

Лекции по алгебре

Лектор: Всемиров Максим Александрович

Содержание

1	Отображения. Композиция отображений.	2
2	Обратимые отображения и их свойства	3
3	Тождественное отображение	4
4	Равносильность инъективности и обратимости слева	4
5	Равносильность сюръективности и обратимости справа	6
6	Инъективное отображение конечного множества на себя является биективным	6
7	Сюръективное отображение конечного множества на себя является биективным	7
8	Бинарные отношения	8
9	Отношение эквивалентности	8
10	Кратные корни	9
11	Число корней многочлена	10
12	Матрицы. Действия над матрицами.	12
13	Матричная конструкция поля комплексных чисел	14

1. Отображения. Композиция отображений.

Def: A, B — множества. $\Gamma_f \subset A \times B$

Γ — график отображения если выполнены два условия:

1. $\forall a \in A \exists b \in B (a, b) \in \Gamma_f$
2. $\forall a \in A \exists b_1, b_2 \in B (a, b_1) \in \Gamma_f \wedge (a, b_2) \in \Gamma_f \Rightarrow b_1 = b_2$

Def: $A, B, \Gamma_f \subset A \times B$

говорим, что задано отображение f из A в B с графиком Γ_f

$$f : A \rightarrow B$$

$$A \xrightarrow{f} B$$

$$(a, b) \in \Gamma_f \Leftrightarrow b = f(a)$$

A — область определения

B — область назначения

$$f : A \rightarrow B$$

$$f_1 : A_1 \rightarrow B_1$$

$$f = f_1 \Leftrightarrow A = A_1, B = B_1, \Gamma_f = \Gamma_{f_1}$$

Def: Композиция отображения

$$A \xrightarrow{f} B \xrightarrow{g} C$$

$$g \circ f : A \rightarrow C$$

$$(g \circ f)(a) = g(f(a))$$

$$\Gamma_{g \circ f}$$

$$(a, c) \in \Gamma_{g \circ f} \Leftrightarrow \exists b \in B (a, b) \in \Gamma_f \wedge (b, c) \in \Gamma_g$$

Область определения $g \circ f$ — область определения f $\text{Dom}(f)$

Область назначения $g \circ f$ — область назначения g $\text{coDom}(f)$

Теорема 1.1. Композиция отображения ассоциативна.

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

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

► Область определения $\text{Dom}(h \circ (g \circ f)) = \text{Dom}(g \circ f) = \text{Dom}(f) = A$

$\text{Dom}((h \circ g) \circ f) = \text{Dom}(f) = A$

Область назначений $\text{Dom}(h \circ (g \circ f)) = \text{coDom}(h) = D$

$$Dom((h \circ g) \circ f) = coDom((h \circ g)) = coDom(h) = D$$

$$\forall a \in A$$

$$(h \circ (g \circ f))(a) = h(g \circ f(a)) = h(g(f(a)))$$

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$



2. Обратимые отображения и их свойства

$$f : A \rightarrow B$$

$\mathfrak{D}\mathfrak{ef}$: f — обратное справа, если $\exists g : B \rightarrow A$

$$f \circ g = id_B$$

f — обратим слева, если $\exists g : B \rightarrow A$

$$g \circ f = id_A$$

f обратимо, если $\exists g : B \rightarrow A$

$$g \circ f = id_A, f \circ g = id_B$$

g — отображение, обратное к f . (обозначение f^{-1})

Теорема 2.1.

1. f обратимо $\Leftrightarrow f$ обратимо слева и справа.
2. f обратимо, то обратное отображение единственно.



1. f обратимо $\Rightarrow f$ обратимо слева и справа.

Если у f есть и левый и правый обратный, то они совпадают.

g — правый обратный к f , h — левый.

$$(h \circ f) \circ g = id_A \circ g = g$$

$$h \circ (f \circ g) = h \circ id_B = h$$

$$\Rightarrow g = h$$

2. Пусть f обратимое и g и h — два обратных. В частности g — обратное справа, h — обратное слева.



