Лекции по алгебре
Лектор: Всемирнов Максим Александрович

Содержание

1. Отображения. Композиция отображений.

$\mathfrak{Def}$: A,B — множества. $\mathit{\Gamma}_f \subset A \times B$
$\mathit{\Gamma}$ — график отображения если выполнены два условия:

1. $\forall a \in A \exists b \in B (a, b) \in \mathit{\Gamma}_f$
2. $\forall a \in A \exists b_1, b_2 \in B (a, b_1) \in \mathit{\Gamma}_f \wedge (a, b_2) \in \mathit{\Gamma}_f \Rightarrow b_1 = b_2$

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

$$f : A \to B$$

$$A \xrightarrow{f} B$$

$(a, b) \in \mathit{\Gamma}_f \Leftrightarrow b = f(a)$
A — область определения
B — область назначения

$$f : A \to B$$

$$f_1 : A_1 \to B_1$$

$$f = f_1 \Leftrightarrow A = A_1, B = B_1, \mathit{\Gamma}_f = \mathit{\Gamma}_{f_1}$$

$\mathfrak{Def}$: Композиция отображения

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

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

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

$$\mathit{\Gamma}_{g \circ f}$$

$$(a, c) \in \mathit{\Gamma}_{g \circ f} \Leftrightarrow \exists b \in B (a, b) \in \mathit{\Gamma}_f \wedge (b, c) \in \mathit{\Gamma}_g$$

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 проообраз 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 ⇔ f — сюръективно.
▶ ⇒
⇐
$f : A \to B$
$\forall b \in B f^{-1}(\{b\}) \neq 0(X_b)$
$g : B \to \cup_{b \in B} X_b$
$g(b) \in X_b = f^{-1}(\{b\}), f(g(b)) = b$
$f^{-1}(\{b\}) = X_b \subset A \Rightarrow \cup_B X_b \subset A$
$a \in A$
$a \in X_{f(a)}$
$g : B \to A$
$\forall b \in B f(g(b)) = b$
$\forall b \in B (f \circ g)(b) = b$
$f \circ g = id_B$
f — обратимо справа.
Следствие 5.1.1.
f — обратимо ⇔ 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

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

◀

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

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

$$f(f(... f(a))) = a$$

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

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

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

(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 $\forall a, b \in AaRb \Rightarrow bRa$
4. R асимметрично, если $\forall a, b \in AaRb \Rightarrow \neg(bRa)$
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. Кольца, тела, поля

$A \neq \varnothing$
$+ : A \times A \to A$
$\cdot : A \times A \to A$

1. ассоциативнсть сложения:

$$\forall a, b, c \in A (a + b) + c = a + (b + c)$$

2. существование нейтрального элемента по сложению:

$$\exists 0 \in A \forall a \in A a + 0 = 0 + a = a$$

3. существование обратного элемента по сложению:

$$\forall a \in A \exists -a \in A a + (-a) = (-a) + a = 0$$

4. коммутативность сложения:
$$\forall a, b \in A a \cdot b = b \cdot a$$

5. ассоциативность умножения:
$$\forall a, b, c \in A a \cdot b = b \cdot a$$

6. коммутативность умножения:
$$\forall a, b \in A a \cdot b = b \cdot a$$

7. существование нейтрального элемента по умножению:

$$\exists 1 \in A \forall a \in A a \cdot 1 = 1 \cdot a = a$$

8. существование обратного элеменрта по умножению:
$$\forall a \in A \setminus \{0\} \exists a^{-1} \in A a \cdot a^{-1} = a^{-1} \cdot a = 1$$

9. дистрибутивность:
   a) $\forall a, b, c \in A (a+b) \cdot c = a \cdot c + b \cdot c$
   b) $\forall a, b, c \in A c \cdot (a+b) = c \cdot a + c \cdot b$

$\mathfrak{Def}$: Кольцо - непустое множество A с операциями $"+"$, $"\cdot"$, удовлетворяющее свойствам 1 - 5, 9 (a, b)

$\mathfrak{Def}$: Кольцо, в котором выполнена аксиома 6 - коммутативное кольцо

$\mathfrak{Def}$: Кольцо, в котором выполнена аксиома 7 - кольцо с единицей

$\mathfrak{Def}$: Тело - кольцо с 1, в котором $1 \neq 0$ и выполнена аксиома 8

$\mathfrak{Def}$: Поле - коммутативное кольцо с 1, в котором $1 \neq 0$ и выполнена аксиома 8 (т.е. все 9 аксиом)

REM: иногда кольца, для которых выполнены аксиомы 1-4, 9 называют ассоциативными кольцами

REM: $(A, +, \cdot)$ - кольцо, $(A, +)$ - абелева группа

Примеры:

- $\mathbb{Z}$ - коммутативное кольцо с 1, но 2 не имеет обратного в $\mathbb{Z} \Rightarrow$ не поле
- N - не кольцо
- $2\mathbb{Z}$ - кольцо без 1
- $\mathbb{Q}, \mathbb{R}$ - поля

Простейшие свойства колец

1. 0 - единственный
2. $-a$ - единственный
3. 1 - единственная (если есть)

   ▶
   $$1 = 1 \cdot 1' = 1$$
   ◀

4. если у a есть обратный по умножению, то он единственен

   ▶
   $$a' = a'aa'' = a''$$
   ◀

5. если в кольце с 1 у элемента a есть 2 левых обратных, то левых обратных к a бесконечно много (упражнение)
6. $0 \cdot a = a \cdot 0 = 0$

   ▶
   $$a \cdot 0 + a \cdot 0 = a(0+0) = a \cdot 0| + (a \cdot 0)'$$
   $$a \cdot 0 + a \cdot 0 + (a \cdot 0)' = a \cdot 0 + (a \cdot 0)' = a \cdot 0 = 0$$
   второе равенство аналогично ◀

7. $a(-b) = (-a)b = -(ab)$

   ▶
$$a + (-a) = 0$$
$$ab + (-a)b = (a + (-a))b = ab = 0$$
$$(-a)b = -ab$$
   второе равенство аналогично ◀

8. $0 = 1, |A| = 1, A = \{0\}$

   ▶
$$a \in Aa = 1 \cdot a = 0 \cdot a = 0$$
◀

$\mathfrak{Def}$: A - кольцо (тело, поле)
$A \supseteq B \neq \varnothing$ - подкольцо (подтело, подполе), если являктся кольцом (телом, полем), относительно сужения операций на B

REM:

- $B \neq \varnothing, B \supset A$ - подкольцо в A если оно замкнуто относительно умножения, сложения, взятия обратного по сложению
- B - подтело, если подкольцо и замкнуто по взятию обратного ненулевого элемента по умножению и содержит элементы отличные от нуля:
  $\forall a, b \in Ba + b \in B$
  $\forall a \in Ba - a \in B$
  $\forall a, b \in Bab \in B$
  $\forall a \in B \setminus a^{-1} \in B$

