

Лекции по алгебре

Лектор: Всемиров Максим Александрович

Авторы конспекта: Егор Суворов, Дмитрий Лапшин, Ольга Черникова, Надежда Бугакова, Всеволод Степенев, Глеб Валин, Елизавета Третьякова

Содержание

1	Отображения. Композиция отображений.	4
2	Обратимые отображения и их свойства	5
3	Тождественное отображение	6
4	Равносильность инъективности и обратимости слева	6
5	Равносильность сюръективности и обратимости справа	8
6	Инъективное отображение конечного множества на себя является биективным	9
7	Сюръективное отображение конечного множества на себя является биективным	9
8	Бинарные отношения	10
9	Отношение эквивалентности	11
10	Группы. Простейшие следствия из аксиом группы	11
11	Подгруппы. Критерий того, что непустое подмножество группы является подгруппой. Пересечение подгрупп	12
12	Два эквивалентных определения подгруппы, порожденной множеством	13
13	Гомоморфизмы групп. Свойства гомоморфизмов	13
14	Циклические группы. Теорема о классификации циклических групп с точностью до изоморфности	15
15	Классы смежности	16
16	Теорема Лагранжа и следствия из нее	16
17	Теорема о разложении перестановки в произведение непересекающихся циклов	17
18	Симметрическая группа. Порождение симметрической группы транспозициями	17
19	Четность перестановки. Теорема об изменении четности перестановки при умножении на транспозицию. Следствия из неё.	18
20	Кольца, тела, поля	20

21	Мультипликативная группа кольца	23
22	Кольца многочленов	23
23	Степень многочлена	25
24	Теорема о деление с остатком	26
25	теорема Безу	26
26	Характеристика кольца	27
27	Производная многочлена	28
28	Кратные корни	29
29	Число корней многочлена	30
30	Алгебраические замкнутые поля	32
31	Метод Ньютона	32
32	Метод Лагранжа	33
33	Биномиальная формула	34
34	Конструкция комплексных чисел, как множества пар.	35
35	Алгебраическая форма записи комплексного числа. Комплексное сопряжение. Свойства комплексного сопряжения.	36
36	Модуль комплексного числа. Мультипликативность модуля. Произведение двух сумм двух квадратов.	37
37	Аргумент комплексного числа. Тригонометрическая форма записи. Арифметические операции над комплексными числами в тригонометрической форме.	38
38	Неравенство треугольника	39
39	Формула Муавра	40
40	Извлечение корней n -й степени из комплексного числа	40
41	Корни из 1. Первообразные корни из 1.	41
42	Приложение комплексных чисел	42
42.1	Суммы косинусов и синусов	42
42.2	Понижение степени	42
43	Многочлены Чебышева	43
44	Теорема о пересечении высот треугольника	44
45	Матрицы. Действия над матрицами.	45

46	Матричная конструкция поля комплексных чисел	47
47	Тело квантернионов	48
48	Конструкция тела кватернионов как множества четверок вещественных чисел.	48
49	Вещественная и мнимая часть квантернионов. Модуль.	49
50	Две суммы четырёх квадратов	49

1. Отображения. Композиция отображений.

Def: A, B — множества. $\Gamma_f \subset A \times B$. Γ_f — 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: Есть A, B и $\Gamma_f \subset A \times B$. Говорим, что задано отображение f из A в B с графиком Γ_f , обозначение:

$$\begin{aligned} f : A &\rightarrow B \\ A &\xrightarrow{f} B \\ (a, b) \in \Gamma_f &\Leftrightarrow b = f(a) \end{aligned}$$

Также называем:

A — областью определения ($A = \text{Dom}(f)$),

B — областью назначения ($B = \text{coDom}(f)$).

Def: Равенство отображений $f : A \rightarrow B$ и $f_1 : A_1 \rightarrow B_1$:

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

Def: Композиция отображений $g \circ f$, где $A \xrightarrow{f} B \xrightarrow{g} C$:

$$\begin{aligned} g \circ f : A &\rightarrow C \\ (g \circ f)(a) &= g(f(a)) \\ (a, c) \in \Gamma_{g \circ f} &\Leftrightarrow \exists b \in B: (a, b) \in \Gamma_f \wedge (b, c) \in \Gamma_g \end{aligned}$$

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 отображений ассоциативна. Если $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, то:

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

► Проверим область определения:

$$\begin{aligned} \text{Dom}(h \circ (g \circ f)) &= \text{Dom}(g \circ f) = \text{Dom}(f) = A \\ \text{Dom}((h \circ g) \circ f) &= \text{Dom}(f) = A \end{aligned}$$

Проверим область назначения:

$$\begin{aligned} \text{Dom}(h \circ (g \circ f)) &= \text{coDom}(h) = D \\ \text{Dom}((h \circ g) \circ f) &= \text{coDom}(h \circ g) = \text{coDom}(h) = D \end{aligned}$$

Проверим, что образ одинаков для любого $a \in A$:

$$\begin{aligned} (h \circ (g \circ f))(a) &= h(g \circ f(a)) = h(g(f(a))) \\ ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) = h(g(f(a))) \end{aligned}$$

2. Обратимые отображения и их свойства

Def: Пусть $f : A \rightarrow B$. Тогда f обратимо справа, если $\exists g : B \rightarrow A$:

$$f \circ g = id_B$$

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

$$g \circ f = id_A$$

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

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

Здесь g — отображение, обратное к f , обозначается $g = f^{-1}$.

Теорема 2.1.

1. f обратимо $\iff f$ обратимо слева и справа.
2. f обратимо \Rightarrow обратное отображение единственно.



1. Покажем, что если у f есть и левый и правый обратный, то они совпадают. Пусть g — правый обратный к f , h — левый, тогда:

$$\begin{aligned}(h \circ f) \circ g &= id_A \circ g = g; \\ h \circ (f \circ g) &= h \circ id_B = h; \\ \Rightarrow g &= h\end{aligned}$$

2. Пусть f обратимо и g, h — два обратных. В частности, g — обратное справа, h — обратное слева, то есть по п.1 они совпадают.



Теорема 2.2. Если $A \xrightarrow{f} B \xrightarrow{g} C$, то:

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



1. Из условия знаем, что существуют:

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

Покажем, что $u \circ v$ — правый обратный к $g \circ f$:

$$\begin{aligned}(g \circ f) \circ (u \circ v) &= g \circ (f \circ (u \circ v)) = \\ &= g \circ ((f \circ u) \circ v) = g \circ (id_B \circ v) = g \circ v = id_C;\end{aligned}$$

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 — сюръекция.

Композиция инъективных — инъекцию.

Композиция биективных — биекция.

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

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

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

3. Тожественное отображение

Def: Пусть есть A . Тогда тождественное отображение $id_A : A \rightarrow A$ задаётся как:

$$\forall a \in A: id_A(a) = a.$$

Γ_{id_A} есть диагональ $A \times A$, то есть $\Gamma_{id_A} = \{(a, a) \mid a \in A\}$

Теорема 3.1. $f : A \rightarrow B$, тогда:

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

Области определения и назначения совпадают.

Пусть $a \in A$. Проверим первое равенство:

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

и второе:

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

4. Равносильность инъективности и обратимости слева

Def: $f : A \rightarrow B$. Тогда f — инъективное отображение (инъекция), если:

$$1. \forall a_1, a_2 \in A, \exists b: (a_1, b) \in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2$$

$$2. \forall a_1, a_2 \in A: f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

Обозначается $f : A \rightarrowtail B$.

Def: Отображение $f : A \rightarrow B$ называется сюръективным (сюръекцией, или «отображение на B »), если:

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

Обозначение: $f : A \twoheadrightarrow B$

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

Обозначение: $f : A \rightarrow B$.

$\mathfrak{D}ef$: Образ $C \subset A$: $f(C) = \{b \in B \mid \exists c \in C b = f(c)\}$.

Полный прообраз $D \subset B$: $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$.

$f(f^{-1}(D)) \subseteq D$, но может не совпадать.

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

$f : A \rightarrow B$ сюръективно $\iff f(A) = B$.

Теорема 4.1. $f : A \rightarrow B, g : B \rightarrow A$. Если $g \circ f = id_A$, то f — инъективно, g — сюръективно.



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

$$\begin{aligned} g(f(a_1)) &= g(f(a_2)); \\ (g \circ f)(a_1) &= (g \circ f)(a_2); \\ id_A(a_1) &= id_A(a_2); \\ a_1 &= a_2; \\ \Rightarrow f &\text{ — инъекция} \end{aligned}$$

2. Пусть $a \in A$ и $b = f(a)$, тогда:

$$\begin{aligned} g(f(a)) &= (g \circ f)(a) = id_A(a) = a; \\ a &= g(b); \\ \Rightarrow \forall a \in A, \exists b \in B: a &= g(b) \Rightarrow g \text{ — сюръекция} \end{aligned}$$

Теорема 4.2. Пусть $f : A \rightarrow B$ и $A \neq \emptyset$. Тогда f обратима слева $\iff f$ инъективна.



1. \Rightarrow

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

2. \Leftarrow

Пусть $C = f(A)$. Построим $h_1 : C \rightarrow A$ такое, что

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

. Проверим, что это график:

(a) Определённость для $c \in C$:

$$\begin{aligned} \forall c \in C, \exists a \in A: (a, c) &\in \Gamma_f; \\ \forall c \in C, \exists a \in A: (c, a) &\in \Gamma_{h_1}; \end{aligned}$$

(b) Однозначность. Знаем, что f инъективно.

$$\begin{aligned} \forall a_1, a_2 \in A, \exists b \in B: (a_1, b) &\in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2; \\ \forall a_1, a_2 \in A, \exists b \in C: (a_1, b) &\in \Gamma_f \wedge (a_2, b) \in \Gamma_f \Rightarrow a_1 = a_2; \\ \forall a_1, a_2 \in A, \exists b \in C: (b, a_1) &\in \Gamma_{h_1} \wedge (b, a_2) \in \Gamma_{h_1} \Rightarrow a_1 = a_2; \end{aligned}$$

$\Rightarrow \Gamma_{h_1}$ — график.