Теорема 2.2. $f : A \rightarrow B, g : B \rightarrow C$

$$g \circ f : A \rightarrow C$$

1. Если f, g обратимы справа, то и $g \circ f$ обратима справа.
2. Если f, g обратимы слева, то и $g \circ f$ обратима слева.
3. Если f, g обратимы, то $g \circ f$ обратима $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$



1.

$$\begin{aligned} u : B &\rightarrow A, f \circ u = id_B \\ v : C &\rightarrow B, g \circ v = id_C \\ (g \circ f) \circ (u \circ v) &= g \circ (f \circ (u \circ v)) = \\ &= g \circ ((f \circ u) \circ v) = g \circ (id_B \circ v) = g \circ v = id_C \end{aligned}$$

$u \circ v$ — правый обратный к $g \circ f$

2. аналогично

3.

$$(g \circ f)(f^{-1} \circ g^{-1}) = g \circ ((f \circ f^{-1}) \circ g^{-1}) = g \circ (id_B \circ g^{-1}) = g \circ g^{-1} = id_C$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1}(g^{-1} \circ g) \circ f = f^{-1} \circ id_B \circ f = f^{-1} \circ f = id_A$$

Следствие 2.2.1. Композиция сюръективных — сюръективна.

Композиция инъективных — инъективна.

Композиция биективных — биекция.

Теорема 2.3. $f : A \rightarrow B$ обратима, тогда f^{-1} обратима и $(f^{-1})^{-1} = f$

► $f \circ f^{-1} = id_B$

$f^{-1} \circ f = id_A \Rightarrow f$ — обратное к f^{-1}

В силу единственности обратного $(f^{-1})^{-1} = f$

3. Тожественное отображение

Def: $id_A : A \rightarrow A$

$\forall a \in A, id_A(a) = a$

id_A — тождественное отображение множества A .

$\Gamma_{id_A} = \text{диагональ } A \times A \{(a, a) | a \in A\}$

Теорема 3.1. $f : A \rightarrow B$

$f \circ id_A = f = id_B \circ f$



Области определения и назначения совпадают.

$\forall y \in B, id_B(y) = y$

$a \in A$

$(f \circ id_A)(a) = f(id_A(a)) = f(a)$

$a \in A$

$(id_B \circ f)(a) = id_B(f(a)) = f(a)$

4. Равносильность инъективности и обратимости слева

Def: A, B

$f : A \rightarrow B, \Gamma_f, f$ — инъективное отображение (инъекция).

$\forall a_1, a_2 \in A \exists b(a_1, b) \in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2$

$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

$f : A \rightarrow B$ — инъективное отображение.

Def: Отображение f называется сюръективным (сюръекцией «отображение на»)

$$\forall b \in B \exists a \in A (b = f(a))$$

$$f : A \twoheadrightarrow B$$

Def: f называется биективным (или биекцией) если f и сюръективно и инъективное.

$$f : A \rightarrow B$$

$$\{b \in B \mid \exists c \in C b = f(c)\} = f(C) \text{ — образ } C.$$

$$\{a \in A \mid f(a) \in D\} = f^{-1}(D) \text{ — полный прообраз } D.$$

$$f(f^{-1}(D)) \subset D \text{ — но не обязательно совпадает.}$$

f инъективно \Leftrightarrow прообраз любого одноэлементного множества содержит не более одного элемента.

$$f \text{ сюръективно } f(A) = B, f : A \rightarrow B$$

Теорема 4.1. $f : A \rightarrow B, g : B \rightarrow A$

$g \circ f = id_A$ тогда f — инъективно, g — сюръективно.



$$1. a_1, a_2 \in A f(a_1) = f(a_2)$$

$$a_1 = a_2$$

$$g(f(a_1)) = g(f(a_2))$$

\uparrow

$$(g \circ f)(a_1) = (g \circ f)(a_2)$$

\uparrow

$$id_A(a_1) = id_A(a_2)$$

\uparrow

$$a_1 = a_2 \Rightarrow f \text{ — инъективна.}$$

$$2. a \in A$$

$$g(f(a)) = (g \circ f)(a) = id_A(a) = a$$

$$b = f(a)$$

$$a = g(b)$$

$$\forall a \in A \exists b \in B a = g(b) \Rightarrow g \text{ — сюръективно.}$$

Теорема 4.2. $f : A \rightarrow B (A \neq \emptyset)$

f обратимо слева $\Leftrightarrow f$ — инъективна.



$$\exists g g \circ f = id_A \Rightarrow f \text{ — инъективно.}$$

\Leftarrow

$$C = f(A)$$

$$h_1 : C \rightarrow A$$

$$(c, a) \in \Gamma_{h_1} \Leftrightarrow (a, c) \in \Gamma_f$$

Почему Γ_{h_1} — график?

$$\forall c \in C \exists a \in A (a, c) \in \Gamma_f$$

$$\forall c \in C \exists a \in A (c, a) \in \Gamma_{h_1}$$

f — инъективно.

$$\forall a_1, a_2 \in A \exists b \in B (a_1, b) \in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2$$

$$\forall a_1, a_2 \in A \exists b \in C (a_1, b) \in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2$$

$$\forall a_1, a_2 \in A \exists b \in C (b, a_1) \in \Gamma_{h_1} \wedge (b, a_2) \in \Gamma_{h_1} \Rightarrow a_1 = a_2$$

$\Rightarrow \Gamma_{h_1}$ — график.