$\mathfrak{Def}$: A, B - кольца
$f : A \to B$
f - гомоморфизм, если:

$$\forall a_1, a_2 \in Af(a_1 + a_2) = f(a_1) + f(a_2)$$
$$\forall a_1, a_2 \in Af(a_1 a_2) = f(a_1)f(a_2)$$

$\mathfrak{Def}$: f - изоморфизм, если f - гомоморфизм и биекция

A, B изоморфны, если существует изоморфизм между A и B

$$A \cong B$$

REM: f - гомоморфизм и $f(0_A)$обратим по сложению, тогда $f(0_A) = 0_B$
▶ $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$, говорим, что у $f(1_A)$ есть обратный по сложению, прибавляем его и получаем: $f(0_A) = 0_B$ ◀
REM: Если f - гомоморфизм и $f(1_A)$ обратим в B то $f(1_A) = 1_B$
▶ $f(1_A) = f(1_A \cdot 1_A) = f(1_A)f(1_A)$, говорим, что у $f(1_A)$ есть обратный по умножению, умножаем на него и получаем: $f(1_A) = 1_B$ ◀
Делимость в кольцах

A - кольцо, $a, b, c \in A, c = ab$
a - левый делитель c
b - правый делитель c
$0 = a, 0 = 0 \cdot b$

$\mathfrak{Def}:$ a, b - нетривиальные делители нуля, если $0 = ab, a \neq 0, b \neq 0$

$\mathfrak{Def}:$ Область целостности - коммутативное кольцо с 1, без нетривиальных делителей нуля

REM: Поле - область целостности $(\forall a, b(ab = 0 \Rightarrow a = 0 \vee b = 0))$

Теорема 10.1. A - область целостности $a \in A \setminus \{0\}$
$ab = ac \Rightarrow b = c$

▶

$$\underbrace{a}_{neq0}(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c$$

◀

11. Мультипликативная группа кольца

$\mathfrak{Def}:$ A - кольцо с 1
$A^* = \{a \in A : \exists b \in Aab = ba = 1\}$
$(A^*, \cdot)$ - мультипликативная группа кольца

Теорема 11.1. A^* - группа по умножению

▶

$$A^* \ni 1_A$$

$$A^* \times A^* \to A^*$$

$$a_1, a_2 \in A \exists b_1, b_2 : a_1 b_1 = b_1 a_1 = 1 \wedge a_2 b_2 = b_2 a_2 = 1$$

$$(a_1 a_2)(b_1 b_2) = a_1 (a_2 b_2) b_1 = a_1 b_1 = 1$$

$$(b_2 b_1)(a_1 a_2) = b_2 (b_1 a_1) a_2 = b_2 a_2 = 1$$

$b_2 b_1$ - обратный к $a_1 a_2$

$$\forall a \in A^* 1 \cdot a = a \cdot 1 = a$$

$$a \in A^* \Rightarrow \exists bab = ba = 1 \Rightarrow b \in A^*$$

обратный к b - это a ◀

Примеры:

- K - поле, $K^* = K \setminus \{0\}$
- $\mathbb{Z}, \mathbb{Z}^* = -1, 1$

12. Кольца многочленов

$\mathfrak{Def}$: A - коммутативное кольцо с 1
$A[x] = \{\underbrace{a_1, a_2, ..}|a_i \in A$, почти все нули $\}$

$A[x]$ - кольцо многочленов от одной переменной над кольцом A

REM: "почти все" - все кроме конечного числа

$\mathfrak{Def}$: $" + " : (a_1, a_2, ...) + (b_1, b_2, ...) = (a_1 + b_1, a_2 + b_2, ...)$

REM: $\exists n, m : a_i = 0, b_i = 0 \forall i > max(n, m) \Rightarrow a_i + b_j = 0$

$\mathfrak{Def}$: $" \cdot " : (a_1, a_2, ...) \cdot (b_1, b_2, ...) = (c_1, c_2, ...)$
где $c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{i+j=n} a_i b_j$

REM: $\exists n, m : a_i = 0, b_j = 0 \forall i > n, j > m \Rightarrow \forall k > n + m \Rightarrow c_k = 0$

▶

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \underbrace{\sum_{i=0}^{n} a_i b_{k-i}}_{0 \le i \le n \Rightarrow k-i \ge k-n \ge n+m-n=m \Rightarrow b_{k-i}=0 \Rightarrow \sum=0} + \underbrace{\sum_{i=n+1}^{k} a_i b_i}_{i>n \Rightarrow a_i=0 \Rightarrow \sum=0} = 0$$

◀

Теорема 12.1. $(A[x], +, \cdot)$ - коммутативное кольцо с 1
▶

1. аксиомы 1 - 4 покомпонентно выполнены в A
2. $\exists 0 = (0, 0, 0, ...)$
3. $\exists 1 = (1, 0, 0, ...)$ $1 \cdot \alpha = \alpha \cdot 1 = \alpha$

   ▶ по определению операции умножения:
   $(a_0, \underbrace{a_0 + a_1 \cdot 1}_{a_1}, \underbrace{...}_{a_2}) = \alpha$ ◀

4. коммутативность:
   $\beta = (b_0, b_1, ...), \alpha = (a_0, a_1, ...) \Rightarrow \alpha\beta = \beta\alpha$

   ▶

$$\alpha\beta = (c_0, c_1, ...) \Rightarrow c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

$$\beta\alpha = (d_0, d_1, ...) \Rightarrow d_k = \sum_{i=0}^{k} b_i a_{k-i} = \sum_{j=0}^{k} b_{k-j} a_j | j = k - i, i = k - j| =$$

$$\underbrace{\sum_{i=0}^{k} b_{k-i} a_i = \sum_{i=0}^{k} a_i b_{k-i}}_{..A-} = c_k$$

◀

5. дистрибутивность (упражнение)

6. ассоциативность:
   $\alpha = (a_0, a_1, ...), \beta = (b_0, b_1, ...), \gamma = (c_0, c_1, ...)$
   $\alpha\beta = d, (\alpha\beta)\gamma = e$
   $\beta\alpha = f, \alpha(\beta\gamma) = g$
   $ek = gk \forall k$

   ▶

$$ek = \sum_{i=0}^{k} f_i c_{k-i} = \sum_{i=0}^{k} (\sum_{j=0}^{i} a_j b_{i-j}) c_{k-i} =$$

   меняем порядок суммирования

$$= \sum_{j=0}^{k} (\sum_{i=j}^{k} a_j b_{i-j} c_{k-i}) = \sum_{j=0}^{k} a_j (\sum_{i=j}^{k} b_{i-j} c_{k-i}) =$$

   делаем замену $l = i - j$

$$= \sum_{j=0}^{k} a_j (\sum_{l=0}^{k-j} b_l c_{k-l-j}) = \sum_{j=0}^{k} a_j f_{k-j} = gk$$

