(a'a)b = b' \cdot 1 \cdot b = b'b = 1.$$
Следовательно, $(ab)^{-1} = b'a'$, то есть $ab \in A^*$.

■

7 Поле

Определение. Коммутативное ассоциативное кольцо с 1 A называется полем, если

$$A^* = A \setminus \{0\},$$

то есть каждый ненулевой элемент обратим. Примеры: $\mathbb{Q}$, $\mathbb{R}$, а также поле вычетов $\mathbb{F}_2$ по модулю 2 (и вообще любое кольцо вычетов по простому модулю).

Замечание Множество $A = \{0\}$ является кольцом, но не является полем, так как 0 в этом случае обратим.

Предложение. *Пусть A — коммутативное ассоциативное кольцо с 1. Тогда A является полем тогда и только тогда, когда в A ровно два идеала.*

Доказательство. Всегда существуют идеалы $\{0\}$ и A. Нужно показать, что других идеалов нет.

Предположим, что $A \neq \{0\}$.

«$\Longrightarrow$». Пусть A — поле и I — идеал в A, отличный от $\{0\}$. Тогда существует элемент $a \in I$, $a \neq 0$. Так как A — поле, $a \in A^*$, то есть существует $a' \in A$ такое, что

$$aa' = 1.$$

Поскольку $a \in I$ и I — идеал, имеем $1 = aa' \in I$. Тогда для любого $b \in A$

$$b = b \cdot 1 \in I,$$

то есть $I = A$.

«$\Longleftarrow$». Пусть в A ровно два идеала: $\{0\}$ и A. Возьмём $a \in A \setminus \{0\}$. Рассмотрим главный идеал, порождённый a:

$$(a) = aA = \{a \cdot x \mid x \in A\}.$$

Так как $a \neq 0$, то $(a) \neq \{0\}$, следовательно, $(a) = A$. Значит, $1 \in (a)$, то есть

$$\exists\, b \in A : \ 1 = a \cdot b.$$

Отсюда $b = a^{-1}$, и a обратим. Так как a был произвольным ненулевым элементом, все ненулевые элементы обратимы, значит, A — поле. ■

Ещё один пример поля.

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

называется квадратичным полем.

Доказательство. Сначала проверим, что $\mathbb{Q}(\sqrt{2})$ — подкольцо в $\mathbb{R}$.

- По сложению $\mathbb{Q}(\sqrt{2})$ является аддитивной подгруппой $(\mathbb{R}, +)$.
- Замкнутость относительно умножения:

  $$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2},$$

  где $aa' + 2bb' \in \mathbb{Q}$ и $ab' + a'b \in \mathbb{Q}$.

Очевидно, что $1 \in \mathbb{Q}(\sqrt{2})$.

Покажем, что

$$\mathbb{Q}(\sqrt{2})^* = \mathbb{Q}(\sqrt{2}) \setminus \{0\}.$$

Пусть $a + b\sqrt{2} \neq 0$. Тогда

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \neq 0,$$

причём $a^2 - 2b^2 \in \mathbb{Q}$. Следовательно,

$$(a + b\sqrt{2})^{-1} = \frac{1}{a^2 - 2b^2}(a - b\sqrt{2}) = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Значит, каждый ненулевой элемент обратим, и $\mathbb{Q}(\sqrt{2})$ — поле. ■

8 Построение поля комплексных чисел

- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}, \qquad i^2 = -1.$
- Операция сложения:
$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i.$$
- Операция умножения:
$$(a + bi) \cdot (a' + b'i) = (aa' - bb') + (ab' + a'b)i.$$

Предложение. $(\mathbb{C}, +, \cdot)$ *является полем.*

Доказательство.
- Коммутативность и ассоциативность сложения следуют из свойств сложения в $\mathbb{R}$.
- $0 + 0i$ — нейтральный элемент по сложению.
- $-a - bi$ — элемент, противоположный к $a + bi$.
- Коммутативность умножения очевидна из симметричности формулы умножения.
- Проверим дистрибутивность:

$$\begin{aligned}(a + bi)\big((a_1 + b_1 i) + (a_2 + b_2 i)\big) &= (a + bi)\big((a_1 + a_2) + (b_1 + b_2)i\big) \\ &= a(a_1 + a_2) - b(b_1 + b_2) + \big(a(b_1 + b_2) + b(a_1 + a_2)\big)i,\end{aligned}$$

$$\begin{aligned}&(a + bi)(a_1 + b_1 i) + (a + bi)(a_2 + b_2 i) \\ &= (aa_1 - bb_1) + (ab_1 + a_1 b)i + (aa_2 - bb_2) + (ab_2 + a_2 b)i \\ &= \big(aa_1 + aa_2 - bb_1 - bb_2\big) + \big(ab_1 + ab_2 + a_1 b + a_2 b\big)i \\ &= a(a_1 + a_2) - b(b_1 + b_2) + \big(a(b_1 + b_2) + b(a_1 + a_2)\big)i.\end{aligned}$$

Равенства совпадают, значит, дистрибутивность выполнена.

- Ассоциативность умножения проверяется прямым вычислением:

$$\begin{aligned}
&(a_1 + b_1 i)\big((a_2 + b_2 i)(a_3 + b_3 i)\big) \\
&= (a_1 + b_1 i)\big((a_2 a_3 - b_2 b_3) + (a_2 b_3 + a_3 b_2) i\big) \\
&= a_1(a_2 a_3 - b_2 b_3) - b_1(a_2 b_3 + a_3 b_2) \\
&+\big(a_1(a_2 b_3 + a_3 b_2) + b_1(a_2 a_3 - b_2 b_3)\big) i \\
&= a_1 a_2 a_3 - a_3 b_1 b_2 - a_1 b_2 b_3 - a_2 b_1 b_3 \\
&+(a_1 a_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1 - b_1 b_2 b_3) i,
\end{aligned}$$

$$\begin{aligned}
&\big((a_1 + b_1 i)(a_2 + b_2 i)\big)(a_3 + b_3 i) \\
&= \big((a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i\big)(a_3 + b_3 i) \\
&= (a_1 a_2 - b_1 b_2) a_3 - (a_1 b_2 + a_2 b_1) b_3 \\
&+\big((a_1 a_2 - b_1 b_2) b_3 + (a_1 b_2 + a_2 b_1) a_3\big) i \\
&= a_1 a_2 a_3 - a_3 b_1 b_2 - a_1 b_2 b_3 - a_2 b_1 b_3 \\
&+(a_1 a_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1 - b_1 b_2 b_3) i.
\end{aligned}$$

  Правая и левая части совпадают, значит, умножение ассоциативно.

- $1 + 0i$ — нейтральный элемент по умножению.
- Для $a + bi \neq 0$ имеем

$$(a + bi)(a - bi) = a^2 - b^2 i^2 = a^2 + b^2.$$

  Тогда

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

  то есть каждый ненулевой элемент обратим.

Значит, выполнены все аксиомы поля, и $\mathbb{C}$ является полем комплексных чисел. ■

- $\mathbb{R}$ является подполем в $\mathbb{C}$.
- Любое число $z \in \mathbb{C}$ можно записать как

$$z = x + iy, \quad x, y \in \mathbb{R}.$$

  Здесь $x = \operatorname{Re} z$ — вещественная часть, $y = \operatorname{Im} z$ — мнимая часть.

- Число z называется чисто мнимым, если $\operatorname{Re} z = 0$.

9 Комплексное сопряжение

Определение. Для числа $z = a + bi$ комплексно сопряжённым называется число

$$\overline{z} = a - bi.$$

Предложение. *Отображение*

$$\mathbb{C} \to \mathbb{C}, \quad z = x + iy \longmapsto \overline{z} = x - iy$$

является автоморфизмом $\mathbb{C}$*, то есть биекцией, для которой*

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \qquad \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$$

Доказательство. 1. Заметим, что $\overline{\overline{z}} = z$ для любого z, следовательно, комплексное сопряжение является обратным к самому себе. Значит, это биекция.

2. Пусть $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$. Тогда

$$\overline{z_1 + z_2} = \overline{(x_1 + x_2) + i(y_1 + y_2)} = (x_1 + x_2) - (y_1 + y_2)i = (x_1 - y_1 i) + (x_2 - y_2 i) = \overline{z_1} + \overline{z_2}.$$

3. Аналогично,

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i,$$

поэтому

$$\overline{z_1 z_2} = (x_1 x_2 - y_1 y_2) - (x_1 y_2 + x_2 y_1)i.$$

С другой стороны,

$$\overline{z_1}\,\overline{z_2} = (x_1 - y_1 i)(x_2 - y_2 i) = (x_1 x_2 - y_1 y_2) - (x_1 y_2 + x_2 y_1)i,$$

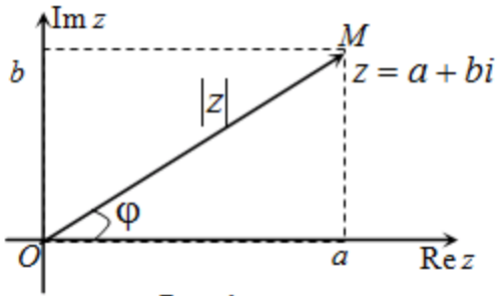
то есть $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.

■

Замечание

1. $z = \overline{z} \iff z \in \mathbb{R}$.
2. $z + \overline{z} \in \mathbb{R}$.
3. $z \cdot \overline{z} \in \mathbb{R}$.

10 Определение модуля и аргумента. Свойства модуля комплексного числа



Определение. Модулем комплексного числа $z = a + bi$ называется число

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

Определение. Пусть $z \in \mathbb{C}$, $r = |z|$. Число $\varphi \in \mathbb{R}$ называется аргументом числа z, если

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

Определение. Представление

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

называется тригонометрической формой комплексного числа.

Свойства модуля. Пусть $z, z_1, z_2 \in \mathbb{C}$.

1. $|z| \geq 0$ и $|z| = 0 \iff z = 0$.
2. $|\overline{z}| = |z|$.
3. $|z|^2 = z \cdot \overline{z}$.

   Доказательство. Если $z = a + bi$, то

   $$z \cdot \overline{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2.$$

   ■

4. Неравенство треугольника:

   $$|z_1 + z_2| \leq |z_1| + |z_2|.$$

   Доказательство. Пусть $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$. Сравним квадраты обеих частей:

   $$|z_1 + z_2|^2 = |(a_1 + a_2) + i(b_1 + b_2)|^2$$
   $$= (a_1 + a_2)^2 + (b_1 + b_2)^2 = a_1^2 + 2a_1a_2 + a_2^2 + b_1^2 + 2b_1b_2 + b_2^2,$$
   $$(|z_1| + |z_2|)^2 = (a_1^2 + b_1^2) + (a_2^2 + b_2^2) + 2|z_1||z_2|.$$

   Неравенство $|z_1 + z_2| \leq |z_1| + |z_2|$ эквивалентно

   $$a_1a_2 + b_1b_2 \leq |z_1||z_2|.$$

   Снова возведём в квадрат:

   $$(a_1a_2 + b_1b_2)^2 \leq (a_1^2 + b_1^2)(a_2^2 + b_2^2),$$

   то есть

   $$2a_1a_2b_1b_2 \leq a_1^2b_2^2 + a_2^2b_1^2,$$

   что эквивалентно

   $$0 \leq (a_1b_2 - a_2b_1)^2.$$

   Последнее верно всегда, поэтому неравенство треугольника доказано. ■

5. $|z_1z_2| = |z_1||z_2|$.

Доказательство. Пусть $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$. Сравним квадраты:

$$\begin{gathered}|z_1 z_2|^2 = |(a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)|^2 \\ = (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 \\ = a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2, \\ |z_1|^2 |z_2|^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2.\end{gathered}$$

Получаем $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$, а значит $|z_1 z_2| = |z_1||z_2|$. ■

11 Существование и «единственность» аргумента комплексного числа

1. Если $z = 0$, то любое вещественное число является его аргументом.
2. Если $z \neq 0$, то существует $\varphi_0 \in \mathbb{R}$ такое, что φ_0 является аргументом z, и при этом $\varphi_0 + 2\pi k$ для любого $k \in \mathbb{Z}$ также является аргументом z.

Доказательство. Пусть $z = x + iy \neq 0$ и $r = |z| = \sqrt{x^2 + y^2} > 0$. Тогда

$$x^2 \leq x^2 + y^2 = r^2 \Rightarrow -r \leq x \leq r,$$

откуда

$$-1 \leq \frac{x}{r} \leq 1.$$

Следовательно, существует $\widetilde{\varphi} \in \mathbb{R}$, такое что

$$\cos \widetilde{\varphi} = \frac{x}{r}.$$

Тогда

$$(\sin \widetilde{\varphi})^2 = 1 - (\cos \widetilde{\varphi})^2 = 1 - \frac{x^2}{r^2} = \frac{r^2 - x^2}{r^2} = \frac{y^2}{r^2},$$

то есть

$$\sin \widetilde{\varphi} = \pm \frac{y}{r}.$$

Если $\sin \widetilde{\varphi} = \dfrac{y}{r}$, положим $\varphi_0 := \widetilde{\varphi}$, иначе $\varphi_0 := -\widetilde{\varphi}$. Тогда

$$\cos \varphi_0 = \frac{x}{r}, \qquad \sin \varphi_0 = \frac{y}{r},$$

и потому

$$z = x + iy = r \cos \varphi_0 + ir \sin \varphi_0 = r(\cos \varphi_0 + i \sin \varphi_0),$$

то есть φ_0 является аргументом числа z.

Далее, если $\varphi = \varphi_0 + 2\pi k$, $k \in \mathbb{Z}$, то

$$\cos \varphi = \cos \varphi_0, \qquad \sin \varphi = \sin \varphi_0,$$

следовательно,

$$r(\cos\varphi + i\sin\varphi) = r(\cos\varphi_0 + i\sin\varphi_0) = z,$$

то есть φ также является аргументом z.

Покажем, что любые два аргумента отличаются на угол, кратный 2π. Пусть α — аргумент числа z. Тогда

$$z = r(\cos\alpha + i\sin\alpha) = r(\cos\varphi_0 + i\sin\varphi_0).$$

Отсюда

$$\cos\alpha = \cos\varphi_0, \qquad \sin\alpha = \sin\varphi_0,$$

что возможно только при $\alpha = \varphi_0 + 2\pi k$, $k \in \mathbb{Z}$. ■

Свойства аргумента.

Пусть $z_1, z_2 \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$,

$$z_1 = |z_1|(\cos\varphi_1 + i\sin\varphi_1), \quad z_2 = |z_2|(\cos\varphi_2 + i\sin\varphi_2).$$

1. $\arg(z_1 z_2) = \arg z_1 + \arg z_2$ (с точностью до $2\pi k$).

   Доказательство.

$$\begin{aligned} z_1 z_2 &= |z_1|(\cos\varphi_1 + i\sin\varphi_1)\,|z_2|(\cos\varphi_2 + i\sin\varphi_2) \\ &= |z_1||z_2|\big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\big) \\ &= |z_1||z_2|\big(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)\big), \end{aligned}$$

   то есть аргумент произведения равен сумме аргументов (плюс $2\pi k$). ■

2. $\arg\dfrac{z_1}{z_2} = \arg z_1 - \arg z_2$ (с точностью до $2\pi k$).

   Доказательство. Из равенства

$$z_1 = \frac{z_1}{z_2}\cdot z_2$$

   получаем

$$\arg z_1 = \arg\frac{z_1}{z_2} + \arg z_2,$$

   а значит

$$\arg\frac{z_1}{z_2} = \arg z_1 - \arg z_2.$$

   ■

   Замечание В частности,

$$\arg\frac{1}{z} = \arg 1 - \arg z = 0 - \arg z = -\arg z.$$

3. $\arg\overline{z} = -\arg z$ (с точностью до $2\pi k$).

Доказательство. Пусть $\arg z = \varphi$, тогда

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

Тогда

$$\overline{z} = |z|(\cos\varphi - i\sin\varphi) = |z|(\cos(-\varphi) + i\sin(-\varphi)),$$

то есть аргумент $\overline{z}$ равен $-\varphi$. ■

12 Умножение и деление чисел в тригонометрической форме. Формула Муавра

Пусть $z \in \mathbb{C}^*$,

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

- **Умножение.**

  Для $z_1, z_2 \in \mathbb{C}^*$,

  $$z_1 z_2 = |z_1||z_2|\big(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\big),$$

  что следует из доказательства для свойства аргумента произведения.

- **Деление.**

  Для $z_1, z_2 \in \mathbb{C}^*$,

$$\begin{aligned}\frac{z_1}{z_2} &= \frac{|z_1|(\cos\varphi_1 + i\sin\varphi_1)}{|z_2|(\cos\varphi_2 + i\sin\varphi_2)} \\ &= \frac{|z_1|(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 - i\sin\varphi_2)}{|z_2|(\cos\varphi_2 + i\sin\varphi_2)(\cos\varphi_2 - i\sin\varphi_2)} \\ &= \frac{|z_1|(\cos\varphi_1\cos\varphi_2 + \sin\varphi_1\sin\varphi_2 + i(\sin\varphi_1\cos\varphi_2 - \cos\varphi_1\sin\varphi_2))}{|z_2|(\cos^2\varphi_2 + \sin^2\varphi_2)} \\ &= \frac{|z_1|}{|z_2|}\big(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)\big).\end{aligned}$$

- **Формула Муавра.**

  Пусть $z = |z|(\cos\varphi + i\sin\varphi)$, тогда для любого $n \in \mathbb{Z}$

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

  Доказательство. – $\mathbf{n > 0}$.

  Доказательство по индукции по n.

  База: $n = 1$ — равенство очевидно.

  Переход: пусть формула верна для $n = k - 1$, то есть

  $$z^{k-1} = |z|^{k-1}\big(\cos((k-1)\varphi) + i\sin((k-1)\varphi)\big).$$

Тогда

$$\begin{aligned} z^k &= z^{k-1}\cdot z \\ &= |z|^{k-1}\big(\cos((k-1)\varphi)+i\sin((k-1)\varphi)\big)\cdot|z|(\cos\varphi+i\sin\varphi) \\ &= |z|^k\big(\cos(k\varphi)+i\sin(k\varphi)\big), \end{aligned}$$

по формуле умножения в тригонометрической форме.

– $\mathbf{n=0}$.

$$z^0 = 1 = |z|^0(\cos 0 + i\sin 0).$$

– $\mathbf{n<0}$.

Пусть $n<0$. Тогда

$$z^n = \frac{1}{z^{-n}}.$$

Из уже доказанного для положительного $-n$ имеем

$$z^{-n} = |z|^{-n}\big(\cos(-n\varphi)+i\sin(-n\varphi)\big) = |z|^{-n}\big(\cos(n\varphi)-i\sin(n\varphi)\big).$$

Тогда

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

что и требовалось.

■

13 Корни из комплексных чисел

Предложение (Формула корней из комплексного числа)**.** *Пусть $z\in\mathbb{C}$, $n\in\mathbb{N}$. Тогда:*

1) *Если $z=0$, то уравнение $w^n=z$ имеет единственный корень $w=0$.*
2) *Если $z=r(\cos\varphi+i\sin\varphi)$, где $r>0$, $\varphi\in\mathbb{R}$, то уравнение $w^n=z$ имеет ровно n попарно различных корней*

$$w_0, w_1, \ldots, w_{n-1},$$

где

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

Доказательство. Первый случай очевиден: если $z=0$, то из $w^n=0$ следует $w=0$.

Рассмотрим теперь случай $z\neq 0$. Пусть $z=r(\cos\varphi+i\sin\varphi)$, где $r>0$. Пусть w — корень уравнения $w^n=z$. Тогда $w\neq 0$ и его можно записать в тригонометрической форме:

$$w=\rho(\cos\psi+i\sin\psi), \quad \rho>0,\ \psi\in\mathbb{R}.$$

Подставим в уравнение:

$$w^n = \rho^n\big(\cos(n\psi) + i\sin(n\psi)\big) = r(\cos\varphi + i\sin\varphi).$$

Отсюда, по равенству модулей и аргументов,

$$\begin{cases} \rho^n = r, \\ n\psi = \varphi + 2\pi k, \quad k \in \mathbb{Z}. \end{cases}$$

Следовательно,

$$\begin{cases} \rho = \sqrt[n]{r}, \\ \psi = \dfrac{\varphi + 2\pi k}{n} \quad \text{для некоторого } k \in \mathbb{Z}. \end{cases}$$

Итак, все корни вида

$$w_k := \sqrt[n]{r}\Big(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\Big), \quad k \in \mathbb{Z}.$$

На этом этапе описаны *все* корни, но среди них могут быть совпадающие. Разберёмся, при каких $k, l \in \mathbb{Z}$ выполняется $w_k = w_l$.

Имеем

$$w_k = w_l \iff \frac{\varphi + 2\pi k}{n} = \frac{\varphi + 2\pi l}{n} + 2\pi s, \quad s \in \mathbb{Z}$$

(так как аргументы комплексных чисел определены с точностью до 2π). Отсюда

$$\frac{k-l}{n} = s \in \mathbb{Z} \iff k - l \in n\mathbb{Z} \iff k \equiv l \pmod{n}.$$

Значит, числа w_k и w_l совпадают тогда и только тогда, когда k и l дают одинаковые остатки при делении на n. Следовательно, чтобы получить полный список попарно различных корней, достаточно взять любой набор представителей классов по модулю n, например

$$k = 0, 1, \ldots, n-1.$$

Таким образом, множество корней уравнения $w^n = z$ есть

$$\{\, w \in \mathbb{C} \mid w^n = z \,\} = \{\, w_k \mid k = 0, 1, \ldots, n-1 \,\},$$

и этих корней ровно n. ■

14 Корни из единицы. Первообразные корни из 1

Предложение. *Рассмотрим частный случай* $z = 1$.

Согласно предыдущей теореме, уравнение

$$w^n = 1$$

имеет n корней на комплексной плоскости.

Обозначим через ζ_k корни степени n из единицы:

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

Эти точки лежат на единичной окружности и являются вершинами правильного n-угольника на комплексной плоскости.

Заметим важное свойство: увеличение аргумента на $\dfrac{2\pi}{n}$ эквивалентно умножению на число модулем 1 и аргументом $\dfrac{2\pi}{n}$, то есть на ζ_1. Иными словами, переход от одного корня из единицы к следующему осуществляется умножением на ζ_1:

$$\zeta_k = \zeta_1^k, \quad k = 0, 1, \ldots, n-1.$$

Более общо, если w_0 — некоторый корень уравнения $w^n = z$ (где $z \neq 0$), то все корни имеют вид

$$w_k = w_0\zeta_k = w_0\zeta_1^k, \quad k = 0, 1, \ldots, n-1.$$

Предложение. *Пусть $n > 1$, $z \in \mathbb{C}^*$, а $w_0, w_1, \ldots, w_{n-1}$ — все корни степени n из z. Тогда их сумма равна нулю:*

$$S := \sum_{k=0}^{n-1} w_k = 0.$$

Доказательство. Как отмечено выше, все корни можно записать в виде

$$w_k = w_0\zeta_k = w_0\zeta_1^k, \quad k = 0, 1, \ldots, n-1,$$

где $\zeta_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Тогда

$$S = \sum_{k=0}^{n-1} w_k = w_0 \sum_{k=0}^{n-1} \zeta_1^k.$$

Но $\zeta_1 \neq 1$ (так как $n > 1$, и ζ_1 имеет аргумент $\frac{2\pi}{n} \not\equiv 0 \pmod{2\pi}$), поэтому по формуле суммы геометрической прогрессии

$$\sum_{k=0}^{n-1} \zeta_1^k = \frac{\zeta_1^n - 1}{\zeta_1 - 1} = \frac{1-1}{\zeta_1 - 1} = 0.$$

Отсюда

$$S = w_0 \cdot 0 = 0.$$

Альтернативно можно рассуждать так: умножим сумму на ζ_1:

$$\zeta_1 S = \zeta_1 w_0 + \zeta_1 w_1 + \cdots + \zeta_1 w_{n-1} = w_1 + w_2 + \cdots + w_0 = S.$$

Тогда $(\zeta_1 - 1)S = 0$. Так как $\zeta_1 \neq 1$, то $S = 0$. ■

Предложение. *Множество*

$$\mu_n := \{\, \zeta \in \mathbb{C} \mid \zeta^n = 1 \,\}$$

является группой по умножению, то есть подгруппой $\mathbb{C}^*$.

Доказательство. Во-первых, $\mu_n \neq \varnothing$, так как $1 \in \mu_n$.

Пусть $\zeta, \tilde{\zeta} \in \mu_n$. Тогда

$$\zeta^n = 1, \quad \tilde{\zeta}^n = 1 \;\Rightarrow\; (\zeta\tilde{\zeta})^n = \zeta^n\tilde{\zeta}^n = 1 \cdot 1 = 1,$$

значит, $\zeta\tilde{\zeta} \in \mu_n$ (замкнутость относительно умножения).

Если $\zeta \in \mu_n$, то $\zeta \neq 0$ и

$$(\zeta^{-1})^n = (\zeta^n)^{-1} = 1^{-1} = 1,$$

то есть $\zeta^{-1} \in \mu_n$ (обратимость).

Ассоциативность умножения и существование нейтрального элемента 1 наследуются от $\mathbb{C}^*$. Следовательно, μ_n — подгруппа $\mathbb{C}^*$. ■

Определение. Группа G называется *циклической*, если существует элемент $g \in G$ такой, что

$$G = \{\, g^k \mid k \in \mathbb{Z} \,\},$$

то есть G состоит из всех целых степеней одного элемента g. Кратко это записывают так: $G = \langle g \rangle$.

Например, $\mathbb{Z}$ по сложению является циклической группой:

$$\mathbb{Z} = \langle 1 \rangle,$$

где 1 — порождающий элемент, а $2 = 1 + 1$, $3 = 1 + 1 + 1$ и т.д.