$h : B \rightarrow A$

возьмем какой-то $a \in A$

$$h(b) = \begin{cases} h_1(b), & h_1(b), b \in C \\ a, & b \notin C \end{cases}$$

$x \in A$

$$(h \circ f)(x) = h(f(x)) = h_1(f(x)) = x$$



5. Равносильность сюръективности и обратимости справа

Аксиома выбора

$B \neq \emptyset, b \in B$

$\exists \Phi : B \rightarrow \cup_{b \in B} X_b$

$\forall b \in B \Phi(b) \in X_b$

Теорема 5.1.

f — обратимо справа $\Leftrightarrow f$ — сюръективно.

► \Rightarrow

\Leftarrow

$f : A \rightarrow B$

$\forall b \in B f^{-1}(\{b\}) \neq \emptyset$

$g : B \rightarrow \cup_{b \in B} X_b$

$g(b) \in X_b = f^{-1}(\{b\}), f(g(b)) = b$

$f^{-1}(\{b\}) = X_b \subset A \Rightarrow \cup_B X_b \subset A$

$a \in A$

$a \in X_{f(a)}$

$g : B \rightarrow A$

$\forall b \in B f(g(b)) = b$

$\forall b \in B (f \circ g)(b) = b$

$f \circ g = id_B$

f — обратимо справа.

Следствие 5.1.1.

f — обратимо $\Leftrightarrow f$ — биективно.



6. Инъективное отображение конечного множества на себя является биективным

Теорема 6.1. A — конечное множество.

$f : A \rightarrow A$, тогда f — биекция.

► f — сюръекция?

$a_0 = a$

$a_{i+1} = f(a_i)$

$\exists m \neq n a_m = a_n m > n$

Лемма 6.1. $a_{m-n} = a$

► Индукция по n . **База:** $n = 0, a_m = a_0 = a$ **Переход** $n \geq 1$

$$f(a_{m-1}) = a_m = a_n = f(a_{n-1})$$

Так как инъекция $a_{m-1} \leq a_{n-1}$

$$a_{m-n} = a_{(m-1)-(n-1)} = a$$

$$a_{m-n} = a$$

$$m - n \geq 1$$

$$a = a_{m-n} = f(a_{m-n-1})$$

а есть образ $a_{m-n-1} \Rightarrow f$ — сюръекция. ◀

7. Сюръективное отображение конечного множества на себя является биективным

Теорема 7.1. A — конечное множество. $f : A \rightarrow A$, тогда f — биекция.



$$1. \forall a \exists n_a \{f \circ f \circ \dots \circ f\}(a) = a$$

$$2. \exists n \forall a (f \circ \dots \circ f)(a) = a$$

3. f — инъекция.

$$a_0 = a$$

$$a_i f^{-1}(\{a_i\}) \neq \emptyset$$

$$\exists a_{i+1} \in f^{-1}(\{a_i\})$$

$$\exists m > n a_m = a_n$$

Лемма 7.1. $a_{m-n} = a$

► Индукция по n . **База:** $n = 0, a_m = a_0 = a$ **Переход:**

$$a_m = a_n$$

$$f(a_m) = f(a_n)$$

$$a_{m-1} = f(a_m) = f(a_n) = a_{n-1}$$

По индукционному предположению

$$a_{m-n} = a_{(m-1)-(n-1)} = a$$

$$a_{m-n} \in f^{-1}(f^{-1} \dots (\{a\}))$$

$$f(f(\dots f(a_{m-n}))) = a$$

$$f(f(\dots f(a))) = a$$

$$(f \circ f \circ \dots)(a) = a$$

$$\forall a \in A \exists n_a \geq 1 \underbrace{(f \circ \dots \circ f)}_{n_a}(a) = a$$

$$k \in \mathbb{N} \underbrace{(f \circ \dots \circ f)}_{n_a k}(a) = a$$

(индукция по k)

$$N = \prod_{a \in A} n_a \underbrace{(f \circ \dots \circ f)}_N(a) = a$$

$$a, b \in A$$

$$f(a) = f(b)$$

$$a = \underbrace{(f \circ \dots \circ f \circ f)}_{N-1}(a) = \underbrace{(f \circ \dots \circ f \circ f)}_{N-1}(b) = b$$



8. Бинарные отношения

Def: На A задано бинарное отношение R , если задано $R \subset A$

$(a, b) \in R$

a и b находятся в отношении с R

aRb

$R = \emptyset$ пустое

$R = A^2$ полное.