Теперь построим $h : B \rightarrow A$. Для этого выберем произвольный $a \in A$ и положим:

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

Проверим, что $h \circ f = id_A$. Рассмотрим $x \in A$:

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



5. Равносильность сюръективности и обратимости справа

Def: Аксиома выбора Пусть есть множество B и семейство X_b : $\forall b \in B: X_b \neq \emptyset$. Тогда

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

такое, что

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

Теорема 5.1.

$f : A \rightarrow B$ — обратимо справа $\Leftrightarrow f$ — сюръективно.



1. \Rightarrow

Очевидно, так как $f(g(B)) = B$.

2. \Leftarrow

Введём семейство X_b для $b \in B$: $X_b = f^{-1}(\{b\}) \neq \emptyset$.

По аксиоме выбора существует $g : B \rightarrow \bigcup_{b \in B} X_b$ (обозначим область назначения g за C).

$f(g(b)) = b$, так как $g(b) \in f^{-1}(\{b\})$.

Покажем, что $C = A$. Так как $X_b = f^{-1}(\{b\}) \subset A$, то $C \subset A$. Обратное включение: возьмём $a \in A$. Знаем, что $a \in X_{f(a)} \Rightarrow a \in C \Rightarrow A \subset C \Rightarrow A = C$. Таким образом $g : B \rightarrow A$.

По построению знаем, что:

$$\begin{aligned} \forall b \in B: f(g(b)) &= b; \\ \forall b \in B: (f \circ g)(b) &= b; \\ f \circ g &= id_B; \\ \Rightarrow f &\text{ обратима справа} \end{aligned}$$



Следствие 5.1.1.

f — обратимо $\Leftrightarrow f$ — биективно.

6. Инъективное отображение конечного множества на себя является биективным

Теорема 6.1. Пусть A — конечное множество и $f : A \rightarrow A$ (инъекция), тогда f — биекция.

► От противного. Возьмём произвольный $a \in A$ не из образа f и положим:

$$a_0 = a; a_{i+1} = f(a_i);$$

Так как A конечно, то $\exists m > n : a_m = a_n$.

Лемма 6.1. $a_{m-n} = a$

► Индукция по n .

• **База:** $n = 0$ и $a_m = a_0$, т.е. $a_{m-n} = a_0 = a$.

• **Переход** $n - 1 \rightarrow n$, при $n \geq 1$:

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

Так как f — инъекция, то $a_{m-1} = a_{n-1}$. Воспользуемся индукционным предположением:

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

Знаем, что $m - n \geq 1 \Rightarrow a = a_{m-n} = f(a_{m-n-1}) \Rightarrow a \in f(A)$. Противоречие. ◀◀

7. Сюръективное отображение конечного множества на себя является биективным

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

► **Краткий план решения:**

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.

1. Строим последовательность $\{a_i\}$:

$$a_0 = a$$

$(a_i : f^{-1}(\{a_i\}) \neq \emptyset)$ так как сюръекция, существует $i + 1$ элемент

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

Множество конечно \Rightarrow

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

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

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

Вернемся к доказательству теоремы.

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

Применем много раз функцию f к обеим частям.

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

Вспомним, что $a_{m-n} = a$.

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

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

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

2.

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

(индукция по k) Возьмем N такое что:

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

3.

$$a, b \in A$$

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

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

8. Бинарные отношения

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

$(a, b) \in R \iff aRb \iff a$ и b находятся в отношении R

Если $R = \emptyset$ — пустое отношение.

Если $R = A^2$ — полное отношение.

Def: Пусть R — бинарное отношение на A , тогда:

1. R рефлексивно, если $\forall a \in A: aRa \iff (a, a) \in R$
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 (ЧУМ).

9. Отношение эквивалентности

Def: R — отношение эквивалентности, если оно рефлексивное, симметрично и транзитивно. Стандартное обозначение: $a \sim b$.

Def: Для $a \in A$ определён класс эквивалентности: $[a] = \{b \in A \mid a \sim b\}$

Теорема 9.1. Пусть $a, b \in A$. Тогда либо $[a] \cap [b] = \emptyset$, либо $[a] = [b]$



1. $[a] \cap [b] = \emptyset$ — всё доказано. Заметим, что тогда $a \not\sim b$, в противном случае $a, b \in [a], [b]$.
2. $\exists c \in [a] \cap [b]$. Тогда $c \sim a$ и $c \sim b \Rightarrow a \sim b$.

Покажем, что $[a] \subset [b]$ и $[b] \subset [a]$:

- (a) $x \in [a] \Rightarrow x \sim a \Rightarrow x \sim b \Rightarrow x \in [b]$
- (b) Аналогично



Множество классов эквивалентности называется фактормножеством по отношению R .

10. Группы. Простейшие следствия из аксиом группы

Def: Бинарная операция на A — отображение $f: A \times A \rightarrow A$

Def: Пусть $G \neq \emptyset, \cdot: G \times G \rightarrow G$. Тогда $\langle G, \cdot \rangle$ — группа, если выполняются следующие свойства:

1. Ассоциативность: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (для любых троек)
2. \exists нейтральный элемент e такой, что $\forall a \in G: a \cdot e = e \cdot a = a$
3. $\forall a \in G, \exists a^{-1}: a \cdot a^{-1} = a^{-1} \cdot a = e$
4. $\forall a, b \in G: a \cdot b = b \cdot a$ — если это свойство выполняется, то группа Абелева (коммутативная).

В дальнейшем под записью ab будет пониматься $a \cdot b$, если, разумеется, не сказано другого.

Пример: Пусть X — множество. $S(X)$ — множество биекций из X в X . Если взять операцию «композиция», получится группа. Ассоциативность композиции знаем, нейтральный элемент — id_X , обратимость биекции тоже знаем. Коммутативность отсутствует.

Пример: Пусть $X = \{1, \dots, n\}$. $S_n = S(\{1, \dots, n\})$ — симметрическая группа степени n , группа перестановок чисел от 1 до n .

Теорема 10.1. Простейшие свойства групп.

1. Единственность нейтрального
2. Единственность обратного
3. Уравнения вида $ax = b$, $ya = b$ имеют решение, причем единственное
4. $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$



1. Пусть существуют два нейтральных элемента e_1, e_2 :

$$e_2 = e_1 e_2 = e_1 \Rightarrow e_2 = e_1$$

2. Пусть a', a'' — обратные к a , тогда:

$$\begin{aligned} a' a a'' &= (a' a) a'' = e a'' = a''; \\ a' a a'' &= a' (a a'') = a' e = a'; \\ a' &= a''; \end{aligned}$$

3. $ax = b \iff b^{-1}ax = e \Rightarrow x = (b^{-1}a)^{-1}$. Так мы доказали одним махом и существование, и единственность (так как обратный элемент существует и единственен).
4. $(a_1 \dots a_n)(a_1^{-1} \dots a_n^{-1}) = (a_1 \dots a_{n-1})(a_n a_n^{-1})(a_{n-1}^{-1} \dots a_1^{-1})$. Центральная скобка равна e . Таким образом избавляемся от всех переменных, получаем, что правая скобка обратна левой.



11. Подгруппы. Критерий того, что непустое подмножество группы является подгруппой. Пересечение подгрупп

Def: Пусть $f: A \rightarrow B$ и $C \subset A$. Введём g — сужение f на C :

$$\begin{aligned} g: C &\rightarrow B \\ \forall c \in C: g(c) &= f(c) \end{aligned}$$

Def: $H \subset G$ — подгруппа в G , если она является группой относительно сужения операции в G на H .

Def: Множество A замкнуто относительно операции \cdot , если $\forall a, b \in A: a \cdot b \in A$

Множество A замкнуто относительно операции взятия обратного, если $\forall a \in A: a^{-1} \in A$

Теорема 11.1. Достаточные условия для подгруппы. Для того, чтобы доказать, что H — подгруппа G ($H \neq \emptyset, H \subset G$), достаточно проверить только замкнутость относительно операций \cdot и взятия обратного элемента.

► Ассоциативность к нам переходит из исходной группы G .

Если существует обратный элемент, то $aa^{-1} = e \in H$

Так как есть замкнутость, то операция \cdot действует из $H \times H$ в H .

Следствие 11.1.1. Пусть $\emptyset \neq H \subset G$ и $\forall a, b \in H: ab^{-1} \in H \Rightarrow H$ — подгруппа.

► Нейтральный элемент есть: $a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

Замкнутость относительно взятия обратного: $\forall a \in H: ea^{-1} \in H \Rightarrow a^{-1} \in H$.



Замкнутость относительно операции \cdot : $\forall a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$. ◀

Теорема 11.2. H_α — подгруппы в G . Тогда $\bigcap H_\alpha$ — подгруппа в G . ▶

$$\begin{aligned} H &= \bigcap H_\alpha; \\ e \in H_\alpha &\Rightarrow e \in H \Rightarrow H \neq \emptyset; \\ a, b \in H &\Rightarrow \forall \alpha: a, b \in H_\alpha \Rightarrow ab \in H_\alpha \Rightarrow ab \in H; \\ a \in H &\Rightarrow \forall \alpha: a \in H_\alpha \Rightarrow a^{-1} \in H_\alpha \Rightarrow a^{-1} \in H; \end{aligned}$$

12. Два эквивалентных определения подгруппы, порожденной множеством

Def: Замыканием множества относительно операции — множество всех элементов, получаемых из элементов этого множества применением данной операции.

Аналогично определяется замыкание относительно множества операций.

В частности, для группы это замыкание A будет выглядеть как:

$$\{a_1^{z_1} a_2^{z_2} \dots | a_i \in A, z_i = \pm 1\}$$

, где A — данное множество.