◀

◀

13. Степень многочлена

Алтернативная запись:
$a = (a, 0, 0, ...)$
$x = (0, 1, 0, ...)$
$x^i = (0, ..., \underbrace{1}_{i-}, ...)$
$(a_0, a_1, a_2, ...) = (a_0, 0, 0, ...) + (0, a_1, 0, 0, ...) + ... =$
$= (a_0, 0, 0, ...) \cdot (1, 0, 0, ...) + (0, a_1, 0, 0, ...) \cdot (0, 1, 0, 0, ...) + ... = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ - альтернативная запись в форме многочлена

$\mathfrak{Def}$: $A[x] = \{a_0 + a_1 x + ... + a_n x^n | n \in \mathbb{N} \cup \{0\} \wedge a_i \in A\}$
$f \in A[x]$ - многочлен
$\mathfrak{Def}$: $f = a_0 + a_1 x + ... + a_n x^n, a_n \neq 0, f \neq 0$
n - степень многочлена f, $n = \deg f$
$f = 0 \Rightarrow \deg f = -\infty$
Теорема 13.1.

1. $deg(f + g) \leq max(\deg f, \deg g)$

2. $deg(fg) \leq \deg f + \deg g)$

   REM: Если A - область целостности, то $\deg(fg) = \deg f + \deg g$

▶

1. следует из доказательства замкнутости относительно сложения:
   $f = a_0 + ... + a_n x^n \wedge a_n \neq 0$
   $g = b_0 + ... + b_m x^m \wedge a_m \neq 0$

2. $fg = c_0 + c_1 + ... + c_{n+m}x^{n+m} + \underbrace{0 + ...}$

   очевидно, что $\deg(fg) = \deg f + \deg g$

3. для области целостности:
   $a_n \neq 0, b_m \neq 0$
   $c_{n+m} = a_n b_m \neq 0 \Rightarrow \deg(fg) = degf + defg$
   Если $f = 0 \vee g = 0$, тогда $\deg(fg) = \underbrace{\deg f}_{-\infty} + \underbrace{\deg g}_{-\infty} = -\infty \Leftrightarrow fg = 0$

◀

Следствие 13.1.1. Если A - область целостности, то и $A[x]$ - область целостности
▶ $f, g \neq 0$
$\deg f, \deg g \geq 0$
$\deg(fg) \geq 0 \Rightarrow fg \neq 0$ ◀
REM: $A = \mathbb{Z}/4\mathbb{Z}, f = 2x, g = 2x^2 \Rightarrow fg = 4x^2 = 0$
Следствие 13.1.2. A - область целостности $\Rightarrow (A[x])^* = A^*$
▶ $" \Rightarrow " \ fg = 1?$
$\deg f + \deg g = 0$ многочлены вида $(*, 0, ...)$
$\deg f = \deg g = 0 \Rightarrow f, g \in A : fg = 1$
$" \Leftarrow "$ если элемент обратим в кольце A, то он обратим и в кольце многочленов ◀

14. Теорема о деление с остатком

Теорема 14.1. A - коммутативное кольцо с 1 $f, g \in A[x]$
$f = a_0 + a_1x + a_2x^2 + ... + a_nx^n, n = \deg f, a_n \in A^*$
тогда $\exists q, r \in A[x] : g = qf + r, \deg r < \deg f$

REM: Если A - область целостности, то такое представление единственно

▶ **Существоване:**
Индукция по $m = \deg g$:
База: $m < n$

$$q = 0, r = g$$

Переход: доказали для всех многочленов $\deg g < m$, докажем для m

$$g = b_mx^m + ... + b_0$$

$$g_1 = g - b_m a_n^{-1} x^{m-n} f$$

коэффицент при x^m в g_1: $b_m - b_m a_n^{-1} a_n = 0 \Rightarrow \deg g_1 < m$
по предположению индукции $g_1 = fq_1 + r_1, \deg r_1 < \deg f$, тогда:

$$r = r_1$$

$$q = q_1 + b_m a_n^{-1} x^{m-n}$$
$$g = fq + r$$

Единственность:
A - область целостности

$$g = fq + r = f\tilde{q} + \tilde{r}, \deg r, \deg \tilde{r} < f$$

$$f(q-\tilde{q}) = \tilde{r} - r$$

если $q-\tilde{q} \neq 0$, то степень левого многочлена $\geq \deg f$ и степень правого $< degf \Rightarrow q-\tilde{q} = 0, r-\tilde{r} = 0 \Rightarrow q = \tilde{q}, r = \tilde{r}$ ◀

REM: условие обратимости старших коэффицентов существенно: $A = \mathbb{Z}$
$f = 2x, g = x^2+1$
в $\mathbb{Z}[x]$ разложения: $g = fq + r, q, r \in \mathbb{Z}[x], degr < degf$ - не существует

15. теорема Безу

Теорема 15.1. (Безу)
A - коммутативное кольцо с 1

$$c \in A, f \in A[x] \Rightarrow \exists q \in A[x] : f(x) = (x-c)q(x) + f(c)$$

▶ Рассмотрим $x-c$, по теоремо о делении с остаток получаем:

$$f(x) = (x-c)q(x) + r_0, \deg r_0 < \deg(x-c) = 1$$

$$r = r_0 \in A$$

$$f(x) = (x-c)q(x) + r_0$$

$$f(c) = (c-c)q(c) + r_0$$

$$f(c) = r_0 \Rightarrow f(x) = (x-c)q(x) + r_0$$

◀

$\mathfrak{Def}$: $A, B, A \subseteq B$, коммутативные с 1
$f \in A[x]$
$c \in B$ - корень f, если $f(c) = 0$

Следствие 15.1.1. c - корень $\Leftrightarrow (x-c)|f$

▶ " $\Leftarrow$ " $f(x) = (x-c)g(x) \Rightarrow f(c) = (c-c)g(c) = 0 \Rightarrow c$ - корень
" $\Rightarrow$ " $f(c) = 0 \Rightarrow$ теорема Безу $\Rightarrow f(x) = (x-c)g(x) + f(c) = (x-c)g(x) \Rightarrow (x-c)|f$ ◀

16. Характеристика кольца

A - кольцо с 1

$\mathfrak{Def}$: Характеристика кольца - наименьшее $n > 0$, т.ч. $\underbrace{1 + ... + 1}_{n} = 0$

$$\mathrm{char} A = n$$

Если такого n нет, тосчитается, что $\mathrm{char} A = 0$

Примеры:

$$\mathrm{char}\mathbb{Z} = 0, \mathrm{char}\mathbb{Q} = 0, \mathrm{char}\mathbb{R} = 0$$

