Лекции по алгебре
Лектор: Всемирнов Максим Александрович

Содержание

1. Отображения. Композиция отображений.

$\mathfrak{Def}$: 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. $\forall a \in A \exists b_1, b_2 \in B (a,b_1) \in \Gamma_f \wedge (a,b_2) \in \Gamma_f \Rightarrow b_1 = b_2$

$\mathfrak{Def}$: $A, B, \Gamma_f \subset A \times B$
говорим, что задано отображение f из A в B с графком Γ_f

$$f : A \to B$$

$$A \xrightarrow{f} B$$

$(a,b) \in \Gamma_f \Leftrightarrow b = f(a)$
A — область определения
B — область назначения

$$f : A \to B$$

$$f_1 : A_1 \to B_1$$

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

$\mathfrak{Def}$: Композиция отображения

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

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

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

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

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

Область определение $g \circ f$ — область определения f Dom(f)
Область назначения $g \circ f$ — область назначения g 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 $Dom(h \circ (g \circ f)) = Dom(g \circ f) = Dom(f) = A$
$Dom((h \circ g) \circ f) = Dom(f) = A$
Область назначений $Dom(h \circ (g \circ f)) = coDom(h) = D$

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

$$\forall a \in A$$

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

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

◀

2. Обратимые отображения и их свойства

$f : A \to B$
$\mathfrak{Def}$: f — обратное справа, если $\exists g : B \to A$
$f \circ g = id_B$
f — обратим слева, если $\exists g : B \to A$
$g \circ f = id_A$
f обратимо, если $\exists g : B \to A$

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

g — отображение, обратное к f.(обозначение f^{-1})
Теорема 2.1.

1. f обратимо $\Leftrightarrow$ f обратимо слава 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. $f : A \to B, g : B \to C$
$g \circ f : A \to C$

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.
$$u : B \to A, f \circ u = id_B$$
$$v : C \to Bg \circ v = id_C$$
$$(g \circ f) \circ (u \circ v) = g \circ (f \circ (u \circ v)) =$$
$$= g \circ ((f \circ u) \circ v) = g \circ (id_B \circ v) = g \circ v = id_C$$

$u \circ v$ — 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. $f : A \to B$ f — 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. Тождественное отображение

$\mathfrak{Def}$: $A, id_A : A \to A$
$\forall a \in A id_A(a) = a$
id_A — тождественное отображение множетсва A.
Γ_{id_A} = диагональ $A \times A\{(a, a)|a \in A\}$
Теорема 3.1. $f : A \to B$
$f \circ id_A = f = id_B \circ f$
▶
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

$\mathfrak{Def}$: A, B
$f : A \to B, \Gamma_f, f$ — инъективное отображение(инъекция).
$\forall a_1, a_2 \in A \exists b(a_1, b) \in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2$
$\forall a_1, a_2 \in A f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
$f : A \rightarrowtail B$ — инъективное отображение.

$\mathfrak{Def}$: Отображение f назывется сюръективным (сюрекцией «отображение на»)
$\forall b \in B \exists a \in A (b = f(a))$
$f : A \twoheadrightarrow B$
$\mathfrak{Def}$: f называется биективным(или биекцией) если f и сюръективно и инъективное.
$f : A \quad B$
$\{b \in B | \exists c \in C b = f(c)\} = f(C)$ — образ C.
$\{a \in A | f(a) \in D\} = f'(D)$ — полный прообраз D.
$f(f^{-1}(D)) \subset D$ — но не обязательно совпадет.
f инъективно $\Leftrightarrow$ прообраз любого одноэлементного множества содержит не более одного элемента.
f сюръективно $f(A) = B, f : A \to B$
Теорема 4.1. $f : A \to B, g : B \to A$
$g \circ f = id_A$ тогда f — инъективно, g — сюръективно.
▶

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

   $a_1 = a_2$

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

   $\Uparrow$

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

   $\Uparrow$

   $id_A(a_1) = id_A(a_2)$

   $\Uparrow$

   $a_1 = a_2 \Rightarrow f$ — инъективна.