Замечание Множество μ_n — циклическая группа:

$$\mu_n = \langle \zeta_1 \rangle = \langle \zeta_{n-1} \rangle,$$

так как все элементы μ_n имеют вид ζ_1^k, $k = 0, 1, \ldots, n-1$, и ζ_1 является корнем из единицы максимального порядка n.

15 Многочлены от одной переменной. Переход к стандартной записи

Пусть R — коммутативное ассоциативное кольцо с единицей.

Определение. Последовательность $(a_0, a_1, \ldots)$ называется *финитной*, если существует число $N \geq 0$ такое, что $a_i = 0$ для всех $i \geq N$.

Определение. Многочленом от одной переменной над R называется финитная последовательность $(a_0, a_1, \ldots)$ элементов R.

Обозначим через $R[x]$ множество всех многочленов от одной переменной с коэффициентами из R.

Предложение. *Операции в* $R[x]$

Пусть $(a_0, a_1, \dots), (b_0, b_1, \dots) \in R[x]$. Тогда:

- сложение:
$$(a_0, a_1, \dots) + (b_0, b_1, \dots) := (a_0 + b_0,\ a_1 + b_1,\ \dots),$$
что снова даёт финитную последовательность;
- умножение:
$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) := (c_0, c_1, \dots), \quad c_n := \sum_{k=0}^{n} a_k\, b_{n-k},\ n = 0, 1, 2, \dots,$$
и эта последовательность тоже финитна.

Замечание Важно, что результат операций в $R[x]$ снова является финитной последовательностью. Если $a_j = 0$ при $j \geq N_1$ и $b_j = 0$ при $j \geq N_2$, то для всех $j \geq N_1 + N_2$ выполняется $c_j = 0$, то есть $(c_0, c_1, \dots)$ финитна.

Переход к стандартной записи:

- Для $a \in R$ положим
$$[a] := (a, 0, 0, \dots).$$
Тогда $[a] + [b] = [a + b]$ и $[a] \cdot [b] = [ab]$, так что удобно отождествлять $[a]$ с a.
- Для $a \in R$ и многочлена $(b_0, b_1, \dots)$ положим
$$a \cdot (b_0, b_1, \dots) := (ab_0, ab_1, \dots).$$
- Пусть $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ — финитная последовательность. Тогда
$$(a_0, a_1, \dots, a_n, 0, \dots) = \sum_{i=0}^{n} (0, \dots, 0, \underbrace{a_i}_{i\text{-е место}}, 0, \dots).$$
Обозначим через x_i последовательность $(0, 0, \dots, 0, 1, 0, \dots)$, где 1 стоит на i-м месте. Тогда
$$(a_0, a_1, \dots, a_n, 0, \dots) = \sum_{i=0}^{n} a_i x_i.$$
- Замечаем, что $x_k \cdot x_1 = x_{k+1}$ для всех $k \geq 0$; по индукции получаем $x_k = x_1^k$.
- Следовательно,
$$\sum_{i=0}^{n} a_i x_i = a_0 + a_1 x_1 + a_2 x_1^2 + \dots + a_n x_1^n.$$
Обозначая $x_1 := x$, приходим к привычной записи
$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n.$$

Предложение. *Кольцо $(R[x], +, \cdot)$ является коммутативным ассоциативным кольцом с единицей.*

Доказательство. 1. Свойства сложения (ассоциативность, коммутативность, существование нуля и противоположного элемента) проверяются покомпонентно и следуют из соответствующих свойств в R.

2. Коммутативность умножения следует из формулы для коэффициентов c_n и коммутативности умножения в R.

3. Дистрибутивность вытекает из определения:

$$c_n = \sum_{k=0}^{n} a_k\, b_{n-k},$$

если заменить b_{n-k} на $b'_{n-k} + b''_{n-k}$ и раскрыть скобки.

4. Ассоциативность удобно проверять в стандартной записи. Пусть

$$a(x) = \sum_{i=0}^{n} a_i x^i, \quad b(x) = \sum_{j=0}^{m} b_j x^j, \quad c(x) = \sum_{k=0}^{\ell} c_k x^k,$$

где $a_i, b_j, c_k \in R$. Тогда

$$(ab)c = \sum_{i,j,k} a_i b_j c_k x^{i+j+k} = a(bc),$$

поскольку умножение в R ассоциативно.

5. Нейтральный элемент по умножению — многочлен $1 = (1, 0, 0, \dots)$, то есть константа $1 \in R$.

■

16 Свойства степени многочлена

Определение. Пусть

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_n \neq 0.$$

Степенью многочлена f называется максимальное число n, для которого $a_n \neq 0$; обозначается $\deg f$. Коэффициент a_n называется старшим коэффициентом, а $a_n x^n$ — старшим членом многочлена.

Замечание Для нулевого многочлена степень по соглашению полагают равной $\deg 0 = -\infty$ (иногда -1); это удобно для формул со степенями.

Предложение. *Пусть $f, g \in R[x]$, $\deg f = m$, $\deg g = n$. Тогда:*

1. $\deg(f+g) \le \max\{m, n\}$. *Возможен строгий знак $<$, если старшие коэффициенты многочленов взаимно уничтожаются. Если $m \neq n$, то* $\deg(f+g) = \max\{m, n\}$.

2. $\deg(fg) \le m + n$.

Доказательство. Если один из многочленов равен нулю, утверждения очевидны, так как $\deg 0$ минимальна по соглашению. Далее считаем $m, n \ge 0$.

1. Пусть $d = \max\{m, n\}$. Тогда

$$f(x) = \sum_{i=0}^{d} a_i x^i, \quad g(x) = \sum_{i=0}^{d} b_i x^i,$$

где при необходимости для одного из многочленов дописаны нулевые коэффициенты при степенях выше его степени. Тогда

$$f(x) + g(x) = \sum_{i=0}^{d} (a_i + b_i) x^i,$$

откуда $\deg(f + g) \leq d$. Если $m \neq n$, то старший коэффициент одного из многочленов не может сократиться, и $\deg(f + g) = d$.

2. Пусть

$$f(x) = \sum_{i=0}^{m} a_i x^i, \quad g(x) = \sum_{j=0}^{n} b_j x^j.$$

Тогда

$$f(x)g(x) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_i b_j x^{i+j},$$

и все степени в произведении не превосходят $m + n$, так что $\deg(fg) \leq m + n$.

■

Замечание Неравенство $\deg(fg) \leq \deg f + \deg g$ может быть строгим, если в кольце R есть делители нуля: в этом случае старший коэффициент произведения может оказаться нулём. Например, в кольце $\mathbb{Z}/4\mathbb{Z}$ многочлен

$$f(x) = \overline{2}x + \overline{1}$$

имеет степень 1, но

$$f(x)^2 = (\overline{2}x + \overline{1})^2 = \overline{4}x^2 + \overline{4}x + \overline{1} = \overline{1},$$

поэтому $\deg(f^2) = 0 < 2 = \deg f + \deg f$. Это означает, что $\mathbb{Z}/4\mathbb{Z}$ не является областью целостности.

Предложение. *Пусть R — область целостности. Тогда:*

1. *Для любых $f, g \in R[x]$ выполнено*

$$\deg(fg) = \deg f + \deg g.$$

2. *Кольцо $R[x]$ является областью целостности.*

Доказательство. 1. Пусть $\deg f = m$, $\deg g = n$, и a_m, b_n — старшие коэффициенты. Так как R — область целостности, $a_m b_n \neq 0$. Коэффициент при x^{m+n} в произведении fg равен $a_m b_n$, значит $\deg(fg) = m + n$.

2. Если $f, g \neq 0$, то $\deg f, \deg g \geq 0$, и по пункту 1 имеем $\deg(fg) = \deg f + \deg g \geq 0$, откуда $fg \neq 0$. Следовательно, в $R[x]$ нет делителей нуля, то есть $R[x]$ — область целостности.

■

Следствие: Пусть R — область целостности. Тогда группа единиц кольца $R[x]$ совпадает с группой единиц кольца R:

$$R[x]^* = R^*.$$

Доказательство. $\subset$ Любой обратимый элемент $u \in R^*$ можно рассматривать как константный многочлен, и он остаётся обратимым в $R[x]$, так что $R^* \subset R[x]^*$.

$\supset$ Пусть $f \in R[x]^*$, то есть существует $g \in R[x]$ такое, что $fg = 1$. Тогда $f, g \neq 0$, и по предыдущей теореме

$$0 = \deg 1 = \deg(fg) = \deg f + \deg g.$$

Так как степени неотрицательны, получаем $\deg f = \deg g = 0$, то есть f и g — константы из R. При этом $fg = 1$ в R, значит $f \in R^*$. Следовательно, $R[x]^* \subset R^*$.

Итак, $R[x]^* = R^*$. ■

17 Теорема о делении с остатком для кольца целых чисел

Предложение. *Пусть $f, g \in R[x]$, $g \neq 0$, и старший коэффициент g обратим в R. Тогда существуют единственные многочлены $q, r \in R[x]$ такие, что:*

1. $f = gq + r$;
2. $\deg r < \deg g$.

Доказательство. Обозначим $\deg g = d$ и запишем

$$g = b_d x^d + \ldots,$$

где b_d — старший коэффициент многочлена g.

Существование. Докажем существование представления индукцией по $n = \deg f$. Если $\deg f < d$, то можно взять $q = 0$ и $r = f$ — это будет базой индукции.

Теперь пусть $\deg f = n \geqslant d$, и обозначим через a_n старший коэффициент f. Рассмотрим многочлен

$$a_n b_d^{-1} x^{n-d} g.$$

У этого многочлена старший член равен $a_n x^n$, как и у f. Поэтому

$$\deg\bigl(f - a_n b_d^{-1} x^{n-d} g\bigr) < n.$$

Интуитивное пояснение шага. *Это в точности тот же приём, который используется при делении многочлена на многочлен "столбиком". Мы смотрим на старшие коэффициенты, домножаем делитель g на подходящий моном x^{n-d} и на отношение старших коэффициентов, чтобы выровнять старшие члены. После вычитания из f получается многочлен меньшей степени.*

По индукционному предположению найдутся многочлены $q_1, r_1 \in R[x]$ такие, что

$$f - a_n b_d^{-1} x^{n-d} g = g q_1 + r_1, \qquad \deg r_1 < \deg g.$$

Тогда

$$f = \big(a_n b_d^{-1} x^{n-d} + q_1\big) g + r_1.$$

Обозначив $q = a_n b_d^{-1} x^{n-d} + q_1$ и $r = r_1$, получаем требуемое представление $f = gq + r$ с $\deg r < \deg g$.

Единственность. Предположим, что существуют два таких представления:

$$f = gq_1 + r_1 = gq_2 + r_2,$$

где $\deg r_1 < \deg g$ и $\deg r_2 < \deg g$. Тогда

$$r_1 - r_2 = g(q_2 - q_1).$$

Левая часть имеет степень строго меньше $d = \deg g$, так как обе разности остатков имеют степень меньше d. Справа же

$$\deg\big(g(q_2 - q_1)\big) = d + \deg(q_2 - q_1),$$

поскольку старший коэффициент g обратим, а у $q_2 - q_1$ либо степень определена (если $q_2 \neq q_1$), либо это нулевой многочлен. Если $q_2 - q_1 \neq 0$, то правая часть имеет степень не меньше d, что невозможно, так как левая часть имеет степень меньше d. Значит, $q_2 - q_1 = 0$, то есть $q_1 = q_2$, и тогда из равенства

$$gq_1 + r_1 = gq_1 + r_2$$

следует $r_1 = r_2$. Теорема доказана. ■

Замечание Наиболее важный частный случай — когда R является полем. В этом случае условие "старший коэффициент обратим" автоматически выполняется для любого ненулевого многочлена g.

Замечание Как и в случае кольца целых чисел, многочлены q и r называются соответственно неполным частным и остатком при делении f на g. Естественно, f делится на g тогда и только тогда, когда $r = 0$.

18 Гомоморфизм подстановки

Для начала напомним, что такое гомоморфизм кольца R в кольцо S. Это отображение (не обязательно биективное) $\varphi : R \to S$ такое, что

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$;
2. $\varphi(ab) = \varphi(a)\varphi(b)$ для всех $a, b \in R$.

Мы будем рассматривать только ассоциативные кольца с единицей и требовать от всех гомоморфизмов, чтобы они были унитарными, то есть выполнялось условие $\varphi(1) = 1$.

Примеры гомоморфизмов:

1. Любое вложение подкольца в кольцо (например, $\mathbb{Z}$ в $\mathbb{Q}$).
2. Отображение $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, сопоставляющее целому числу его класс вычетов по модулю m.
3. Комплексное сопряжение $\mathbb{C} \to \mathbb{C}$.

Предложение. *Пусть B — кольцо, A — его подкольцо, причём элементы A коммутируют с любыми элементами B:*

$$\forall a \in A,\, \forall b \in B\colon ab = ba.$$

Обозначим через $A[b]$ подкольцо кольца B, порождённое A и элементом $b \in B$. Зафиксируем $b \in B$. Тогда отображение

$$\begin{aligned}\varphi_b\colon A[x] &\longrightarrow A[b],\\ a_n x^n + \cdots + a_1 x + a_0 &\longmapsto a_n b^n + \cdots + a_1 b + a_0\end{aligned}$$

является гомоморфизмом колец.

О чём здесь речь?

Если у вас есть кольцо многочленов $A[x]$, то вы можете вместо переменной x подставлять элементы некоторого большего кольца B, содержащего A. Подстановка b вместо x даёт гомоморфизм из $A[x]$ в подкольцо $A[b] \subset B$. Если вы сначала сложите многочлены, а потом подставите b, вы получите тот же результат, что и при подстановке b в каждый многочлен с последующим сложением. То же самое верно и для произведения.

Важно, что подставлять можно не только элементы самого кольца A, но и элементы надкольца B (которое даже не обязано быть коммутативным), при условии, что элементы A коммутируют с элементом b.

Далее, при доказательстве теоремы будем обозначать $\varphi_b(f)$ через $f(b)$; этот элемент можно называть результатом подстановки b в f.

Доказательство. Легко видеть, что для любых $f, g \in A[x]$ выполняется

$$(f+g)(b) = f(b) + g(b)$$

и что

$$1(b) = 1.$$

Таким образом, уже проверено, что φ_b сохраняет сумму и единицу.

Осталось проверить, что

$$(fg)(b) = f(b)\, g(b).$$

В силу дистрибутивности и уже установленного свойства $(f+g)(b) = f(b) + g(b)$ достаточно рассмотреть случай мономов.

Пусть

$$f(x) = cx^m, \quad g(x) = dx^n,$$

где $c, d \in A$. Тогда

$$fg = cdx^{m+n},$$

и

$$(fg)(b) = (cdx^{m+n})(b) = cd\, b^{m+n}.$$

Так как элементы A (в частности, c и d) коммутируют с b, имеем

$$cd\, b^{m+n} = c\, b^m\, d\, b^n = (cb^m)(db^n) = f(b)\, g(b).$$

Отсюда следует, что φ_b сохраняет произведение, то есть является гомоморфизмом колец. ■

В частности, всегда можно подставить в многочлен $f \in A[x]$ любой элемент самого кольца A (берём $B = A$ и $b \in A$). Результат подстановки тесно связан с делением с остатком, как видно из следующей теоремы.

19 Теорема Безу. Число корней многочлена над областью

Предложение. *Пусть $f \in R[x]$, $c \in R$. Тогда остаток при делении f на $\big(x - c\big)$ равен $f(c)$.*

Доказательство. По теореме о делении с остатком имеем

$$f(x) = \big(x - c\big)g(x) + r(x),$$

где $\deg r < 1$, то есть r является константным многочленом. Подставляя $x = c$, получаем

$$f(c) = \big(c - c\big)g(c) + r(c) = r(c) = r,$$

так как значение константного многочлена в любой точке равно самой этой константе. ■

Замечание Иногда это утверждение называют *второй теоремой Безу*, а *первой теоремой Безу* считают её частный случай: $f(c) = 0$ тогда и только тогда, когда f делится на $\big(x - c\big)$.

Пусть $f \in R[x]$. Элементы кольца R (или некоторого его надкольца S), для которых $f(c) = 0$, называются корнями f в R (соответственно в S). Например, многочлен $x^4 - 2 \in \mathbb{Z}[x]$ имеет 0 корней в $\mathbb{Z}$, 2 корня в $\mathbb{R}$ и 4 корня в $\mathbb{C}$.

Предложение. *Пусть R — область целостности, $f \in R[x]$ — ненулевой многочлен,* $\deg f = d \geqslant 0$. *Тогда число* попарно различных *корней f в R не превосходит d.*

Доказательство. Доказательство проведём индукцией по степени $d = \deg f$.

При $d = 0$ многочлен f является ненулевой константой и не имеет корней в R, так что утверждение верно.

Пусть теперь $d > 0$ и теорема уже доказана для всех степеней $< d$. Если у f нет корней в R, то утверждение очевидно.

Предположим, что корни есть, и пусть

$$c_1, \ldots, c_l \in R$$

— все попарно различные корни многочлена f в R. Возьмём один из них, например c_l. По теореме Безу из равенства $f(c_l) = 0$ следует, что

$$f(x) = \big(x - c_l\big)g(x)$$

для некоторого $g \in R[x]$.

Для каждого $i = 1, \ldots, l - 1$ имеем

$$0 = f(c_i) = \big(c_i - c_l\big)g(c_i).$$

Так как $c_i \neq c_l$, то $c_i - c_l \neq 0$. Используя то, что R — область целостности (произведение ненулевых элементов не может быть нулём), заключаем, что

$$g(c_i) = 0$$

для всех $i = 1, \ldots, l-1$.

Таким образом, $c_1, \ldots, c_{l-1}$ — попарно различные корни многочлена g, причём ясно, что $\deg g = d - 1$. По индукционному предположению число различных корней g в R не превосходит $d - 1$, то есть $l - 1 \leqslant d - 1$. Отсюда $l \leqslant d$, что и требовалось. ■

Замечание Здесь существенно, что R — область целостности. Например, многочлен $x^2 - \overline{1}$, рассматриваемый как элемент $(\mathbb{Z}/8\mathbb{Z})[x]$ (или $(\mathbb{Z}/15\mathbb{Z})[x]$, или вообще над некоторыми нетелами), может иметь больше корней, чем его степень (проверьте это как упражнение).

20 Формальное и функциональное равенство многочленов от одной переменной

Предложение. *Пусть R — бесконечная область целостности, $f, g \in R[x]$ таковы, что они задают одинаковые отображения из R в R, то есть*

$$f(a) = g(a) \quad \textit{для всех } a \in R.$$

Тогда $f = g$ как многочлены.

Формальное равенство многочленов означает равенство всех их коэффициентов. Из формального равенства всегда следует функциональное: если коэффициенты совпадают, то и значения на всех $a \in R$ совпадают.

Доказательство. Рассмотрим многочлен

$$h(x) = f(x) - g(x).$$

По условию теоремы для любого $a \in R$ имеем

$$h(a) = f(a) - g(a) = 0,$$

то есть каждый элемент $a \in R$ является корнем многочлена h.

Если бы h был ненулевым многочленом, то, поскольку R — область целостности, число его различных корней в R не могло бы превышать $\deg h$, то есть было бы конечно. Но R по условию бесконечно, а элементы R дают бесконечное множество корней h, что возможно только в случае $h = 0$.

Следовательно, $h(x) = 0$ как многочлен, то есть $f = g$. ■

Замечание Здесь важны оба условия: и то, что R — область целостности, и то, что она бесконечна. Например, если $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — поле из p элементов (p — простое число), то многочлены

x^p и x задают одно и то же отображение $\mathbb{F}_p \to \mathbb{F}_p$ (это следует из малой теоремы Ферма), хотя формально они различны.

Вообще, в любом кольце $R[x]$ с конечным R найдутся формально различные, но функционально равные многочлены (подумайте, как это доказать, используя ограниченность числа возможных отображений $R \to R$).

21 Делимость и ассоциированные элементы. Определение НОД

Пусть R — коммутативное ассоциативное кольцо с единицей.

Определение. Элемент $x \in R$ *делит* элемент $y \in R$, если существует такой элемент $z \in R$, что

$$y = x \cdot z.$$

В этом случае пишут $x \mid y$. Можно также сказать, что y лежит в главном идеале, порождённом элементом x.

Определение. Элемент $d \in R$ называется *наибольшим общим делителем* (НОД) элементов $a, b \in R$, если выполняются два условия:

- $d \mid a$ и $d \mid b$;
- если $d' \mid a$ и $d' \mid b$ для некоторого $d' \in R$, то $d' \mid d$.

Определение. Элементы $a, b \in R$ называются *ассоциированными*, если $a \mid b$ и $b \mid a$.

Лемма. *Пусть d — НОД элементов a и b в R, а $d' \in R$. Тогда элемент d' также является НОД a и b тогда и только тогда, когда d' ассоциирован с d.*

Лемма. *Пусть R — область целостности, $a, b \in R$. Тогда элементы a и b ассоциированы тогда и только тогда, когда*

$$b = a \cdot \varepsilon$$

для некоторого обратимого элемента $\varepsilon \in R$.

Доказательство. Докажем оба направления.

"$\Longleftarrow$": если

$$b = a \cdot \varepsilon$$

для некоторого обратимого элемента $\varepsilon \in R$, то сразу имеем $a \mid b$. Поскольку ε обратим, существует $\varepsilon^{-1} \in R$ и

$$a = b \cdot \varepsilon^{-1},$$

откуда $b \mid a$. Следовательно, a и b ассоциированы.

"$\Longrightarrow$": предположим, что a и b ассоциированы, то есть

$$a \mid b \quad \text{и} \quad b \mid a.$$

Тогда существуют элементы $\varepsilon, \varepsilon' \in R$ такие, что

$$b = a\varepsilon, \qquad a = b\varepsilon'.$$

Подставляя первое равенство во второе, получаем

$$a = a\varepsilon\varepsilon'.$$

Переносим в одну сторону:

$$a(\varepsilon\varepsilon' - 1) = 0.$$

Если $a \neq 0$, то, так как R — область целостности (в ней нет делителей нуля), из равенства выше следует

$$\varepsilon\varepsilon' - 1 = 0,$$

то есть $\varepsilon\varepsilon' = 1$, и, следовательно, ε обратим.

Если же $a = 0$, то из ассоциированности следует и $b = 0$. В этом случае можно взять $\varepsilon = 1$, и равенство $b = a\varepsilon$ также выполняется тривиально. ■

22 Евклидовы кольца и область главных идеалов

Область целостности R называется *евклидовой областью* (или евклидовым кольцом), если существует функция

$$\nu\colon R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geqslant 0},$$

такая, что выполняются следующие условия:

1. если $d \mid a$ и $d \neq 0$, то $\nu(d) \leqslant \nu(a)$, причём равенство имеет место тогда и только тогда, когда d и a ассоциированы;
2. для любых $a, b \in R$ при $b \neq 0$ существует представление

   $$a = bq + r,$$

   где либо $r = 0$, либо $\nu(r) < \nu(b)$.

Функция ν называется *евклидовой нормой*.

Пример 1. *Кольцо целых чисел $\mathbb{Z}$ евклидово, если положить $\nu(a) = |a|$ для $a \neq 0$.*

Замечание В качестве евклидовой нормы на $\mathbb{Z}$ можно взять, например, функцию $\nu(a) = 17|a|+3$ — свойства евклидовости сохранятся.

Пример 2. Для любого поля K кольцо многочленов $K[X]$ евклидово, если в качестве евклидовой нормы взять степень многочлена: $\nu(f) = \deg f$ для $f \neq 0$. Таким образом, у нас уже есть бесконечно много евклидовых колец.

Пример 3. Евклидовым является и кольцо целых гауссовых чисел

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

В качестве евклидовой нормы берут квадрат модуля:

$$\nu(a + bi) = a^2 + b^2.$$

Пример 4. Если K — поле, то кольцо формальных степенных рядов $K[[X]]$ тоже является евклидовой областью. В качестве евклидовой нормы можно взять функцию порядка:

$$\operatorname{ord}\left(\sum_{i=0}^{\infty} a_i X^i\right) = \min\{\, i \mid a_i \neq 0 \,\}.$$

Известно, что ряд $f \in K[[X]]$ обратим тогда и только тогда, когда $\operatorname{ord} f = 0$. Следовательно, любой ряд порядка d ассоциирован с X^d, и делимость в $K[[X]]$ описывается так: если f, g — два ненулевых ряда, то

$$f \mid g \quad \Longleftrightarrow \quad \operatorname{ord} f \leqslant \operatorname{ord} g.$$

Пример 5. Рассмотрим локализацию кольца целых по простому числу 5:

$$\mathbb{Z}_{(5)} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z},\ 5 \nmid b \right\}.$$

Это также пример евклидовой области (подходящую норму можно подобрать, например, через 5-адический порядок).

Замечание Можно встретить определение евклидова кольца, в котором первая аксиома (про сравнение норм делителя и кратного) не упоминается. Оно эквивалентно приведённому выше, но на практике обычно менее удобно.

Замечание Любое поле формально удовлетворяет определению евклидова кольца, если положить евклидову норму тождественно равной нулю на всех ненулевых элементах. Все требования деления с остатком в этом случае выполняются тривиально.

Определение. Пусть R — коммутативное кольцо и $a \in R$. Множество

$$(a) = \{ax \mid x \in R\}$$

называется *главным идеалом*, порождённым элементом a.

Пример неглавного идеала. Рассмотрим кольцо многочленов $\mathbb{Z}[X]$ и множество

$$I = \{f \in \mathbb{Z}[X] \mid 2 \mid f(0)\},$$

то есть все многочлены с чётным свободным членом. Легко проверить, что I является идеалом, но не может быть порождён одним элементом, значит, это неглавный идеал.

Теперь покажем, что любой идеал в евклидовом кольце R является главным, то есть имеет вид

$$(c) = \{ca \mid a \in R\}$$

для некоторого $c \in R$.

Предложение. *В евклидовом кольце все идеалы главные.*

Доказательство. Пусть R — произвольное евклидово кольцо с евклидовой нормой ν, и пусть $I \subset R$ — идеал.