Def: Подгруппа, порожденная множеством — замыкание этого множества относительно операций \cdot и взятия обратного элемента

Def: Подгруппа, порожденная множеством — пересечение всех подгрупп, содержащих это множество

REM: Предыдущие два определения действительно задают подгруппы, именно это мы доказывали в предыдущих теоремах

Теорема 12.1. Равносильность определений подгруппы, порожденной множеством.

Пусть $M \subset G$, G — группа, A — замыкание M относительно операций \cdot и взятия обратного элемента, $B = \bigcap \{H \in 2^G | H \supset M \wedge H \text{ — подгруппа } G\}$.

Тогда $A = B$.

▶ $A \subset B$, так как любая подгруппа, содержащая M , должна содержать замыкание M .

Но так как A — подгруппа, то $B \subset A$.

$\Rightarrow A = B$. ◀

13. Гомоморфизмы групп. Свойства гомоморфизмов

Def: H, G — группы, $f: G \rightarrow H$

1. f — гомоморфизм, если $\forall a, b \in G: f(ab) = f(a)f(b)$
2. f — изоморфизм, если f — и гомоморфизм, и биекция

Def: H, G — группы. Если между H, G есть изоморфизм, то группы называются изоморфными: $H \cong G$

Теорема 13.1. Свойства гомоморфизма.

1. $f(e_G) = e_H$
2. $f(x^{-1}) = (f(x))^{-1}$

3. $f(G)$ — подгруппа H

4. $G \xrightarrow{f} H \xrightarrow{g} K$, f, g — гомоморфизмы, тогда $g \circ f : G \rightarrow K$ — тоже гомоморфизм

5. $f : G \rightarrow H$ — изоморфизм, тогда $f^{-1} : H \rightarrow G$ — изоморфизм



1. $f(e_G) = f(e_G e_G) = f(e_G) f(e_G) = e_H e_H = e_H$

2. $f(e_G) = f(x x^{-1}) = f(x) f(x^{-1}) = e_H \Rightarrow f(x^{-1}) = (f(x))^{-1}$

3. Покажем замкнутость относительно операции \cdot

$$\begin{aligned} e_H &\in f(G); \\ c, d \in f(G) &\iff \exists a, b \in G : c = f(a), d = f(b); \\ cd = f(a)f(b) &= f(ab) \Rightarrow cd \in f(G); \end{aligned}$$

Покажем замкнутость относительно взятия обратного (из пункта 2 теоремы):

$$f(a)^{-1} = f(a^{-1}) \in f(G)$$

Таким образом, $f(G)$ — подгруппа.

4. Пусть $a, b \in G$, тогда:

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

5.

$$\begin{aligned} c, d &\in H; \\ \exists a, b \in G : c &= f(a); d = f(b); \\ a &= f^{-1}(c); b = f^{-1}(d); \\ f^{-1}(cd) &= ab = f^{-1}(c)f^{-1}(d); \end{aligned}$$

Тогда f^{-1} — изоморфизм

Следствие 13.1.1.

1. $G \cong G$ (взяли id_G).

2. $G \cong H \Rightarrow H \cong G$

3. $G \cong H, H \cong K \Rightarrow G \cong K$

Пример: пусть $G = H = \langle \mathbb{R}, + \rangle$, тогда $x \rightarrow e^x$ — изоморфизм.



14. Циклические группы. Теорема о классификации циклических групп с точностью до изоморфности

Def: Группа G — циклическая группа, если она порождена одним элементом (то есть замыкание этого элемента в группе порождает группу). Обозначение: $G = \langle a \rangle$

Примеры:

1. $\langle \mathbb{Z}, + \rangle = \langle 1 \rangle$
2. $e = \langle e \rangle$ — тривиальная группа
3. $n \in \mathbb{N}$, C_n — группа поворотов на угол $\frac{2\pi k}{n}$, $C_n = \langle \frac{2\pi}{n} \rangle$

Def: Степени

$$\begin{aligned} i > 0 : a^i &= \underbrace{aa \dots a}_i \\ a^{-i} &= \underbrace{a^{-1}a^{-1} \dots a^{-1}}_i \\ a^{m+n} &= a^m a^n \end{aligned}$$

Теорема 14.1. Лемма о делении с остатком. $\forall n \in \mathbb{N}, a \in \mathbb{Z} : \exists!$ (существуют и единственны) $q, r \in \mathbb{Z} : 0 \leq r < n : a = qn + r$

► Существование:

$$\begin{aligned} q &= \left\lfloor \frac{a}{n} \right\rfloor \\ nq &\leq a < nq + n \\ r &= a - nq \end{aligned}$$

Единственность (от противного):

$$\begin{aligned} a &= nq_1 + r_1 = nq_2 + r_2; 0 \leq r_1, r_2 < n; \\ 0 &= n * (q_1 - q_2) + (r_1 - r_2), n|q_1 - q_2| = |r_1 - r_2| \end{aligned}$$

Так как $n \geq 1$, то левая часть хотя бы n , а правая — строго меньше n . Противоречие. ◀

Теорема 14.2. Теорема о классификации циклических групп с точностью до изоморфности. Всякая циклическая группа изоморфна либо $(\mathbb{Z}, +)$, либо C_n , $n \in \mathbb{N}$

► $G = \langle a \rangle$. Рассмотрим отображение $i \rightarrow a^i$, $i \in \mathbb{Z}$.

- Если все элементы различны, то получили изоморфизм $(i + j \leftrightarrow a^{i+j} = a^i a^j)$
- В противном случае $\exists i > j : a^i = a^j \Rightarrow a^{i-j} = e$. Пусть n — наименьшее число такое, что $a^n = e$. Тогда $G = \{e = a^0, a^1, a^2, \dots, a^{n-1}\}$, $G \leftrightarrow C_n$, $a^k a^l = a^{(k+l) \bmod n}$

Def: G — группа. Если G конечна, то порядком G называют число элементов в ней, иначе порядок равен ∞

Def: $a \in G$ и $n \in \mathbb{N}$ — минимальное число такое, что $a^n = e$. Тогда n — порядок элемента a . Если такого элемента нет, то порядок a равен ∞

REM: Альтернативное определение: порядок элемента равен порядку циклической группы, порожденной этим элементом

15. Классы смежности

Есть группа G и ее подгруппа H . Введем отношение $\sim: a \sim b \iff a^{-1}b \in H$. Докажем, что это отношение — отношение эквивалентности:

$$\begin{aligned} a^{-1}a &= e \in H \Rightarrow a \sim a; \\ a \sim b &\Leftrightarrow a^{-1}b \in H \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \Leftrightarrow b \sim a; \\ \left. \begin{aligned} a \sim b &\Leftrightarrow a^{-1}b \in H; \\ b \sim c &\Leftrightarrow b^{-1}c \in H; \end{aligned} \right\} &\Rightarrow a^{-1}c = a^{-1}bb^{-1}c \in H \Rightarrow a \sim c; \end{aligned}$$

Рассмотрим класс эквивалентности элемента a :

$$\begin{aligned} [a] &= \{b \in G \mid a^{-1}b \in H\} = \\ &= \{b \in G \mid \exists h \in H: a^{-1}b = h\} = \\ &= \{b \in G \mid \exists h \in H: b = ah\} \end{aligned}$$

Словами: класс эквивалентности a — это образ отображения $f: H \rightarrow G$, где $f(h) = ah$.

Def: $aH = [a]$ — левый класс смежности по подгруппе H , Ha — правый класс смежности по подгруппе H (определяется симметрично).

Рем: Левые классы смежности для разных элементов или не пересекаются, или совпадают, так как aH — класс эквивалентности. Аналогично для правых классов.

Пример: $G = S_3$ — группа перестановок из трех элементов. Пусть $H = \langle (12) \rangle = \{e, (12)\}$. Тогда $(13)H = \{(13), (123)\}$, $H(13) = \{(13), (132)\}$.

16. Теорема Лагранжа и следствия из нее

Лемма 16.1. $H \subset G$, $f: H \rightarrow aH$, $f(h) = ah$, H — подгруппа. Тогда f — биекция. В частности, из этого будет следовать, что $|H| = |aH|$, то есть мощности всех левых классов смежности равны друг другу

► Заметим, что это отображение — сюръекция по определению aH (у каждого элемента есть прообраз). Докажем, что это инъекция.

От противного: пусть $ah_1 = ah_2$, домножим слева на a^{-1} , получим $h_1 = h_2$.

Таким образом, f — биекция. ◀

Def: Число левых классов смежности по H называется индексом H в G . Обозначение: $[G : H]$

Теорема 16.1. Теорема Лагранжа. Пусть G — конечная группа, возьмём элемент a и его левые классы смежности aH_α . Очевидно, что $G = \bigcup aH_\alpha$ и $H_{\alpha_1} \cap H_{\alpha_2} = \emptyset$. Тогда $|G| = [G : H] \cdot |H|$

► Все эти классы имеют одинаковую мощность, равную $|H|$ (по лемме). Тогда $|G| = [G : H] \cdot |H|$, так как эти классы не пересекаются. ◀

Следствие 16.1.1. Количество правых и левых классов смежности одинаково (достаточно провести аналогичные действия для правых классов смежности)

Следствие 16.1.2. Порядок любой подгруппы делит порядок конечной группы.

Следствие 16.1.3. Порядок любого элемента делит порядок конечной группы (рассмотрим циклическую подгруппу, порожденную этим элементом)

Следствие 16.1.4. Группа порядка p (где p — простое число) циклическа, так как порядок любого элемента равен либо 1 (e), либо p (все остальные), а тогда все элементы кроме e порождают всю группу порядка p .

17. Теорема о разложении перестановки в произведение непесекающихся циклов

Теорема 17.1. Всяка перестановка может быть представлена в виде произведения непесекающихся циклов.