2. $a \in A$

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

   $b = f(a)$

   $a = g(b)$

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

◀

Теорема 4.2. $f : A \to B (A \neq 0)$
f обратимо слева $\Leftrightarrow$ f — инъективна.
▶ $\Rightarrow$
$\exists g g \circ f = id_A \Rightarrow f$ — инъективно.
$\Leftarrow$
$C = f(A)$
$h_1 : C \to A$
$(c, a) \in \Gamma_{h_1} \Leftrightarrow (a, c) \in \Gamma_f$
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.
$h : B \to A$
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
$B 0 \neq X_b, b \in B$
$\exists \Phi : B \to \cup_{b \in B} X_b$
$\forall b \in B \Phi(b) \in X_b$
Теорема 5.1.
f — обратимо справа $\Leftrightarrow$ f — сюръективно.
▶ $\Rightarrow$
$\Leftarrow$
$f : A \to B$
$\forall b \in B f^{-1}(\{b\}) \neq 0 (X_b)$
$g : B \to \cup_{b \in B} X_b$
$g(b) \in X_b = f^{-1}(\{b\}), f(g(b)) = b$
$f^{-1}(\{b\}) = X_b \subset A \Rightarrow \cup_B X_b \subset A$
$a \in A$
$a \in X_{f(a)}$
$g : B \to A$
$\forall b \in B f(g(b)) = b$
$\forall b \in B (f \circ g)(b) = b$
$f \circ g = id_B$
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.
$f : A \rightarrowtail A$, 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. $f : A \twoheadrightarrow A$, тогда f — биекция.
▶

1. $\forall a \exists n_a \{f \circ f \circ ... \circ f\}(a) = a$
2. $\exists n \forall a (f \circ ... \circ f)(a) = a$
3. f — инъекция.

$$a_0 = a$$

$$a_i f^{-1}(\{a_i\}) \neq 0$$

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

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

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

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

◀

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

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

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

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

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

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

(индукция по k)

$$N = \prod_{a \in A} n_a \, \underbrace{(f \circ ... \circ f)}_{N}(a) = a$$

$$a, b \in A$$

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

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

◀

8. Бинарные отношения

$\mathfrak{Def}$: На A задано бинарное отношение R, если задано $R \subset A$
$(a, b) \in R$
a и b находятся в отношение с R
aRb
R $= 0$ пустое
$R = A^2$ полное.
$\mathfrak{Def}$: $A, R \subset A^2$

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 $\forall a, b, c \in A(aRb \wedge bRc) \Rightarrow aRc$

$\mathfrak{Def}$: R называется отношением несторого частичного порядка, если оно рефлексивно, транзетивно и антисимметрино.

$\mathfrak{Def}$: R называется отношением сторого частичного порядка, если оно антирефлексивно, транзетивно и асимметрино.

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

9. Отношение эквивалентности

$\mathfrak{Def}$: 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 $[a] \cap [b] = 0$, либо $[a] = [b]$
▶

1. $[a] \cap [b] = 0$ — 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)

$\mathfrak{Def}$: 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, $char A = 0, f \in A[x], f \neq 0$

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 доказаному c — корень f' кратности l - 1.

$$l - 1 = k - 1$$
$$l = k$$

◀

REM: Предположение $char A = 0$ 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

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

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

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

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 $(x-d)^a | f \Leftrightarrow (x-d)^a | g$
▶ $\Leftarrow$

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

$\Rightarrow$ 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 $a - 1 \to a$ $a - 1$ 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 индукционномупредположению.

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

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

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

$$(x-d)f_1 = (x-c)^k g_1$$
$$\Rightarrow x-d|g_1$$
(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 $degf$

▶ Индукция по $degf$

1. **База:** $degf = 0, f = const \neq 0$ нет корней.
2. **Переход:** f c — корень f кратности k. $f = (x-c)^k g, g(c) \neq 0$ c — не корень g.