Если $I = \{0\}$, то это главный идеал, порождённый нулём:

$$I = (0).$$

Рассмотрим теперь случай $I \neq \{0\}$. Выберем в I произвольный ненулевой элемент c с минимальным возможным значением $\nu(c)$ среди всех ненулевых элементов I, и покажем, что $I = (c)$.

Включение $(c) \subset I$ очевидно: из $c \in I$ следует

$$(c) = \{ca \mid a \in R\} \subset I.$$

Докажем обратное включение $I \subset (c)$. Пусть $a \in I$ — произвольный элемент. По определению евклидовой области, существуют $q, r \in R$ такие, что

$$a = cq + r,$$

где либо $r = 0$, либо $\nu(r) < \nu(c)$.

Так как $a \in I$ и $c \in I$, а I — идеал, имеем

$$r = a - cq \in I.$$

Если бы $r \neq 0$, то мы получили бы ненулевой элемент $r \in I$ с $\nu(r) < \nu(c)$, что противоречит минимальности $\nu(c)$. Следовательно, $r = 0$, и потому $a = cq$, то есть $a \in (c)$.

Таким образом, $I \subset (c)$ и, вместе с уже доказанным включением $(c) \subset I$, получаем $I = (c)$. ■

Определение. Области целостности, в которых все идеалы главные, называются *областями главных идеалов* (ОГИ, или по-английски PID — principal ideal domains).

23 Существование и линейное представление НОД в области главных идеалов

Предложение. *Пусть R — область главных идеалов.*

1. *Если $a, b \in R$, то у пары a, b существует наибольший общий делитель.*
2. *Если d — НОД a и b, то существует представление*

$$d = am + bn$$

для некоторых $m, n \in R$.

Доказательство. Можно считать, что хотя бы один из элементов a и b отличен от нуля.

Рассмотрим множество

$$I = \{am + bn \mid m, n \in R\}.$$

Это идеал в R; принято обозначать его (a, b) и называть идеалом, порождённым элементами a и b.

Так как R — область главных идеалов, существует элемент $d \in R$ такой, что

$$I = (a, b) = (d).$$

Тогда, во-первых, $a, b \in I = (d)$, откуда следует

$$d \mid a \quad \text{и} \quad d \mid b.$$

Во-вторых, из равенства $I = (d)$ следует, что сам элемент d лежит в I, то есть

$$d = am_0 + bn_0$$

для некоторых $m_0, n_0 \in R$, что и даёт линейное представление НОД.

Покажем, что d действительно является наибольшим общим делителем a и b в принятом ранее смысле.

Пусть $d' \in R$ — любой общий делитель a и b, то есть

$$d' \mid a \quad \text{и} \quad d' \mid b.$$

Тогда d' делит любую линейную комбинацию a и b, в частности

$$d' \mid (am_0 + bn_0) = d.$$

Таким образом, d делит a и b, а любой общий делитель d' делит d, то есть d — НОД a и b. ■

24 Свойства взаимно простых элементов в евклидовом кольце. Неприводимые элементы

Так как всякая евклидова область является областью главных идеалов, будем формулировать и доказывать результаты в терминах ОГИ.

Определение. Пусть R — область главных идеалов. Элементы $a, b \in R$ называются *взаимно простыми*, если их НОД ассоциирован с единицей, то есть один (а значит, и любой) наибольший общий делитель a и b ассоциирован с 1.

Альтернативное определение. Элементы $a, b \in R$ взаимно просты тогда и только тогда, когда существуют $m, n \in R$ такие, что

$$am + bn = 1.$$

Доказательство. "$\Longrightarrow$": пусть d — НОД a и b. В области главных идеалов по предыдущей теореме существует представление

$$d = am_0 + bn_0$$

для некоторых $m_0, n_0 \in R$. Если d ассоциирован с 1 (то есть $d = u$ или $d = u^{-1}$ для некоторого обратимого u), то, домножив на обратимый элемент, получаем представление

$$1 = am + bn$$

для некоторых $m, n \in R$.

"$\Longleftarrow$": пусть существуют $m, n \in R$ такие, что

$$am + bn = 1.$$

Возьмём d — НОД a и b. Тогда

$$d \mid a \quad \text{и} \quad d \mid b,$$

следовательно, d делит любую линейную комбинацию a и b, в частности $d \mid 1$. Отсюда следует, что d ассоциирован с 1, а значит, a и b взаимно просты по первому определению. ■

Если элементы a и b взаимно просты, то единицу всегда можно представить в виде $am + bn$ для некоторых $m, n \in R$, и это условие эквивалентно взаимной простоте.

Иными словами, взаимная простота равносильна существованию линейного представления единицы через a и b.

Определение. Неприводимый элемент в коммутативном кольце R с единицей — это такой элемент $a \in R$, что:

- $a \neq 0$;
- $a \notin R^*$ (не является обратимым);
- из представления $a = bc$ следует, что либо $b \in R^*$, либо $c \in R^*$.

Элементы $a \in R$, которые не являются ни неприводимыми, ни обратимыми, ни нулём, называют *приводимыми*.

Неприводимые элементы в $\mathbb{Z}$ — это (с точностью до ассоциированности) простейшие числа. В кольце $K[X]$ над полем K любой многочлен степени 1 неприводим, а многочлены большей степени могут как быть, так и не быть неприводимыми. Например, многочлен X^2+1 неприводим как элемент $\mathbb{R}[X]$, но разлагается на линейные множители в $\mathbb{C}[X]$:

$$X^2 + 1 = (X + i)(X - i).$$

Лемма. *Пусть K — поле и $f \in K[X]$ — многочлен степени 2 или 3. Тогда f приводим тогда и только тогда, когда имеет корень в K.*

Доказательство. Если $f(a) = 0$ для некоторого $a \in K$, то по теореме Безу $(X - a) \mid f$, то есть

$$f(X) = (X - a)g(X)$$

для некоторого $g \in K[X]$, и, следовательно, f приводим.

Обратно, пусть f приводим, то есть $f = gh$ с ненулевыми ненасильными множителями $g, h \in K[X]$ и $\deg g, \deg h \geqslant 1$. Тогда

$$\deg f = \deg g + \deg h \leqslant 3,$$

откуда следует, что хотя бы один из многочленов g или h имеет степень 1 (линейный многочлен). Линейный многочлен над полем всегда имеет корень, значит, либо g, либо h имеет корень в K, который одновременно является корнем f. ■

Однако многочлен степени $\geqslant 4$ может не иметь корней и при этом быть приводимым. Например, в кольце $\mathbb{R}[X]$ многочлен

$$X^4 + X^2 + 1 = (X^2 + 1)^2 - X^2 = (X^2 + X + 1)(X^2 - X + 1)$$

приводим, но вещественных корней не имеет.

Лемма. *Пусть R — область главных идеалов, а $p, f \in R$, причём p неприводимый. Тогда либо $p \mid f$, либо $(p, f) = 1$ (то есть p и f взаимно просты).*

Доказательство. Пусть d — НОД элементов p и f. Тогда $d \mid p$, а значит, d либо обратим, либо ассоциирован с p (так как p неприводим).

Если d обратим, то $(p, f) = 1$ по определению взаимной простоты. Если же d не обратим, то он ассоциирован с p, то есть $d = pu$ для некоторого обратимого $u \in R$. В этом случае из того, что $d \mid f$, следует $p \mid f$. ■

Предложение. *Пусть R — область главных идеалов, а $p \in R$ — неприводимый элемент. Если $p \mid ab$ для некоторых $a, b \in R$, то $p \mid a$ или $p \mid b$. Иными словами, в ОГИ каждый неприводимый элемент является простым.*

Доказательство. Предположим противное: пусть $p \nmid a$ и $p \nmid b$. Тогда по предыдущей лемме имеем

$$(p, a) = 1 \quad \text{и} \quad (p, b) = 1.$$

Следовательно, существуют $m, n, m', n' \in R$ такие, что

$$pm + an = 1, \qquad pm' + bn' = 1.$$

Перемножим эти равенства:

$$1 = (pm + an)(pm' + bn') = p(\, pmm' + mbn' + anm' \,) + abnn'.$$

По условию теоремы $p \mid ab$, значит, существует $k \in R$ такой, что $ab = pk$. Тогда

$$abnn' = p(knn'),$$

и всё выражение справа является кратным p, то есть $p \mid 1$. Это невозможно (так как p не обратим), противоречие.

Следовательно, наше предположение неверно и, значит, если $p \mid ab$, то $p \mid a$ или $p \mid b$. ■

25 Факториальность евклидова кольца

Будем обозначать ассоциированные элементы как $a \sim b$.

В области целостности R справедливо:

$$a \sim b \iff a = \varepsilon b,$$

где $\varepsilon \in R^*$ (то есть один элемент получается из другого умножением на обратимый).

Определение. Факториальное кольцо (или область факторизации) — это область целостности R, в которой выполнены следующие свойства:

1. Любой элемент $a \in R$, отличный от нуля и не являющийся обратимым, раскладывается в произведение неприводимых:
$$a = p_1 \cdots p_s,$$
где все p_i — неприводимые элементы.

2. Такое разложение *почти единственно*: если

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

где все p_i и q_j неприводимы, а $s, t > 0$, то $s = t$ и после перестановки сомножителей выполнено

$$p_1 \sim q_1, \ \ldots, \ p_s \sim q_s.$$

ОЦ $\supset$ **ФК** $\supset$ **ОГИ** $\supset$ **ЕО**: любая евклидова область является областью главных идеалов, каждая область главных идеалов факториальна, а всякая факториальная область — область целостности.

Предложение. *Евклидово кольцо (евклидова область) является факториальным кольцом.*

Доказательство. Пусть R — евклидово кольцо, ν — соответствующая евклидова норма.

1. Существование разложения на неприводимые. Докажем индукцией по $n \in \mathbb{Z}_{\geq 0}$, что любой элемент $a \neq 0$ с $\nu(a) \leq n$ либо обратим, либо раскладывается в произведение неприводимых.

База индукции, $n = 0$. Пусть $\nu(a) = 0$. Рассмотрим деление единицы на a:

$$1 = aq + r,$$

где либо $r = 0$, либо $\nu(r) < \nu(a) = 0$. Второй случай невозможен, так как норма не может быть отрицательной, значит $r = 0$ и $1 = aq$, то есть a обратим.

Переход. Пусть $n > 0$ и утверждение верно для всех элементов с нормой $< n$. Рассмотрим $a \in R$ с $\nu(a) = n$. Если a обратим или неприводим, всё уже выполнено. Предположим, что a не обратим и приводим, то есть

$$a = bc$$

с необратимыми элементами $b, c \in R$. По определению евклидовой нормы имеем

$$\nu(b) < \nu(a), \quad \nu(c) < \nu(a),$$

поэтому по индукционному предположению и b, и c раскладываются в произведения неприводимых. Тогда и a раскладывается в произведение неприводимых. Существование доказано.

2. Единственность разложения (с точностью до порядка и ассоциированности). Пусть

$$p_1 \cdots p_s = q_1 \cdots q_t,$$

где все p_i и q_j — неприводимые элементы. Без ограничения общности будем считать, что $s \geq t$. Докажем единственность по индукции по s.

Если $s = 1$, то имеем

$$p_1 = q_1 \cdots q_t.$$

Так как слева стоит неприводимый элемент, то справа не может быть нетривиального произведения необратимых, значит $t = 1$ и $p_1 \sim q_1$.

Пусть теперь $s > 1$. Из равенства

$$p_1 \cdots p_s = q_1 \cdots q_t$$

следует, что

$$p_s \mid q_1 \cdots q_t.$$

Так как в евклидовой области (а значит, и в ОГИ) неприводимые элементы являются простыми, из $p_s \mid q_1 \cdots q_t$ вытекает, что $p_s \mid q_i$ для некоторого i. Перенумеровав при необходимости множители справа, можем считать, что $i = t$. Тогда из неприводимости p_s и q_t следует

$$p_s \sim q_t,$$

то есть существует обратимый элемент $\varepsilon \in R^*$ такой, что

$$p_s = \varepsilon q_t.$$

Подставляя это в исходное равенство и сокращая на q_t, получаем

$$(\varepsilon p_1) p_2 \cdots p_{s-1} = q_1 \cdots q_{t-1}.$$

Здесь произведение слева по-прежнему состоит из неприводимых элементов (умножение на обратимый элемент не нарушает неприводимость). Применяя индукционное предположение к этой новой равенству, получаем единственность разложения с точностью до перестановки и ассоциированности. ■

26 p-адический показатель и каноническое разложение

Определение. Пусть R — факториальное кольцо (область факторизации), а $p \in R$ — неприводимый элемент. Для любого $a \in R$ определим *p-адический показатель* (или p-адическую валюацию)

$$v_p(a) = \sup\{\, n \in \mathbb{Z}_{\geq 0} \mid p^n \mid a \,\}.$$

Замечание Обычно дополнительно полагают $v_p(0) = +\infty$.

Предложение. *Пусть $a \neq 0$. Тогда $v_p(a) = n$ тогда и только тогда, когда*

$$a = p^n c, \quad p \nmid c.$$

Доказательство. "$\Longrightarrow$": если $v_p(a) = n$, то по определению $p^n \mid a$ и $p^{n+1} \nmid a$. Первое означает, что существует $c \in R$ такое, что

$$a = p^n c.$$

Если бы $p \mid c$, то $c = pc'$, и тогда $a = p^{n+1} c'$, то есть $p^{n+1} \mid a$, что противоречит максимальности n. Поэтому $p \nmid c$.

"$\Longleftarrow$": пусть $a = p^n c$ и $p \nmid c$. Тогда

$$p^n \mid a,$$

то есть $v_p(a) \geq n$. Если бы $v_p(a) \geq n+1$, то существовал бы элемент $d \in R$ такой, что

$$a = p^{n+1} d.$$

Тогда

$$p^n c = p^{n+1} d \quad \Longrightarrow \quad c = pd,$$

откуда $p \mid c$, противореча условию. Значит, $v_p(a) = n$. ■

Предложение. *Пусть $a \neq 0$, $b \neq 0$. Тогда*

$$v_p(ab) = v_p(a) + v_p(b).$$

Доказательство. Обозначим $n = v_p(a)$ и $m = v_p(b)$. По предыдущей теореме можно записать

$$a = p^n c, \quad b = p^m d,$$

где $p \nmid c$ и $p \nmid d$. Тогда

$$ab = p^n c \cdot p^m d = p^{n+m} \cdot cd.$$

Если бы $p \mid cd$, то, так как p в факториальном кольце является простым элементом (неприводимый в ФК всегда прост), из $p \mid cd$ следовало бы $p \mid c$ или $p \mid d$, что противоречит выбору c и d. Следовательно, $p \nmid cd$, и по предыдущей теореме имеем

$$v_p(ab) = n + m.$$

■

Разложение элемента факториального кольца на неприводимые неоднозначно в двух аспектах:

1. можно менять порядок множителей;
2. каждый множитель определён с точностью до ассоциированности.

От второго можно избавиться, если в каждом классе ассоциированности неприводимых элементов зафиксировать по одному представителю.

Пример. В кольце целых чисел $\mathbb{Z}$ (которое факториально) любой ненулевой элемент можно разложить на простые (с точностью до ассоциированности). Но при разложении можно менять знаки: например,

$$6 = 2 \cdot 3 = (-2) \cdot (-3).$$

Можно условиться, что разлагаем только на положительные простые, а если число было отрицательным, то выносим отдельно множитель -1. Например,

$$10 = 2 \cdot 5, \quad -10 = (-1) \cdot 2 \cdot 5.$$

Тогда разложение становится единственным с точностью до перестановки множителей.

Предложение. *Пусть R — факториальное кольцо, а P — множество неприводимых элементов R, содержащее ровно по одному представителю из каждого класса ассоциированных неприводимых. Тогда любой элемент $a \in R$, $a \neq 0$, единственным образом с точностью до перестановки представляется в виде*

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)},$$

где $\varepsilon \in R^*$, а почти все показатели $v_p(a)$ равны нулю (то есть произведение на самом деле конечно).

Доказательство. По определению факториальности любое $a \neq 0$ можно разложить в произведение неприводимых:

$$a = q_1 q_2 \cdots q_s.$$

Для каждого i выберем $\varepsilon_i \in R^*$ и $p_i \in P$ так, чтобы $q_i = \varepsilon_i p_i$ (то есть p_i ассоциирован с q_i). Тогда

$$a = \varepsilon_1 p_1 \cdot \varepsilon_2 p_2 \cdots \varepsilon_s p_s = (\varepsilon_1 \varepsilon_2 \cdots \varepsilon_s) \cdot p_1 p_2 \cdots p_s.$$

Обозначим

$$\varepsilon = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_s \in R^*.$$

Группируя одинаковые множители $p \in P$, можно переписать это как

$$a = \varepsilon \prod_{p \in P} p^{v_p(a)},$$

где $v_p(a)$ — число вхождений p (с учётом кратности) в разложение a на элементы множества P.

Единственность следует из единственности факторизации в факториальном кольце и того, что в P выбран ровно один представитель из каждого класса ассоциированных неприводимых: разные наборы показателей $v_p(a)$ дали бы два различных разложения на неприводимые, что противоречит факториальности. ■

Пример. Как уже отмечалось, для $R = \mathbb{Z}$ в качестве P обычно берут множество всех положительных простых чисел. Для $R = K[X]$, где K — поле, в качестве P обычно выбирают множество *унитарных* (то есть приведённых, со старшим коэффициентом 1) неприводимых многочленов. Тогда любое $f \in K[X]$ можно представить в виде

$$f = \varepsilon\, p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s},$$

где $\varepsilon \in K^*$ (если $f \neq 0$; для $f = 0$ каноническая факторизация не рассматривается), а $p_1, \ldots, p_s$ — попарно неассоциированные унитарные неприводимые многочлены, и $n_1, \ldots, n_s \in \mathbb{N}$.

27 Кратные корни, сумма кратностей корней многочлена

Вспомним, что по теореме Безу для $a \in R$ выполнено:

$$f(a) = 0 \iff (X - a) \mid f.$$

Определение. Пусть $f \in R[X]$, $f \neq 0$, и $a \in R$ — корень f. *Кратностью* корня a называется наибольшее целое число $n \geq 1$ такое, что $(X - a)^n \mid f$.

Определение. Корень кратности 1 называется *простым*, кратности 2 — *двойным*, кратности 3 — *тройным* и т.д. Корень кратности ≥ 2 называется *кратным корнем*.

Предложение. *Пусть R — поле, $f \in R[X]$, $\deg f = d \geq 1$, $a_1, \ldots, a_s$ — все попарно различные корни f в R, а $n_1, \ldots, n_s$ — их кратности. Тогда*

$$n_1 + \cdots + n_s \leq d.$$

Доказательство. Так как над полем многочлены степени 1 неприводимы, можно записать каноническое разложение

$$f(X) = \varepsilon\, (X - a_1)^{n_1} (X - a_2)^{n_2} \cdots (X - a_s)^{n_s} g(X),$$

где $\varepsilon \in R^*$, а $g \in R[X]$ не имеет корней среди a_i. Тогда по свойству степени многочлена над областью целостности

$$d = \deg f = \deg \varepsilon + \sum_{i=1}^{s} \deg\big((X-a_i)^{n_i}\big) + \deg g = 0 + \sum_{i=1}^{s} n_i + \deg g.$$

Отсюда

$$d = n_1 + \cdots + n_s + \deg g \ \geq \ n_1 + \cdots + n_s,$$

что и требовалось. Равенство $d = \deg(fg) = \deg f + \deg g$ корректно, потому что поле является областью целостности и при умножении ненулевых многочленов старший коэффициент не обнуляется. ■

28 Производная многочлена, её свойства

Определение. Пусть R — коммутативное кольцо и

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in R[X].$$

(Формальной) производной многочлена f называется многочлен

$$f'(X) = n a_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2 X + a_1.$$

Предложение. *Пусть $f, g \in R[X]$. Тогда:*

1. $(f+g)' = f' + g'$;
2. $(fg)' = f'g + fg'$;
3. *если $n \in \mathbb{N}$, то* $(f^n)' = n f^{n-1} f'$.

Доказательство. 1. Линейность производной непосредственно вытекает из определения: производная суммы полиномов равна сумме производных соответствующих мономов.

2. Сначала проверим правило произведения для мономов. Пусть $f = aX^n$, $g = bX^m$. Тогда

$$\begin{aligned}(fg)' &= (abX^{n+m})' = ab(n+m)X^{n+m-1} \\ &= abnX^{n+m-1} + abmX^{n+m-1} \\ &= (naX^{n-1})(bX^m) + (aX^n)(mbX^{m-1}) \\ &= f'g + fg'.\end{aligned}$$

Пусть теперь f — моном, а

$$g = g_0 + g_1 + \cdots + g_m,$$

где каждый g_i — моном. Тогда, используя линейность,

$$\begin{aligned}(fg)' &= \left(\sum_{i=0}^{m} f g_i\right)' = \sum_{i=0}^{m} (f g_i)' \\ &= \sum_{i=0}^{m} (f' g_i + f g_i') = f' \sum_{i=0}^{m} g_i + f \sum_{i=0}^{m} g_i' \\ &= f'g + fg'.\end{aligned}$$

Наконец, для произвольных f и g разлагаем каждое в сумму мономов и применяем те же рассуждения по очереди к каждому слагаемому, пользуясь уже доказанными линейностью и случаем «моном на произвольный полином».

3. Докажем формулу $(f^n)' = nf^{n-1}f'$ по индукции по n. При $n = 1$ получаем $(f^1)' = f'$, что верно.

   Пусть формула верна для некоторого $n \geq 1$. Тогда

   $$f^{n+1} = f^n \cdot f,$$

   и по правилу произведения

   $$(f^{n+1})' = (f^n f)' = (f^n)' f + f^n f'.$$

   По индукционному предположению $(f^n)' = nf^{n-1}f'$, поэтому

   $$\begin{aligned}(f^{n+1})' &= nf^{n-1}f' \cdot f + f^n f' \\ &= nf^n f' + f^n f' \\ &= (n+1)f^n f',\end{aligned}$$

   что и требовалось.

■

29 Кратные корни и производная

Предложение. *Пусть K — поле, $f \in K[X]$, $f \neq 0$, $a \in K$. Тогда a является кратным корнем f тогда и только тогда, когда*

$$f(a) = 0 \quad и \quad f'(a) = 0.$$

Доказательство. "$\Longrightarrow$": пусть a — корень кратности как минимум 2. Тогда

$$f(X) = (X-a)^2 h(X)$$

для некоторого многочлена $h \in K[X]$. Очевидно, $f(a) = 0$. Для производной имеем

$$\begin{aligned}f'(X) &= \big((X-a)^2 h(X)\big)' = \big((X-a)^2\big)' h(X) + (X-a)^2 h'(X) \\ &= 2(X-a)h(X) + (X-a)^2 h'(X) \\ &= (X-a)\big(2h(X) + (X-a)h'(X)\big),\end{aligned}$$

откуда сразу следует $f'(a) = 0$.

"$\Longleftarrow$": пусть $f(a) = f'(a) = 0$. Тогда по теореме Безу можно написать

$$f(X) = (X-a)g(X)$$

для некоторого $g \in K[X]$. Дифференцируя, получаем

$$f'(X) = \big((X-a)g(X)\big)' = (X-a)'g(X) + (X-a)g'(X) = g(X) + (X-a)g'(X).$$

Из условия $f'(a) = 0$ следует

$$0 = f'(a) = g(a),$$

то есть $g(a) = 0$, и, значит, $(X-a) \mid g(X)$. Следовательно, $(X-a)^2 \mid f(X)$, и a — кратный корень f. ■

Следствие:Пусть K — поле, $f \in K[X]$, $f \neq 0$, $a \in K$, и обозначим через D наибольший общий делитель многочленов f и f'. Тогда a является кратным корнем f тогда и только тогда, когда $D(a) = 0$.

Доказательство.

$$\begin{aligned} a \text{ — кратный корень } f &\iff f(a) = f'(a) = 0 \\ &\iff (X-a) \mid f \text{ и } (X-a) \mid f' \\ &\iff (X-a) \mid D \\ &\iff D(a) = 0. \end{aligned}$$

Здесь используется определение НОД в $K[X]$ и то, что $K[X]$ является областью главных идеалов. ■

Определение. *Характеристика* кольца K с единицей. Если не существует натурального числа n такого, что

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}} = 0,$$

то говорят, что $\operatorname{char} K = 0$. В противном случае характеристикой называется

$$\operatorname{char} K = \min \left\{ n \in \mathbb{N} \,\middle|\, \underbrace{1 + 1 + \cdots + 1}_{n \text{ раз}} = 0 \right\}.$$

Замечание Для поля характеристика может быть только либо нулём, либо простым числом.

Примеры.

$$\operatorname{char} \mathbb{Z} = 0, \qquad \operatorname{char}(\mathbb{Z}/m\mathbb{Z}) = m.$$

Предложение. *Пусть K — поле нулевой характеристики, $f \in K[X]$, $a \in K$ — корень f кратности $s \geq 2$. Тогда a является корнем f' кратности в точности $s-1$.*

Доказательство. Представим

$$f(X) = (X-a)^s g(X),$$

где $(X-a) \nmid g(X)$, так что $g(a) \neq 0$. Тогда

$$\begin{aligned} f'(X) &= \big((X-a)^s g(X)\big)' \\ &= \big((X-a)^s\big)' g(X) + (X-a)^s g'(X) \\ &= s(X-a)^{s-1} g(X) + (X-a)^s g'(X) \\ &= (X-a)^{s-1}\big(s g(X) + (X-a) g'(X)\big). \end{aligned}$$

Обозначим

$$h(X) = sg(X) + (X - a)g'(X).$$

Тогда

$$h(a) = sg(a).$$

Поскольку $\operatorname{char} K = 0$, число s не обращается в нуль в K, а $g(a) \neq 0$, значит $h(a) \neq 0$. Следовательно, $(X - a) \nmid h(X)$, и a является корнем f' кратности ровно $s - 1$. ■

30 Разложение многочлена по степеням заданного многочлена

Предложение. *Пусть K — поле, $f, g \in K[X]$, $f \neq 0$, $d = \deg g \geq 1$. Тогда f можно единственным образом представить в виде*

$$f = h_n g^n + h_{n-1} g^{n-1} + \cdots + h_1 g + h_0,$$

где $n \geq 0$, $h_0, \ldots, h_n \in K[X]$, $h_n \neq 0$, и для всех i выполняется неравенство $\deg h_i \leq d - 1$.