Def: $A, R \subset A^2$

1. R рефлексивно, если $\forall a \in A, aRa(a, a) \in R$
2. R антирефлексивно, если $\forall a \in A \neg(aRa)$
3. R симметрично, если $\forall a, b \in A aRb \Rightarrow bRa$
4. R асимметрично, если $\forall a, b \in A aRb \Rightarrow \neg(bRa)$
5. R антисимметрично, если $\forall a, b \in A (aRb \wedge bRa) \Rightarrow a = b$
6. R транзитивно, если $\forall a, b, c \in A (aRb \wedge bRc) \Rightarrow aRc$

Def: R называется отношением нестрогого частичного порядка, если оно рефлексивно, транзитивно и антисимметрично.

Def: R называется отношением строгого частичного порядка, если оно антирефлексивно, транзитивно и асимметрично.

Если на A задано отношение частичного порядка, то A — частично упорядоченное множество.

9. Отношение эквивалентности

Def: R отношение эквивалентности, если оно рефлексивное, симметричное и транзитивное $a \sim b$.

A, R — отношение эквивалентности. $a \in A[a] = \{b \in A | a \sim b\}$ — класс эквивалентности.

Теорема 9.1. $A, \sim a, b \in A$

Тогда либо $[a] \cap [b] = \emptyset$, либо $[a] = [b]$



1. $[a] \cap [b] = \emptyset$ — все доказано.

$$2. \exists c \in [a] \cap [b]$$

$$[a] = [b]?$$

$$x \in [a], a \sim x$$

$$c \in [a], a \sim c \Rightarrow c \sim a$$

$$c \in [b], b \sim c$$

$$b \sim c, c \sim a, a \sim x$$

$$b \sim a, a \sim x$$

$$b \sim x \Rightarrow x \sim [b]$$

$$[a] \subset [b]$$

$$[b] \subset [a]$$

Множество классов эквивалентности называется фактормножеством. 

10. Кратные корни

A — поле. $f \in A[x], f \neq 0$ c — корень f в $A \Leftrightarrow (x - c) | f$ в $A[x]$ (теорема Безу)

Def: Если для некоторого $k \geq 2$, $(x - c)^k | f$, но $(x - c)^{k+1} \nmid f$, то говорим, что c — корень f кратности k .

c — корень f кратности k , если $f(x) = (x - c)^k g(x), (x - c) \nmid g(x) \Leftrightarrow f(x) = (x - c)^k g(x), g(c) \neq 0$

Теорема 10.1. A — поле, $\text{char } A = 0, f \in A[x], f \neq 0$

c — корень f кратности $k \geq 1 \Leftrightarrow$

1. c — корень f .

2. c — корень f' кратности $k - 1$.



\Rightarrow

$$f = (x - c)^k g(x), g(c) \neq 0 \Rightarrow c \text{ — корень}$$

$$f' = k(x - c)^{k-1} g(x) + (x - c)^k g' = (x - c)^{k-1} (kg + (x - c)g')$$

$$\Rightarrow (x - c)^{k-1} | f'$$

c — не корень $kg + (x - c)g'$

$$kg(c) + (x - c)g'(c) = kg(c) \neq 0$$

\Leftarrow

c — корень $f \Rightarrow$ корень f кратности l , по доказанному c — корень f' кратности $l - 1$.

$$l - 1 = k - 1$$

$$l = k$$



РЕМ: Предположение $\text{char } A = 0$ существенно.

$$\mathbb{F}_2, f = x^7 + x^2$$

0 — корень кратности 2.

$$f' = x^6$$

0 — кратности 6.