$\mathbb{F}_2, \mathbb{F}_3$ - поля из 2-х и 3-х элементов соответсвенно

$$\mathrm{char}\mathbb{F}_2 = 2, \mathrm{char}\mathbb{F}_3 = 3$$

REM: A - поле $\Rightarrow \mathrm{char} A$ либо 0, либо простое число
▶

1. $\forall n \underbrace{1+...+1}_{n} \neq 0 \Rightarrow \text{char}A = 0$

2. $\text{char}A > 0 \underbrace{1+...+1}_{n} = 0, n > 1$ т.к. в поле $1 \neq 0$
   $n = ab, 1 < a, b < n$
   по дистрибутивности $\Rightarrow \underbrace{1+...+1}_{a} = 0 \vee \underbrace{1+...+1}_{b} = 0 \Rightarrow$ наименьшее n, чтобы $\underbrace{1+...+1}_{n} = 0$ должно быть простым

◀

17. Производная многочлена

A - коммутативное кольцо с 1
$f \in A[x]$
$f = a_n x^n + ... + a_0$
$K \in \mathbb{N}, K \cdot a = \underbrace{a+...+a}_{K} = \underbrace{1+..+1}_{K} a$
$0 \cdot a = 0$

$\mathfrak{Def}$: $f' = n \cdot a_n x^{n-1} + ... + 2a_2 x + a_1 = \sum_k = 0^n k a_n x^{k-1}$
($k = 0$ - фиктивное слагаемое, $0 \cdot a_0 x^{-1} = 0$)

Теорема 17.1. свойства производной

1. $(f+g)' = f' + g'$
   $f_1 + ... + f_k = f_1' + ... + f_k'$
2. $c \in A, (c \cdot f)' = c \cdot f'$
3. $(fg)' = f'g + fg'$
4. $(f_1 \cdot f_2 \cdot ... \cdot f_k)' = f_1' \cdot f_2 \cdot ... f_k + f_1 \cdot f_2' \cdot ... \cdot f_k + ... + f_1 \cdot .. \cdot f_k'$
5. A - поле, $f \in A[x]$
   - $\text{char}A = 0$ $f' = 0 \Leftrightarrow f = \text{const}$
   - $\text{char}A = p > 0$ $f' = 0 \Leftrightarrow f \in A[x^p]$

▶

1. упражнение
2. упражнение
3. доказываем по частям:
   - $f = x^n, g = x^m$

$$(fg)' = (x^{n+m})' = (n+m)x^{n+m-1} = nx^{n-1}x^m + x^n m x^{m-1} = f'g + fg'$$

   - $f = x^n, g = \sum_{k=0}^m c_k x^k$

$$(fg)' = (\sum_{k=0}^m c_k x^n x^k)' = \sum_{k=0}^m c_k (x^n x^k)' =$$

$$= \sum_{k=0}^m c_k (f' x^k + f k x^{k-1}) = f' \sum_{k=0}^m c_k x^k + f \sum_{k=0}^m k x^{k-1}) = f'g + fg'$$

- $f=\sum_{k=0}^{n} a_k x^k, g$ - произвольный многочлен

$$(fg)'=\sum_{k=0}^{n} a_k(x^k g)'=\sum_{k=0}^{n} a_k(kx^{k-1}g+x^k g')=$$

$$=g\sum_{k=0}^{n} ka_k x^{k-1}+g'\sum_{k=0}^{n} a_k x^k=f'g+fg'$$

4. упражнение

5. следствие п.4

6. - $\mathrm{char} A=0$

$$f=c_0+c_1x+...+c_nx^n$$
$$0=f'=c_1+2c_2x+...+nc_nx^{n-1}$$
$$\forall k, kc_k=0\,\underbrace{(1+1+...+1)}_{\neq 0,k}c_k=0\Rightarrow f=c_0=\mathrm{const}$$

обратное очевидно

- $\mathrm{char} A=p>0, f'=\sum_{k=1}^{n} kc_k x^{k-1}$ $\forall k\geq 1 kc_k=0$ Пусть $p\nmid k, k=pq+r, 1<r<p$

$$kc_k=\underbrace{(1+1+...+1)}_{k}c_k=(\underbrace{\underbrace{1+...+1}_{p}+..+\underbrace{1+...+1}_{p}}_{q}+\underbrace{1+...+1}_{r})c_k=\underbrace{(1+..+1)}_{\neq 0,r,..0<r<\mathrm{char} A}c_k$$

$$\Rightarrow c_k=0$$

$"\Leftarrow"$ $f=c_0+c_px^p+c_{2p}x^2p+..\in A[x^p]$
Если $f=\sum_{j=0}^{r} c_{jp}x^{jp}$, то $f'=\sum_{j=0}^{r} j\underbrace{p}_{=0,\mathrm{char} A=p}c_{jp}x^{jp-1}=0$

◀

18. 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 18.1. A — поле, $charA=0, f\in A[x], f\neq 0$

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

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

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

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

19. Число корней многочлена

Лемма 19.1. 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 19.2. 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 19.1. 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 19.1.1. 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 19.1.2. Если A — область целостности.
$|A| = \infty$ и $\tilde{f} = \tilde{g}$, то и $f = g$

20. Алгебраические замкнутые поля

$\mathfrak{Def}$: Поле A — алгебраически замкнуто, если любой $f \in A[x] \backslash A$ имеет в A хотя бы 1 корень.
Теорема 20.1. Следующие условия равносильны.

1. A — 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.

◀

21. Метод Ньютона

$\mathfrak{Def}$: A — поле.

x_1	$x_2 \dots$	x_n
y_1	$y_2 \dots$	y_n

$x_i \neq x_j$
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 21.1. 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. $i \rightarrow i + 1$

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

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

22. Метод Лагранжа

$\begin{array}{c|c|c} x_1 & x_2 \dots x_i & x_n \\ \hline 0 & 0 \dots 1 & 0 \end{array}$
$degL_i < n$
$L_i = \frac{(x-x_1)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_1)\dots(x_i-x_n)}$
$\begin{array}{c|c|c} x_1 & x_2 \dots & x_n \\ \hline y_1 & y_2 \dots & y_n \end{array}$

$$f = y_1L_1 + y_2L_2 + \dots + y_nL_n$$
$$f(x_i) = \sum_{j=1}^{n} y_jL_j(x_i) = y_iL_i(x_i) = y_i$$
$$f(x) = \sum_{k=1}^{n} y_kL_k$$
$$L_k(x) = \frac{(x - x_1) \dots (x - x_n)}{(x_k - x_1) \dots (x_k - x_n)}$$
$$g(x) = (x - x_1) \dots (x - x_n)$$

Числитель $L_k = \frac{g(x)}{(x - x_k)}$

$$g'(x) = 1(x - x_2) * \dots * (x - x_n) +$$
$$(x - x_1)1 \dots (x - x_n) + \dots$$

$g'(x_k)$ — знаменатель L_k $degf \leq n$

$$f(x) = \sum_{k=1}^{n} f(x_k) \frac{g(x)}{(x - x_k)g'(x_k)}$$

23. Биномиальная формула

𝔇𝔢𝔣:

$$(((A[x_1])[x_2])[x_3] \dots)[x_n]$$

кольцо многочленов от n переменных.

$$(A[x_2])[x_1] = (A[x_1])[x_2]$$

$$x_1 \to x_1$$

$$x_2 \to x_2$$

$$\sum c_{i_1, i_2} x_1^{i_1} x_2^{i_2}$$

$A[x_1, \dots, x_n]$ — кольцо многочленов от нескольких переменных.

$$\sum c_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$$

Биномиальная формула: $(x = y)^n = ?$ **Биномиальные коэффициенты:** $C_n^k = \frac{n!}{k!(n-k)!}$

Лемма 23.1.