О чём эта теорема?

Если у вас есть два ненулевых многочлена над полем и степень g не меньше 1, то f можно разложить по степеням g так, чтобы все коэффициенты-разность множители h_i имели степень меньше, чем $\deg g$. Это похоже на запись натурального числа в системе счисления: мы раскладываем число по степеням основания системы, а коэффициентами берём цифры, «меньшие основания».

Например, $10 = 1 \cdot 3^2 + 0 \cdot 3 + 1 = 101_3$. С многочленами делаем то же самое: в качестве «цифр» выступают многочлены степени строго меньше $\deg g$, а основанием служит g. Просто последовательно делим с остатком: делим f на g, получаем остаток h_0; неполное частное снова делим на g, получаем остаток h_1 и т.д., пока не придём к нулю. Так и возникает нужное представление.

Доказательство. Проведём доказательство по индукции по $l = \deg f$.

<u>База: $l < d$.</u> В этом случае можно взять $n = 0$ и $h_0 = f$. Тогда $\deg h_0 = \deg f < d$, так что все условия теоремы выполнены.

Для единственности заметим, что из общей формы разложения следует

$$\deg f = \deg(h_n g^n) = \deg h_n + nd,$$

где $\deg h_n \leq d - 1$. Если бы $n \geq 1$, то

$$\deg f \geq d,$$

что противоречит предположению $l = \deg f < d$. Значит, $n = 0$ и разложение однозначно.

<u>Переход: $l \geq d$.</u> Разделим f на g с остатком:

$$f = gq + r,$$

где $q, r \in K[X]$ и $\deg r < d$. Так как $K[X]$ — область целостности, имеем

$$\deg f = \deg(gq) = \deg g + \deg q = d + \deg q,$$

откуда

$$\deg q = l - d < l.$$

По индукционному предположению многочлен q можно единственным образом представить в виде

$$q = h_n g^n + h_{n-1} g^{n-1} + \cdots + h_1 g + h_0,$$

где все $h_i \in K[X]$, $\deg h_i \leq d-1$, $h_n \neq 0$. Умножая это равенство на g и прибавляя остаток r, получаем

$$f = gq + r = h_n g^{n+1} + h_{n-1} g^n + \cdots + h_1 g^2 + h_0 g + r.$$

Обозначим $h'_0 = r$, $h'_1 = h_0$, $\ldots$, $h'_{n+1} = h_n$. Тогда

$$f = h'_{n+1} g^{n+1} + h'_n g^n + \cdots + h'_1 g + h'_0,$$

где $\deg h'_i \leq d-1$ (так как $\deg r < d$ и все $\deg h_i \leq d-1$), а $h'_{n+1} = h_n \neq 0$. Это даёт существование разложения для $\deg f = l$.

Для единственности предположим, что

$$f = \sum_{i=0}^{n} h_i g^i = \sum_{i=0}^{m} \tilde{h}_i g^i,$$

где все $h_i, \tilde{h}_i$ удовлетворяют условиям теоремы. Перепишем оба разложения в виде

$$f = gQ + R = g\tilde{Q} + \tilde{R},$$

где

$$Q = \sum_{i=1}^{n} h_i g^{i-1}, \quad R = h_0, \qquad \tilde{Q} = \sum_{i=1}^{m} \tilde{h}_i g^{i-1}, \quad \tilde{R} = \tilde{h}_0.$$

Тогда $\deg R, \deg \tilde{R} < d$. По единственности деления f на g с остатком имеем

$$Q = \tilde{Q}, \quad R = \tilde{R}.$$

То есть $h_0 = \tilde{h}_0$, а для Q и $\tilde{Q}$, как многочленов меньшей степени, можно применить индукционное предположение, откуда $h_i = \tilde{h}_i$ при всех $i \geq 1$. Следовательно, разложение единственно. ■

31 Формула Тейлора

Пусть K — поле характеристики 0, $f \in K[X]$, $\deg f = n \geq 0$, и $a \in K$.

Предложение (Формула Тейлора для многочленов)**.** *Многочлен f можно единственным образом представить в виде*

$$f(X) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} (X-a)^k.$$

Доказательство. По теореме о разложении по степеням заданного многочлена применим её к многочлену $g(X) = X - a$. Так как $\deg g = 1$, все коэффициенты h_k в разложении

$$f(X) = \sum_{k=0}^{n} h_k(X)\,(X-a)^k$$

имеют степень ≤ 0 и, следовательно, являются константами из K. Обозначим их через $c_k \in K$:

$$f(X) = \sum_{k=0}^{n} c_k (X-a)^k.$$

Покажем, что

$$c_k = \frac{f^{(k)}(a)}{k!} \quad \text{для всех } k = 0, \ldots, n.$$

Взяв r-ю формальную производную, получаем

$$f^{(r)}(X) = \sum_{k=r}^{n} c_k\, k(k-1)\ldots(k-r+1)\,(X-a)^{k-r}.$$

Подставляя $X = a$, видим, что все слагаемые, кроме одного, обращаются в нуль (потому что содержат положительную степень $(X-a)$), и остаётся только член при $k = r$:

$$f^{(r)}(a) = r!\,c_r.$$

Так как характеристика поля K равна 0, числа $1, 2, \ldots, r$ не обращаются в нуль в K, а значит, $r!$ обратим в K, и

$$c_r = \frac{f^{(r)}(a)}{r!}.$$

Подставляя найденные c_k обратно в разложение, получаем формулу Тейлора:

$$f(X) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}\,(X-a)^k.$$

Единственность разложения уже обеспечена теоремой о разложении по степеням многочлена $X - a$, так как там разложение единственно, а коэффициенты c_k заданы однозначно. ■

Первый семестр. Вторая четверть

32 Алгебраически замкнутые поля и основная теорема алгебры

Определение. Поле K называется *алгебраически замкнутым*, если любой ненулевой многочлен $f \in K[X]$ положительной степени имеет хотя бы один корень в K.

Предложение (Основная теорема алгебры)**.** *Поле комплексных чисел $\mathbb{C}$ алгебраически замкнуто.*

Предложение. *Если поле K алгебраически замкнуто, то многочлен $f \in K[X]$ неприводим тогда и только тогда, когда* $\deg f = 1$.

Доказательство. Пусть $\deg f \geq 2$. Так как K алгебраически замкнуто, существует корень $a \in K$ такой, что $f(a) = 0$. По теореме Безу линейный множитель $x - a$ делит f, то есть $f = (x - a)g$ для некоторого $g \in K[X]$ положительной степени. Тогда f приводим, что противоречит предположению о его неприводимости. ■

Отсюда следует, что любой ненулевой многочлен $f \in K[X]$ над алгебраически замкнутым полем раскладывается в произведение линейных множителей:

$$f(x) = c \prod_{i=1}^{\ell} (x - a_i)^{n_i},$$

где $c \in K^*$, числа a_i — попарно различные корни f, а $n_i \in \mathbb{N}$ — их кратности. Коэффициент c совпадает со старшим коэффициентом многочлена f.

33 Комплексные корни вещественных многочленов

Предложение. *Пусть $f \in \mathbb{R}[X]$ и $a \in \mathbb{C}$ — корень многочлена f. Тогда комплексно-сопряжённое число $\overline{a}$ также является корнем f той же кратности.*

Доказательство. Пусть l — кратность корня a. Тогда существует многочлен $g \in \mathbb{C}[X]$ такой, что

$$f = (X - a)^l g, \qquad g(a) \neq 0.$$

Комплексное сопряжение является автоморфизмом поля $\mathbb{C}$, поэтому для любых $g_1, g_2 \in \mathbb{C}[X]$ выполняется $\overline{g_1 g_2} = \overline{g_1}\,\overline{g_2}$.

Применяя сопряжение к равенству $f = (X-a)^l g$, получаем

$$(X-\overline{a})^l\,\overline{g} = \overline{(X-a)^l g} = \overline{f}.$$

Так как коэффициенты f вещественные, имеем $\overline{f} = f$, откуда

$$f = (X-\overline{a})^l\,\overline{g}.$$

Отсюда видно, что $\overline{a}$ — корень f кратности не меньше l. Покажем, что его кратность равна ровно l. Подставляя $\overline{a}$ в $\overline{g}$, получаем

$$\overline{g}(\overline{a}) = \overline{g(a)} \neq 0,$$

поэтому множитель $X-\overline{a}$ входит в f именно в степени l. ■

Все невещественные корни многочлена $f \in \mathbb{R}[X]$ образуют пары комплексно-сопряжённых чисел $(a_i, \overline{a_i})$. Поэтому каноническое разложение f над $\mathbb{C}$ можно записать так:

$$f(X) = c\prod_{i=1}^{k}\bigl((X-a_i)^{m_i}(X-\overline{a_i})^{m_i}\bigr)\prod_{j=1}^{\ell}(X-b_j)^{n_j},$$

где $b_j \in \mathbb{R}$ — вещественные корни.

Перемножая сопряжённую пару линейных множителей, имеем

$$(X-a_i)(X-\overline{a_i}) = X^2 - (a_i+\overline{a_i})X + a_i\overline{a_i} = X^2 - 2\operatorname{Re} a_i\, X + |a_i|^2 \in \mathbb{R}[X].$$

Следовательно, разложение f в кольце $\mathbb{R}[X]$ можно переписать в виде

$$f(X) = c\prod_{i=1}^{k}\bigl(X^2 - 2\operatorname{Re} a_i\, X + |a_i|^2\bigr)^{m_i}\prod_{j=1}^{\ell}(X-b_j)^{n_j}.$$

34 Неприводимые многочлены над полями вещественных и комплексных чисел

Предложение. *Унитарные (монные) неприводимые многочлены в $\mathbb{R}[X]$ имеют вид:*

1. *линейные многочлены $X-a$, где $a \in \mathbb{R}$;*
2. *квадратичные многочлены X^2+pX+q, где $p, q \in \mathbb{R}$ и дискриминант отрицателен: $p^2-4q < 0$.*

Доказательство. Линейный многочлен $X-a$ имеет степень 1, поэтому его нельзя представить в виде произведения двух нетривиальных многочленов; следовательно, он неприводим.

Монный многочлен второй степени $X^2 + pX + q$ разлагается над $\mathbb{R}$ в произведение линейных множителей тогда и только тогда, когда у него есть вещественный корень, то есть когда дискриминант неотрицателен. Следовательно, такой многочлен неприводим над $\mathbb{R}$ в точности при $p^2 - 4q < 0$.

Пусть теперь $\deg f \geq 3$ и $f \in \mathbb{R}[X]$ унитарен. По основной теореме алгебры многочлен f над $\mathbb{C}$ раскладывается в произведение линейных множителей. Невещественные корни попарно комплексно-сопряжены, и произведение каждой пары даёт неприводимый над $\mathbb{R}$ квадратичный множитель; вещественные корни порождают линейные множители. В итоге f представляется в $\mathbb{R}[X]$ в виде произведения по крайней мере двух ненетривиальных множителей, то есть является приводимым. ■

В $\mathbb{C}[X]$ неприводимыми являются только линейные многочлены вида $X - a$, где $a \in \mathbb{C}$, поскольку поле $\mathbb{C}$ алгебраически замкнуто.

35 Поле частных области целостности

Определение. Полем частных области целостности R называется наименьшее поле, содержащее подкольцо, изоморфное R.

Элементы поля частных удобно представлять в виде формальных дробей $\frac{a}{b}$, где $a, b \in R$ и $b \neq 0$. Опишем стандартную конструкцию такого поля.

Рассмотрим множество пар

$$R \times (R \setminus \{0\})$$

и введём на нём отношение: $(a, b) \sim (a', b')$ тогда и только тогда, когда $ab' = a'b$.

Рефлексивность и симметричность очевидны. Проверим транзитивность. Если $(a, b) \sim (a', b')$ и $(a', b') \sim (a'', b'')$, то

$$ab' = a'b, \qquad a'b'' = a''b'.$$

Домножая первое равенство на b'', а второе на b, получаем

$$ab'b'' = a'bb'' = a''bb'.$$

Так как R — область целостности и $b' \neq 0$, можно сократить на b', и остаётся равенство $ab'' = a''b$, то есть $(a, b) \sim (a'', b'')$. Значит, $\sim$ — отношение эквивалентности.

Обозначим через $Q(R)$ соответствующее фактор-множество:

$$Q(R) = \big(R \times (R \setminus \{0\})\big) / \sim .$$

Класс пары (a, b) будем обозначать дробью $\frac{a}{b}$; горизонтальная черта пока лишь обозначает класс эквивалентности, а не деление в кольце R. Условие $(a, b) \sim (a', b')$ переписываем как

$$\frac{a}{b} = \frac{a'}{b'}.$$

Определим сложение и умножение на $Q(R)$:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

Предложение. *Структура $(Q(R), +, \cdot)$ является полем.*

Доказательство. Сначала проверим корректность определений. Если $\frac{a}{b} = \frac{a'}{b'}$, то по определению эквивалентности $ab' = a'b$, и

$$\frac{a}{b} = \frac{ab'}{bb'} = \frac{a'b}{bb'} = \frac{a'}{b'}$$

показывает, что переход к эквивалентной дроби сводится к домножению числителя и знаменателя на один и тот же ненулевой элемент и последующему сокращению. Такие преобразования не меняют результата сложения и умножения, поэтому операции корректно определены на классах.

Коммутативность и ассоциативность сложения и умножения следуют из соответствующих свойств в R; общий случай сводится к случаю одинаковых знаменателей, если заменить дроби на эквивалентные с общим знаменателем. Элемент $\frac{0}{1}$ является нейтральным по сложению, а $\frac{-a}{b}$ — противоположным к $\frac{a}{b}$.

Для умножения нейтральным элементом служит $\frac{1}{1}$. Если $a \neq 0$, то дробь $\frac{a}{b}$ имеет мультипликативно обратный элемент $\frac{b}{a}$, поскольку

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$

Дистрибутивность умножения относительно сложения также сводится к случаю одинаковых знаменателей и далее к дистрибутивности в R. Таким образом, все аксиомы поля выполнены. ■

Предложение (Замечание)**.** *Отображение*

$$\iota \colon R \to Q(R), \qquad \iota(r) = \frac{r}{1},$$

является инъективным гомоморфизмом колец, поэтому R естественно отождествляется с подкольцом поля $Q(R)$.

Примеры.

1. Для $R = \mathbb{Z}$ получаем $Q(\mathbb{Z}) = \mathbb{Q}$.
2. Для $R = K[X]$ поле частных $Q(K[X])$ обозначают через $K(X)$; его элементы — дробно-рациональные функции от одной переменной с коэффициентами из K.

36 Поле дробно-рациональных функций. Правильные дроби

Поле дробно-рациональных функций от одной переменной над полем K — это поле частных кольца $K[X]$, которое обозначают через $K(X)$.

Предложение (Несократимое представление)**.** *Пусть R — факториальное кольцо. Тогда любой элемент $s \in Q(R)$ представим в виде $s = \frac{p}{q}$, где $p, q \in R$ взаимно просты. Такое представление единственно с точностью до умножения p и q на один и тот же элемент из R^*.*

Доказательство. Пусть $s = \frac{a}{b}$, где $a, b \in R$, и пусть $d = (a, b)$ — их наибольший общий делитель. Тогда $a = da'$, $b = db'$ с взаимно простыми a', b', и

$$s = \frac{a}{b} = \frac{da'}{db'} = \frac{a'}{b'}.$$

Пусть теперь

$$s = \frac{p}{q} = \frac{p'}{q'}$$

— две записи, в которых пары (p, q) и (p', q') взаимно просты. Из равенства $pq' = p'q$ следует, что p делит $p'q$, а так как $(p, q) = 1$, получаем $p \mid p'$. Аналогично, $p' \mid p$, поэтому $p' = \varepsilon p$ для некоторого обратимого $\varepsilon \in R^*$. Подставляя в равенство $pq' = p'q$, находим $q' = \varepsilon q$. ■

Предложение (Лемма о степени)**.** *Пусть $s \in K(X)$, $s = \frac{p}{q}$, где $p, q \in K[X]$, $q \neq 0$. Тогда число $\deg p - \deg q$ не зависит от выбора представления s в виде $\frac{p}{q}$.*

Доказательство. Если $\frac{p}{q} = \frac{p_1}{q_1}$, то $pq_1 = p_1 q$. Отсюда

$$\deg p + \deg q_1 = \deg p_1 + \deg q,$$

и, следовательно, $\deg p - \deg q = \deg p_1 - \deg q_1$. ■

Таким образом, корректно определена *степень* рациональной дроби:

$$\deg s = \deg \frac{p}{q} = \deg p - \deg q.$$

Определение. Рациональная дробь $s \in K(X)$ называется *правильной*, если $\deg s < 0$, то есть степень числителя меньше степени знаменателя.

В частности, нулевая дробь считается правильной, а любой ненулевой многочлен — нет. Из определения легко следует, что сумма и произведение правильных дробей также являются правильными дробями.

Предложение (Разложение на многочлен и правильную дробь)**.** *Любая рациональная дробь однозначно представляется в виде суммы многочлена и правильной дроби.*

Доказательство. Пусть $s = \frac{p}{q}$, где $p, q \in K[X]$, $q \neq 0$. Разделим p с остатком на q: существуют единственные многочлены $l, r \in K[X]$ такие, что

$$p = ql + r, \qquad \deg r < \deg q \text{ или } r = 0.$$

Тогда

$$s = \frac{p}{q} = \frac{ql + r}{q} = l + \frac{r}{q},$$

где l — многочлен, а $\frac{r}{q}$ — правильная дробь.

Пусть также

$$s = l_1 + \frac{r_1}{q_1}$$

— другое представление с правильной дробью. Тогда

$$l - l_1 = \frac{r_1}{q_1} - \frac{r}{q}.$$

Правая часть — разность правильных дробей и, значит, сама является правильной дробью. Многочлен может быть одновременно правильной дробью только в случае, когда он равен нулю. Следовательно, $l = l_1$, а $\frac{r}{q} = \frac{r_1}{q_1}$, то есть представление единственно. ■

37 Примарные дроби. Лемма о дроби со знаменателем, разложенным на два взаимно простых множителя

Предложение. *Пусть $f, g \in K[X]$ взаимно просты. Тогда любую рациональную дробь со знаменателем fg можно представить в виде суммы дробей со знаменателями f и g: для любого $a \in K[X]$ найдутся такие $u, v \in K[X]$, что*

$$\frac{a}{fg} = \frac{u}{f} + \frac{v}{g}.$$

Доказательство. Из взаимной простоты многочленов f и g следует существование многочленов $c, d \in K[X]$, для которых

$$cf + dg = 1$$

(расширенный алгоритм Евклида). Домножая равенство на $\frac{a}{fg}$, получаем

$$\frac{a}{fg} = \frac{a(cf + dg)}{fg} = \frac{ac}{g} + \frac{ad}{f}.$$

Достаточно положить $u = ad$, $v = ac$. ■

Определение. Рациональная дробь называется *примарной*, если её можно представить в виде $\frac{a}{p^n}$, где p — неприводимый многочлен, а $n \in \mathbb{N}$.

Если нужно указать конкретный неприводимый многочлен p, говорят также, что дробь $\frac{a}{p^n}$ является *p-примарной*.

38 Разложение правильной дроби в сумму правильных примарных дробей

Предложение. *Любую правильную рациональную дробь можно единственным образом представить в виде суммы нескольких ненулевых правильных p-примарных дробей, где p — различные унитарные неприводимые многочлены.*

Доказательство. Пусть s — правильная дробь, и её знаменатель в несократимом виде разложен как

$$s = p_1^{m_1} \cdots p_t^{m_t},$$

где p_i — попарно различные унитарные неприводимые многочлены. Применяя предыдущую лемму последовательно $t - 1$ раз, разложим дробь s в сумму:

$$s = \frac{a_1}{p_1^{m_1}} + \cdots + \frac{a_t}{p_t^{m_t}},$$

где $a_i \in K[X]$. Каждое слагаемое можно записать в виде суммы многочлена и правильной дроби:

$$\frac{a_i}{p_i^{m_i}} = f_i + \frac{b_i}{p_i^{m_i}},$$

где $\deg b_i < \deg p_i^{m_i}$ или $b_i = 0$. Складывая, получаем представление

$$s = f + \frac{b_1}{p_1^{m_1}} + \cdots + \frac{b_t}{p_t^{m_t}},$$

где $f = f_1 + \cdots + f_t$ — многочлен, а оставшиеся слагаемые — правильные p_i-примарные дроби.

Поскольку исходная дробь s была правильной, разность $s - f$ также правильна. Но $s - f$ совпадает с суммой правильных дробей справа, значит и сам многочлен f должен быть правильной дробью, что возможно только при $f = 0$. Поэтому

$$s = \frac{b_1}{p_1^{m_1}} + \cdots + \frac{b_t}{p_t^{m_t}},$$

и все слагаемые здесь — правильные примарные дроби.

Пусть теперь у s есть два различных разложения на ненулевые правильные примарные дроби (в несократимом виде):

$$s = \sum_{i=1}^{r} \frac{c_i}{q_i^{n_i}} = \sum_{j=1}^{r'} \frac{d_j}{r_j^{k_j}},$$

где все q_i, r_j — унитарные неприводимые и во всех суммах попарно различны. Вычтем одно разложение из другого и отбросим нулевые слагаемые:

$$\frac{c_1}{p_1^{n_1}} + \cdots + \frac{c_\ell}{p_\ell^{n_\ell}} = 0,$$

где дроби попарно несократимы и $p_1, \ldots, p_\ell$ — различные неприводимые многочлены.

Приведём левую часть к общему знаменателю $P = p_1^{n_1} \cdots p_\ell^{n_\ell}$. Получаем

$$\frac{C}{P} = 0$$

для некоторого ненулевого многочлена C, поскольку ни одна дробь не равна нулю. Отсюда $C = 0$, что невозможно. Противоречие показывает, что начальные два разложения совпадают. ■

39 Простейшие дроби. Разложение правильной дроби в сумму простейших

Определение. Простейшей дробью называется любая рациональная дробь вида $\dfrac{a}{p^n}$, где p — унитарный неприводимый многочлен, $n \in \mathbb{N}$, а числитель a — ненулевой многочлен степени меньше $\deg p$.

Предложение. *Каждая ненулевая правильная p-примарная дробь единственным образом представляется в виде суммы простейших дробей.*

Доказательство. Пусть дана правильная p-примарная дробь $\dfrac{a}{p^n}$. Разделим a на p с остатком:

$$a = q_1 p + r_1, \qquad \deg r_1 < \deg p.$$

Тогда

$$\frac{a}{p^n} = \frac{q_1 p + r_1}{p^n} = \frac{r_1}{p^n} + \frac{q_1}{p^{n-1}}.$$

Если $n > 1$, применим ту же операцию к q_1:

$$q_1 = q_2 p + r_2, \qquad \deg r_2 < \deg p,$$

и получим

$$\frac{a}{p^n} = \frac{r_1}{p^n} + \frac{r_2}{p^{n-1}} + \frac{q_2}{p^{n-2}}.$$

Продолжая процесс, на шаге $n-1$ получим

$$q_{n-1} = q_n p + r_n, \qquad \deg r_n < \deg p.$$

Так как дробь изначально правильная, на последнем шаге имеем $q_n = 0$, и

$$\frac{q_{n-1}}{p} = \frac{r_n}{p}$$

— простейшая дробь. В итоге получаем разложение

$$\frac{a}{p^n} = \frac{r_1}{p^n} + \frac{r_2}{p^{n-1}} + \cdots + \frac{r_n}{p},$$

где каждая дробь $\dfrac{r_k}{p^{n-k+1}}$ либо простейшая, либо равна нулю.

Докажем единственность. Пусть существуют два разложения одной и той же ненулевой правильной p-примарной дроби:

$$\frac{r_n}{p^n} + \cdots + \frac{r_1}{p} = \frac{s_n}{p^n} + \cdots + \frac{s_1}{p},$$

где $\deg r_i, \deg s_i < \deg p$ и некоторые коэффициенты могут быть нулевыми. Перенесём всё в одну сторону:

$$\frac{r_n - s_n}{p^n} + \cdots + \frac{r_1 - s_1}{p} = 0.$$

Домножая на p^n, получаем тождество многочленов

$$(r_n - s_n) + p(r_{n-1} - s_{n-1}) + \cdots + p^{n-1}(r_1 - s_1) = 0.$$

Пусть m — максимальный индекс, при котором $r_m \neq s_m$. Тогда старший по кратности множитель p^m в этой сумме имеет коэффициент $r_m - s_m$, чья степень меньше $\deg p$. Правая часть при этом кратна p, а значит и $r_m - s_m$ кратен p, что возможно только при $r_m - s_m = 0$. Получаем противоречие с выбором m. Следовательно, все $r_i = s_i$, и разложение единственно. ■

Предложение. *Любая ненулевая правильная дробь единственным образом представляется в виде суммы простейших дробей с попарно различными знаменателями.*

Доказательство. Пусть s — ненулевая правильная дробь. Сначала разложим s в сумму правильных примарных дробей по предыдущей теореме. Затем каждую ненулевую примарную дробь разложим в сумму простейших дробей. В совокупности это даёт представление s в виде суммы простейших дробей.

Знаменатели в этом разложении попарно различны: каждая p-примарная дробь даёт только знаменатели вида p^k, и разные неприводимые многочлены p не могут дать ассоциированные степени.