   Все корни g — это в точности все корни f(кроме c), причем кратность сохраняется.

   Число корней g(с учетом кратности) $\leq degg$

   число корней $f = k+$число корней $g \leq k + degg = degf$

◀

REM: Предположение, что A — область целостности существенно.
$\mathfrak{Def}$:
$$A, f \in A[x]$$
$$\tilde{f} : A \to A$$
$$c \to f(c)$$
$$f, g \tilde{f} = \tilde{g}$$

Примеры:
$$A = \mathbb{F}_2$$
$$f = 0, g = x^2 + x$$
$$\tilde{f} : 0 \to 0, 1 \to 0$$
$$\tilde{g} : 0 \to 0, 1 \to 0$$

Следствие 11.1.1. A — область целостности.
$$f, g \in A[x], |A| > \max(degf, degg)$$
Тогда, если $\tilde{f} = \tilde{g}$, то $f = g$.

▶ f - g
$$f \tilde{-} g = \tilde{f} - \tilde{g} \text{ — тождественно не нулевое отображение}$$
$$\forall c \in A, f(c) - g(c) = 0$$
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. Алгебраические замкнутые поля

$\mathfrak{Def}$: Поле А — алгебраически замкнуто, если любой $f \in A[x] \backslash A$ имеет в А хотя бы 1 корень.
Теорема 12.1. Следующие условия равносильны.

1. А — алгебраически замкнуто.
2. $\forall f \in A[x]$ с $\deg f \geq 1$ делится на линейный многочлен.
3. $\forall f \in A[x]$ с $\deg f \geq 1$ имеет $degf$ корней (с учетом кратности).
4. $\forall f \in A[x]$ с $degf \geq 1$ полностью раскладывается на линейные множества в колце многочленов.

▶ $1 \Leftrightarrow 2$(следствие теоремы Безу)
$3 \Rightarrow 1$ очевидно.
$1 \Rightarrow 3$ Индукция и $degf$

1. **База:** $degf = 1$

   $ax = b$

   $x = \frac{b}{a}$ — корень.

2. **Переход:** $fdegf \geq 2$

   $\exists c \in A$ корень f кратности $k \geq 1, f = (x-c)^k g$

   По индукционному предположению число корней g = deg g.

   Все корни f отличные от c это в точности корни g, причем той же кратности.

   Число корней $f = k+$ число корней g = k + deg g = deg f.

   $4 \Rightarrow 2$ очевидно.

   $2 \Rightarrow 4$ индукция по deg f.

◀

13. Метод Ньютона

$\mathfrak{Def}$: A — поле. $\begin{array}{c|c|c} x_1 & x_2 \dots & x_n \\ \hline y_1 & y_2 \dots & y_n \end{array}$
$x_i \neq x_j$
Интерполяционная задача: найти многочлен f, deg f< n, $f(x_i) = y_i, i = 1, \dots, n$
Пусть f имеет решение f

$$g = (x - x_1) \dots (x - x_n)$$

$f_1 = f + gh$ — тоже решение.
$f_1(x_1) = f(x_i) + g(x_i)h(x_i) = f(x_i) = y_i$
Теорема 13.1. Единственность. В данной постановке задача имеет не более одного решения.
▶ Пусть f, f_1 — решение одной задачи.
$f(x_i) = f_1(x_i) = y_i, degf, degf_1 < n$
$f - f_1$ принимают 0 в $x_1 \dots x_n$
$deg(f - f_1) < n \Rightarrow f - f_1 = 0 \Rightarrow f = f_1$ ◀
Метод Ньютона $\begin{array}{c|c|c} x_1 & x_2 \dots & x_n \\ \hline y_1 & y_2 \dots & y_n \end{array}$ $f_i(x), degf_i < i$
f_i решает интерприционную задачу на первых i точках.