1. $C_n^0 = 1$
2. $C_n^n = 1$
3. $C_n^k + C_n^{k+1} = C_{n+1}^{k+1}$
4. $C_n^k = C_n^{n-k}$

▶

$$C_n^k + C_n^{k+1} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k+1)!\,(n-k-1)!} =$$

$$= \frac{n!\,(k+1) + n!\,(n-k)}{(k+1)! \dots (n-k)!} = \frac{n!\,(n+1)}{(k+1)!\,(n+1-(k+1))!} = C_{n+1}^{k+1}$$

◀

𝔇𝔢𝔣:

-	0	1	2	3	4
0	1	-	-	-	-
1	1	1	-	-	-
2	1	2	1	-	-
3	1	3	3	1	-
4	1	4	6	4	1

Теорема 23.1. Биномиальная формула.

$$(x+y)^k = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$$

▶ Индукция по n

1. n = 0

$$1 = C_0^0 x^0 y^0 = 1$$

2. n = 1

$$x + y = C_1^0 x^1 y^0 + C_1^1 x^0 y^1$$

3. $n \to n+1$

$$(x+y)^{n+1} = (x+y)^n(x+y) = (\sum_{k=0}^{n} C_n^k)x^k y^{n-k})(x+y) =$$

$$= \sum_{k=0}^{n} C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^{n} C_n^k x^k y^{n-k+1} =$$

$$= C_n^n x^{n+1} + \sum_{k=0}^{n-1} C_n^k x^{k+1} y^{n-k} + \sum_{k=1}^{n} C_n^k x^k y^{n-k+1} + C_n^0 y^{n+1} =$$

$$= C_{n+1}^{n+1} x^{n+1} + \sum_{k=1}^{n} C_n^{k-1} x^k y^{n+1-k} + \sum_{k=1}^{n} C_n^k x^k y^{n-k+1} + C_{n+1}^0 y^{n+1} =$$

$$= C_{n+1}^{n+1} x^{n+1} + \sum_{k=1}^{n} (C_n^{k-1} + C_n^{k-1}) x^k y^{n+1-k} + C_{n+1}^0 y^{n+1} =$$

$$= \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}$$

◀

Следствие 23.1.1.

1. $\sum_{k=0}^{n} C_n^k = 2^k$
2. $\sum_{k \text{четное}} C_n^k = 2^{n-1}$
3. $\sum_{k \text{нечетное}} C_n^k = 2^{n-1}$

24. Конструкция комплексных чисел, как множества пар.

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

- $+ : \mathbb{R}^2 \mapsto \mathbb{R}^2$
  $(a,b) + (c,d) \mapsto (a+c, b+d)$
- $* : \mathbb{R}^2 \mapsto \mathbb{R}^2$
  $(a,b) * (c,d) \mapsto (ac - bd, ad + bc)$

Теорема 24.1. $\mathbb{R}^2$ с введёнными операциями является полем.
$\mathfrak{Def}$: Это поле называется полем комплексных чисел $\mathbb{C}$ (Complex).
▶ Упр.
Некотрые заметки:

1. $0_c = (0,0)$
2. $-(a,b) = (-a,-b)$
3. $(1,0) * (a,b) = (a,b)$

4. $(a,b) \neq 0,\ (a,b)^{-1} - ?$

$$(a,b)^{-1} = (c,d) \Leftrightarrow (a,b) * (c,d) = (1,0)$$

$$+\begin{cases} ac - bd = 1| \cdot a,\ \cdot(-b) \\ bc + ad = 0| \cdot b,\ \cdot a \end{cases}$$

$$\begin{cases} (a^2+b^2) \cdot c = a \\ (a^2+b^2) \cdot d = -b \end{cases}$$

$$\Rightarrow a = \frac{a}{a^2+b^2},\ d = \frac{-b}{a^2+b^2}$$

Найденные значения корректны, т.к. $(a,b) \neq 0 \Rightarrow a^2+b^2 > 0$

◀

25. Алгебраическая форма записи комплексного числа. Комплексное сопряжение. Свойства комплексного сопряжения.

$\mathbb{R} \mapsto \mathbb{C}:\ a \mapsto (a,0)$ - инъективный гомоморфизм колец:

$$\begin{cases} \varphi(a+b) = \varphi(a) + \varphi(b) \\ \varphi(ab) = \varphi(a) * \varphi(b): \quad (a,0)*(b,0) = (ab-0, 0+0) = (ab,0) \end{cases}$$

$\mathbb{C} \supseteq \varphi(\mathbb{R}) = \{(a,0)|a \in \mathbb{R}\}$
$\varphi(\mathbb{R}) \cong \mathbb{R}$, поэтому говорят, что $\mathbb{R} \subseteq \mathbb{C}$, имея в виду, что $\varphi(\mathbb{R}) \subseteq \mathbb{C}$
$i = (0,1) \Rightarrow i^2 = (-1,0)$
$\mathfrak{Def}$: $(a,b) = (a,0)*(1,0) + (b,0)*(0,1) = a + bi$ - алгебраическая запись числа.
a называется вещественной частью комплексного числа($a = Re(z), z \in \mathbb{C}$)
b называется мнимой частью комплексного числа($b = Im(z), z \in \mathbb{C}$)
$\mathfrak{Def}$: $z \in \mathbb{C},\ z = a + bi,\ a,b \in \mathbb{R}$
$\overline{z}$ называется комплексно сопряжённым с z, если $\overline{z} = a - bi$
REM: Сопряжение $\equiv$ симметрия относительно вещественной оси.
Рисунок1.
Свойства:

1. $\overline{\overline{z}} = z$
2. $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$
3. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

3'. $\overline{z_1 + z_2 + \dots + z_n} = \overline{z_1} + \overline{z_2} + \dots + \overline{z_n}$ (По индукции из св-ва 3.)

4. $\overline{z_1 * z_2} = \overline{z_1} * \overline{z_2}$

4'. $\overline{z_1 * z_2 * \dots * z_n} = \overline{z_1} * \overline{z_2} * \dots * \overline{z_n}$ (По индукции из св-ва 4.)