Единственность следует из единственности разложения на примарные дроби и единственности разложения каждой примарной дроби на простейшие. ■

Пример. Разложим дробь $\dfrac{1}{X^5+X^3}$ над $\mathbb{R}[X]$. Разложим знаменатель на неприводимые множители:

$$X^5+X^3 = X^3(X^2+1).$$

Предположим разложение

$$\frac{1}{X^5+X^3} = \frac{A}{X} + \frac{B}{X^2} + \frac{C}{X^3} + \frac{DX+E}{X^2+1},$$

где $A, B, C, D, E \in \mathbb{R}$. Домножая обе части на $X^3(X^2+1)$, получаем тождество многочленов

$$1 = AX^2(X^2+1) + BX(X^2+1) + C(X^2+1) + (DX+E)X^3.$$

Приравнивая коэффициенты одноимённых степеней X, можно найти A, B, C, D, E методом неопределённых коэффициентов. Подстановки и вычисления здесь опускаются.

40 Действия над матрицами и их свойства

Определение. Матрицей над кольцом R называется прямоугольная таблица, составленная из элементов кольца R.

Матрицу A размера $m \times n$ задают указанием всех её коэффициентов $a_{ij} \in R$ при $1 \le i \le m$, $1 \le j \le n$; пишут $A = (a_{ij})$. Множество всех матриц размера $m \times n$ над кольцом R обозначается через $M(m, n, R)$.

Определение. Квадратная матрица — это матрица, у которой число строк совпадает с числом столбцов. Множество всех квадратных матриц порядка n над R обозначают через $M(n, R)$.

Основные операции над матрицами.

1. *Сложение.*
$$A, B \in M(m, n, R), \qquad (A+B)_{ij} = A_{ij} + B_{ij}.$$

2. *Умножение матриц.*
$$A \in M(m, n, R),\ B \in M(n, p, R), \qquad (AB)_{ik} = \sum_{j=1}^{n} A_{ij}B_{jk}.$$

3. *Умножение на скаляр.*

$$A \in M(m,n,R),\ \lambda \in R, \qquad (\lambda A)_{ij} = \lambda A_{ij}.$$

4. *Транспонирование.*

$$A \in M(m,n,R),\ A^T \in M(n,m,R), \qquad (A^T)_{ij} = A_{ji}.$$

Предложение (Свойства операций над матрицами)**.** *Пусть R — коммутативное кольцо. Тогда для любых матриц A, B, C (там, где операции определены) и любых $\lambda, \mu \in R$ выполняются тождества:*

1. $A + (B + C) = (A + B) + C$;
2. *существует нулевая матрица* 0 *такая, что* $A + 0 = 0 + A = A$;
3. *для любой матрицы* A *существует матрица* $-A$ *такая, что* $A + (-A) = (-A) + A = 0$;
4. $A + B = B + A$;
5. $A(BC) = (AB)C$;
6. $A(B + C) = AB + AC$;
7. $(B + C)A = BA + CA$;
8. $\lambda(A + B) = \lambda A + \lambda B$;
9. $(\lambda + \mu)A = \lambda A + \mu A$;
10. $(\lambda A)B = \lambda(AB) = A(\lambda B)$;
11. $(\lambda\mu)A = \lambda(\mu A)$;
12. $(A + B)^T = A^T + B^T$;
13. $(AB)^T = B^T A^T$.

Доказательство. Все равенства проверяются поэлементно из определений операций и аксиом кольца R. Например,

$$(A + B)_{ij} = A_{ij} + B_{ij}, \quad \big((A + B) + C\big)_{ij} = A_{ij} + B_{ij} + C_{ij} = \big(A + (B + C)\big)_{ij},$$

что доказывает ассоциативность сложения. Аналогично, $(AB)^T_{ij} = (AB)_{ji} = \sum_k A_{jk}B_{ki} = (B^T A^T)_{ij}$. Остальные свойства разбираются так же. ■

Определение. Единичной матрицей порядка n называется квадратная матрица E_n, у которой на главной диагонали стоят единицы, а на всех остальных позициях — нули.

Предложение. *Для любой матрицы $A \in M(m,n,R)$ выполнено*

$$E_m \cdot A = A \cdot E_n = A.$$

Доказательство. Запишем по определению:

$$(E_m A)_{ik} = \sum_{j=1}^{m} (E_m)_{ij} A_{jk}.$$

В матрице E_m элемент $(E_m)_{ij}$ равен 1 только при $j = i$ и равен 0 иначе, поэтому в сумме остаётся единственное слагаемое A_{ik}. Значит, $(E_m A)_{ik} = A_{ik}$ для всех i, k, то есть $E_m A = A$. Равенство $AE_n = A$ доказывается аналогично, по столбцам. ■

Следствие: С множеством $M(n, R)$, операциями сложения и умножения матриц и единицей E_n оно образует ассоциативное кольцо с единицей.

Определение. Квадратная матрица $A \in M(n, R)$ называется *обратимой*, если существует матрица $A^{-1} \in M(n, R)$ такая, что

$$AA^{-1} = A^{-1}A = E_n.$$

Замечание Множество всех обратимых матриц $M(n, R)^\times$ по умножению образует группу, обозначаемую $GL(n, R)$.

Предложение. *Если матрица $A \in M(n, R)$ обратима, то и матрица A^T обратима, причём*

$$(A^T)^{-1} = (A^{-1})^T.$$

Доказательство. Из равенства $AA^{-1} = E_n$, применяя транспонирование и пользуясь формулой $(AB)^T = B^T A^T$, получаем

$$(A^{-1})^T A^T = (AA^{-1})^T = E_n^T = E_n.$$

Аналогично из $A^{-1}A = E_n$ следует $A^T(A^{-1})^T = E_n$. Значит, матрица A^T обратима, а её обратная равна $(A^{-1})^T$. ■

41 Элементарные преобразования и элементарные матрицы

Элементарные преобразования строк. Пусть $A \in M(m, n, R)$. Элементарными преобразованиями строк называются:

1. прибавление к строке i строки j, домноженной на скаляр $\lambda \in R$;
2. перестановка местами строк с номерами i и j;
3. домножение строки i на обратимый скаляр $\varepsilon \in R^*$.

Замечание Аналогично определяются элементарные преобразования столбцов матрицы.

Элементарные матрицы. Обозначим через E_m единичную матрицу размера $m \times m$, а через e_{ij} — матрицу того же размера с единственной единицей в позиции (i, j) и нулями на остальных местах.

1. *Прибавление строки.* Пусть $\lambda \in R$ и $i \neq j$. Положим

$$T_{ij}(\lambda) = E_m + \lambda e_{ij}.$$

Тогда умножение слева на $T_{ij}(\lambda)$ реализует прибавление к i-й строке матрицы A строки j, умноженной на λ:

$$T_{ij}(\lambda)A$$

получается из A заменой i-й строки на (строка i) + $\lambda \cdot$ (строка j).

Доказательство. Матрица $T_{ij}(\lambda)$ совпадает с E_m во всех строках, кроме i-й. В i-й строке стоят два ненулевых элемента: 1 в столбце i и λ в столбце j. При умножении на столбец k матрицы A получаем

$$(T_{ij}(\lambda)A)_{ik} = 1 \cdot a_{ik} + \lambda \cdot a_{jk} = a_{ik} + \lambda a_{jk},$$

то есть новая i-я строка — это старая i-я плюс λ умножить на j-ю строку. Остальные строки не меняются. ■

2. *Перестановка строк.* Пусть $S_{ij} = E_m - e_{ii} - e_{jj} + e_{ij} + e_{ji}$ (при $i \neq j$). Тогда умножение слева на S_{ij} переставляет строки i и j местами.

   Доказательство. Матрица S_{ij} совпадает с единичной во всех строках, кроме i-й и j-й. В i-й строке стоит единица в столбце j, а в j-й — единица в столбце i. Поэтому i-я строка произведения $S_{ij}A$ совпадает с j-й строкой A, а j-я — с i-й строкой A. Остальные строки не изменяются. ■

3. *Умножение строки на скаляр.* Пусть $\varepsilon \in R^*$ и

   $$D_i(\varepsilon) = E_m + (\varepsilon - 1)e_{ii}.$$

   Тогда умножение слева на $D_i(\varepsilon)$ домножает i-ю строку матрицы A на скаляр ε.

   Доказательство. Матрица $D_i(\varepsilon)$ отличается от E_m только в элементе (i, i): там стоит ε вместо 1. Поэтому i-я строка произведения $D_i(\varepsilon)A$ равна

   $$(0, \ldots, 0, \varepsilon, 0, \ldots, 0) \cdot A = \varepsilon \cdot (\text{строка } i \text{ матрицы } A),$$

   а остальные строки остаются без изменений. ■

Замечание Используя свойство $(AB)^T = B^T A^T$, нетрудно видеть, что элементарным преобразованиям столбцов матрицы соответствуют умножения *справа* на те же элементарные матрицы.

42 Приведение матрицы к ступенчатому виду элементарными преобразованиями строк

Определение. Пусть $A \in M_{m\times n}(F)$, где F — поле. Матрица A называется *ступенчатой*, если существуют индексы $1 \leq j_1 < j_2 < \cdots < j_r \leq n$ такие, что

- для всех $i = 1, \ldots, r$ элемент $a_{ij_i} \neq 0$ (ведущий элемент / пивот строки i);
- для всех $i = 1, \ldots, r$ и всех $j < j_i$ выполняется $a_{ij} = 0$;
- для всех $i > r$ строка i нулевая.

Ненулевые элементы $a_{1j_1}, \ldots, a_{rj_r}$ называются *ведущими (пивотами)*.

$$\begin{pmatrix} 0 & \cdots & 0 & a_{1j_1} & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & a_{2j_2} & * \\ \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & a_{rj_r} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

Алгоритм приведения к ступенчатому виду. Работаем над полем F и используем три типа элементарных преобразований строк: перестановки строк, умножение строки на ненулевой скаляр и прибавление к строке кратной другой строки.

1. Найдём первый столбец, содержащий ненулевой элемент; обозначим его номер через j_1. Перестановкой строк поднимем ненулевой элемент в позицию $(1, j_1)$.
2. Обнулим все элементы ниже a_{1j_1}, прибавляя к нижним строкам подходящие кратные первой строки.
3. Мысленно «забыв» первую строку и столбцы левее j_1, повторим те же шаги для ближайшего столбца $j_2 > j_1$, затем для $j_3, \ldots$.

На некотором шаге j_r процесс завершится, и матрица примет ступенчатый вид.

43 Приведение матрицы к простейшему виду элем. преобразованиями строк и столбцов

Для начала приведем матрицу к ступенчатому виду.

Заметим, что ведущие элементы можно превратить в единицы с помощью элементарных преобразований третьего типа. А именно: $\forall i \in 1..r$ проведем преобразование $D_i(1/a_{ij_i})$.

Теперь воспользуемся элементарными преобразованиями столбцов.

С помощью преобразований первого типа обнулим в строках $1..r$ все элементы кроме ведущих. Рассмотрим это на примере первой строки. Для всех $j > j_1$ мы проведем преобразование $T_{jj_1}(-a_{1j})$. Таким образом, элемент a_{1j} станет равен $a_{1j} + 1 * (-a_{1j}) = 0$. Проделав это для всех строк $1..r$, получим следующую матрицу:

$$\begin{pmatrix} 0 & \ldots & 0 & 1 & 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 0 & \ldots & 0 & 1 & 0 & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

После этого перестановкой столбцов можно добиться того, что единицы будут стоять в позициях $(1,1), (2,2), \ldots, (r,r)$. Полученная матрица называется окаймленной единичной матрицей:

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

44 PDQ-разложение. Разложение матрицы в произведение элементарных

Теорема 1. *Пусть K — поле, $A \in M(m,n,K)$.*

Тогда существуют элементарные матрицы $P_1,\dots,P_s \in M(m,K)$ и $Q_1,\dots,Q_t \in M(n,K)$ (где $s,t \geqslant 0$), такие что

$$P_s \dots P_1 \cdot A \cdot Q_1 \dots Q_t = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = D,$$

где $0 \leq r \leq \min(m,n)$ — ранг матрицы A. Матрица D называется окаймлённой единичной матрицей.

Доказательство. Из алгоритма приведения к ступенчатому виду (метод Гаусса) известно, что существуют элементарные матрицы $P_1,\dots,P_s \in M(m,K)$ такие, что

$$P_s \dots P_1 \cdot A$$

— ступенчатая матрица по строкам.

Далее, с помощью элементарных преобразований строк третьего типа можно сделать все ведущие элементы равными 1. Это соответствует домножению слева на элементарные матрицы вида $D_i(\lambda)$, умножающих i-ю строку на ненулевой скаляр $\lambda \in K$.

После этого элементарными преобразованиями *столбцов* (домножениями справа на элементарные матрицы Q_j) занулим во всех ненулевых строках все элементы, кроме ведущих. Затем перестановкой столбцов добьёмся того, чтобы ведущие столбцы стали первыми r столбцами. В результате получаем матрицу вида

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in M(m,n,K),$$

что и требовалось. ■

Следствие: Пусть K — поле, $A \in M(m,n,K)$. Тогда матрицу A можно представить в виде

$$A = PDQ,$$

где

$$D = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \quad P \in GL(m,K), \quad Q \in GL(n,K),$$

причём P и Q являются произведениями элементарных матриц.

Доказательство. По теореме выше существуют элементарные матрицы $P_1,\dots,P_t$ и $Q_1,\dots,Q_s$ такие, что

$$P_t \dots P_1 \cdot A \cdot Q_1 \dots Q_s = D.$$

Тогда

$$A = P_1^{-1} \dots P_t^{-1}\, D\, Q_s^{-1} \dots Q_1^{-1}.$$

Положим

$$P := P_1^{-1} \dots P_t^{-1}, \qquad Q := Q_s^{-1} \dots Q_1^{-1}.$$

Известно, что обратная к элементарной матрице также элементарна:

$$S_{ij}^{-1} = S_{ij}, \quad D_i^{-1}(\varepsilon) = D_i(\varepsilon^{-1}), \quad T_{ij}^{-1}(\lambda) = T_{ij}(-\lambda),$$

поэтому P и Q — произведения элементарных матриц. Отсюда $A = PDQ$. ■

Замечание Любая обратимая квадратная матрица является произведением элементарных матриц (докажем ниже). [web:81]

Следствие: Пусть $A \in M(n, K)$ и

$$A = P_t \dots P_1 \cdot D \cdot Q_1 \dots Q_s, \quad P_i, Q_j \text{ — элементарные матрицы}, \quad D = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Тогда

$$A \in GL(n, K) \iff r = n.$$

Доказательство.

"$\Longleftarrow$": Если $r = n$, то

$$D = E_n, \quad A = P_t \dots P_1\, E_n\, Q_1 \dots Q_s = P_t \dots P_1 Q_1 \dots Q_s.$$

Произведение обратимых (элементарных) матриц обратимо, значит $A \in GL(n, K)$.

"$\Longrightarrow$": Пусть A обратима. Тогда

$$D = P_t \dots P_1\, A\, Q_1 \dots Q_s = P_t \dots P_1\, A\, Q_1 \dots Q_s$$

также обратима как произведение обратимых матриц. Но при $r < n$ последняя строка D нулевая, то есть D не может быть обратимой. Противоречие. Значит, $r = n$.

■

Следствие: Пусть $A \in M(n, K)$. Тогда

$$A \in GL(n, K) \iff A \text{ является произведением элементарных матриц.}$$

Доказательство.

"$\Longleftarrow$": Любая элементарная матрица обратима, а произведение обратимых матриц опять обратимо, следовательно, произведение элементарных матриц принадлежит $GL(n, K)$.

"$\Longrightarrow$": Для обратимой матрицы A по PDQ-разложению имеем

$$A = PDQ, \quad D = E_n,$$

а значит $A = PQ$, где P и Q — произведения элементарных матриц. Следовательно, и A — произведение элементарных матриц.

■

45 Разложение перестановки в произведение транспозиций и элементарных транспозиций

Определение. Пусть X — множество. Обозначим

$$S(X) = \{f : X \to X \mid f \text{ — биекция}\}.$$

На $S(X)$ вводится операция композиции:

$$(S(X), \circ), \quad (g, f) \mapsto g \circ f.$$

Определение. Пусть $X = \{1, 2, \ldots, n\}$. Тогда $S(X)$ обозначают через S_n и называют *симметрической группой* степени n. [web:111]

Предложение. *Любая перестановка из S_n раскладывается в произведение транспозиций.*

Доказательство. Рассмотрим произвольную перестановку $\pi \in S_n$. Начнём с тождественной перестановки id и покажем, что последовательным домножением справа на транспозиции можно получить π.

В табличной записи перестановки сначала добьёмся того, чтобы в нижней строке под числом 1 стояло значение $\pi(1)$: для этого поменяем местами столбец 1 со столбцом, в котором стоит $\pi(1)$. Далее поставим на второе место в нижней строке число $\pi(2)$. Так как π — биекция, то $\pi(1) \neq \pi(2)$, поэтому где-то справа от первого столбца есть столбец с $\pi(2)$; поменяем его со вторым столбцом. На k-м шаге добиваемся того, чтобы первые k чисел в нижней строке были $\pi(1), \ldots, \pi(k)$.

В конце концов, после конечного числа таких перестановок столбцов (транспозиций), мы получим табличную запись перестановки π, то есть π представима в виде произведения транспозиций. ■

Предложение. *Любая транспозиция раскладывается в произведение нечётного числа* элементарных транспозиций*, то есть транспозиций вида $(k\ k+1)$ (соседних элементов). [web:117]*

Доказательство. Неформально задача такова: разрешено менять местами только соседние элементы в строке, а нужно поменять местами два элемента, стоящих далеко друг от друга. Делается это следующим образом:

- последовательно «продвигаем» левый из двух элементов направо до второго, меняя его с соседями (элементарные транспозиции);
- меняем получившиеся соседние элементы местами ещё одной элементарной транспозицией;
- затем «отгоняем» второй элемент обратно на исходное место левого, снова последовательностью элементарных транспозиций.

При этом нужные два элемента меняются местами, а каждый элемент между ними участвует ровно в двух соседних перестановках (на пути «туда» и «обратно»), поэтому в итоге возвращается на своё место.

Формально, для транспозиции τ_{ij}, $i < j$, имеем разложение

$$\tau_{ij} = \tau_{i,i+1} \circ \tau_{i+1,i+2} \circ \cdots \circ \tau_{j-2,j-1} \circ \tau_{j-1,j} \circ \tau_{j-2,j-1} \circ \cdots \circ \tau_{i+1,i+2} \circ \tau_{i,i+1},$$

то есть τ_{ij} представлена в виде произведения $2(j-i)-1$ элементарных транспозиций — это нечётное число. ■

46 Чётность и знак перестановки

Определение. Пусть $\pi \in S_n$. Пара индексов (i, j) называется *инверсией* для перестановки π, если $i < j$ и $\pi(i) > \pi(j)$. Число инверсий перестановки π обозначается через $\mathrm{inv}(\pi)$ и называется *числом инверсий* π.

Определение. Перестановка $\pi \in S_n$ называется *чётной*, если $\mathrm{inv}(\pi)$ чётно, и *нечётной* в противном случае.

Определение. *Знак* перестановки π определяется формулой

$$\mathrm{sgn}(\pi) = (-1)^{\mathrm{inv}(\pi)}.$$

Предложение. *Пусть $\pi \in S_n$, а $\tau_{ij} \in S_n$ — транспозиция.*

Тогда

$$\mathrm{sgn}(\pi \circ \tau_{ij}) = -\mathrm{sgn}(\pi).$$

Доказательство. Сначала рассмотрим случай, когда τ_{ij} — *элементарная* транспозиция, то есть $\tau_{i,i+1}$.

Обозначим

$$\pi' = \pi \circ \tau_{i,i+1}.$$

В двухрядной записи это означает, что в нижней строке перестановки на местах i и $i+1$ элементы просто поменялись местами:

$$\pi' = \begin{pmatrix} \dots & i & i+1 & \dots \\ \dots & \pi(i+1) & \pi(i) & \dots \end{pmatrix}.$$

Рассмотрим, как меняется число инверсий.

- Если $\{k, l\} \cap \{i, i+1\} = \varnothing$, то пара (k, l) никак не затрагивает позиции i и $i+1$, поэтому

$$(k, l) \text{ — инверсия для } \pi \iff (k, l) \text{ — инверсия для } \pi'.$$

- Пусть $k \in \{i, i+1\}$, а $l \notin \{i, i+1\}$. Рассмотрим пары (i, l) и $(i+1, l)$. Здесь l либо больше обоих i и $i+1$, либо меньше обоих (так как индексы целые и $l \neq i, i+1$). При переходе от π к π' значения на местах i и $i+1$ просто меняются местами, поэтому суммарное количество инверсий, в которых участвуют пары (i, l) и $(i+1, l)$, остаётся тем же и для π, и для π'.
- Если $k, l \in \{i, i+1\}$, то единственная пара — это $(i, i+1)$. Она была инверсией для π тогда и только тогда, когда $\pi(i) > \pi(i+1)$. В перестановке π' значения на этих позициях поменялись местами, поэтому

$$(i, i+1) \text{ — инверсия для } \pi \iff (i, i+1) \text{ не является инверсией для } \pi'.$$

  То есть число инверсий меняется ровно на 1.

Итак, при домножении на элементарную транспозицию число инверсий изменяется на ± 1, следовательно,

$$\operatorname{inv}(\pi') = \operatorname{inv}(\pi) \pm 1 \quad \Longrightarrow \quad \operatorname{sgn}(\pi') = -\operatorname{sgn}(\pi).$$

Теперь рассмотрим произвольную транспозицию τ_{ij}, $i < j$. По предыдущей теореме о разложении транспозиций она представима в виде произведения нечётного числа элементарных транспозиций:

$$\tau_{ij} = \prod_{l=1}^{2t+1} \sigma_l, \quad \sigma_l \text{ — элементарные транспозиции.}$$

Каждый множитель σ_l меняет знак перестановки, поэтому

$$\operatorname{sgn}(\pi \circ \tau_{ij}) = \operatorname{sgn}(\pi)\,(-1)^{2t+1} = -\operatorname{sgn}(\pi).$$

■

Следствие: Пусть $\pi = \sigma_1 \dots \sigma_s$, где σ_i — транспозиции.

Тогда

$$\operatorname{sgn}(\pi) = (-1)^s.$$

Доказательство. Используем индукцию по s.

База: $s = 1$. Тогда

$$\operatorname{sgn}(\sigma_1) = \operatorname{sgn}(e \circ \sigma_1) = -\operatorname{sgn}(e) = -1 = (-1)^1.$$

Переход: пусть утверждение верно для произведения из $s-1$ транспозиций. Тогда

$$\operatorname{sgn}(\sigma_1 \dots \sigma_s) = -\operatorname{sgn}(\sigma_1 \dots \sigma_{s-1}) = -(-1)^{s-1} = (-1)^s.$$

■

Теорема 2. *Пусть* $\pi, \rho \in S_n$.

Тогда

$$\operatorname{sgn}(\pi \circ \rho) = \operatorname{sgn}(\pi)\ \operatorname{sgn}(\rho).$$

Доказательство. Представим

$$\pi = \sigma_1 \dots \sigma_s, \quad \rho = \sigma'_1 \dots \sigma'_t,$$

где все σ_i, σ'_j — транспозиции. Тогда

$$\operatorname{sgn}(\pi) = (-1)^s, \qquad \operatorname{sgn}(\rho) = (-1)^t.$$

Кроме того,

$$\pi \circ \rho = \sigma_1 \dots \sigma_s \sigma'_1 \dots \sigma'_t,$$

то есть это произведение $s + t$ транспозиций, а значит

$$\operatorname{sgn}(\pi \circ \rho) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \operatorname{sgn}(\pi)\ \operatorname{sgn}(\rho).$$

■

Предложение. *Обозначим*

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$$

— множество чётных перестановок в S_n. Тогда A_n является подгруппой группы S_n.

Доказательство.

- Нейтральный элемент e чётен, так как $\operatorname{sgn}(e) = 1$, следовательно, $e \in A_n$.
- Если $\pi, \rho \in A_n$, то

  $$\operatorname{sgn}(\pi) = \operatorname{sgn}(\rho) = 1,$$

  откуда

  $$\operatorname{sgn}(\pi \circ \rho) = \operatorname{sgn}(\pi)\ \operatorname{sgn}(\rho) = 1,$$

  то есть $\pi\rho \in A_n$.
- Если $\pi \in A_n$, то

  $$\operatorname{sgn}(\pi \circ \pi^{-1}) = \operatorname{sgn}(e) = 1 = \operatorname{sgn}(\pi)\ \operatorname{sgn}(\pi^{-1}),$$

  а значит $\operatorname{sgn}(\pi^{-1}) = 1$ и $\pi^{-1} \in A_n$.

Проверены замкнутость, наличие единицы и обратимости, значит A_n — подгруппа S_n. ■

Предложение. *Пусть $n \geqslant 2$.*

Тогда

$$|A_n| = \frac{n!}{2}.$$

Доказательство. Рассмотрим отображение

$$\lambda : A_n \longrightarrow S_n \setminus A_n, \quad \sigma \longmapsto \sigma \circ \tau_{12},$$

где τ_{12} — транспозиция (1 2).

Так как τ_{12} нечётна, произведение $\sigma \circ \tau_{12}$ нечётно, следовательно, λ действительно принимает значения в $S_n \setminus A_n$.

Инъективность: пусть $\lambda(\sigma) = \lambda(\sigma')$. Тогда

$$\sigma \circ \tau_{12} = \sigma' \circ \tau_{12} \quad \Longrightarrow \quad \sigma = \sigma'.$$

Сюръективность: пусть $\pi \in S_n \setminus A_n$ — нечётная перестановка. Тогда $\pi \circ \tau_{12}$ чётна, то есть принадлежит A_n, и

$$\lambda(\pi \circ \tau_{12}) = (\pi \circ \tau_{12}) \circ \tau_{12} = \pi.$$

Значит, λ — биекция между A_n и $S_n \setminus A_n$.