Def: $\sigma \in S_n, j \in \{1, \dots, n\}$. j – неподвижная точка относительно σ , если $\sigma(j) = j$

► Индукция по m – числу подвижных точек σ (число подвижных точек = n – число неподвижных точек).

База: $m = 0 \Leftrightarrow n$ – число неподвижных точек, то есть $\forall j \in \{1, \dots, n\} \sigma(j) = j$, то есть $\sigma = id$

Переход: $m > 0 \Rightarrow \exists i : \sigma(i) \neq i$ – с него и начнём.

$$i_1 = i$$

$$i_2 = \sigma(i_1)$$

$$i_3 = \sigma(i_2) = \sigma^2(i_1)$$

...

И так до тех пор, пока не встретим повторение (а его мы обязательно встретим, потому что чисел у нас всего n – конечное число)

$$i_1 \mapsto i_2 \mapsto \dots \mapsto i_k \mapsto i_{k+1} \text{ – уже встречался.}$$

Заметим, что $i_{k+1} \neq i_j \forall j \in \{2, \dots, n\}$ в силу инъективности σ (иначе у какого-то элемента было бы два различных прообраза – i_{j-1} и i_{k+1}) $\Rightarrow i_{k+1} = i_1$.

Итак, мы получили цикл $\tau = (i_1, i_2, \dots, i_k)$.

Рассмотрим $\sigma\tau^{-1}$.

Неподвижные точки $\sigma\tau^{-1}$ – это неподвижные точки σ плюс $i_1, i_2, \dots, i_k \Rightarrow \sigma\tau^{-1}$ и τ – незацепляющиеся \Rightarrow (по индукционному предположению) $\sigma\tau^{-1} = \prod_{j=1}^r \tau_j$.

Домножим обе части равенства на τ и получим, что $\sigma = (\prod_{j=1}^r \tau_j)\tau$ – произведение незацепляющихся циклов.



Теорема 17.2. Следствие. S_n порождается всеми циклами (так как для каждой σ можно выбрать свой набор).

Небольшой забавный бонус:

$\sigma = \prod_{j=1}^r \tau_j$, где τ_j – попарно непесекающиеся циклы. Тогда $\sigma^m = (\prod_{j=1}^r \tau_j)^m$, так как непесекающиеся циклы коммутируют.

Def: Прядок цикла – его длина.

Def: Прядок σ – наименьшее общее кратное длин циклов при разложении σ на непесекающиеся циклы.

Def: Цикловым типом $\sigma \in S_n$ называется набор длин её непесекающихся циклов, упорядоченных по неубыванию, + набор единиц для неподвижных элементов.

18. Симметрическая группа. Порождение симметрической группы транспозициями

S_n – биекции на $\{1, \dots, n\}$

S_n – симметрическая группа (группа перестановок) степени n .

$\tau, \sigma \in S_n$

В произведении $\sigma\tau$ первой выполняется перестановка τ .

Def: Цикл (i_1, i_2, \dots, i_k) – это перестановка σ , такая что $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_k) = i_1$ и $\sigma(j) = j$, где $j \notin \{i_1, \dots, i_k\}, 1 \leq j \leq n$

$(i_1, i_2, \dots, i_k) = (i_2, i_3, \dots, i_k) = \dots = (i_s, i_{s+1}, \dots, i_k, i_1, \dots, i_{s-1})$
 k – длина цикла. Порядок цикла длины k равен k . $(i_1, i_2, \dots, i_k)^k = id$

Def: Транспозиция – цикл длины 2. (i, j) – i и j меняются местами, остальные остаются на месте.

Def: $(i_1, i_2, \dots, i_k), (j_1, j_2, \dots, j_s)$ – циклы. Эти циклы называются незацепляющимися (непересекающимися) если $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_s\} = \emptyset$

Их легко перемножать. Если σ, τ – непересекающиеся циклы, то $\sigma\tau = \tau\sigma$.

Теорема 18.1. S_n порождается транспозициями.

► Покажем, что любой цикл (i_1, i_2, \dots, i_k) есть произведение транспозиций $(i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$. Заметим, что если применить это произведение к перестановке (вот просто взять и последовательно применить справа налево все транспозиции аккуратно), то мы и получим тот же самый результат, как и от применения исходного цикла.

Осталось лишь заметить, что каждая из остальных $n - k$ точек либо неподвижная, либо также лежит на каком-то цикле – абить циклы на произведение транспозиций мы только что научились.



19. Четность перестановки. Теорема об изменении четности перестановки при умножении на транспозицию. Следствия из неё.

Def: $\sigma \in S_n; i, j \in \{1, \dots, n\}$. i, j образуют инверсию относительно σ , если $i < j$, а $\sigma(i) > \sigma(j)$.

Def: $INV(\sigma)$ – множество всех инверсий относительно σ .

Def: σ – четная, если $|INV(\sigma)|$ четно.

Def: σ – нечетная, если $|INV(\sigma)|$ нечетно.

Теорема 19.1. $\sigma \in S_n, \tau = (ij)$ — транспозиция. Тогда σ и $\sigma\tau$ имеют различную четность..

► Не умаляя общности, будем считать, что $i < j$. Тогда

$$\sigma = (\sigma(1) \dots \sigma(i) \dots \sigma(j) \dots \sigma(n))$$

$$\sigma\tau = (\sigma(1) \dots \sigma(j) \dots \sigma(i) \dots \sigma(n))$$

σ		$\sigma\tau$	
$(kl), \{k, l\} \cap \{i, j\} = \emptyset$	есть инверсия	$(kl), \{k, l\} \cap \{i, j\} = \emptyset$	есть инверсия
$(kl), \{k, l\} \cap \{i, j\} = \emptyset$	есть инверсия	$(kl), \{k, l\} \cap \{i, j\} = \emptyset$	есть инверсия
$(ki), k < i$	есть	$(kj), k < i$	есть
$(ki), k < i$	нет	$(kj), k < i$	нет
$(ki), k > j$	есть	$(kj), k > j$	есть
$(kj), k < i$	есть	$(ki), k < i$	есть
$(kj), k < i$	нет	$(ki), k < i$	нет
$(kj), k > j$	есть	$(ki), k > j$	есть
$(kj), k > j$	нет	$(ki), k > j$	нет
$\sigma(\sigma(i)\sigma(k)\sigma(j))$			
$\sigma\tau(\sigma(j)\sigma(k)\sigma(i))$			
$(ki), i < k < j$	есть	$(kj), i < k < j$	нет
$(ki), i < k < j$	нет	$(kj), i < k < j$	есть
$(kj), i < k < j$	есть	$(ki), i < k < j$	нет
$(kj), i < k < j$	нет	$(ki), i < k < j$	есть
$(i\ j)$	есть	$(i\ j)$	нет
$(i\ j)$	нет	$(i\ j)$	есть

Как глубокоуважаемый читатель уже догадался, самое интересное здесь - это последние 6 строк.

$r = \{k | i < k < j \wedge (ik) \text{ образует инверсию} \}$

$s = \{k | i < k < j \wedge (kj) \text{ образует инверсию} \}$

$|Inv(\sigma\tau)| = |Inv(\sigma)| - r + (j - i - 1 - r) - s + (j - i - 1 - s) \pm 1 \Rightarrow \text{четность изменилась.}$



Теорема 19.2. Следствия.

1. $\sigma = \prod_{j=1}^r \tau_j$, τ_j – транспозиция.

σ четна(нечетна) \Leftrightarrow число сомножителей четно(нечетно, соответственно).



” \Leftarrow : ” id четна. При каждом добавлении τ_j четность меняется.

” \Rightarrow ” : σ четна, r – число транспозиций, и если у него другая четность, то приходим к противоречию.



2. $\sigma \in S_n$, τ – транспозиция. σ и $\tau\sigma$ имеют различную четность. (из первого следствия)
3. При перемножении двух перестановок их четность меняется так же, как при суммировании их четностей как чисел.
4. Множество четных перестановок – подгруппа S_n (знакопеременная группа). Обозначается A_n .



(a) Непусто(id четна)

(b) Замкнуто(по третьему следствию)

(c) Обратный элемент к $\sigma = \prod_{j=1}^{2r} \tau_j$ – это $\sigma^{-1} = \prod_{j=1}^{2r} \tau_{2r+1-j}$



20. Кольца, тела, поля

$$\begin{aligned} A &\neq \emptyset \\ + : A \times A &\rightarrow A \\ \cdot : A \times A &\rightarrow A \end{aligned}$$

1. ассоциативность 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:

$$\forall a, b \in A a + b = b + a$$

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 элемента по умножению:

$$\forall a \in A \setminus \{0\} \exists a^{-1} \in A a \cdot a^{-1} = a^{-1} \cdot a = 1$$

9. дистрибутивность:

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

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

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

Def: Кольцо, в котором выполнена аксиома 6 - коммутативное кольцо

Def: Кольцо, в котором выполнена аксиома 7 - кольцо с единицей

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

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



$$a' = a' a a'' = a''$$



5. если в кольце с 1 у элемента a есть 2 левых обратных, то левых обратных к a бесконечно много (упражнение)

6. $0 \cdot a = a \cdot 0 = 0$



$$\begin{aligned} a \cdot 0 + a \cdot 0 &= a(0 + 0) = a \cdot 0 + (a \cdot 0)' \\ a \cdot 0 + a \cdot 0 + (a \cdot 0)' &= a \cdot 0 + (a \cdot 0)' = a \cdot 0 = 0 \end{aligned}$$

второе равенство аналогично



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



$$\begin{aligned} a + (-a) &= 0 \\ ab + (-a)b &= (a + (-a))b = ab = 0 \\ (-a)b &= -ab \end{aligned}$$

второе равенство аналогично



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



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



Def: A - кольцо (тело, поле)

$A \supseteq B \neq \emptyset$ - подкольцо (подтело, подполе), если являются кольцом (телом, полем), относительно сужения операций на B

REM:

- $B \neq \emptyset, B \supset A$ - 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:
 $\forall a, b \in B a + b \in B$
 $\forall a \in B a - a \in B$
 $\forall a, b \in B ab \in B$
 $\forall a \in B \setminus a^{-1} \in B$

Def: A, B - кольца

$f : A \rightarrow B$

f - гомоморфизм, если:

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

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

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

$$0 = a, 0 = 0 \cdot b$$

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

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 20.1. A - область целостности $a \in A \setminus \{0\}$

$$ab = ac \Rightarrow b = c$$

►

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

◀

21. Мультипликативная группа кольца

Def: A - кольцо с 1

$$A^* = \{a \in A : \exists b \in A ab = ba = 1\}$$

(A^*, \cdot) - мультипликативная группа кольца

Теорема 21.1. A^* - группа по умножению



$$A^* \ni 1_A$$

$$A^* \times A^* \rightarrow A^*$$

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

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

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

$b_2 b_1$ - 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, $K^* = K \setminus \{0\}$
- $\mathbb{Z}, \mathbb{Z}^* = -1, 1$

22. Кольца многочленов

Def: A - коммутативное кольцо с 1

$$A[x] = \{\underbrace{a_1, a_2, \dots}_{\text{почти все нули}} \mid a_i \in A, \text{ почти все нули} \}$$

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

REM: «почти все» — все кроме конечного числа

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

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

$$\text{Def: } "\cdot" : (a_1, a_2, \dots) \cdot (b_1, b_2, \dots) = (c_1, c_2, \dots)$$

$$\text{где } c_n = \sum_{i=0}^n a_i b_{n-i} = \sum_{i+j=n} a_i b_j$$

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



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

Теорема 22.1. $(A[x], +, \cdot)$ - коммутативное кольцо с 1

1. аксиомы 1 - 4 покомпонентно выполнены в A

2. $\exists 0 = (0, 0, 0, \dots)$

3. $\exists 1 = (1, 0, 0, \dots)$ $1 \cdot \alpha = \alpha \cdot 1 = \alpha$

► по определению операции умножения:

$$(a_0, \underbrace{a_0 + a_1 \cdot 1}_{a_1}, \underbrace{\ddots}_{a_2}) = \alpha$$

4. коммутативность:

$$\beta = (b_0, b_1, \dots), \alpha = (a_0, a_1, \dots) \Rightarrow \alpha\beta = \beta\alpha$$



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

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

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

5. дистрибутивность (упражнение)

6. ассоциативность:

$$\alpha = (a_0, a_1, \dots), \beta = (b_0, b_1, \dots), \gamma = (c_0, c_1, \dots)$$

$$\alpha\beta = d, (\alpha\beta)\gamma = e$$

$$\beta\gamma = f, \alpha(\beta\gamma) = g$$

$$e_k = g_k \forall k$$



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

меняем порядок суммирования

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

делаем замену $l = i - j$

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

23. Степень многочлена

Алтернативная запись:

$$a = (a, 0, 0, \dots)$$

$$x = (0, 1, 0, \dots)$$

$$x^i = (0, \dots, \underset{i\text{-ая позиция}}{1}, \dots)$$

$$(a_0, a_1, a_2, \dots) = (a_0, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + \dots =$$

$$= (a_0, 0, 0, \dots) \cdot (1, 0, 0, \dots) + (0, a_1, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots) + \dots = a_0 + a_1x + a_2x^2 + \dots + a_nx^n - \text{альтерна-}$$

тивная запись в форме многочлена

$$\text{Def: } A[x] = \{a_0 + a_1x + \dots + a_nx^n | n \in \mathbb{N} \cup \{0\} \wedge a_i \in A\}$$

$f \in A[x]$ - многочлен

$$\text{Def: } f = a_0 + a_1x + \dots + a_nx^n, a_n \neq 0, f \neq 0$$

n - степень многочлена f , $n = \deg f$

$$f = 0 \Rightarrow \deg f = -\infty$$

Теорема 23.1.

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

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

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



1. следует из доказательства замкнутости относительно сложения:

$$f = a_0 + \dots + a_nx^n \wedge a_n \neq 0$$

$$g = b_0 + \dots + b_mx^m \wedge a_m \neq 0$$

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

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

3. для области целостности:

$$a_n \neq 0, b_m \neq 0$$

$$c_{n+m} = a_nb_m \neq 0 \Rightarrow \deg(fg) = \deg f + \deg g$$

$$\text{Если } f = 0 \vee g = 0, \text{ тогда } \deg(fg) = \underbrace{\deg f}_{-\infty} + \underbrace{\deg g}_{-\infty} = -\infty \Leftrightarrow fg = 0$$

Следствие 23.1.1. Если A - область целостности, то и $A[x]$ - область целостности

$$\blacktriangleright f, g \neq 0$$

$$\deg f, \deg g \geq 0$$

$$\deg(fg) \geq 0 \Rightarrow fg \neq 0$$

$$\text{REM: } A = \mathbb{Z}/4\mathbb{Z}, f = 2x, g = 2x^2 \Rightarrow fg = 4x^2 = 0$$

Следствие 23.1.2. A - область целостности $\Rightarrow (A[x])^* = A^*$

$$\blacktriangleright " \Rightarrow " fg = 1?$$

$$\deg f + \deg g = 0 \text{ многочлены вида } (*, 0, \dots)$$

$$\deg f = \deg g = 0 \Rightarrow f, g \in A : fg = 1$$

" \Leftarrow " если элемент обратим в кольце A , то он обратим и в кольце многочленов

24. Теорема о делении с остатком

Теорема 24.1. A - коммутативное кольцо с 1 $f, g \in A[x]$

$$f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, n = \deg f, a_n \in A^*$$

тогда $\exists q, r \in A[x] : g = qf + r, \deg r < \deg f$

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

► **Существование:**

Индукция по $m = \deg g$:

База: $m < n$

$$q = 0, r = g$$

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

$$g = b_mx^m + \dots + b_0$$

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

коэффициент при x^m в g_1 : $b_m - b_ma_n^{-1}a_n = 0 \Rightarrow \deg g_1 < m$

по предположению индукции $g_1 = fq_1 + r_1, \deg r_1 < \deg f$, тогда:

$$r = r_1$$

$$q = q_1 + b_ma_n^{-1}x^{m-n}$$

$$g = fq + r$$

Единственность:

A - область целостности

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

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

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

РЕМ: условие обратимости старших коэффициентов существенно: $A = \mathbb{Z}$

$$f = 2x, g = x^2 + 1$$

в $\mathbb{Z}[x]$ разложения: $g = fq + r, q, r \in \mathbb{Z}[x], \deg r < \deg f$ - не существует

25. теорема Безу

Значение многочлена в точке

$A \subset B$ — коммутативное кольцо с 1.

$$f \in A[x], f = a_nx^n + \dots + a_0, c \in B$$

$$f(c) = a_nc^n + \dots + a_0 = \sum_{k=0}^n a_kc^k \text{ — значение многочлена в точке}$$

$$A[x] \subset B[x]$$

$$f \in A[x]$$

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

$$c \rightarrow f(c)$$

$$(\tilde{f} + (*)\tilde{g})(c) = \tilde{f}(c) + (*)\tilde{g}(c)$$

$$f + \tilde{(*)}g = \tilde{f} + (*)\tilde{g}$$

Теорема 25.1. (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 теореме о делении с остатком получаем:

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

$$r = r_0 \in A$$

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

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

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

Def: $A, B, A \subseteq B$, коммутативные с 1

$$f \in A[x]$$

$c \in B$ - корень f , если $f(c) = 0$

Следствие 25.1.1. 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 $\Rightarrow f(x) = (x - c)g(x) + f(c) = (x - c)g(x) \Rightarrow (x - c) | f$

26. Характеристика кольца

A - кольцо с 1

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

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

Если такого n нет, то считается, что $\text{char} A = 0$

Примеры:

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

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

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

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



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

$$2. \text{char} A > 0 \underbrace{1 + \dots + 1}_n = 0, n > 1 \text{ т.к. в поле } 1 \neq 0$$

$$n = ab, 1 < a, b < n$$

$$\text{по дистрибутивности} \Rightarrow \underbrace{1 + \dots + 1}_a = 0 \vee \underbrace{1 + \dots + 1}_b = 0 \Rightarrow \text{наименьшее } n, \text{ чтобы } \underbrace{1 + \dots + 1}_n = 0$$

должно быть простым



27. Производная многочлена

A - коммутативное кольцо с 1

$$f \in A[x]$$

$$f = a_n x^n + \dots + a_0$$

$$K \in \mathbb{N}, K \cdot a = \underbrace{a + \dots + a}_K = \underbrace{1 + \dots + 1}_K a$$

$$0 \cdot a = 0$$

$$\text{Def: } f' = n \cdot a_n x^{n-1} + \dots + 2a_2 x + a_1 = \sum_k = 0^n k a_n x^{k-1}$$

$$(k = 0 - \text{фиктивное слагаемое, } 0 \cdot a_0 x^{-1} = 0)$$

Теорема 27.1. свойства производной

$$1. (f + g)' = f' + g'$$

$$f_1 + \dots + f_k = f'_1 + \dots + f'_k$$

$$2. c \in A, (c \cdot f)' = c \cdot f'$$

$$3. (fg)' = f'g + fg'$$

$$4. (f_1 \cdot f_2 \cdot \dots \cdot f_k)' = f'_1 \cdot f_2 \cdot \dots \cdot f_k + f_1 \cdot f'_2 \cdot \dots \cdot f_k + \dots + f_1 \cdot \dots \cdot f'_k$$

$$5. A - \text{поле}, f \in A[x]$$

$$\bullet \text{char} A = 0 \quad f' = 0 \Leftrightarrow f = \text{const}$$

$$\bullet \text{char} A = p > 0 \quad f' = 0 \Leftrightarrow f \in A[x^p]$$



1. упражнение

2. упражнение

3. доказываем по частям:

$$\bullet f = x^n, g = x^m$$

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

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

$$\begin{aligned} (fg)' &= \left(\sum_{k=0}^m c_k x^n x^k \right)' = \sum_{k=0}^m c_k (x^n x^k)' = \\ &= \sum_{k=0}^m c_k (f' x^k + f k x^{k-1}) = f' \sum_{k=0}^m c_k x^k + f \sum_{k=0}^m k c_k x^{k-1} = f'g + fg' \end{aligned}$$