Следствие 10.1.1. A — поле характеристики 0. $0 \neq f \in A[x]$, c — корень f кратности $\geq k \Leftrightarrow$ выполняется равенство

$$0 = f(c) = f'(c) = \dots = f^{(k-1)}(c)$$

$$f^{(k)} = (f^{(k-1)})'$$

$$(fg)^{(n)} = \sum_{r=0}^n C_n^r f^{(r)} g^{(n-r)}$$

11. Число корней многочлена

Лемма 11.1. A — область целостности. $0 \neq f, g \in A[x]$

c — корень f кратности k , корень g кратности $l \Rightarrow$

c — корень fg кратности $k + l$



$$f = (x - c)^k f_1, f_1(c) \neq 0$$

$$g = (x - c)^l g_1, g_1(c) \neq 0$$

$$fg = (x - c)^{k+l} f_1 g_1$$

$$f_1(c) g_1(c) \neq 0$$

$\Rightarrow c$ — корень fg кратности $k + l$.

Лемма 11.2. A — область целостности. Какие бы ни были $c \neq d \in A$, $0 \neq f, g \in A[x]$, $a, k \in \mathbb{N}$, такие, что $f = (x - c)^k g, g(c) \neq 0$, то $(x - d)^a | f \Leftrightarrow (x - d)^a | g$



$$(x - d)^a | g \Rightarrow (x - d)^a | f$$

\Rightarrow Индукция по a . База:

$$a = 1$$

$$x - d | f \Rightarrow f(d) = 0$$

$$(c - d)^k g(d) = 0 \Rightarrow g(d) = 0$$

$$\Rightarrow (x - d) | g$$

Переход $a - 1 \rightarrow a$ $a - 1$ для всех f и g удовлетворяет условию леммы

$$f = (x - c)^k g$$

$$(x - d)^a | f \Rightarrow (x - d)^{a-1} | f$$

$(x - d)^{a-1} | d$ по индукционному предположению.

$$f = (x - d)^a f_1$$

$$g = (x - d)^{a-1} g_1$$

$$(x - d)^a f_1 = (x - c)^k (x - d)^{a-1} g_1$$

$$(x-d)f_1 = (x-c)^k g_1$$

$$\Rightarrow x-d | g_1$$

(по доказанному при $a = 1$)

$$(x-d)^a | g$$

Теорема 11.1. A — область целостности. $0 \neq f \in A[x] \Rightarrow$ число корней f с учетом кратности не превосходит $\deg f$

► Индукция по $\deg f$

1. **База:** $\deg f = 0, f = \text{const} \neq 0$ нет корней.
2. **Переход:** f с — корень f кратности k . $f = (x-c)^k g, g(c) \neq 0$ с — не корень g .
Все корни g — это в точности все корни f (кроме c), причем кратность сохраняется.
Число корней g (с учетом кратности) $\leq \deg g$
число корней $f = k + \text{число корней } g \leq k + \deg g = \deg f$

REM: Предположение, что A — область целостности существенно.

Def:

$$A, f \in A[x]$$

$$\tilde{f} : A \rightarrow A$$

$$c \rightarrow f(c)$$

$$f, g \tilde{f} = \tilde{g}$$

Примеры:

$$A = \mathbb{F}_2$$

$$f = 0, g = x^2 + x$$

$$\tilde{f} : 0 \rightarrow 0, 1 \rightarrow 0$$

$$\tilde{g} : 0 \rightarrow 0, 1 \rightarrow 0$$

Следствие 11.1.1. A — область целостности.

$$f, g \in A[x], |A| > \max(\deg f, \deg g)$$

Тогда, если $\tilde{f} = \tilde{g}$, то $f = g$.

► $f - g$

$$f - g = \tilde{f} - \tilde{g} \text{ — тождественно не нулевое отображение}$$

$$\forall c \in A, f(c) - g(c) = 0$$

Число корней $f - g > \deg(f - g) \Rightarrow f - g = 0$

Следствие 11.1.2. Если A — область целостности.

$|A| = \infty$ и $\tilde{f} = \tilde{g}$, то и $f = g$

12. Матрицы. Действия над матрицами.

Def: R — кольцо. Матрицей называется таблица элементов кольца

$$(a_{ij}) = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = \\ = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Def: Множество матриц заданного размера (m строк, n столбцов) на данном кольце R

$$M(m, n, R) = \left\{ (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \right\}$$

Def: Сложение матриц

$$+ : M(m, n, R) \times M(m, n, R) \rightarrow M(m, n, R)$$

$$(a_{ij}) + (b_{ij}) \mapsto (a_{ij} + b_{ij})$$

Лемма 12.1. $\langle M(m, n, R), + \rangle$ есть абелева группа.