Отсюда

$$|A_n| = |S_n \setminus A_n| \quad \Longrightarrow \quad |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

■

47 Определение определителя. Определитель транспонированной матрицы

Определение. Пусть $A \in M(n, R)$, где R — коммутативное кольцо, и $A = (a_{ij})$. *Определитель* матрицы A — это элемент $|A| \in R$, заданный формулой

$$|A| = \det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Интуитивно эта формула устроена так: для каждой перестановки $\sigma \in S_n$ выбираются элементы $a_{1,\sigma(1)}, a_{2,\sigma(2)}, \ldots, a_{n,\sigma(n)}$ — по одному из каждой строки и каждого столбца, они перемножаются, и затем все такие произведения суммируются с коэффициентами $\operatorname{sgn}(\sigma) = \pm 1$.

Примеры.

- Определитель матрицы 2×2:

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

- Определитель матрицы 3×3:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{31}a_{22} - a_{11}a_{23}a_{32}.$$

Предложение. *Для любой квадратной матрицы $A = (a_{ij})$ над коммутативным кольцом выполняется равенство*

$$|A^T| = |A|.$$

Доказательство. По определению

$$|A^T| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{\sigma(i),i}.$$

В произведении поменяем индексирование, записав его по строкам:

$$\prod_{i=1}^{n} a_{\sigma(i),i} = \prod_{i=1}^{n} a_{i,\sigma^{-1}(i)}.$$

Тогда

$$|A^T| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma^{-1}(i)}.$$

Отображение $\sigma \mapsto \sigma^{-1}$ — биекция множества S_n на себя, поэтому, переобозначив перестановку σ^{-1} через τ, получаем

$$|A^T| = \sum_{\tau \in S_n} \operatorname{sgn}(\tau^{-1}) \cdot \prod_{i=1}^{n} a_{i,\tau(i)}.$$

Из свойств знака перестановки известно, что $\operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\tau)$. Следовательно,

$$|A^T| = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) \cdot \prod_{i=1}^{n} a_{i,\tau(i)} = |A|.$$

■

48 Линейность определителя по строкам и столбцам

Предложение (Линейность по строке)**.** *Пусть $A \in M(n, R)$, R — коммутативное кольцо, и $1 \le k \le n$.*

1. *(***Аддитивность по строке***) Пусть k-я строка матрицы A представлена в виде суммы двух строк:*

   $$k\text{-я строка } A = (\dots, a'_{kj}, \dots) + (\dots, a''_{kj}, \dots).$$

   Обозначим через A' и A'' матрицы, полученные из A заменой k-й строки соответственно на $(a'_{k1}, \dots, a'_{kn})$ и $(a''_{k1}, \dots, a''_{kn})$, остальные строки те же. Тогда

   $$|A| = |A'| + |A''|.$$

   Доказательство. По определению детерминанта

   $$|A| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

   В каждом слагаемом множитель из k-й строки имеет вид $a_{k,\sigma(k)} = a'_{k,\sigma(k)} + a''_{k,\sigma(k)}$. Раскрывая скобки и группируя члены, получаем

   $$|A| = |A'| + |A''|.$$

   ■

2. *(***Однородность по строке***) Пусть B получается из A умножением k-й строки на скаляр $\lambda \in R$:*

   $$k\text{-я строка } B = \lambda \cdot k\text{-я строка } A.$$

   Тогда

   $$|B| = \lambda\,|A|.$$

   Доказательство. В формуле для $|B|$ в каждом произведении $\prod_{i=1}^{n} b_{i,\sigma(i)}$ только один множитель, соответствующий $i = k$, равен $\lambda a_{k,\sigma(k)}$, остальные совпадают с $a_{i,\sigma(i)}$. Поэтому

   $$|B| = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, \lambda a_{k,\sigma(k)} \prod_{i \ne k} a_{i,\sigma(i)} = \lambda \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} = \lambda |A|.$$

   ■

Предложение (Линейность по столбцу)**.** *Определитель линеен по каждому столбцу отдельно.*

Доказательство. Линейность по столбцу сводится к линейности по строке с помощью транспонирования:

$$|A| = |A^T|,$$

детерминант матрицы A^T линеен по строкам, а строки A^T — это столбцы A. ■

Следствие: Если в матрице есть нулевая строка (или нулевой столбец), то её определитель равен нулю: достаточно взять во втором свойстве линейности $\lambda = 0$.

49 Кососимметричность определителя по строкам и столбцам

Предложение. *Пусть A — квадратная матрица, у которой совпадают i-я и j-я строки, $i \neq j$. Тогда*

$$|A| = 0.$$

Доказательство. Разобьём сумму по перестановкам на чётные и нечётные:

$$|A| = \sum_{\sigma \in A_n} \prod_{k=1}^{n} a_{k,\sigma(k)} \; - \sum_{\sigma \in S_n \setminus A_n} \prod_{k=1}^{n} a_{k,\sigma(k)}.$$

Как и раньше, рассмотрим биекцию

$$\lambda : A_n \longrightarrow S_n \setminus A_n, \quad \sigma \longmapsto \sigma \circ \tau_{ij},$$

где τ_{ij} — транспозиция $(i\ j)$, меняющая местами числа i и j. Тогда во второй сумме можно заменить пробегание по $S_n \setminus A_n$ на пробегание по A_n:

$$|A| = \sum_{\sigma \in A_n} \prod_{k=1}^{n} a_{k,\sigma(k)} \; - \sum_{\sigma \in A_n} \prod_{k=1}^{n} a_{k,(\sigma \circ \tau_{ij})(k)}.$$

Обозначим

$$P(\sigma) = \prod_{k=1}^{n} a_{k,\sigma(k)}, \quad P'(\sigma) = \prod_{k=1}^{n} a_{k,(\sigma \circ \tau_{ij})(k)}.$$

Тогда

$$|A| = \sum_{\sigma \in A_n} \big(P(\sigma) - P'(\sigma)\big).$$

Поскольку i-я и j-я строки совпадают, имеем

$$a_{i,\sigma(j)} = a_{j,\sigma(j)}, \quad a_{j,\sigma(i)} = a_{i,\sigma(i)},$$

а для всех $k \neq i, j$ множители не меняются при переходе от σ к $\sigma \circ \tau_{ij}$. Поэтому

$$P(\sigma) = P'(\sigma)$$

для любого $\sigma \in A_n$, и тем самым

$$P(\sigma) - P'(\sigma) = 0.$$

Значит, вся сумма равна нулю:

$$|A| = \sum_{\sigma \in A_n} 0 = 0.$$

■

Следствие: Кососимметричность по столбцам доказывается аналогично с помощью транспонирования: если в A совпадают два столбца, то в A^T совпадают две строки, а так как $|A^T| = |A|$, то и в этом случае $|A| = 0$.

50 Поведение определителя при элементарных преобразованиях матрицы

Предложение. *Пусть $A \in M(n, R)$, R — коммутативное кольцо. Рассмотрим элементарные преобразования строк (аналогичные утверждения верны для столбцов).*

1. *При ЭП I типа (прибавление к строке кратной другой строки) определитель не изменяется.*
2. *При ЭП II типа (перестановка двух строк) определитель меняет знак.*
3. *При ЭП III типа (умножение строки на $\varepsilon \in R$) определитель умножается на ε.*

Доказательство. Обозначим строки матрицы A через

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix}, \quad A_i \text{ — } i\text{-я строка.}$$

3. ЭП III типа. Если матрица B получается из A умножением k-й строки на скаляр ε, то по линейности детерминанта по строке

$$|B| = \varepsilon\,|A|.$$

1. ЭП I типа. Пусть матрица A' получается из A заменой i-й строки на $A_i + \lambda A_j$ (при $i \neq j$):

$$A' = \begin{pmatrix} A_1 \\ \vdots \\ A_i + \lambda A_j \\ \vdots \\ A_n \end{pmatrix}.$$

По аддитивности по i-й строке

$$|A'| = \begin{vmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_n \end{vmatrix} + \begin{vmatrix} A_1 \\ \vdots \\ \lambda A_j \\ \vdots \\ A_n \end{vmatrix} = |A| + \lambda \begin{vmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_j \\ \vdots \\ A_n \end{vmatrix}.$$

Во второй матрице две строки совпадают, поэтому её определитель равен нулю. Значит, $|A'| = |A|$.

2. ЭП II типа. Пусть A' получается из A перестановкой i-й и j-й строк ($i \neq j$):

$$A' = \begin{pmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix}.$$

Рассмотрим матрицу

$$B = \begin{pmatrix} A_1 \\ \vdots \\ A_i + A_j \\ \vdots \\ A_i + A_j \\ \vdots \\ A_n \end{pmatrix},$$

в которой i-я и j-я строки совпадают. Тогда $|B| = 0$.

С другой стороны, по линейности по i-й и j-й строкам:

$$|B| = \begin{vmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_i + A_j \\ \vdots \\ A_n \end{vmatrix} + \begin{vmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i + A_j \\ \vdots \\ A_n \end{vmatrix}.$$

В каждом из этих определителей ещё раз раскладываем по строке i или j:

$$|B| = \underbrace{\begin{vmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_i \\ \vdots \\ A_n \end{vmatrix}}_{=0} + \begin{vmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{vmatrix} + \begin{vmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_i \\ \vdots \\ A_n \end{vmatrix} + \underbrace{\begin{vmatrix} A_1 \\ \vdots \\ A_j \\ \vdots \\ A_j \\ \vdots \\ A_n \end{vmatrix}}_{=0}.$$

То есть

$$0 = |B| = |A| + |A'| \implies |A'| = -|A|.$$

■

Замечание Утверждения для столбцов получаются применением тех же рассуждений к транспонированной матрице: $|A| = |A^T|$.

51 Критерий обратимости матрицы в терминах определителя

Предложение. *Пусть K — поле, $A \in M(n, K)$. Тогда*

$$A \in GL(n, K) \iff |A| \neq 0.$$

Доказательство. **“$\Longrightarrow$”:** Пусть A обратима. Тогда A можно представить как произведение элементарных матриц:

$$A = P_1 \dots P_m.$$

Определитель каждой элементарной матрицы равен либо 1, либо -1, либо ненулевому скаляру $\varepsilon \in K^\times$, поэтому он всегда отличен от нуля. Отсюда

$$|A| = |P_1| \dots |P_m| \neq 0.$$

“$\Longleftarrow$”: Предположим, что A не обратима. Тогда по ранговому разложению

$$A = PDQ,$$

где P, Q — обратимые матрицы (произведения элементарных), а

$$D = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \quad r < n.$$

В матрице D есть нулевая строка, поэтому $|D| = 0$. Тогда

$$|A| = |P|\,|D|\,|Q| = 0.$$

Получили: если A не обратима, то $|A| = 0$. Контрапозиция даёт: $|A| \neq 0 \Rightarrow A$ обратима. ■

52 Определитель произведения матриц

Предложение. *Пусть $A, B \in M(n, K)$, где K — поле. Тогда*

$$|AB| = |A| \cdot |B|.$$

Доказательство. Разберём два случая.

1) A не обратима. Тогда $|A| = 0$. Из критерия обратимости следует, что A имеет ранг меньше n, следовательно, AB тоже имеет ранг меньше n и не обратима. Значит, $|AB| = 0$. Получаем

$$|AB| = 0 = |A| \cdot |B|.$$

2) A обратима. Тогда

$$A = P_1 \dots P_m,$$

где P_i — элементарные матрицы. Докажем по индукции по m, что

$$|AB| = |A|\,|B|.$$

База: $m = 0$, тогда $A = E_n$. Имеем

$$|AB| = |E_n B| = |B| = |E_n| \cdot |B| = |A| \cdot |B|.$$

Переход: пусть утверждение верно для произведения из $m - 1$ элементарных матриц. Запишем

$$A = P_1(P_2 \dots P_m).$$

Рассмотрим матрицу $C = P_2 \dots P_m B$. Для любого элементарного P_1 известно, что

$$|P_1 C| = |P_1| \cdot |C|.$$

Тогда

$$|AB| = |P_1(P_2 \dots P_m B)| = |P_1| \cdot |P_2 \dots P_m B|.$$

По индукционному предположению

$$|P_2 \dots P_m B| = |P_2 \dots P_m| \cdot |B|.$$

Следовательно,

$$|AB| = |P_1| \cdot |P_2 \dots P_m| \cdot |B| = |P_1 \dots P_m| \cdot |B| = |A| \cdot |B|.$$

■

53 Определитель блочно-треугольной матрицы

Предложение. *(Определитель блочно-верхнетреугольной матрицы)*

$A = \begin{pmatrix} B & * \\ 0 & C \end{pmatrix}$, *где* $B \in M(m, R),\ C \in M(n-m, R)$

$\Longrightarrow |A| = |B| \cdot |C|$

Доказательство. $\rho \in S_m, \sigma \in S_{n-m}$

Введем $[\rho, \sigma] \in S_n \quad [\rho, \sigma](j) = \begin{cases} \rho(j), j \leqslant m \\ \sigma(j-m)+m, j \geqslant m+1 \end{cases}$

$inv([\rho, \sigma]) = inv\ \rho + inv\ \sigma$

$sgn([\rho, \sigma]) = sgn\ \rho \cdot sgn\ \sigma$

$|A| = \sum\limits_{\pi \in S_n} sgn\ \pi \cdot \prod\limits_{i=1}^{n} a_{i,\pi(i)} = \circledast$

Если $\exists i \geqslant m+1 : \pi(i) \leqslant m \Longrightarrow a_{i,\pi(i)} = 0$

$\circledast = \sum\limits_{\pi \in S_n} sgn\ \pi \cdot \prod\limits_{i=1}^{n} a_{i,\pi(i)} =$

Сумму берем по тем π, что переводит числа от $m+1$ до n в числа $m+1$ до n

$$\sum_{\rho \in S_m} \sum_{\sigma \in S_{n-m}} sgn[\rho, \sigma] \prod_{i=1}^{n} a_{i,[\rho,\sigma](i)} = \sum_{\rho \in S_m} \sum_{\sigma \in S_{n-m}} sgn\ \sigma \cdot sgn\ \rho \cdot \prod_{i=1}^{m} a_{i,\rho(i)} \prod_{i=1}^{n-m} a_{m+i,m+\sigma(i)} =$$

$$(\sum_{\rho \in S_m} sgn\ \rho \prod_{i=1}^{m} a_{i,\rho(i)})(\sum_{\rho \in S_{n-m}} sgn\ \sigma \prod_{i=1}^{n-m} a_{m+i,m+\sigma(i)}) = |B| \cdot |C| \qquad \blacksquare$$

Следствие: $A = \begin{pmatrix} B & 0 \\ * & C \end{pmatrix} \Longrightarrow |A| = |B| \cdot |C|$

Доказательство. $|A| = \left|A^T\right| = \begin{vmatrix} B^T & * \\ 0 & C^T \end{vmatrix} = \left|B^T\right| \cdot \left|C^T\right| = |B| \cdot |C|$ $\blacksquare$

Следствие: $A = \begin{pmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \Longrightarrow |A| = a_{11} \dots a_{nn}$

Доказательство. Воспользуемся индукцией по n

База: $n = 1$ - тривиально

Переход: $|A| \overset{\text{предл.}}{=} \begin{vmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{n-1,n-1} \end{vmatrix} \cdot a_{nn} \overset{\text{ИП}}{=} a_{11} \dots a_{n-1,n-1} \cdot a_{nn}$ $\blacksquare$

54 Определитель матрицы с почти нулевой строкой

Предложение. *Пусть*

$$A = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & m & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix},$$

где m — элемент на пересечении i-й строки и j-го столбца.

Тогда

$$|A| = (-1)^{i+j} \cdot m \cdot |M_{ij}|,$$

где M_{ij} — минор, полученный путём вычёркивания из A строки i и столбца j, а $|M_{ij}|$ — определитель этого минора (алгебраическое дополнение к элементу m).

Доказательство. 1) $i = j = 1$, т.е.

$$A = \begin{pmatrix} m & 0 & \cdots & 0 \\ \vdots & & & \\ \vdots & & M_{11} & \\ \vdots & & & \end{pmatrix}.$$

Тогда $|A| = m \cdot |M_{11}| = (-1)^{1+1} \cdot m \cdot |M_{11}|$.

2) Общий случай.

Переставляя строки и столбцы, перемещаем i-ю строку на первое место (требуется $i-1$ перестановка) и j-й столбец на первое место (требуется $j-1$ перестановка). Получаем матрицу

$$A' = \begin{pmatrix} m & 0 & \cdots & 0 \\ \vdots & & & \\ \vdots & & M_{ij} & \\ \vdots & & & \end{pmatrix}.$$

По первому пункту $|A'| = m \cdot |M_{ij}|$. Учитывая знак от перестановок:

$$|A| = (-1)^{i-1} \cdot (-1)^{j-1} \cdot |A'| = (-1)^{i+j} \cdot m \cdot |M_{ij}|.$$

■

55 Разложение определителя по строке (столбцу)

Определение. Величина $A_{ij} = (-1)^{i+j} \cdot |M_{ij}|$ называется *алгебраическим дополнением* к элементу a_{ij} матрицы A.

Предложение. *Пусть* $A = (a_{ij}) \in M(n, R)$.

Тогда для любого k, *где* $1 \leqslant k \leqslant n$, *справедливо разложение по* k*-й строке:*

$$|A| = a_{k1}A_{k1} + a_{k2}A_{k2} + \cdots + a_{kn}A_{kn} = \sum_{j=1}^{n} a_{kj}A_{kj}.$$

Доказательство. Используя полилинейность и кососимметричность определителя, разобьём k-ю строку на сумму строк с одним ненулевым элементом:

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

$$= \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{k2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} + \cdots$$

$$+ \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}.$$

По предыдущей теореме каждый определитель равен $a_{kj} \cdot A_{kj}$, откуда

$$|A| = a_{k1}A_{k1} + a_{k2}A_{k2} + \cdots + a_{kn}A_{kn}.$$

■

Замечание Аналогично, разложение определителя по k-му столбцу имеет вид:

$$|A| = a_{1k}A_{1k} + a_{2k}A_{2k} + \cdots + a_{nk}A_{nk} = \sum_{i=1}^{n} a_{ik}A_{ik}.$$

Лемма 3. *О фальшивом разложении определителя.*

Пусть $A \in M(n, R)$ *и* $1 \leqslant i, j \leqslant n$, *где* $i \neq j$.

Тогда

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0.$$

Доказательство. Рассмотрим матрицу A', полученную из A заменой j-й строки на i-ю:

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_j \\ \vdots \\ A_n \end{pmatrix}, \quad A' = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_i \text{ (j-я строка)} \\ \vdots \\ A_n \end{pmatrix}.$$

Матрица A' имеет две одинаковые строки, поэтому $|A'| = 0$. С другой стороны, разлагая $|A'|$ по j-й строке (которая совпадает с i-й строкой матрицы A) и используя алгебраические дополнения из матрицы A, получаем:

$$0 = |A'| = a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn}.$$

■

56 Взаимная матрица. Явный вид обратной матрицы

Определение. Пусть $A \in M(n, R)$. Взаимная (присоединённая, союзная) матрица определяется как

$$\widetilde{A} := \left(A_{ji}\right)_{i,j=1}^{n},$$

где $A_{ij} = (-1)^{i+j} |M_{ij}|$ — алгебраическое дополнение к элементу a_{ij} матрицы A; то есть в позиции (i, j) матрицы $\widetilde{A}$ стоит дополнение A_{ji}.

Взаимная матрица — это транспонированная матрица алгебраических дополнений.

Предложение. *Справедливо*

$$A \cdot \widetilde{A} \;=\; \widetilde{A} \cdot A \;=\; |A| \cdot E_n \;=\; \begin{pmatrix} |A| & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & |A| \end{pmatrix}.$$

Доказательство. Рассмотрим элементы произведения:

$$(A\widetilde{A})_{ij} \;=\; a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn}.$$

Если $i = j$, то это разложение детерминанта $|A|$ по i-й строке, откуда $(A\widetilde{A})_{ii} = |A|$. Если $i \neq j$, то по лемме о «фальшивом» разложении сумма равна нулю, то есть $(A\widetilde{A})_{ij} = 0$. Аналогично, разлагая по столбцу, получаем $\widetilde{A}A = |A|E_n$. ■

Замечание Для $\widetilde{A} \cdot A = |A| \cdot E_n$ используется разложение по столбцу.

Следствие:Пусть $A \in M(n,K)$, где K — поле, и $|A| \neq 0$ (или более общо: в коммутативном кольце R элемент $|A|$ обратим, то есть $|A| \in R^*$). Тогда

$$A^{-1} = |A|^{-1}\,\widetilde{A}.$$

Доказательство. Из $A\widetilde{A} = |A|E_n$ следует $A\,(|A|^{-1}\widetilde{A}) = E_n$ и $(|A|^{-1}\widetilde{A})\,A = E_n$. ■

Следствие:Если $|A| \in R^*$, то $A \in GL(n,R)$.

Замечание Верно и обратное: если $A \in GL(n,R)$ (где R — коммутативное кольцо с единицей), то $|A| \in R^*$.

Доказательство. Из $A^{-1}A = E_n$ и мультипликативности детерминанта получаем

$$1 = |E_n| = |A^{-1}A| = |A^{-1}| \cdot |A|.$$

Следовательно, $|A|$ обратим в R, то есть $|A| \in R^*$. ■

57 Линейное пространство. Определение, примеры, простейшие свойства

Определение. Пусть K — поле, V — множество. Структура **линейного пространства** на V над K задаётся операциями

$$+ : V \times V \to V, \qquad \cdot : K \times V \to V,$$

удовлетворяющими аксиомам:

1. $(V,+)$ — абелева группа;
2. дистрибутивность по векторам: $\alpha \cdot (v_1 + v_2) = \alpha v_1 + \alpha v_2$;
3. дистрибутивность по скалярам: $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 v + \alpha_2 v$;
4. ассоциативность умножения на скаляр: $\alpha_1(\alpha_2 \cdot v) = (\alpha_1\alpha_2) \cdot v$;
5. единица поля действует тождественно: $1 \cdot v = v$.

Элементы V называются векторами (обычно латинские буквы), элементы K — скалярами (часто греческие).

Примеры.

1. Пространство матриц фиксированного размера $M(m,n,K)$. Частные случаи — матрицы-столбцы и матрицы-строки; далее используем столбцы и обозначаем

   $$K^m := M(m,1,K),$$

   называя это арифметическим m-мерным пространством над K.
2. Нуль-пространство $V = \{\overline{0}\}$. Операции: $\overline{0} + \overline{0} := \overline{0}$, $\alpha \cdot \overline{0} := \overline{0}$.
3. Многочлены $K[X]$; также подпространства ограниченной степени, например

   $$V := \{\, f \in K[X] \mid \deg f \leq 5 \,\}.$$

4. $K = \mathbb{R}$, $V = \mathbb{R}_{>0}$ с операциями

$$v_1 + v_2 := v_1 v_2, \qquad \alpha \cdot v := v^\alpha.$$

Доказательство. (a) $(V, +)$ — абелева группа, так как $(\mathbb{R}_{>0}, \cdot)$ — абелева группа.

(b) Дистрибутивность по векторам: $\alpha \cdot (v_1 + v_2) = (v_1 v_2)^\alpha = v_1^\alpha v_2^\alpha = \alpha \cdot v_1 + \alpha \cdot v_2$ (с учётом того, что «+» в V — это умножение чисел).

(c) Дистрибутивность по скалярам: $(\alpha_1 + \alpha_2) \cdot v = v^{\alpha_1 + \alpha_2} = v^{\alpha_1} v^{\alpha_2} = \alpha_1 \cdot v + \alpha_2 \cdot v$.

(d) Ассоциативность: $\alpha_1(\alpha_2 \cdot v) = (v^{\alpha_2})^{\alpha_1} = v^{\alpha_1 \alpha_2} = (\alpha_1 \alpha_2) \cdot v$.

(e) Единица: $1 \cdot v = v^1 = v$.

■

5. $K = \mathbb{F}_2 = \mathbb{Z}/(2)$, M — любое множество, $V := 2^M$ (множество всех подмножеств). Пусть

$$v_1 + v_2 := v_1 \triangle v_2, \qquad 1 \cdot v := v, \quad 0 \cdot v := \varnothing.$$

Доказательство. (a) $(V, +)$ — абелева группа: симметрическая разность коммутативна, ассоциативна, нейтральный элемент $\varnothing$, обратный к v — само v.

(b) Дистрибутивность по векторам:

$$\alpha \cdot (v_1 + v_2) = \begin{cases} v_1 \triangle v_2, & \alpha = 1, \\ \varnothing, & \alpha = 0 \end{cases} = \alpha \cdot v_1 + \alpha \cdot v_2.$$

(c) Дистрибутивность по скалярам:

$$(\alpha_1 + \alpha_2) \cdot v = \begin{cases} v, & \alpha_1 \neq \alpha_2, \\ \varnothing, & \alpha_1 = \alpha_2 \end{cases} = \alpha_1 \cdot v + \alpha_2 \cdot v.$$

(d) Ассоциативность умножения на скаляр очевидна из таблицы $0, 1$.

(e) $1 \cdot v = v$ по определению.

■

Некоторые свойства линейных пространств.

1. $0 \cdot v = \overline{0}$.

Доказательство. $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$. Прибавляя противоположный элемент к $0 \cdot v$, получаем $0 \cdot v = \overline{0}$. ■

2. $\alpha \cdot \overline{0} = \overline{0}$.

Доказательство. $\alpha \cdot \overline{0} = \alpha \cdot (\overline{0} + \overline{0}) = \alpha \cdot \overline{0} + \alpha \cdot \overline{0}$, откуда $\alpha \cdot \overline{0} = \overline{0}$. ■

3. Если $\alpha v = \overline{0}$, то либо $\alpha = 0$, либо $v = \overline{0}$ (для поля K).