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

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

4. упражнение

5. следствие п.4

6. • $\text{char} A = 0$

$$\begin{aligned}f &= c_0 + c_1 x + \dots + c_n x^n \\ 0 &= f' = c_1 + 2c_2 x + \dots + n c_n x^{n-1} \\ \forall k, k c_k &= 0 \underbrace{(1 + 1 + \dots + 1)}_{\neq 0, k} c_k = 0 \Rightarrow f = c_0 = \text{const}\end{aligned}$$

обратное очевидно

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

$$\begin{aligned}k c_k &= \underbrace{(1 + 1 + \dots + 1)}_k c_k = \underbrace{(\underbrace{1 + \dots + 1}_p + \dots + \underbrace{1 + \dots + 1}_p + \underbrace{1 + \dots + 1}_r)}_q c_k = \underbrace{(1 + \dots + 1)}_{\neq 0, r, \dots, 0 < r < \text{char} A} c_k \\ &\Rightarrow c_k = 0\end{aligned}$$

$$\begin{aligned}" \Leftarrow " \quad f &= c_0 + c_p x^p + c_{2p} x^{2p} + \dots \in A[x^p] \\ \text{Если } f &= \sum_{j=0}^r c_{jp} x^{jp}, \text{ то } f' = \sum_{j=0}^r j \underbrace{p}_{=0, \text{char} A=p} c_{jp} x^{jp-1} = 0\end{aligned}$$



28. Кратные корни

A — поле. $f \in A[x], f \neq 0$ с — 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 с — корень f кратности k .

с — 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 28.1. A — поле, $\text{char} A = 0, f \in A[x], f \neq 0$

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

1. с — корень f .

2. с — корень f' кратности $k - 1$.



\Rightarrow

$$\begin{aligned}f &= (x - c)^k g(x), g(c) \neq 0 \Rightarrow c \text{ — корень} \\ f' &= k(x - c)^{k-1} g(x) + (x - c)^k g' = (x - c)^{k-1} (kg + (x - c)g') \\ &\Rightarrow (x - c)^{k-1} | f'\end{aligned}$$

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 $l - 1$.

$$l - 1 = k - 1$$

$$l = k$$

REM: 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 28.1.1. A — поле характеристики 0 . $0 \neq f \in A[x]$, c — корень f кратности $\geq k \Leftrightarrow$ выполняется равенство

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

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

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

29. Число корней многочлена

Лемма 29.1. 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 29.2. 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 $a-1 \rightarrow a$ 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 29.1. 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 29.1.1. 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 29.1.2. Если A — область целостности.

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

30. Алгебраические замкнутые поля

Def: Поле A — алгебраически замкнуто, если любой $f \in A[x] \setminus A$ имеет в A хотя бы 1 корень.

Теорема 30.1. 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 $\deg f$ корней (с учетом кратности).
4. $\forall f \in A[x]$ с $\deg f \geq 1$ полностью раскладывается на линейные множестве в колце многочленов.

► $1 \Leftrightarrow 2$ (следствие теоремы Безу)

$3 \Rightarrow 1$ очевидно.

$1 \Rightarrow 3$ Индукция и $\deg f$

1. **База:** $\deg f = 1$

$$ax = b$$

$$x = \frac{b}{a} \text{ — корень.}$$

2. **Переход:** $\deg f \geq 2$

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

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 $\deg f$.

31. Метод Ньютона

Def: A — поле. $\frac{x_1}{y_1} \mid \frac{x_2 \dots}{y_2 \dots} \mid \frac{x_n}{y_n}$

$$x_i \neq x_j$$

Интерполяционная задача: найти многочлен f , $\deg f < n$, $f(x_i) = y_i, i = 1, \dots, n$

Пусть f имеет решение f

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

$$f_1 = f + gh \text{ — тоже решение.}$$

$$f_1(x_1) = f(x_i) + g(x_i)h(x_i) = f(x_i) = y_i$$

Теорема 31.1. Единственность. В данной постановке задача имеет не более одного решения.

► Пусть f, f_1 — решение одной задачи.

$$f(x_i) = f_1(x_i) = y_i, \deg f, \deg f_1 < n$$

$f - f_1$ принимают 0 в $x_1 \dots x_n$

$$\deg(f - f_1) < n \Rightarrow f - f_1 = 0 \Rightarrow f = f_1$$

Метод Ньютона $\frac{x_1 \mid x_2 \dots \mid x_n}{y_1 \mid y_2 \dots \mid y_n} f_i(x), \deg f_i < i$

f_i решает интерпретиционную задачу на первых i точках.

$$1. i = 1 \quad f_1(x) = y_1$$

$$2. i \rightarrow i + 1$$

$$f_i \rightarrow f_{i+1}$$

$$f_{i+1}(x) = f_i(x) + c_i(x - x_1) \dots (x - x_i)$$

$$y_{i+1} = f_{i+1}(x_{i+1}) = f_i(x_{i+1}) + c_i(x_{i+1} - x_1) \dots (x_{i+1} - x_i)$$

$$c_i = \frac{y_{i+1} - f_i(x_{i+1})}{(x_{i+1} - x_1) \dots (x_{i+1} - x_i)}$$

$$\deg f_{i+1} < i + 1$$

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

32. Метод Лагранжа

$$\frac{x_1 \mid x_2 \dots x_i \mid x_n}{0 \mid 0 \dots 1 \mid 0}$$

$$\deg L_i < n$$

$$L_i = \frac{(x - x_1) \dots (x - x_{i-1})(x - x_{i+1}) \dots (x - x_n)}{(x_i - x_1) \dots (x_i - x_n)}$$

$$\frac{x_1 \mid x_2 \dots \mid x_n}{y_1 \mid y_2 \dots \mid y_n}$$

$$f = y_1 L_1 + y_2 L_2 + \dots + y_n L_n$$

$$f(x_i) = \sum_{j=1}^n y_j L_j(x_i) = y_i L_i(x_i) = y_i$$

$$f(x) = \sum_{k=1}^n y_k L_k$$

$$L_k(x) = \frac{(x - x_1) \dots (x - x_n)}{(x_k - x_1) \dots (x_k - x_n)}$$

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

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

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

$$(x - x_1)1 \dots (x - x_n) + \dots$$

$$g'(x_k) \text{ — знаменатель } L_k \quad \deg f \leq n$$

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

33. Биномиальная формула

Def:

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

кольцо многочленов от n переменных.

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

$$x_1 \rightarrow x_1$$

$$x_2 \rightarrow x_2$$

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

$A[x_1, \dots, x_n]$ — 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 33.1.

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



$$\begin{aligned} C_n^k + C_n^{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \\ &= \frac{n!(k+1) + n!(n-k)}{(k+1)!(n-k)!} = \frac{n!(n+1)}{(k+1)!(n+1-(k+1))!} = C_{n+1}^{k+1} \end{aligned}$$



	-	0	1	2	3	4
	0	1	-	-	-	-
Def:	1	1	1	-	-	-
	2	1	2	1	-	-
	3	1	3	3	1	-
	4	1	4	6	4	1

Теорема 33.1. 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. $n \rightarrow n + 1$

$$\begin{aligned}
(x + y)^{n+1} &= (x + y)^n(x + y) = \left(\sum_{k=0}^n C_n^k x^k y^{n-k}\right)(x + y) = \\
&= \sum_{k=0}^n C_n^k x^{k+1} y^{n-k} + \sum_{k=0}^n C_n^k x^k y^{n-k+1} = \\
&= C_n^n x^{n+1} + \sum_{k=0}^{n-1} C_n^k x^{k+1} y^{n-k} + \sum_{k=1}^n C_n^k x^k y^{n-k+1} + C_n^0 y^{n+1} = \\
&= C_{n+1}^{n+1} x^{n+1} + \sum_{k=1}^n C_n^{k-1} x^k y^{n+1-k} + \sum_{k=1}^n C_n^k x^k y^{n-k+1} + C_{n+1}^0 y^{n+1} = \\
&= C_{n+1}^{n+1} x^{n+1} + \sum_{k=1}^n (C_n^{k-1} + C_n^k) x^k y^{n+1-k} + C_{n+1}^0 y^{n+1} = \\
&= \sum_{k=0}^{n+1} C_{n+1}^k x^k y^{n+1-k}
\end{aligned}$$

Следствие 33.1.1.

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

34. 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 34.1. \mathbb{R}^2 с введенными операциями является полем.

Def: Это поле называется полем комплексных чисел \mathbb{C} (Complex).

► Упр.

Некоторые заметки:

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

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

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

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

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

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

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

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

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

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

$$\mathbb{C} \supseteq \varphi(\mathbb{R}) = \{(a, 0) | a \in \mathbb{R}\}$$

$\varphi(\mathbb{R}) \cong \mathbb{R}$, поэтому говорят, что $\mathbb{R} \subseteq \mathbb{C}$, имея в виду, что $\varphi(\mathbb{R}) \subseteq \mathbb{C}$

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

Def: $(a, b) = (a, 0) * (1, 0) + (b, 0) * (0, 1) = a + bi$ - алгебраическая запись числа.