Def: Транспонирование — переворот матрицы

$$^T : M(m, n, R) \rightarrow M(n, m, R)$$

$$(a_{ij})^T = (a_{ji})$$

Def: Умножение матриц

$$\times : M(m, n, R) \times M(n, k, R) \rightarrow M(m, k, R)$$

$$(a_{ij}) \times (b_{ij}) = (c_{ij})$$

$$c_{ij} = \sum_{l=1}^n a_{il} b_{lj}$$

Умножение можно запомнить как «строка на столбец».

Почему же умножение именно такое? Рассмотрим систему линейных преобразований

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ y_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots = \vdots + \vdots + \ddots + \vdots \\ y_n = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{cases}$$

Теперь её можно записать как

$$(a_{ij}) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

Также, если мы аналогично выразим

$$(b_{ij}) \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

то результирующее преобразование

$$(c_{ij}) \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

можно выразить как

$$(c_{ij}) = (a_{ij})(b_{ij})$$

Теорема 12.1. Свойства умножения матриц.

1. $A: n \times m, B: m \times k, C: k \times l$

$$A(BC) = (AB)C$$

2. $A, B: n \times m, C: m \times k$

$$(A + B)C = AC + BC$$

3. $A, B: n \times m, C: k \times n$

$$C(A + B) = CA + CB$$

4. $A: n \times m, B: m \times k, R$ коммутативное кольцо.

$$(AB)^T = B^T A^T$$

► Надо расписывать суммы

1. $BC \Leftrightarrow D: m \times l, AD \Leftrightarrow E: n \times l, AB \Leftrightarrow F: n \times k, FC \Leftrightarrow G: n \times l$. Таким образом, E и G совпадают размерами.

$$e_{ij} = \sum_{x=1}^m a_{ix} d_{xj} = \sum_{x=1}^m a_{ix} \left(\sum_{y=1}^k b_{xy} c_{yj} \right) = \sum_{x=1}^m \sum_{y=1}^k a_{ix} b_{xy} c_{yj}$$

$$g_{ij} = \sum_{y=1}^k f_{iy} c_{yj} = \sum_{y=1}^k \left(\sum_{x=1}^m a_{ix} b_{xy} \right) c_{yj} = \sum_{y=1}^k \sum_{x=1}^m a_{ix} b_{xy} c_{yj}$$

Таким образом $e_{ij} = g_{ij}$

- 2.

$$\begin{aligned} ((A + B)C)_{ij} &= \sum_{x=1}^m (A + B)_{ix} c_{xj} = \sum_{x=1}^m (a_{ix} + b_{ix}) c_{xj} = \sum_{x=1}^m (a_{ix} c_{xj} + b_{ix} c_{xj}) = \\ &= \sum_{x=1}^m a_{ix} c_{xj} + \sum_{x=1}^m b_{ix} c_{xj} = (AC)_{ij} + (BC)_{ij} = (AC + BC)_{ij} \end{aligned}$$

3. Аналогично

- 4.

$$((AB)^T)_{ij} = (AB)_{ji} = \sum_{x=1}^m a_{jx} b_{xi} = \sum_{x=1}^m b_{ix}^T a_{xj}^T = (B^T A^T)_{ij}$$

Заметим, что умножение не коммутативно. ◀

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

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

Def: Умножение на скаляр:

$$\times : R \times M(m, n, R) \rightarrow M(m, n, R)$$

$$\lambda(a_{ij}) = (\lambda a_{ij})$$

Теперь рассмотрим квадратные матрицы — матрицы, у которых количество строк и столбцов совпадают.

Теорема 12.2. Кольцо квадратных матриц. $M(n, n, R)$ — кольцо с единицей. Если $2 \mid n$, то в нём есть делители нуля.

Все необходимые свойства уже доказаны.

13. Матричная конструкция поля комплексных чисел

$$M(2, \mathbb{R})$$

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

Утверждение. \mathcal{C} — коммутативное кольцо с единицей.

► Операции замкнуты:

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & -b_1 - b_2 \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 & -a_1 b_2 - a_2 b_1 \\ a_2 b_1 + a_1 b_2 & -b_1 b_2 + a_1 a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 & -(a_1 b_2 + a_2 b_1) \\ a_1 b_2 + a_2 b_1 & a_1 a_2 - b_1 b_2 \end{pmatrix}$$

Как видно, операции коммутативны. Единица есть:

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

Таким образом, \mathcal{C} — коммутативное подкольцо с единицей. ◀

Утверждение.

$$\mathbb{C} \equiv \mathcal{C}$$

► Отображение очевидно:

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

Все операции переходят друг в друга, базовые операции (сложение, умножение на скаляр, перемножение) переходят в себя, сопряжение — в транспонирование. ◀