Доказательство. При $\alpha \neq 0$ умножаем на α^{-1}: $v = \alpha^{-1}(\alpha v) = 1 \cdot v = v$ и потому $v = \overline{0}$. ■

4. $(-\alpha)v = -(\alpha v)$.

   Доказательство. $(-\alpha)v + (\alpha v) = ((-\alpha) + \alpha)v = 0 \cdot v = \overline{0}$, то есть $(-\alpha)v$ — противоположный к αv. ■

58 Система образующих линейного пространства, свойства. Подпространство

Определение. V – ЛП/K, $v_1, \ldots, v_n \in V$, $\alpha_1, \ldots, \alpha_n \in K$.
$\alpha_1 v_1 + \cdots + \alpha_n v_n$ – **линейная комбинация** векторов $v_1, \ldots, v_n$ с коэффициентами $\alpha_1, \ldots, \alpha_n$.

Определение. V – ЛП/K, $v_1, \ldots, v_n \in V$. $0 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_n$ – **тривиальная** линейная комбинация.

Определение. Множество всех линейных комбинаций называется **линейной оболочкой**.
$\mathrm{Lin}(v_1, ..., v_n) := \{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid \alpha_1, \ldots, \alpha_n \in K\}$ – **линейная оболочка** векторов $v_1, \ldots, v_n$.

Определение. V – ЛП/K, $v_1, \ldots, v_n \in V$.
Если $\mathrm{Lin}(v_1, \ldots, v_n) = V$, то $v_1, \ldots, v_n$ – **система образующих** (для) V или **порождающая система**.

Предложение. *Пусть* $W = \mathrm{Lin}(v_1, \ldots, v_n)$, $v_n \in \mathrm{Lin}(v_1, \ldots, v_{n-1})$. *Тогда* $W = \mathrm{Lin}(v_1, \ldots, v_{n-1})$.

Доказательство.

$W \supset \mathrm{Lin}(v_1, \ldots, v_{n-1})$:

Линейную комбинацию $n-1$ векторов можно рассматривать как линейную комбинацию n векторов, где n-ый вектор имеет нулевой коэффициент:
$\alpha_1 v_1 + \cdots + \alpha_{n-1} v_{n-1} = \alpha_1 v_1 + \cdots + \alpha_{n-1} v_{n-1} + 0 \cdot v_n$.

$W \subset \mathrm{Lin}(v_1, \ldots, v_{n-1})$:

$v_n \in \mathrm{Lin}(v_1, \ldots, v_{n-1}) \Rightarrow v_n = \beta_1 v_1 + \cdots + \beta_{n-1} v_{n-1}$. Поэтому любую линейную комбинацию n векторов можно представить в виде линейной комбинации $n-1$ векторов:
$\alpha_1 v_1 + \cdots + \alpha_n v_n = \alpha_1 v_1 + \cdots + \alpha_{n-1} v_{n-1} + \alpha_n \cdot (\beta_1 v_1 + \cdots + \beta_{n-1} v_{n-1}) = (\alpha_1 + \alpha_n \beta_1) \cdot v_1 + (\alpha_2 + \alpha_n \beta_2) \cdot v_2 + \cdots + (\alpha_{n-1} + \alpha_n \beta_{n-1}) \cdot v_{n-1}$

■

Определение. V – **конечномерное** линейное пространство, если $\exists n \in \mathbb{N} : \exists v_1, \ldots, v_n \in V : V = \mathrm{Lin}(v_1, \ldots, v_n)$.

Примеры:

1. $M(m, n, K)$ – конечномерное ЛП/K, т.к. $M(m, n, K) = \mathrm{Lin}(e_{ij} \mid i = 1..m, j = 1..n)$, где e_{ij} – матричная единица.
2. $K[X]$ – бесконечномерное.

Доказательство. Пусть $v_1, \ldots, v_n$ – система образующих. Пусть $d := \max\{\deg v_i \mid i = 1..n\}$. Тогда $\max\{\deg v \mid v \in \mathrm{Lin}(v_1, \ldots, v_n)\} = d$, но $K[X]$ содержит многочлены степени $d+1$. ■

Определение. $W \subset V$ называется **линейным подпространством** V, если выполняются след. свойства:

1. $\overline{0} \in W$ – содержит 0;
2. $W + W \subset W$ – замкнуто относительно сложения;
3. $KW \subset W$ – замкнуто относительно умножения.

Замечание W – подгруппа относительно сложения.

Доказательство. Наличие нуля и замкнутость относительно сложения выполняются. Ещё нужно для подгруппы, чтобы были противоположные элементы. Но т.к. K – поле, то наличие $-w = (-1) \cdot w$ (это равенство было доказано ранее) гарантируется третьим свойством. ■

Примеры:

1. $0 = \overline{0}, V$ – тривиальные подпространства V.
2. $V = K^3 = M(1, 3, K)$;
   $W = \left\{ \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} \;\middle|\; \alpha + \beta + \gamma = 0 \right\}$ – линейное подпространство V.
   Более того, $\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ -\alpha - \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$. А значит $W = \mathrm{Lin}(\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix})$.
3. $\mathrm{Lin}(v_1, \ldots, v_n)$ – линейная оболочка каких-то векторов из линейного пространства тоже является линейным подпространством.

   Можно говорить не “линейная оболочка”, а “порождаемое векторами подпространство”.
4. $V = K[X]$;
   $W_d = \{f \mid \deg f \leqslant d\}$ – лин. подпр-во V.

   Более того, $W_d = \mathrm{Lin}(1, x, x^2, \ldots, x^d)$.

59 Линейно зависимые семейства, свойства

Предложение.

Пусть V – ЛП/K. $v_1, \ldots, v_n \in V$. Эквивалентны следующие два свойства:

1. $\exists \alpha_1, \ldots, \alpha_n \in K$, т.ч. $\exists i : \alpha_i \neq 0$ и $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$.
   Другими словами, сущ. нетривиальная линейная комбинация данных векторов, равная 0.
2. $\exists j \in \{1..n\} : v_j \in \mathrm{Lin}(v_i \mid i \neq j)$.
   Другими словами, v_j является линейной комбинацией остальных векторов.

Доказательство.

“1 ⇒ 2”:

$\exists j : \alpha_j \neq 0$;
$\alpha_1 v_1 + ... + \alpha_n v_n = 0$,
$\alpha_1 v_1 + ... + \alpha_{j-1} v_{j-1} + \alpha_{j+1} v_{j+1} + ... + \alpha_n v_n = -\alpha_j v_j$;
Т.к. $\alpha_j \neq 0$, мы можем поделить на α_j;

$$v_j = \left(-\frac{\alpha_1}{\alpha_j}\right) v_1 + \cdots + \left(-\frac{\alpha_{j-1}}{\alpha_j}\right) v_{j-1} + \left(-\frac{\alpha_{j+1}}{\alpha_j}\right) v_{j+1} + \cdots + \left(-\frac{\alpha_n}{\alpha_j}\right) v_n \in \mathrm{Lin}(v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n)$$

“2 ⇒ 1”:

$$v_j \in \mathrm{Lin}(v_i \mid i \neq j) \Rightarrow v_j = \sum_{i \neq j} \beta_i v_i;$$

$$\sum_{i \neq j} \beta_i v_i - v_j = \sum_{i=1}^{n} \beta_i v_i = 0, \text{ где } \beta_j = -1.$$

Получаем нетривиальную линейную комбинацию, т.к. при векторе v_j коэффициент $-1 \neq 0$.

■

Определение.
$v_1, \ldots, v_n$ – **линейно зависимая система** (**ЛЗС**), если выполняются условия из предложения.
$v_1, \ldots, v_n$ – **линейно независимая система** (**ЛНС**) в противном случае.

Предложение.

1. $v_1, \ldots, v_n$ – ЛЗС $\Rightarrow \forall \sigma \in S_n \;\; v_{\sigma(1)}, \ldots, v_{\sigma(n)}$ – ЛЗС.
2. С ЛЗС:
   $v_1, \ldots, v_n$ – ЛЗС, $v \in V \Rightarrow v_1, \ldots, v_n, v$ – ЛЗС.

   С ЛНС:
   $v_1, \ldots, v_n$ – ЛНС $\Rightarrow \forall i = 1..n \;\; v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ – ЛНС.
3. $\exists i : v_i = 0 \Rightarrow v_1, \ldots, v_n$ – ЛЗС.
4. $v_1, \ldots, v_n$ – ЛНС, $v \in V$ Тогда: $v_1, \ldots, v_n, v$ – ЛЗС $\Longleftrightarrow v \in \mathrm{Lin}(v_1, \ldots, v_n)$.

Доказательство.

1. Тривиально.
2. С ЛЗС:
   $\exists \alpha_1, \ldots, \alpha_n \in K \mid \exists \alpha_i \neq 0$ и $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ – нетрив. ЛК $\Longrightarrow \alpha_1 v_1 + \cdots + \alpha_n v_n + 0 \cdot v = 0$ – тоже нетрив. ЛК.

   С ЛНС:
   Аналогично.
3. $1 \cdot v_i + \sum\limits_{j \neq i} 0 \cdot v_j = 0$ – нетривиальная ЛК.
4. “$\Longleftarrow$”:
   По определению ЛЗС.

“$\Longrightarrow$”:
$v_1, \ldots, v_n, v$ – ЛЗС $\Rightarrow \exists \alpha_1, \ldots, \alpha_{n+1} \in K \mid \exists \alpha_i \neq 0$ и $\alpha_1 v_1 + \cdots + \alpha_n v_n + \alpha_{n+1} v = 0$. Предположим, что $\alpha_{n+1} = 0 \Rightarrow \alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ – нетрив. ЛК $\Rightarrow v_1, \ldots, v_n$ – ЛЗС. Противоречие.
Таким образом, $\alpha_{n+1} \neq 0$, значит $v = \sum\limits_{i=1}^{n} \frac{-\alpha_i}{\alpha_{n+1}} v_i \Rightarrow v \in \mathrm{Lin}(v_1, \ldots, v_n)$.

■

60 Теорема о линейной зависимости линейных комбинаций

Теорема.

Пусть $v_1, \ldots, v_m \in V$, $w_1, \ldots, w_n \in \mathrm{Lin}(v_1, \ldots, v_m)$, $n > m$. Тогда $w_1, \ldots, w_n$ – ЛЗС.

Доказательство. Индукция по m.

База. $m = 1$:

$w_1, \ldots, w_n \in \mathrm{Lin}(v_1) \Rightarrow w_1 := \alpha v_1$.
Если $\alpha = 0$, то $w_1 = 0 \Rightarrow w_1, \ldots, w_n$ – ЛЗС по доказанному ранее свойству.
Если $\alpha \neq 0$, то $v_1 = \alpha^{-1} w_1 \Rightarrow v_1 \in \mathrm{Lin}(w_1) \Rightarrow w_1, \ldots, w_n \in \mathrm{Lin}(w_1) \Rightarrow w_1, w_2$ – ЛЗС $\Rightarrow w_1, \ldots, w_n$ – ЛЗС по доказанному ранее свойству.

Переход. $m - 1 \longrightarrow m$:

$$
\begin{aligned}
w_1 &= \alpha_{11} v_1 + \cdots + \alpha_{1m} v_m, \\
w_2 &= \alpha_{21} v_1 + \cdots + \alpha_{2m} v_m, \\
&\vdots \\
w_n &= \alpha_{n1} v_1 + \cdots + \alpha_{nm} v_m.
\end{aligned}
$$

Рассмотрим случаи:

- $\alpha_{1m} = \alpha_{2m} = \cdots = \alpha_{nm} = 0$
  $\Rightarrow w_1, \ldots, w_n \in \mathrm{Lin}(v_1, \ldots, v_{m-1})$.
  $n > m > m - 1 \overset{\text{ИП}}{\Longrightarrow} w_1, \ldots, w_n$ – ЛЗС.
- $\exists j : \alpha_{jm} \neq 0$. НУО, $j = n$.
  Тогда $w_i - \frac{\alpha_{im}}{\alpha_{nm}} w_n \in \mathrm{Lin}(v_1, \ldots, v_{m-1})$, т.к. мы занулили коэф. при v_m,
  $n > m \Rightarrow n - 1 > m - 1 \overset{\text{ИП}}{\Longrightarrow} w_1 - \frac{\alpha_{1m}}{\alpha_{nm}} w_n, \ldots, w_{n-1} - \frac{\alpha_{(n-1)m}}{\alpha_{nm}} w_n$ – ЛЗС
  $\Rightarrow \exists \beta_1, \ldots, \beta_{n-1} \mid \exists \beta_i \neq 0$ и $\sum\limits_{i=1}^{n-1} \beta_i (w_i - \frac{\alpha_{im}}{\alpha_{nm}} w_n) = 0$
  $\Rightarrow \sum\limits_{i=1}^{n-1} \beta_i (w_i - \frac{\alpha_{im}}{\alpha_{nm}} w_n) := \beta_1 w_1 + \cdots + \beta_{n-1} w_{n-1} + \gamma w_n = 0$, независимо от γ сущ. $\beta_i \neq 0$ по ИП, поэтому это будет нетривиальная ЛК $w_1, \ldots, w_n \Rightarrow w_1, \ldots, w_n$ – ЛЗС.

■

61 Равносильные определения базиса

Определение. Пусть V – ЛП/K, $e_1, \dots, e_n \in V$. Набор $(e_1, \dots, e_n)$ называется **базисом линейного пространства** V, если $\forall v \in V \ \exists! \alpha_1, \dots, \alpha_n \in K : \alpha_1 e_1 + \dots + \alpha_n e_n = v$, другими словами, любой вектор из пространства единственным образом раскладывается в линейную комбинацию базисных векторов.

Определение. Пусть V, V' – ЛП/K. Отображение $\varphi : V \to V'$ называется **изоморфизмом линейных пространств**, если выполняются два свойства:

1. φ – биекция;
2. $\forall v_1, v_2 \in V \ \forall \alpha_1, \alpha_2 \in K \ \ \varphi(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 \varphi(v_1) + \alpha_2 \varphi(v_2)$.

Пример:
$\varphi : M(m, n, K) \to M(n, m, K)$,
$\varphi : A \mapsto A^T$,
φ – изоморфизм ЛП.

Предложение.

Пусть V – ЛП/K, $e_1, \dots, e_n \in V$. Тогда следующие свойства эквивалентны:

1. $e_1, \dots, e_n$ – базис V;
2. $\varphi : K^n \to V$
   $\varphi : \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mapsto \sum_{i=1}^{n} \alpha_i e_i$
   φ – изоморфизм ЛП;
3. $e_1, \dots, e_n$ – линейно независимая порождающая система,
   т.е. $e_1, \dots, e_n$ – ЛНС, и $V = \mathrm{Lin}(e_1, \dots, e_n)$;
4. $e_1, \dots, e_n$ – минимальная порождающая система для V, т.е. нельзя удалить из этого набора ни один вектор так, чтобы система осталась порождающей;
5. $e_1, \dots, e_n$ – максимальная линейно независимая система, т.е. нельзя добавить ни один вектор из V так, чтобы система осталась линейно независимой.

Доказательство.

$2 \Rightarrow 1$: φ – биекция $\Rightarrow \forall v \in V \ \exists! \alpha_1, \dots, \alpha_n \in K : \alpha_1 e_1 + \dots + \alpha_n e_n = v$, что по определению означает, что $e_1, \dots, e_n$ – базис V.

$1 \Rightarrow 2$: $\varphi(\alpha a + \beta b) = \alpha \varphi(a) + \beta \varphi(b)$ очевидно выполняется для любых $\alpha_1, \dots, \alpha_n \in K$.

Докажем теперь, что φ – биекция. По опр. базиса $\forall v \in V \ \exists! \alpha_1, \dots, \alpha_n \in K : \alpha_1 e_1 + \dots + \alpha_n e_n = v$. Заметим, что по сути $\alpha_1, \dots, \alpha_n$ – это $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, а $\alpha_1 e_1 + \dots + \alpha_n e_n$ – это $\varphi \left(\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \right)$.

Т.е. из опр. базиса видно, что каждому вектору из V сопоставлен ровно один столбец из K^n, значит φ – биекция.

$1 \Rightarrow 3$: Раз любой вектор раскладывается в линейную комбинацию базисных векторов, очевидно, что $e_1, \dots, e_n$ – порождающая система. Проверим линейную независимость. Рассмотрим $\alpha_1 e_1 + \dots + \alpha_n e_n = \overline{0} = 0 \cdot e_1 + \dots + 0 \cdot e_n$. Т.к. $\overline{0}$ – это тоже вектор, то в силу единственности разложения $\alpha_1 = \dots = \alpha_n = 0$. Таким образом, не существует нетривиальной ЛК $e_1, \dots, e_n$, равной $\overline{0}$, значит $e_1, \dots, e_n$ – ЛНС.

$3 \Rightarrow 1$: Т.к. это порождающая система, необходимо доказать только единственность. Пусть $\alpha_1 e_1 + \dots + \alpha_n e_n = \beta_1 e_1 + \dots + \beta_n e_n$. Перенесём всё в левую часть и воспользуемся законом дистрибутивности. $(\alpha_1 - \beta_1)e_1 + \dots + (\alpha_n - \beta_n)e_n = \overline{0}$. $e_1, \dots, e_n$ – ЛНС $\Rightarrow \alpha_1 - \beta_1 = \dots = \alpha_n - \beta_n = 0 \Rightarrow \alpha_1 = \beta_1, \dots, \alpha_n = \beta_n$.

$3 \Rightarrow 4$: Предположим, что $e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n$ – порождающая система. НУО, $i = n$. Т.е. $V = \mathrm{Lin}(e_1, \dots, e_{n-1})$. Но тогда $e_n \in \mathrm{Lin}(e_1, \dots, e_{n-1}) \Rightarrow e_1, \dots, e_n$ – ЛЗС. Противоречие.

$4 \Rightarrow 3$: Предположим, что $e_1, \dots, e_n$ – ЛЗС. НУО, $e_n \in \mathrm{Lin}(e_1, \dots, e_{n-1})$. Тогда $V = \mathrm{Lin}(e_1, \dots, e_n) = \mathrm{Lin}(e_1, \dots, e_{n-1}) \Rightarrow e_1, \dots, e_{n-1}$ – порождающая система. Противоречие.

$3 \Rightarrow 5$: Это порождающая система $\Rightarrow V = \mathrm{Lin}(e_1, \dots, e_n) \Rightarrow \forall v \in V \;\; v \in \mathrm{Lin}(e_1, \dots, e_n) \Rightarrow$ $e_1, \dots, e_n, v$ – ЛЗС.

$5 \Rightarrow 3$: Возьмём $v \in V$. $e_1, \dots, e_n$ – ЛНС, но $e_1, \dots, e_n, v$ – ЛЗС $\Rightarrow v \in \mathrm{Lin}(e_1, \dots, e_n) \Rightarrow e_1, \dots, e_n$ – порождающая система.

■

62 Размерность. Свойства пространств заданной размерности

Предложение.

Пусть $(e_1, \dots, e_n)$, $(e'_1, \dots, e'_m)$ – базисы V – ЛП/K. Тогда $n = m$.

Доказательство. Предположим, что это не так. Пусть $n > m$. $e'_1, \dots, e'_m$ – базис $\Rightarrow e_1, \dots, e_n \in \mathrm{Lin}(e'_1, \dots, e'_m)$. Но $n > m \Rightarrow$ по теореме о линейной зависимости линейных комбинаций $e_1, \dots, e_n$ – ЛЗС, но это противоречит 3-ему свойству теоремы о равносильных определениях базиса. Значит, $n = m$. ■

Предложение.

Из любой системы образующих V – ЛП/K – можно выделить базис.

Доказательство. Пусть $V = \mathrm{Lin}(v_1, \dots, v_n)$. Выберем в $v_1, \dots, v_n$ наименьшую по мощности подсистему, являющуюся системой образующих. Другими словами, рассмотрим все подмножества $v_1, \dots, v_n$, оставим из них только те, что являются системой образующих, и выберем из них подмножество с наименьшим количеством элементов. Это можно сделать, т.к. у конечного множества существует конечное число подмножеств. Получаем минимальную порождающую систему. Значит, по свойству 4 из теоремы о равносильных определениях базиса это базис. ■

Следствие: У любого конечномерного пространства есть базис.

Определение. Пусть V – конечномерное пространство. Его **размерностью** называется число векторов в любом его базисе. Обозначается она $\dim V$.

Примеры:

1. $V := M(m, n, K)$. Любая матрица $A = (a_{ij}) \in V$ преставима в виде линейной комбинации матричных единиц $A = \sum_{i,j} a_{ij} \cdot e_{ij}$. Откуда видно, что $e_{11}, \ldots, e_{mn}$ – базис V, и $\dim V = mn$.
2. $\dim K^n = n$.
3. Считается, что $\dim \{ \overline{0} \} = 0$.

Лемма 4.

Пусть V – ЛП, $\dim V = n$; $v_1, \ldots, v_N \in V$, $N > n$. Тогда $v_1, \ldots, v_N$ – ЛЗС.

Доказательство.

Непосредственно из теоремы о линейной зависимости линейных комбинаций. ■

Предложение.

Пусть V – конечномерное ЛП; $v_1, \ldots, v_n$ – ЛНС. Тогда её можно дополнить до базиса.

Доказательство. Если $V = \mathrm{Lin}(v_1, \ldots, v_n)$, то $v_1, \ldots, v_n$ – базис по свойству 3 т. о равносильных опр. базиса, иначе $\exists v_{n+1} \in V, v_{n+1} \notin \mathrm{Lin}(v_1, \ldots, v_n) \Rightarrow v_1, \ldots, v_{n+1}$ – тоже ЛНС. Если $V = \mathrm{Lin}(v_1, \ldots, v_{n+1})$, то $v_1, \ldots, v_{n+1}$ – базис, иначе повторяем действия.

Пусть $m = \dim V$. Тогда $v_1, \ldots, v_{m+1}$ – ЛЗС $\Rightarrow$ алгоритм завершится. ■

Следствие:

Пусть $\dim V = n$; $e_1, \ldots, e_n \in V$. Тогда следующие утверждения эквивалентны:

1. $e_1, \ldots, e_n$ – базис.
2. $e_1, \ldots, e_n$ – ЛНС.
3. $e_1, \ldots, e_n$ – порождающая система.

Доказательство.

$1 \Rightarrow 2, 3$: Очевидно.

$2 \Rightarrow 1$: ЛНС можно дополнить до базиса, но базис состоит из n векторов $\Rightarrow e_1, \ldots, e_n$ – базис.

$3 \Rightarrow 1$: из порождающей системы можно выделить базис, но базис состоит из n векторов $\Rightarrow$ $e_1, \ldots, e_n$ – базис. ■

63 Размерность подпространства. Классификация конечномерных пространств

Предложение.

Пусть $\dim V = n$; $W \subset V$ – подпространство. Тогда:

1. W – конечномерное; $\dim W \leq n$.
2. $\dim W = n \Rightarrow W = V$.

Доказательство.

1. Предположим, что W – бесконечномерное или $\dim W > n$. Если $W = \{\overline{0}\}$, то тут всё очевидно. Пусть $W \neq \{\overline{0}\}$.
   Тогда $\exists w_1 \in W, w_1 \neq \overline{0}$.
   Если $n \geqslant 1$, то $\exists w_1 \in W, w_2 \notin \mathrm{Lin}(w_1)$.
   Если $n \geqslant 2$, то $\exists w_2 \in W, w_3 \notin \mathrm{Lin}(w_1, w_2)$.
   ...
   $\exists w_n \in W, w_n \notin \mathrm{Lin}(w_1, \ldots, w_{n-1})$.
   Таким образом $w_1, \ldots, w_n$ – ЛНС и не базис W, т.е. $\mathrm{Lin}(w_1, \ldots, w_n) \subsetneq W$, но $w_1, \ldots, w_n \in V$ и $\dim V = n \Rightarrow w_1, \ldots, w_n$ – базис $V \Rightarrow \mathrm{Lin}(w_1, \ldots, w_n) \subsetneq W \subset V = \mathrm{Lin}(w_1, \ldots, w_n)$. Противоречие.
2. Пусть $w_1, \ldots, w_n$ – базис W. Тогда $w_1, \ldots, w_n$ – ЛНС $\Rightarrow w_1, \ldots, w_n$ – базис $V \Rightarrow V = \mathrm{Lin}(w_1, \ldots, w_n) = W$.

■

Теорема.

Пусть V, V' – конечномерные ЛП$/K$. Тогда $V \cong V' \Leftrightarrow \dim V = \dim V'$.

Доказательство.

"$\Longrightarrow$": Пусть $e_1, \ldots, e_n$ – базис V, $\varphi : V \xrightarrow{\sim} V'$. Возьмём $v' \in V'$. φ – биекция $\Rightarrow \exists \varphi^{-1}$. Пусть $v := \varphi^{-1}(v')$. Пусть $v = \alpha_1 e_1 + \cdots + \alpha_n e_n$. Тогда $v' = \varphi(\alpha_1 e_1 + \cdots + \alpha_n e_n) = \alpha_1 \varphi(e_1) + \cdots + \alpha_n \varphi(e_n)$. Т.к. φ – биекция, то $\varphi(e_1), \ldots, \varphi(e_n)$ различны. Пусть $v' = \beta_1 \varphi(e_1) + \cdots + \beta_n \varphi(e_n)$. Т.к. v' – изоморфизм, $v' = \varphi(\beta_1 e_1 + \cdots + \beta_n e_n)$. Т.к. φ – биекция, $v = \beta_1 e_1 + \cdots + \beta_n e_n$. Но $e_1, \ldots, e_n$ – базис $V \Rightarrow \forall i\ \alpha_i = \beta_i$. Значит, такое разложение v' единственно и найдётся для всякого $v' \Rightarrow \varphi(e_1), \ldots, \varphi(e_n)$ – базис $V' \Rightarrow \dim V' = n = \dim V$.