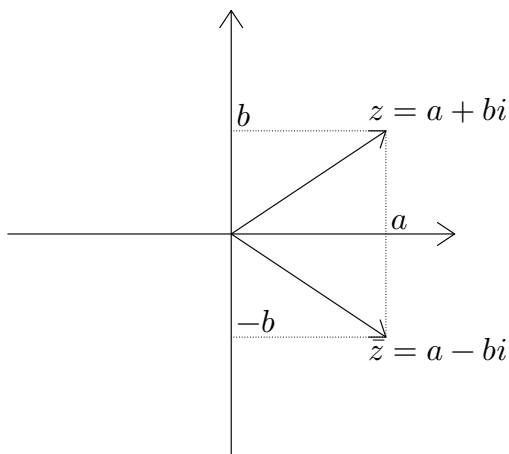
a называется вещественной частью комплексного числа ($a = \operatorname{Re}(z), z \in \mathbb{C}$)

b называется мнимой частью комплексного числа ($b = \operatorname{Im}(z), z \in \mathbb{C}$)

Def: $z \in \mathbb{C}, z = a + bi, a, b \in \mathbb{R}$

\bar{z} называется комплексно сопряжённым с z , если $\bar{z} = a - bi$

REM: Сопряжение \equiv симметрия относительно вещественной оси.



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: $f(z) = a_0 + a_1z + \dots + a_nz^n$

$$\overline{f(z)} = \overline{a_0 + a_1z + \dots + a_nz^n} = \overline{a_0} + \overline{a_1z} + \dots + \overline{a_nz^n} = \overline{a_0} + \overline{a_1} \cdot \overline{z} + \dots + \overline{a_n} \cdot \overline{z^n} = a_0 + a_1\overline{z} + \dots + a_n\overline{z^n} = a_0 + a_1\overline{z} + \dots + a_n\overline{z}^n = f(\overline{z}) \quad \blacktriangleleft$$

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

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

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

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.

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

$$z \in \mathbb{C}$$

$$z\overline{z} = a^2 + b^2$$

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 $k = 1, 2, 4, 8$.

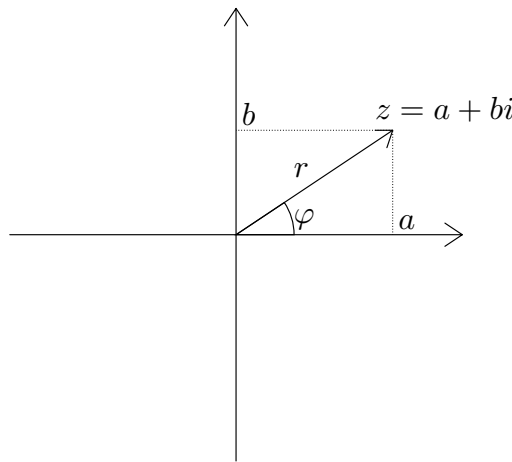
$k = 1$: мультипликативность $|\mathbb{R}|$

$k = 2$: мультипликативность $|\mathbb{C}|$

$k = 4$: мультипликативность модуля кватернионов

$k = 8$: мультипликативность модуля октав

37. Аргумент комплексного числа. Тригонометрическая форма записи. Арифметические операции над комплексными числами в тригонометрической форме.



$z \in \mathbb{C}$, $z = a + bi \Rightarrow (a, b)$ - 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.

Def: φ - аргумент $z(\arg z)$

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.

Def: $[\varphi] = \{\varphi + 2\pi k | k \in \mathbb{Z}\}$ $\text{Arg } z = [\varphi] \Leftrightarrow \arg z = \varphi$

Пусть $z = a + bi |z| = \sqrt{a^2 + b^2}$. $\arg z = ?$:

1. $a > 0$

$$\frac{b}{a} = \tg \varphi, \varphi \in (-\pi/2, \pi/2) \Rightarrow \arg z = \arctg\left(\frac{b}{a}\right)$$

2. $a < 0$

$$\varphi \in (\pi/2, 3\pi/2) \Rightarrow \arg z = \pi + \arctg\left(\frac{b}{a}\right)$$

3. $a = 0, b > 0$

$$\arg z = \pi/2$$

4. $a = 0, b < 0$

$$\operatorname{arg} z = -\pi/2$$

Def: Тригонометрическая форма записи числа

$z = a + bi = r \cos \varphi + i r \sin \varphi = r(\cos \varphi + i \sin \varphi)$, 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:

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

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

38. Неравенство треугольника

Теорема 38.1.

$$||z_1| - |z_2|| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|$$

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:

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

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

$$\begin{aligned} (z_1 \pm z_2)^2 &= (r_1 \cos \varphi_1 \pm r_2 \cos \varphi_2)^2 + (r_1 \sin \varphi_1 \pm r_2 \sin \varphi_2)^2 = \\ &= r_1^2 \cos^2 \varphi_2 \pm 2r_1 r_2 \cos \varphi_1 \cos \varphi_2 + r_2^2 \cos^2 \varphi_2 + r_1^2 \sin^2 \varphi_1 \pm 2r_1 r_2 \sin \varphi_1 \sin \varphi_2 + r_2^2 \sin^2 \varphi_2 = \\ &= r_1^2 + r_2^2 \pm 2r_1 r_2 (\cos \varphi_1 \cos \varphi_2 + \sin \varphi_1 \sin \varphi_2) = r_1^2 + r_2^2 \pm 2r_1 r_2 \cos(\varphi_1 - \varphi_2) \\ |z_1 \pm z_2|^2 &\leq r_1^2 + r_2^2 + 2r_1 r_2 = (r_1 + r_2)^2 = (|z_1| + |z_2|)^2 \end{aligned}$$

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 — аналогично через

$$|z_1 \pm z_2|^2 \geq r_1^2 + r_2^2 - 2r_1 r_2 = (r_1 - r_2)^2 = (|z_1| - |z_2|)^2$$



39. Формула Муавра

Теорема 39.1. $z = r(\cos \varphi + i \sin \varphi)$, $z \neq 0$, $n \in \mathbb{Z}$. Тогда

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



- Если $n \in \mathbb{N}$, то очевидно из умножения в тригонометрической форме.
- Если $n = 0$, то написано $1 = 1$.
- Если $n = -1$:

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

- Если $n < 0$:

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



40. Извлечение корней n -й степени из комплексного числа

Def: $n \in \mathbb{N}, z \in \mathbb{C}$

$$w \in \mathbb{C}: w^n = z$$

w — корень n -й степени из z .

- $z = 0 \Rightarrow w^n = 0$. $r = |w| \wedge r^n = 0 \Rightarrow r = 0 \Rightarrow w = 0$.
- $z \neq 0$. $|z| = R$, $\arg z = \varphi$. $r = |w|$, $\psi = \arg w$.

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

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

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

Рассмотрим k и k' такие, что

$$k = ns + k', 0 \leq k' < n$$

Тогда $w_k = w_{k'}$, так как $\arg w_k = \arg w_{k'} + 2\pi s$. Значит, мы можем рассматривать только $k = 0..(n-1)$. При таких k аргументы попарно неэквивалентны.

Если корни n -й степени есть, то их не более n , и они совпадают с какими-то из чисел w_0, w_1, \dots, w_{n-1} . Но все w_k являются корнями, значит корней ровно n , и они ровно такие. Второй вариант доказать, что корней не более n — рассмотреть многочлен. w — корень, тогда w — корень многочлена $t^n - z$, а корней многочлена не больше n .

41. Корни из 1. Первообразные корни из 1.

Def: ε — корень из 1 степени n , если

$$\varepsilon = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, k = 0..(n-1)$$

Def: ε — первообразный корень единицы степени n , если ε не является корнем меньшей степени.

Утверждение. ε — первообразный корень степени n тогда и только тогда, когда $(n, k) = 1$.

► Если дробь $\frac{k}{n}$ сократима, то

$$\frac{k}{n} = \frac{k'}{n'}; n' < n$$

Но тогда ε — корень степени n' :

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

Следствие 41.0.1. Число первообразных корней степени n из 1 равно функции Эйлера

$$\varphi(n) = |\{k \mid 1 \leq k \leq n, (k, n) = 1\}|$$

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		

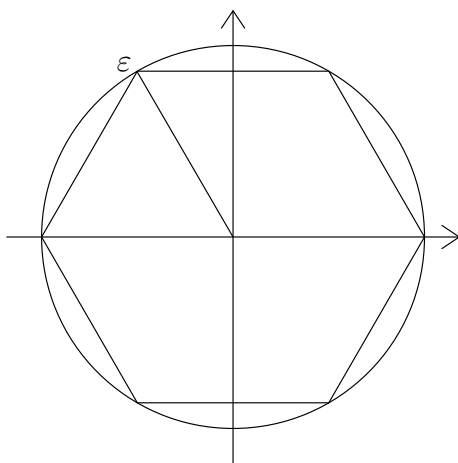
Для $n = 6$:

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

Упражнения:

- $n > 2 \Rightarrow \varphi(n)$ — чётно.
- $n = \text{const}$, $G_n = \{ \varepsilon \mid \varepsilon \text{ — корень из 1 степени } n \}$. Тогда $|G_n| = n \Rightarrow G_n$ — группа по умножению и $G_n \cong C_n$.
- $S = \{ z \in \mathbb{C} \mid |z| = 1 \}$. Доказать, что S — группа относительно умножения.
- $G = \bigcup_{n=1}^{\infty} G_n$. 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:



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 $\arg \varepsilon = \frac{2\pi k}{n}$

42. Приложение комплексных чисел

42.1. Суммы косинусов и синусов

$$A = 1 + \cos \varphi + \cos 2\varphi + \dots + \cos n\varphi$$

$$\varphi \neq 2\pi k, k \in \mathbb{Z}$$

$$B = 0 + \sin \varphi + \sin 2\varphi + \dots + \sin n\varphi$$

$$\begin{aligned} A + Bi &= 1 + (\cos \varphi + i \sin \varphi) + (\cos 2\varphi + i \sin 2\varphi) + \dots + (\cos n\varphi + i \sin n\varphi) = \\ &= 1 + (\cos \varphi + i \sin \varphi) + (\cos \varphi + i \sin \varphi)^2 + \dots + (\cos \varphi + i \sin \varphi)^n \end{aligned}$$