5. $f \in \mathbb{R}[x]$ $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ Тогда: $\overline{f(z)} = f(\overline{z})$
6. • $z + \overline{z} \in \mathbb{R}$

- $z * \overline{z} \in \mathbb{R},\ z * \overline{z} \geq 0$
- $z * \overline{z} \Leftrightarrow z = 0$

Два последних пункта следуют из того, что $z * \overline{z} = a^2 + b^2$

▶ Только 5 свойство: $f(z) = a_0 + a_1 z + \dots + a_n z^n$ $\overline{f(z)} = \overline{a_0 + a_1 z + \dots + a_n z^n} = \overline{a_0} + \overline{a_1 z} + \dots + \overline{a_n z^n} = \overline{a_0} + \overline{a_1} \cdot \overline{z} + \dots + \overline{a_n} \cdot \overline{z^n} = a_0 + a_1 \overline{z} + \dots + a_n \overline{z^n} = a_0 + a_1 \overline{z} + \dots + a_n \overline{z}^n = f(\overline{z})$ ◀

$\overline{z}$(Сопряжение): $\mathbb{C} \mapsto \mathbb{C}$ - гомоморфизм из $\mathbb{C}$ в $\mathbb{C}$:

$$\begin{cases} \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \\ \overline{z_1 \cdot z_1} = \overline{z_1} \cdot \overline{z_2} \end{cases}$$

$\overline{z} \cdot \overline{z} = id \Rightarrow$ сопряжение - нетождественный изоморфизм из $\mathbb{C}$ на себя(автоморфизм).

$\mathfrak{Def}:$ Автоморфизм - изоморфизм поля с самим собой.

7. $z \neq 0,\ z \cdot \overline{z} = |z|^2,\ |z| \neq 0$(т.к. $z \neq 0$)

$$z \cdot \frac{\overline{z}}{|z|^2} = 1 \Rightarrow \boxed{z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{a - bi}{a^2 + b^2}}$$

PS: определение и проч. про модуль в следующем вопросе.

26. Модуль комплексного числа. Мультипликативность модуля. Произведение двух сумм двух квадратов.

$z \in \mathbb{C}$
$z\overline{z} = a^2 + b^2$
$\mathfrak{Def}:$ $\sqrt{z\overline{z}} = |z|$ - модуль z.
Свойство: $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$
▶

$$z_1 = a + bi,\ z_2 = c + di$$
$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

◀

REM: Для $\mathbb{Z}[a, b, c, d]$(кольцо многочленов) тоже верно.
Напоминание: φ - мультипликативна $\Leftrightarrow \varphi(ab) = \varphi(a)\varphi(b)$. $\Rightarrow$ Модуль мультипликативен.
Вопрос: при каких k $\exists\ c_i:\ (a_1^2 + \dots + a_k^2)(b_1^2 + \dots + b_k^2) = (c_1^2 + \dots + c_k^2)$, где c_i - полиномы от a_j и b_l.
Ответ: Только для $k = 1, 2, 4, 8$.
$k = 1$: мультипликативность $|\mathbb{R}|$
$k = 2$: мультипликативность $|\mathbb{C}|$
$k = 4$: мультипликативность модуля кватернионов
$k = 8$: мультипликативность модуля октав

27. Аргумент комплексного числа. Тригонометрическая форма записи. Арифме- тические операции над комплексными числами в тригонометрической форме.

Рисунок2.

$z \in \mathbb{C},\ z = a + bi \Rightarrow (a, b)$ - координата в декартовой системе координат.
В полярной системе координат два других параметра: r - радиус вектор, φ - угол.

$$\begin{cases} a = r\cos(\varphi) \\ b = r\sin(\varphi) \end{cases}$$

Пары (r, φ) и $(r, \varphi + 2\pi k)$ определяют одну и ту же точку на комплексной плоскости.
$\mathfrak{Def}$: φ - аргумент $z(argz)$

Для любого вещественного числа $arg = 0$.

$\mathbb{R}, \sim$: $\varphi_1 \sim \varphi_2 \Leftrightarrow \varphi_1 - \varphi_2 = 2\pi k, k \in \mathbb{Z}$
Упр.: Доказать, что $\sim$ отношение эквивалентности.
$\mathfrak{Def}$: $[\varphi] = \{\varphi + 2\pi k | k \in \mathbb{Z}\}$ Arg z $= [\varphi] \Leftrightarrow argz = \varphi$
Пусть $z = a + bi |z| = \sqrt(a^2 + b^2)$. arg z = ?:

1. $a > 0$
$$\frac{b}{a} = \operatorname{tg}\varphi,\ \varphi \in (-\pi/2, \pi/2) \Rightarrow argz = \operatorname{arctg}(\frac{b}{a})$$
2. $a < 0$
$$\varphi \in (\pi/2, 3\pi/2) \Rightarrow argz = \pi + \operatorname{arctg}(\frac{b}{a})$$
3. $a = 0, b > 0$
$$argz = \pi/2$$
4. $a = 0, b < 0$
$$argz = -\pi/2$$

$\mathfrak{Def}$: Тригонометрическая форма записи числа

$z = a + bi = r\cos\varphi + ir\sin\varphi = r(\cos\varphi + i\sin\varphi)$, где r - модуль($r \geq 0$), а φ - аргумент комплексного числа.

$|\cos\varphi + i\sin\varphi| = \sqrt{\cos^2\varphi + \sin^2\varphi} = 1$
Свойство: $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1),\ z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$
Тогда:

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

$$\boxed{|z_1 z_2| = r_1 r_2 = |z_1||z_2|, \quad Arg(z_1 z_2) = Arg(z_1) + Arg(z_2)}$$

28. Неравенство треугольника

Теорема 28.1. $||z_1| - |z_2|| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|$

Причём:

1. $|z_1 + z_2| = |z_1| + |z_2| \Leftrightarrow z_1$ и z_2 лежат на одном луче, проведённом из начала координат.
2. $|z_1 - z_2| = |z_1| + |z_2| \Leftrightarrow z_1$ и z_2 лежат на дополнительных лучах, проведённых из начала координат.
3. $|z_1 + z_2| = ||z_1| - |z_2|| \Leftrightarrow z_1$ и z_2 лежат на дополнительных лучах, проведённых из начала координат.
4. $|z_1 - z_2| = ||z_1| - |z_2|| \Leftrightarrow z_1$ и z_2 лежат на одном луче, проведённом из начала координат.