"$\Longleftarrow$": $\dim V = \dim V' = n \Rightarrow V \cong K^n$ и $V' \cong K^n$. Пусть $\varphi : V \xrightarrow{\sim} K^n$, $\varphi' : V' \xrightarrow{\sim} K^n$. Т.к. φ и φ' – изоморфизмы (а значит и биекции), то отн. $(\varphi')^{-1} \circ \varphi : V \xrightarrow{\sim} V'$ будет изоморфизмом V и V'.

■

Следствие: Отношение изоморфности конечномерных ЛП – отношение эквивалентности.

Доказательство.

1. Рефлексивность: всегда можно построить автоморфизм, переводящий векторы "1 к 1".

2. Симметричность: очевидно, т.к. изоморфизм – биекция.
3. Транзитивность: пусть V_1, V_2, V_3 – конечномерные ЛП/K, $V_1 \cong V_2$, $V_2 \cong V_3 \Rightarrow \dim V_1 = \dim V_2 = \dim V_3 \Rightarrow \dim V_1 = \dim V_3 \Rightarrow V_1 \cong V_3$.

■

64 Свойства матриц перехода между базисами

Определение. Пусть $e_1, e_2, \ldots, e_n$ (E) — базис V.

$v \in V$, тогда по определению базиса $v = \alpha_1 e_1 + \cdots + \alpha_n e_n$. Тогда $\alpha_1, \alpha_2, \ldots, \alpha_n$ — координаты v в базисе E.

$$[v]_E = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^n$$

Определение. $E' = (e'_1, e'_2, \ldots, e'_n)$, $[v]_{E'}$ — другой базис, другие координаты вектора v в нём.

$e'_j = c_{1j}e_1 + \cdots + c_{nj}e_n,\ j = 1, \ldots, n$

$$C = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{pmatrix}$$

$[e'_j]_E$ — j-ый столбец матрицы C.

Заметим, что $E' = E \cdot C$.

Пояснение: *Вообще мы говорили только об умножении матриц над одним кольцом, но чисто формально можно забить сейчас, так как умеем умножать скаляр на вектор.*

Тогда C — матрица перехода от базиса E к E'. Второе обозначение — $M_{E \to E'}$.

Предложение. *Пусть* $C_1 = M_{E \to E'}$, $C_2 = M_{E' \to E''} \Longrightarrow M_{E \to E''} = C_1 \cdot C_2$

Доказательство. $E' = E \cdot C_1,\ E'' = E' \cdot C_2$

$E'' = (E \cdot C_1) \cdot C_2 = E \cdot (C_1 \cdot C_2),\ E'' = E \cdot M_{E \to E''}$

E — базис $\Longrightarrow M_{E \to E''} = C_1 \cdot C_2$. ■

Следствие: $M_{E' \to E} = M^{-1}_{E \to E'}$; в частности, $M_{E \to E'} \in GL(n, k)$.

Доказательство. $M_{E \to E'} \cdot M_{E' \to E} = M_{E \to E} = E_n$

$M_{E' \to E} \cdot M_{E \to E'} = M_{E' \to E'} = E_n$ ■

65 Изменение координат вектора при замене базиса

Определение. Пусть $e_1, e_2, \ldots, e_n$ (E) — базис V.

$v \in V$, тогда по определению базиса $v = \alpha_1 e_1 + \cdots + \alpha_n e_n$. Тогда $\alpha_1, \alpha_2, \ldots, \alpha_n$ — координаты v в базисе E.

$$[v]_E = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \in K^n$$

Определение. $E' = (e'_1, e'_2, \ldots, e'_n)$, $[v]_{E'}$ — другой базис, другие координаты вектора v в нём.

$e'_j = c_{1j}e_1 + \cdots + c_{nj}e_n,\ j = 1, \ldots, n$

$$C = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{pmatrix}$$

$[e'_j]_E$ — j-ый столбец матрицы C.

Заметим, что $E' = E \cdot C$.

Пояснение: *Вообще мы говорили только об умножении матриц над одним кольцом, но чисто формально можно забить сейчас, так как умеем умножать скаляр на вектор.*

Тогда C — матрица перехода от базиса E к E'. Второе обозначение — $M_{E \to E'}$.

Предложение. *Пусть* $X = [v]_E$, $X' = [v]_{E'}$

Тогда $X = M_{E \to E'} \cdot X'$.

Доказательство. $v = E \cdot X = E' \cdot X'$ и $E' = E \cdot M_{E \to E'}$.

$E \cdot X = (E \cdot M_{E \to E'}) \cdot X' = E \cdot (M_{E \to E'} \cdot X')$

E — базис $\Longrightarrow X = M_{E \to E'} \cdot X'$.

■

66 Ранг набора векторов. Столбцовый и строчный ранг матрицы

Определение. Ранг набора векторов $v_1, v_2, \ldots, v_m \in V$:

$\mathrm{rk}(v_1, \ldots, v_m) := \dim \mathrm{Lin}(v_1, \ldots, v_m)$ (есть обозначение $rank$, rg)

Предложение. $\mathrm{rk}(v_1, \ldots, v_m)$ *равен максимальному числу линейно независимых (ЛН) векторов среди* $v_1, \ldots, v_m$.

Доказательство. Пусть $r = \mathrm{rk}(v_1, \ldots, v_m)$. Нужно доказать: среди $v_1, \ldots, v_m$

1. можно выбрать r ЛН векторов:

   $W = \mathrm{Lin}(v_1, \ldots, v_m)$. Среди $v_1, \ldots, v_m$ можно выбрать базис (т.к. это порождающая система) – это r ЛН векторов.

2. нельзя выбрать больше r ЛН векторов:

   В W нет ЛНС из более, чем r, векторов.

■

Определение. $A \in M(m, n, K)$

Столбцовый ранг A — ранг совокупности её столбцов.

Строчный ранг A — ранг совокупности её строк.

Замечание Столбцовый ранг A = строчному рангу A^T. Строчный ранг A = столбцовому рангу A^T.

67 Равенство столбцового и строчного ранга

Предложение. *Столбцовый и строчный ранги A не изменяются при элем. преоб. строк и столбцов. (докажем про оба ранга только для строк; для столбцов транспонируем матрицу)*

Доказательство. Пусть $A[1,], \ldots, A[m,]$ — строки A.
$A' = T_{ij}(\lambda) \cdot A$
$A'[i,] = A[i,] + \lambda A[j,]$
$A'[k,] = A[k,]$, $k \neq i$

$\mathrm{Lin}(A'[1,], \ldots, A'[m,]) = \mathrm{Lin}(A[1,], \ldots, A[m,])$ — верно и для элем. преобр. 2 и 3 типов

$\Longrightarrow \mathrm{rk}(A'[1,], \ldots, A'[m,]) = \mathrm{rk}(A[1,], \ldots, A[m,])$.

Для доказательства про столбцлвый ранг докажем лемму:

Лемма 5. *Пусть $A' = UA$, $U \in GL(m, K)$; $A[, i_1], \ldots, A[, i_l]$ — ЛЗС $\Longrightarrow$ $A'[, i_1], \ldots, A'[, i_l]$ — ЛЗС*

Доказательство. $i_1 < \cdots < i_l$

$\alpha_1 A[, i_1] + \cdots + \alpha_l A[, i_l] = 0$, $\exists s : \alpha_s \neq 0$

$$A \cdot \begin{pmatrix} 0 \\ i_1 : \alpha_1 \\ \vdots \\ 0 \\ \vdots \\ i_l : \alpha_l \\ 0 \end{pmatrix} = \sum_{k=1}^{l} \alpha_k A[, i_k] = 0$$

$\Longrightarrow UA \cdot \begin{pmatrix} \\ \vdots \\ \\ \end{pmatrix} = 0$

$\Longrightarrow \sum_{k=1}^{l} \alpha_k A'[, i_k] = 0$

■

Пусть r — столбцовый ранг A.

В A есть r ЛН столбцов $A[, i_1]$, …, $A[, i_r] \Longrightarrow A'[, i_1]$, …, $A'[, i_r]$ — ЛНС (если ЛЗС, то т.к. $A = UA'$, по лемме $A[, i_1]$, …, $A[, i_r]$ — ЛЗС)

Любые $r+1$ столбцов A — ЛЗС $\Longrightarrow$ любые $r+1$ столбцов A' — ЛЗС.

Т.е. столбцовый ранг A' равен r для любой $A' = UA$.

■

Следствие:Строчный ранг матрицы равен столбцовому рангу.

Доказательство. У $D = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$

Первые r строк/столбцов ЛН, любые $r+1$ строка/столбец ЛЗ (есть 0) $\Longrightarrow$ для D оба ранга равны r.

$A \rightsquigarrow D$ с помощью элем. преобр., которые по предложению не меняют оба ранга.

■

$\operatorname{rk} A =$ столбцовому рангу $=$ строчному рангу

68 Ранг произведения матриц. Связь ранга с PDQ-разложением

Предложение.

1. $\operatorname{rk} A^T = \operatorname{rk} A$ *(очевидно из доказанного выше)*
2. $\operatorname{rk} AB \le \min\{\operatorname{rk} A, \operatorname{rk} B\}$

Доказательство. Докажем, что утверждение $\Longleftrightarrow \begin{cases} \operatorname{rk} AB \le \operatorname{rk} A \\ \operatorname{rk} AB \le \operatorname{rk} B \end{cases}$

$(AB)[, j] = \sum_i B[i, j] \cdot \operatorname{rk} A[, i] \ \in \operatorname{Lin}(A[, 1],\ A[, 2],\ \dots)$

$\operatorname{Lin}((AB)[, 1],\ (AB)[, 2],\ \dots) \subset \operatorname{Lin}(A[, 1],\ A[, 2],\ \dots) \Longrightarrow \operatorname{rk} AB \le \operatorname{rk} A$

$\operatorname{rk} AB = \operatorname{rk}(AB)^T = \operatorname{rk}(B^T A^T) \le \operatorname{rk} B^T = \operatorname{rk} B$

■

Следствие:Пусть $A \in M(m, n, K)$, $U \in GL(m, K)$, $V \in GL(n, K)$. Тогда $\operatorname{rk} UA = \operatorname{rk} AV = \operatorname{rk} A$.

Доказательство. $\operatorname{rk} UA \le \operatorname{rk} A$

$\operatorname{rk} A = \operatorname{rk}(U^{-1}UA) \le \operatorname{rk} UA \Longrightarrow \operatorname{rk} UA = \operatorname{rk} A$

Аналогично, $\operatorname{rk} AV = \operatorname{rk} A$.

■

Следствие: $A \in M(m,n,K)$. Равносильны утверждения:

1. $\operatorname{rk} A = r$
2. $A = PDQ$, $P \in GL(m,K)$, $Q \in GL(n,K)$, $D = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$

Доказательство.

$2 \Rightarrow 1$: $\operatorname{rk} D = r \Longrightarrow \operatorname{rk} PDQ = r$

$1 \Rightarrow 2$: $A = PDQ$, $P \in GL(m,K)$, $Q \in GL(n,K)$, $D = \begin{pmatrix} E_l & 0 \\ 0 & 0 \end{pmatrix}$

$\operatorname{rk} PDQ = l \Longrightarrow r = l$

■

69 Условия эквивалентные обратимости матрицы

Предложение. *$A \in M(n,K)$. Тогда след. утверждения эквивалентны:*

1. *$A \in GL(n,K)$*
2. *$|A| \neq 0$ (вырожденная)*
3. *A обратима слева*
4. *A обратима справа*
5. *$\operatorname{rk} A = n$*
6. *Столбцы A — ЛНС*
7. *Строки A — ЛНС*

Доказательство.

$1 \Leftrightarrow 2$: очевидно

$5 \Leftrightarrow 6$: тривиально

$5 \Leftrightarrow 7$: тривиально

$1 \Rightarrow 3$: тривиально

$1 \Rightarrow 4$: тривиально

$3 \Rightarrow 5$: $BA = E_n$

$\operatorname{rk} BA \leq \operatorname{rk} A$, $\operatorname{rk} BA = \operatorname{rk} E_n = n \Longrightarrow \operatorname{rk} A = n$

$4 \Rightarrow 5$: аналогично

$5 \Rightarrow 1:$ $A = PDQ$, тогда по утверждению выше $\operatorname{rk} D = n \Longrightarrow D = E_n$

$A = PQ \in GL(n, K)$

■

70 Минорный ранг

Определение. Подматрица B матрицы A — матрица, полученная из A путем вычеркивания некоторых строк и некоторых столбцов.

Определение. Минор матрицы A порядка r — определитель какой-либо квадратной подматрицы A порядка r.

Предложение. *Пусть* $\operatorname{rk} A = r$. *Тогда в* A *есть ненулевой минор порядка* r *и нет ненулевого минора порядка больше* r.

Доказательство. В A есть r ЛН столбцов. A' — подматрица из этих столбцов.

$\operatorname{rk} A' = r \Longrightarrow$ в A' есть r ЛН строк. A'' — подматрица из этих строк.

$A'' \in M(r, K)$

$\operatorname{rk} A'' = r \Longrightarrow |A''| \neq 0 \Longrightarrow$ существует ненулевой минор порядка r.

Пусть $s > r$, B — подматрица A $s \times s$, т.ч. $|B| \neq 0$

Пусть C — подматрица A $m \times s$, т.ч. B — подматрица C.

Столбцы B ЛН $\Longrightarrow$ столбцы C ЛН (очевидно) $\Longrightarrow$ в A есть s ЛН столбцов $\Longrightarrow \operatorname{rk} A \geq s > r$ — противоречие.

■

71 Системы линейных уравнений. Классификация. Метод Гаусса

Определение. Система m линейных уравнений с n неизвестными имеет вид:

$$(*) \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \vdots + \cdots + \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

где $a_{ij}, b_i \in K \quad (i = 1, \ldots, m;\ j = 1, \ldots, n)$

$A = (a_{ij})$ — матрица СЛУ $(*)$

$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ — столбец правых частей СЛУ $(*)$

$(A|b) \in M(m, n+1, K)$ — расширеная матрица СЛУ $(*)$

Определение. $X = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$ — является решением $(*)$, если при подстановке $x_1 := \xi_1, \ldots, x_n := \xi_n$, мы получаем m верных равенств.

То есть если $AX = b$

Предложение. $(A|b) \to (A'|b')$ *с помощью ЭП строк* $\Longrightarrow$ *системы с расширенными матрицами* $(A|b)$ *и* $(A'|b')$ *эквивалентны.*

Доказательство.

$$(A'|b') = U \cdot (A|b), \quad U \in GL(m, K)$$
$$AX = b \Longleftrightarrow UAX = Ub \Longleftrightarrow A'X = b'$$

■

Классификация СЛУ

Определение. Если $b = 0$, то СЛУ $(*)$ однородная, иначе неоднородная.

Определение. СЛУ $(*)$ называется совместной, если $\{X|AX = b\} \neq \varnothing$, иначе — система несовместная.

Определение. Совместная система называется определённой, если её решение единственно, иначе — система неопределённая.

Замечание Однородная система — совместная. $(A \cdot 0 = 0)$

Метод Гаусса

Этапы:

I: $(A|b) \overset{\text{ЭП строк}}{\longrightarrow} \underbrace{(A'|b')}_{\text{ступенчатая}}$

II:

$$\begin{pmatrix} 0 & \ldots & 0 & a_{1j} & \ldots & | & \ldots \\ 0 & \ldots & 0 & a_{2j} & \ldots & | & \ldots \\ \vdots & \ldots & \vdots & \vdots & \ldots & | & \ldots \\ 0 & \ldots & 0 & \ldots & | & \ldots \text{ r-ая} & \\ 0 & \ldots & 0 & 0 & \ldots & | & 0 \\ \vdots & \ldots & \vdots & \vdots & \ldots & | & \ldots \\ 0 & \ldots & 0 & 0 & \ldots & | & 0 \end{pmatrix}$$

a_{rj_r} — ведущий элемент последней ненулевой строки

(a) $j_r = n+1$
$0 \cdot x_1 + \dots + 0 \cdot x_n = a_{rj_r} \neq 0 \Longrightarrow (*)$ несовместная.

(b) $j_r \leqslant n$
$x_{j1}, \dots, x_{jr}$ — главные неизвестные.
Остальные — свободные неизвестные.
$x_s := \xi_s \in K, \quad s \notin \{j_1, \dots, j_r\}$
$x_{j_r} = a^{-1}_{rj_r}(b_r - a_{rj_r+1}x_{r+1} - \dots - a_{rn}x_n)$
$x_{j_{r-1}} = a^{-1}_{(r-1)j_{r-1}}(b_{r-1} - a_{(r-1)j_{r-1}+1}x_{j_{r-1}+1} - \dots - a_{r-1}x_?$
$\dots$
$x_1 = \dots$
Решение уравнения зависит от $n-r$ параметров.

Получили $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = F(\xi_1, \dots, \xi_{n-r})$

В частности: если $(*)$ совместная, то она определённая $\Longleftrightarrow \operatorname{rk}(A|b) = n$

блять что вообще происходит..., кто просил его писать на графическом планшете?

72 Теорема Крамера

Предложение 6. *Крамера.*

Пусть $A \in M(n, K),\ b \in K^n$

Два утверждения эквиваленты:

1. *СЛУ с расширенной матрицей* $(A|b)$ *совместная определённая*
2. $|A| \neq 0$

Доказательство.

$2 \Longrightarrow AX = b \Longleftrightarrow A^{-1}AX = A^{-1}b \Longleftrightarrow X = A^{-1}b$

$1 \Longrightarrow 2$

От противного: $|A| = 0 \Longrightarrow \operatorname{rk} A < n$

Но у совместной определённой системы $\operatorname{rk} A = n$ (противоречие)

■

Формулы Крамера.

$A^{-1} = \frac{1}{|A|} \cdot \widetilde{A}$

$\widetilde{A} = (A_{ji}), \quad \widetilde{A}[i,j] = A_{ji}$

$x_i = b_1 A^{-1}[i,1] + \dots + b_n A^{-1}[i,n] =$

$= \frac{1}{|A|} \underbrace{(b_1 A_{1i} + \cdots + b_n A_{ni})}_{\Delta_i}$

$$\Delta_i = \begin{vmatrix} & & \text{i столб} & & \\ a_{11} & \dots & b_1 & \dots & a_{1n} \\ \vdots & \dots & \vdots & \dots & \vdots \\ a_{n1} & \dots & b_n & \dots & a_{nn} \end{vmatrix}$$

$\Delta_i = |A\{A_i \rightsquigarrow b\}|$ (определитель матрицы A, у которой мы заменили i-ый столбец на столбец b)

$x_i = \frac{\Delta_i}{|A|}$ — формулы Крамера.

Предложение. *Множество решений однородной системы с n неизвестными — линейное подпространство в K^n.*

Доказательство. Пусть x_1, x_2 — решения, $\alpha_1, \alpha_2 \in K$

Тогда $A(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 \underbrace{Ax_1}_{=0} + \alpha_2 \underbrace{Ax_2}_{=0} = 0$ ■

73 Теорема Кронекера-Капелли. Критерий определённости совместной системы

Предложение 7. *Кронекера-Капелли.*

Система с расширеной матрицей $(A|b)$ совместна $\iff \operatorname{rk}(A|b) = \operatorname{rk} A$

Доказательство. $\operatorname{rk} A = \dim \underbrace{\operatorname{Lin}(A_1, \dots, A_n)}_{\text{w}}, \quad A_i = A[\ , i]$

$$\operatorname{rk}(A|b) = \dim \underbrace{\operatorname{Lin}(A_1, \dots, A_n, b)}_{\text{v}}$$

$$\dim w = \dim v \iff w = v \iff b \in w \iff \exists \alpha_1, \dots, \alpha_n \in K : \alpha_1 A_1 + \cdots + \alpha_n A_n = b$$

$$\iff \exists \alpha_1, \dots, \alpha_n \in K : A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = b \iff \text{СДУ с расширенной матрицей } (A|b) \text{ совместная}$$

■

Замечание Дополнение к т. К-К: совместная система является определённой $\iff \operatorname{rk} A = n$

В частности если в совместной системе $m < n$, то система неопределённая.

74 Линейные отображения. Примеры. Ядро и образ

Определение. V, W — линейные пространства над полем K.

Отображение $\mathcal{A} : V \to W$ называется линейным, если

$$\forall v_1, v_2 \in V,\ \forall \alpha_1, \alpha_2 \in K :$$
$$\mathcal{A}(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 \mathcal{A}(v_1) + \alpha_2 \mathcal{A}(v_2)$$

Замечание Вместо этого условия можно требовать

$$\begin{cases} \mathcal{A}(v_1 + v_2) = \mathcal{A}(v_1) + \mathcal{A}(v_2) \ \text{ (гомоморфизм групп)} \\ \mathcal{A}(\alpha v) = \alpha \mathcal{A}(v) \end{cases}$$

$\mathrm{Hom}(V, W) := \{\mathcal{A} \mid \mathcal{A} : V \to W\}$ — множество линейных отображений из V в W.

Примеры:

1. $V = W = K[x]$
   $\mathcal{A} : f \mapsto f'$
2. $\mathrm{id}_V : V \mapsto V$ (изоморфизм на себя)
3. $\lambda \in K$
   $[\lambda] : V \to V$
   $v \mapsto \lambda v$ — гомотетия;
   $\mathrm{id}_V = [1]$ — тождественное отображение является частным случаем.
4. $0 : V \to W$
   $v \mapsto 0$
5. $A \in M(m, n, K)$
   $\mathcal{A} : K^n \to K^m$
   $C \mapsto AC$, где C — столбец

Предложение. $\mathcal{A} \in \mathrm{Hom}(U, V), \mathcal{B} \in \mathrm{Hom}(V, W)$

Тогда $\mathcal{B} \circ \mathcal{A} \in \mathrm{Hom}(U, W)$

Доказательство. Очевидно ■

Определение. Пусть $\mathcal{A} \in \mathrm{Hom}(V, W)$

$$\mathrm{Im}\,\mathcal{A} = \{\mathcal{A}(v) \mid v \in V\} \text{ — образ}$$
$$\mathrm{Ker}\,\mathcal{A} = \{v \mid \mathcal{A}(v) = 0\} \text{ — ядро}$$

Предложение.

1. $\mathrm{Im}\,\mathcal{A}$ — *подпространство* W
2. $\mathrm{Ker}\,\mathcal{A}$ — *подпространство* V

Доказательство.

1. $w_1, w_2 \in \mathrm{Im}\,\mathcal{A}$
   $\alpha_1 w_1 + \alpha_2 w_2 \overset{?}{\in} \mathrm{Im}\,\mathcal{A}$
   $w_1 = \mathcal{A}(v_1),\ w_2 = \mathcal{A}(v_2)$
   $\alpha_1 w_1 + \alpha_2 w_2 = \mathcal{A}(\alpha_1 v_1 + \alpha_2 v_2) \in \mathrm{Im}\,\mathcal{A}$

2. $v_1, v_2 \in \operatorname{Ker}\mathcal{A}$
$\mathcal{A}(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1\mathcal{A}(v_1) + \alpha_2\mathcal{A}(v_2) =$
$= \alpha_1 \cdot 0 + \alpha_2 \cdot 0 = 0$
$\Longrightarrow \alpha_1 v_1 + \alpha_2 v_2 \in \operatorname{Ker}\mathcal{A}$

■

75 Связь между размерностями ядра и образа

Предложение. *Пусть* $\dim V = n < +\infty$
$\mathcal{A} \in \operatorname{Hom}(V, W)$
Тогда $\operatorname{Im}\mathcal{A}$ *конечномерен и* $\dim\operatorname{Ker}\mathcal{A} + \dim\operatorname{Im}\mathcal{A} = n$

Доказательство. $\operatorname{Ker}\mathcal{A} \subset V$

$\Longrightarrow \operatorname{Ker}\mathcal{A}$ конечномерен.

$\underbrace{e_1, \ldots, e_m}_{\text{ЛНС в V}}$ — любой базис $\operatorname{Ker}\mathcal{A}$

Пусть $e_{m+1}, \ldots, e_n$ — дополнение до базиса V.

Докажем, что $\mathcal{A}(e_{m+1}), \ldots, \mathcal{A}(e_n)$ — базис $\operatorname{Im}\mathcal{A}$.

Доказательство.

$$w \in \operatorname{Im}\mathcal{A} \Longrightarrow w = \mathcal{A}(v), v \in V$$
$$v = \alpha_1 e_1 + \cdots + \alpha_n e_n$$
$$\mathcal{A}(v) = \underbrace{\alpha_1\mathcal{A}(e_1)}_{=0} + \cdots + \underbrace{\alpha_m\mathcal{A}(e_m)}_{=0} + \alpha_{m+1}\mathcal{A}(e_{m+1}) + \cdots + \alpha_n\mathcal{A}(e_n) =$$
$$= \alpha_{m+1}\mathcal{A}(e_{m+1}) + \cdots + \alpha_n\mathcal{A}(e_n) \in Lin(\mathcal{A}(e_{m+1}) + \cdots + \mathcal{A}(e_n))$$

Проверим их линейную независимость:

$$\beta_1\mathcal{A}(e_{m+1}) + \cdots + \beta_{n-m}\mathcal{A}(e_n) = 0$$
$$\mathcal{A}(\underbrace{\beta_1 e_{m+1} + \cdots + \beta_{n-m}e_n}_{\Rightarrow \in \operatorname{Ker}\mathcal{A}}) = 0$$
$$\beta_1 e_{m+1} + \cdots + \beta_{n-m}e_n = \alpha_1 e_1 + \cdots + \alpha_m e_m$$
$$e_1, \ldots, e_n \text{ — ЛНС} \Longrightarrow \text{все } \alpha_i \text{ и } \beta_i = 0$$
$$\text{Т.о. } \mathcal{A}(e_{m+1}), \ldots, \mathcal{A}(e_n) \text{ — базис } \operatorname{Im}\mathcal{A}$$
$$\dim\operatorname{Im}\mathcal{A} = n - m = \dim V - \dim\operatorname{Ker}\mathcal{A}$$

■

■