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

$$A + Bi = 1 + z + z^2 + \dots + z^n \stackrel{z \neq 1}{=} \frac{1 - z^{n+1}}{1 - z}$$

$$A = \operatorname{Re} \frac{1 - z^{n+1}}{1 - z}, B = \operatorname{Im} \frac{1 - z^{n+1}}{1 - z}$$

$$z = w^2, w = \cos \frac{\varphi}{2} + i \sin \frac{\varphi}{2}$$

$$\begin{aligned} \frac{1 - z^{n+1}}{1 - z} &= \frac{1 - w^{2(n+1)}}{1 - w^2} = \frac{w^{2(n+1)} - 1}{w^2 - 1} = \frac{w^{n+1}}{w} \frac{w^{n+1} - w^{-(n+1)}}{w - w^{-1}} = \\ &= w^n \frac{w^{n+1} - \bar{w}^{n+1}}{w - \bar{w}} = \left(\cos \frac{n\varphi}{2} + i \sin \frac{n\varphi}{2} \right) \frac{2i \sin \frac{\varphi(n+1)}{2}}{2i \sin \frac{\varphi}{2}} \end{aligned}$$

$$A = \frac{\cos \frac{n\varphi}{2} \sin \frac{(n+1)\varphi}{2}}{\sin \frac{\varphi}{2}}; B = \frac{\sin \frac{n\varphi}{2} \sin \frac{(n+1)\varphi}{2}}{\sin \frac{\varphi}{2}}$$

42.2. Понижение степени

$$\cos^n \varphi; \sin^n \varphi$$

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

$$z^{-1} = \bar{z}; \cos \varphi = \frac{z + z^{-1}}{2}$$

$$\begin{aligned} \cos^n \varphi &= \left(\frac{z + z^{-1}}{2} \right)^n = \frac{1}{2^n} \sum_{k=0}^n C_n^k z^{n-k} (z^{-1})^k = \frac{1}{2^n} \sum_{k=0}^n \binom{n}{k} z^{n-2k} = \\ &= \frac{1}{2^n} \left(\sum_{0 \leq k < \frac{n}{2}} \binom{n}{k} z^{n-2k} + \sum_{\frac{n}{2} < k \leq n} \binom{n}{k} z^{n-2k} + \begin{cases} \binom{n}{\frac{n}{2}} & n \text{ четно} \\ 0, & n \text{ нечетно} \end{cases} \right) \end{aligned}$$

$$n - k \Leftrightarrow k', \frac{n}{2} < k \leq n \Rightarrow 0 \leq k' < \frac{n}{2}; \binom{n}{k} = \binom{n}{n-k} = \binom{n}{k'}; z^{n-2k} = z^{n-2(n-k')} = z^{-(n-2k')}$$

$$\cos^n \varphi = \frac{1}{2^n} \left(\sum_{0 \leq k < \frac{n}{2}} \binom{n}{k} (z^{n-2k} + z^{-(n-2k)}) + \begin{cases} \binom{n}{\frac{n}{2}} & n \text{ четно} \\ 0 & n \text{ нечетно} \end{cases} \right)$$

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

$$\cos^n \varphi = \frac{1}{2^n} \left(\sum_{0 \leq k < \frac{n}{2}} \binom{n}{k} \cos(n-2k)\varphi + \begin{cases} C_n^{\frac{n}{2}} & n \text{ четно} \\ 0 & n \text{ нечетно} \end{cases} \right)$$

43. Многочлены Чебышева

Теорема 43.1. Существуют 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 $\varphi \neq 2\pi k$
- $T_0(x) = 1$, $T_1(x) = x$, $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$
- $U_0(x) = 0$, $U_1(x) = 1$, $U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x)$

Def: Многочлены T_n и U_n называются многочленами Чебышева первого и второго рода соответственно.

Пример:

$$T_0(x) = 1$$

$$T_1(x) = x$$

$$T_2(x) = 2x^2 - 1$$

$$T_3(x) = 4x^3 - 3x$$

$$U_0(x) = 0$$

$$U_1(x) = 1$$

$$U_2(x) = 2x$$

$$\cos 0\varphi = 1$$

$$\cos 1\varphi = \cos \varphi$$

$$\cos 2\varphi = 2 \cos^2 \varphi - 1$$

$$\cos 3\varphi = 4 \cos^3 \varphi - 3 \cos \varphi$$

$$\frac{\sin 0\varphi}{\sin \varphi} = 0$$

$$\frac{\sin 1\varphi}{\sin \varphi} = 1$$

$$\frac{\sin 2\varphi}{\sin \varphi} = 2 \cos \varphi$$

$$U_3(x) = 4x^2 - 1$$

$$\sin 3\varphi = (4 \cos^2 \varphi - 1) \sin \varphi$$

► U_n, T_n — многочлены с целыми коэффициентами по их заданию. $\deg T_n = n$, $\deg U_n = n - 1$ (индукция по n).

Докажем $\cos n\varphi = T_n(\cos \varphi)$ индукцией по n .

База: $n = 0, 1$.

Переход:

$$\begin{aligned} z &= \cos \varphi + i \sin \varphi \\ \cos(n+1)\varphi &= \frac{z^{n+1} + z^{-(n+1)}}{2} = (z + z^{-1}) \frac{z^n + z^{-n}}{2} - \frac{z^{n-1} + z^{-(n-1)}}{2} = \\ &= 2 \cos \varphi \cos n\varphi - \cos(n-1)\varphi = 2 \cos \varphi T_n(\cos \varphi) - T_{n-1}(\cos \varphi) = T_{n+1}(\cos \varphi) \end{aligned}$$

Таким образом, для T_n всё доказано.

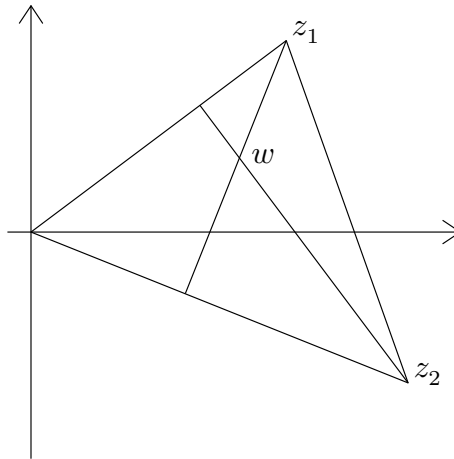
Доказательство для U_n : аналогично через

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



44. Теорема о пересечении высот треугольника

Теорема 44.1. Высоты треугольника. 3 высоты треугольника пересекаются в одной точке.



$(a, b), (c, d)$ — точки. Тогда $(a, b) \perp (c, d) \Leftrightarrow ac + bd = 0$ — скалярное произведение.

$$z_1 = a + bi, z_2 = c + di, \operatorname{Re}(z_1 \bar{z}_2) = ac + bd$$

Известно, что $(z_1 - w) \perp z_2$ и $(z_2 - w) \perp z_1$.

Надо доказать, что $w \perp z_1 - z_2$.

$$\begin{aligned} \begin{cases} z_1 - w \perp z_2 \Leftrightarrow \operatorname{Re}((z_1 - w)\bar{z}_2) = 0 \\ z_2 - w \perp z_1 \Leftrightarrow \operatorname{Re}((z_2 - w)\bar{z}_1) = 0 \end{cases} &\Rightarrow \operatorname{Re}(z_1 \bar{z}_2 - z_2 \bar{z}_1 + w(\bar{z}_1 - \bar{z}_2)) = 0 \Leftrightarrow \\ &\Leftrightarrow \operatorname{Re}(z_1 \bar{z}_2 - z_2 \bar{z}_1) + \operatorname{Re}(w(\bar{z}_1 - \bar{z}_2)) = 0 \end{aligned}$$

$z_1 \bar{z}_2 - z_2 \bar{z}_1$ — чисто мнимое, поэтому

$$\operatorname{Re}(z_1 \bar{z}_2 - z_2 \bar{z}_1) \Rightarrow \operatorname{Re}(w(\overline{z_1 - z_2})) = 0$$

Упражнение:

1. Медианы.
2. Биссектрисы.

45. 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 45.1. $\langle M(m, n, R), + \rangle$ 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

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

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 45.1. 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. $BC \rightleftharpoons D: m \times l, AD \rightleftharpoons E: n \times l, AB \rightleftharpoons F: n \times k, FC \rightleftharpoons G: n \times l$. 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 45.2. 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.

46. 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 и 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. \mathcal{C} — поле.

► Найдём обратный:

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

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. ◀

47. 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 47.1. 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:

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

Коммутативности нет:

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

48. Конструкция тела кватернионов как множества четвёрок вещественных чисел.

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

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

$$\mathfrak{i}\mathfrak{j} = \mathfrak{k} = -\mathfrak{j}\mathfrak{i}$$

$$\mathfrak{j}\mathfrak{k} = \mathfrak{i} = -\mathfrak{k}\mathfrak{j}$$

$$\mathfrak{k}\mathfrak{i} = \mathfrak{j} = -\mathfrak{i}\mathfrak{k}$$

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

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

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

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

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, a_1b_2 + a_2b_1 + c_1d_2 - c_2d_1, a_1c_2 + a_2c_1 - b_1d_2 + b_2d_1, a_1d_2 + a_2d_1 + b_1c_2 - b_2c_1)$$

Оно натурально изоморфно \mathcal{H} .

49. Вещественная и мнимая часть квантернионов. Модуль.

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

Def: Сопряжение

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

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

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

Def: Модуль

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

50. Две суммы четырёх квадратов

Можно показать, что модуль мультипликативен.

$$\begin{aligned} |\alpha\beta| &= |\alpha||\beta| \Leftrightarrow (a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = \\ &= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 + \\ &\quad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2 \end{aligned}$$