▶ Так как все величины неотрицательны, то исходной неравенство равносильно следующему:

$$||z_1| - |z_2||^2 \leq |z_1 \pm z_2|^2 \leq (|z_1| + |z_2|)^2$$

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

$$|z_1 \pm z_2|^2 = (r_1\cos\varphi_1 \pm r_2\cos\varphi_2)^2 + (r_1\sin\varphi_1 \pm r_2\sin\varphi_2)^2 = r_1^2\cos^2\varphi_2 \pm 2r_1r_2\cos\varphi_1\cos\varphi_2 +$$
$$+ r_2^2\cos^2\varphi_2 + r_1^2\sin^2\varphi_1 \pm 2r_1r_2\sin\varphi_1\sin\varphi_2 + r_2^2\sin^2\varphi_2 = r_1^2 + r_2^2 \pm 2r_1r_2(\cos\varphi_1\cos\varphi_2 + \sin\varphi_1\sin\varphi_2) =$$
$$= r_1^2 + r_2^2 \pm 2r_1r_2\cos(\varphi_1 - \varphi_2)$$
$$|z_1 \pm z_2|^2 \leq r_1^2 + r_2^2 + 2r_1r_2 = (r_1 + r_2)^2 = (|z_1| + |z_2|)^2$$

1. Если знак $+$, то равенство $\Leftrightarrow \cos(\varphi_1 - \varphi_2) = 1 \Leftrightarrow \varphi_1 - \varphi_2 = 2\pi k, k \in \mathbb{Z} \Leftrightarrow \varphi_1 = \varphi_2 + 2\pi k, k \in \mathbb{Z}$, то есть z_1 и z_2 лежат на одном луче.
2. Если знак $+$, то равенство $\Leftrightarrow \cos(\varphi_1 - \varphi_2) = -1 \Leftrightarrow \varphi_1 - \varphi_2 = 2\pi k + \pi, k \in \mathbb{Z} \Leftrightarrow \varphi_1 = \varphi_2 + 2\pi k + \pi, k \in \mathbb{Z}$, то есть z_1 и z_2 лежат на дополнительных лучах.

Левое неравенство - Упражнение. ◀

29. Формула Муавра

Теорема 29.1. $z = r(\cos\varphi + i\sin\varphi): \quad r = |z|, \varphi = arg(z), z \neq 0, n \in \mathbb{Z}$
Тогда $z^n = r^n(\cos\varphi n + i\sin\varphi n)$

▶

- Если $n \in \mathbb{N}$, то очевидно.
- $n = 0$, $1 = 1$.
- $n = -1:$

  $$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{\overline{r(\cos\varphi + i\sin\varphi)}}{r^2} = r^{-1}(\cos\varphi - i\sin\varphi) = r^{-1}(\cos -\varphi + i\sin -\varphi)$$

  чтд.
- Общий случай: $n < 0$.

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

  чтд.

◀

30. Извлечение корней n-й степени из комплексного числа

$n \in \mathbb{N}, z \in \mathbb{Z}$
$\mathfrak{Def}:$ $w \in \mathbb{Z}, w^n = z$
w - корень n-ой степени из z.

- $z = 0 \Rightarrow w^n = 0$. $r = |w|, r^n = 0 \Rightarrow r = 0 \Rightarrow w = 0$

- $z \neq 0$. $|z| = R, arg(z) = \varphi \Rightarrow z = R(\cos\varphi + i\sin\varphi)$ Пусть w существует.

  $r = |w|, \psi = arg(w)$. $w^n = r^n(\cos n\psi + i\sin n\psi) = R(\cos\varphi + i\sin\varphi) = z \Rightarrow r^n = R, r = \sqrt[n]{R}$

  $n\psi = \varphi + 2\pi k, k \in \mathbb{Z} \Rightarrow \psi = \frac{\varphi+2\pi k}{n}, k \in \mathbb{Z}$

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

  Рассмотрим k и k' такие, что $k = ns + k', 0 \leq k' < n$. Тогда $w_k = w_{k'}$, т.к. $arg(w_k) = arg(w_{k'}) + 2\pi s$

  Значит, мы можем рассматривать только $k = 0, \dots, n-1$. При таких k аргументы попарно неэквивалентны.

  Если корни n-ой степени есть, то их $\leq n$, и они совпадают с какими-то из чисел $w_0, w_1, \dots, w_{n-1}$.

  Но для всех $w_k, k = 0, 1, \dots, n-1$ $w_k^n = z \Rightarrow$ корней ровно n, и они ровно такие.

  Второй вариант доказать, что корней $\leq n$ рассмотреть многочлен:

  $w^n = z, w$ - корень $\Rightarrow w$-корень многочлена $t^n - z = 0$, а корней многочлена $\leq n$.

31. Корни из 1. Первообразные корни из 1

$\mathfrak{Def}$: $\varepsilon = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, k = 0, \dots, n-1$

ε - корень из 1 степени n. Если $k = 0$, $\varepsilon = 1$

ε - первообразный корень степени n, если ε не является корнем из 1 меньшей степени.

Утверждение. ε - первообразный корень степени $n \Leftrightarrow (n, k) = 1$

▶ Если дробь k/n сократима, то $k/n = k'/n', n' < n \Rightarrow \varepsilon$ - корень степени n':

$$\varepsilon = \cos\frac{2\pi k}{n'} + i\sin\frac{2\pi k}{n'}$$

◀

Следствие 31.0.1.

Число первообразных корней степени n из 1 равно функции Эйлера: $\varphi(n) = \{k | 1 \leq k \leq n, (k, n) = 1\}$

n	все корни	первообразные корни	$\varphi(n)$
1	1	1	1
2	1,-1	-1	1
3	1,$-\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$	$-\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$	2
4	$\pm 1, \pm i$	$\pm i$	2
6	$\pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$	$\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$	2
8	Упражнение		
12	Упражнение		

Для $n = 6$:

$$x^6 - 1 = (x^2)^3 - 1 = (x^2 - 1)(x^4 + x^2 + 1) = (x^2 + x + 1)(x^2 - x + 1)(x - 1)(x + 1)$$

Упражнение:

1. $n > 2 \Rightarrow \varphi(n)$ - чётно.

2. $n = Const, G_n = \{\varepsilon | \varepsilon$ - корень из 1 степени $n\}$. Тогда $|G_n| = n \Rightarrow G_n$ - группа по умножению и $G_n \cong C_n$.

3. $S = \{z \in \mathbb{C} | |z| = 1\}$ Доказать, что S - группа относительно умножения.

4. $G = \bigcup\limits_{n=1}^{\inf} G_n$ Доказать, что G - группа. Доказать, что в G есть счётная система образующих, но нет конечной системы образующих. Доказать, что каждый элемент G имеет конечный порядок.