1. i = 1 $f_1(x) = y_1$
2. $i \to i+1$

$$f_i \to f_{i+1}$$
$$f_{i+1}(x) = f_i(x) + c_i(x - x_1)\dots(x - x_i)$$
$$y_{i+1} = f_{i+1}(x_{i+1}) = f_i(x_{i+1}) + c_i(x_{i+1} - x_1)\dots(x_{i+1} - x_i)$$
$$c_i = \frac{y_{i+1} - f_i(x_{i+1})}{(x_{i+1} - x_1)\dots(x_{i+1} - x_i)}$$
$$deg f_{i+1} < i+1$$

REM: $c_1 = \frac{y_2 - y_1}{x_2 - x_1}$

14. Матрицы. Действия над матрицами.

$\mathfrak{Def}$: R — кольцо. Матрицей называется таблица элементов кольца

$$(a_{ij}) = (a_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}} =$$

$$= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

$\mathfrak{Def}$: Множество матриц заданного размера (m строк, n столбцов) на данном кольце R

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

$\mathfrak{Def}$: Сложение матриц

$$+\colon M(m, n, R) \times M(m, n, R) \to M(m, n, R)$$

$$(a_i j) + (b_i j) \mapsto (a_{ij} + b_{ij})$$

Лемма 14.1. $\langle M(m, n, R), + \rangle$ есть абелева группа.
$\mathfrak{Def}$: Транспонирование — переворот матрицы

$${}^T\colon M(m, n, R) \to M(n, m, R)$$

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

$\mathfrak{Def}$: Умножение матриц

$$\times\colon M(m, n, R) \times M(n, k, R) \to M(m, k, R)$$

$$(a_i j) \times (b_i j) = (c_i j)$$

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

Умножение можно запомнить как «строка на столбец».

Почему же умножение именно такое? Рассмотирм систему линейных преобразований

$$\begin{cases} y_1 &= a_{11}x_1 &+ a_{12}x_2 &+ \cdots &+ a_{1m}x_m \\ y_2 &= a_{21}x_1 &+ a_{22}x_2 &+ \cdots &+ a_{2m}x_m \\ \vdots &= \vdots &+ \vdots &+ \ddots &+ \vdots \\ y_n &= a_{n1}x_1 &+ a_{n2}x_2 &+ \cdots &+ a_{nm}x_m \end{cases}$$

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 14.1. Свойства умножения матриц.

1. $A\colon n \times m$, $B\colon m \times k$, $C\colon k \times l$
$$A(BC) = (AB)C$$
2. $A, B\colon n \times m$, $C\colon m \times k$
$$(A+B)C = AC + BC$$
3. $A, B\colon n \times m$, $C\colon k \times n$
$$C(A+B) = CA + CB$$
4. $A\colon n \times m$, $B\colon m \times k$, R коммутативное кольцо.
$$(AB)^T = B^T A^T$$

▶ Надо расписывать суммы

1. $BC \leftrightharpoons D\colon m \times l$, $AD \leftrightharpoons E\colon n \times l$, $AB \leftrightharpoons F\colon n \times k$, $FC \leftrightharpoons G\colon n \times l$. 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.
$$((A+B)C)_{ij} = \sum_{x=1}^{m}(A+B)_{ix}c_{xj} = \sum_{x=1}^{m}(a_{ix}+b_{ix})c_{xj} = \sum_{x=1}^{m}(a_{ix}c_{xj}+b_{ix}c_{xj}) =$$
$$= \sum_{x=1}^{m} a_{ix}c_{xj} + \sum_{x=1}^{m} b_{ix}c_{xj} = (AC)_{ij} + (BC)_{ij} = (AC+BC)_{ij}$$

3. Аналогично

4.
$$((AB)^T)_{ij} = (AB)_{ji} = \sum_{x=1}^{m} a_{jx}b_{xi} = \sum_{x=1}^{m} b^T_{ix}a^T_{xj} = (B^TA^T)_{ij}$$

◀

Заметим, что умножение не коммутативно.

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

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

$\mathfrak{Def}$: Умножение на скаляр:

$$\times\colon R \times M(m,n,R) \to M(m,n,R)$$

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

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

Теорема 14.2. 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.