Геометрический смысл: Рисунок3. Корни из 1 лежат в вершинах правильного n-угольника, вписанного в круг радиуса 1.
$\varepsilon \in G_n, f : z \mapsto \varepsilon z$, тогда f - это поворот на угол $arg(\varepsilon) = 2\pi k/n$

32. Многочлены Чебышева

Теорема 32.1. $\exists$ многочлены $T_n(x), U_n(x)$ такие, что:

- $\cos n\varphi = T_n(\cos\varphi)$
- $\frac{\sin n\varphi}{sin\varphi} = U_n(\cos\varphi)$ при $\varphi \neq 2\pi k$
- $T_0(x) = 1, T_1(x) = x, T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$
- $U_0(x) = 0, U_1(x) = 1, U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$

$\mathfrak{Def}$: Многочлены T_n и U_n называются многочленами Чебышева первого и второго рода соответсвенно.
Пример:
$T_0 = 1, T_1(x) = x, T_2(x) = 2x^2 - 1$ и $\cos 2\varphi = 2\cos^2\varphi - 1, T_3(x) = 4x^3 - 3x$ и $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$
$U_0 = 0, U_1 = 1, U_2 = 2x$ и $\frac{\sin 2\varphi}{\sin\varphi} = 2\cos\varphi$, $U_3(x) = 4x^2 - 1$ и $\sin 3\varphi = (4\cos^2\varphi - 1)\sin\varphi$
▶
U_n, T_n - многочлены с целыми коэффициентами по их заданию.
$degT_n = n, degU_n = n - 1$(Индукция по n).
$cosn\varphi = T_n(\cos\varphi)$
Индуция по n:
База:
$n = 0, n = 1$
Переход:

$$z = \cos\varphi + i\sin\varphi$$

$$cos(n+1)\varphi = \frac{z^{n+1} + z^{-(n+1)}}{2} = (z + z^{-1})\frac{z^n + z^{-n}}{2} - \frac{z^{n-1} + z^{-(n-1)}}{2} =$$

$$= 2\cos\varphi\cos n\varphi - \cos{(n-1)\varphi} = 2\cos\varphi T_n(\cos\varphi) - T_{n-1}(\cos\varphi) = T_{n+1}(\cos\varphi)$$

Доказательство для U_n упражнение.

$$\frac{\sin n\varphi}{\sin\varphi} = \frac{z^n - z^{-n}}{z - z^{-1}}$$

◀

33. 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 33.1. $\langle M(m, n, R), +\rangle$ 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 33.1. 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. $$((AB)^T)_{ij} = (AB)_{ji} = \sum_{x=1}^{m} a_{jx} b_{xi} = \sum_{x=1}^{m} b^T_{ix} a^T_{xj} = (B^T A^T)_{ij}$$

◀

Заметим, что умножение не коммутативно.

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

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

$\mathfrak{Def}$: 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 33.2. 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.

34. Матричная конструкция поля коплексных 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:

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

$$\begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - a_2b_1 \\ a_2b_1 + a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{pmatrix}$$

Как видно, операции и коммутативны. Единица есть:

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

Таким образом, — коммутативное подкольцо с единицей. ◀

Утверждение. $\mathcal{C}$ — поле.

▶ Найдём обратный:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Leftrightarrow \begin{cases} aa' - bb' = 1 \\ ab' + a'b = 0 \end{cases} \xLeftrightarrow{a,b \neq 0} \begin{cases} a' = a\dfrac{1}{a^2+b^2} \\ b' = -b\dfrac{1}{a^2+b^2} \end{cases}$$

◀

Утверждение.

$$\mathbb{C} \sim \mathcal{C}$$

▶ 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. ◀

35. Тело квантернионов

$$M(2, \mathbb{C})$$
$$\mathcal{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}$$

Теорема 35.1. Тело квантернионов. $\mathcal{H}$ — тело (поле без коммутативности умножения).

▶ Операции замкнуты:

$$\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} + \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 + z_2 & w_1 + w_2 \\ -\bar{w}_1 - \bar{w}_2 & \bar{z}_1 + \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 + z_2 & w_1 + w_2 \\ -\overline{w_1 + w_2} & \overline{z_1 + z_2} \end{pmatrix}$$

$$\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \bar{w}_2 & z_1 w_2 + w_1 \bar{z}_2 \\ -\bar{w}_1 z_2 - \bar{z}_1 \bar{w}_2 & -\bar{w}_1 w_2 + \bar{z}_1 \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \bar{w}_2 & z_1 w_2 + w_1 \bar{z}_2 \\ -\overline{z_1 w_2 + w_1 \bar{z}_2} & \overline{z_1 z_2 + w_1 \bar{w}_2} \end{pmatrix}$$

Свойства сложения уже видны. Единица есть. Найдём обратный:

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \begin{pmatrix} z' & w' \\ -\bar{w'} & \bar{z'} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Leftrightarrow \begin{cases} zz' - w\bar{w'} = 1 \\ zw' + w\bar{z'} = 0 \end{cases} \overset{z, w \neq 0}{\Longleftrightarrow} \begin{cases} z' = \bar{z} \dfrac{1}{|z|^2 + |w|^2} \\ w' = -w \dfrac{1}{|z|^2 + |w|^2} \end{cases}$$

◀

Коммутативности нет:

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

36. Конструкция тела кватернионов как множества четверок вещественных чисел.

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = a\mathbb{1} + b\mathbb{i} + c\mathbb{j} + d\mathbb{k}$$

$$\mathbb{i}^2 = \mathbb{j}^2 = \mathbb{k}^2 = -\mathbb{1}$$
$$\mathbb{i}\mathbb{j} = \mathbb{k} = -\mathbb{j}\mathbb{i}$$
$$\mathbb{j}\mathbb{k} = \mathbb{i} = -\mathbb{k}\mathbb{j}$$
$$\mathbb{k}\mathbb{i} = \mathbb{j} = -\mathbb{i}\mathbb{k}$$

$\mathfrak{Def}$: $\mathbb{H}$ — множество квантернионов как четвёрок вещественных чисел.

$$\mathbb{H} = \{(a, b, c, d) \mid a, b, c, d \in \mathbb{R}\}$$

$$(a_1, b_1, c_1, d_1) + (a_2, b_2, c_2, d_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2)$$
$$(a_1, b_1, c_1, d_1)(a_2, b_2, c_2, d_2) =$$
$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2, a_1 b_2 + a_2 b_1 + c_1 d_2 - c_2 d_1, a_1 c_2 + a_2 c_1 - b_1 d_2 + b_2 d_1, a_1 d_2 + a_2 d_1 + b_1 c_2 - b_2 c_1)$$

Оно натруально изоморфно $\mathcal{H}$.

37. Вещественная и мнимая часть квантернионов. Модуль.

$$\alpha = \underbrace{a\mathbb{1}}_{\text{вещественная}} + \underbrace{b\mathbb{i} + c\mathbb{j} + d\mathbb{k}}_{\text{мнимая}}$$

$$\bar{\alpha} = a\mathbb{1} - b\mathbb{i} - c\mathbb{j} - d\mathbb{k}$$

$$\alpha + \bar{\alpha} \in \mathbb{R}$$

$$\alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_+$$

$\mathfrak{Def}$: Модуль

$$|\alpha| = \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2 + c^2 + d^2}$$
