Университет ИТМО
Факультет ПИиКТ

ЛИНЕЙНАЯ АЛГЕБРА

I СЕМЕСТР

Лектор: *Дмитрий Валерьевич Карпов*

Автор: *Александр Калиев*
Проект на GitHub

осень 2023

Содержание

1 2023-09-08 – 1

1.1 Ring and field

Let K be a set, we call it's elements *numbers*. Two operations are also defined:

$+ : K \times K \mapsto K$

$\cdot : K \times K \mapsto K.$

Properties:

1. (Ассоциативность $+$): $\forall a,b,c \in K : (a+b)+c = a+(b+c)$
2. (Commutativity $+$): $\forall a,b \in K : a+b = b+a$
3. Zero: $\exists 0 \in K : a+0 = a$
4. (Inverse element for $+$): $\forall a \in K \exists(-a) \in K : a+(-a) = 0$
5. (Distributivity): $\forall a,b,c \in K : a\cdot(b\cdot c) = (a+b)\cdot c \;\&\; a\cdot(b+c) = a\cdot b + a\cdot c$
6. (Associativity $\cdot$): (ab)c = a(bc)
7. (Commutativity $\cdot$): ab = ba
8. (Neutral element $\cdot$): $\exists 1 : \forall a \in K : 1\cdot a = a.$
9. (Inverse element for $\cdot$):

$$\forall a \in K \setminus \{0\}\, \exists (a)^{-1} \in K : a\cdot(a)^{-1} = (a)^{-1}\cdot a = 1$$

- ▷ $1-6 \Rightarrow K - ring$
- ▷ $1-7 \Rightarrow K - commutative\ ring$
- ▷ $1-6\ \&\ 8 \Rightarrow K - ring\ with\ 1$
- ▷ $1-6, 8, 9 \Rightarrow K - body$
- ▷ $1-9 \Rightarrow K - field$

Свойство 1.1.1. Zero is the only one.

Доказательство. Let there be 0_1 and 0_2. Then:

$$0_1 = 0_1 + 0_2 = 0_2 + 0_1 = 0_2.$$

□

Свойство 1.1.2. $\forall a \in K$, the reverse element for $+$ is the only one.

Доказательство. Let there be 2 reverse elements for $a \in K$: b_1 & b_2. Then:

$$b_1 = b_1 + 0 = b_1 + (a + b_2) = (b_1 + a) + b_2 = 0 + b_2 = b_2$$

□

Свойство 1.1.3. $\forall a \in K : -(-a) = a$

Доказательство. $a = a + ((-a) + (-(-a))) = (a + (-a)) + (-(-a)) = (-(-a))$ □

Свойство 1.1.4. No more than 1 unit in a ring.

Доказательство. Let there be 1_1 & 1_2. Then:

$$1_1 = 1_1 \cdot 1_2 = 1_2.$$

□

Определение 1.1. Let K be a ring with 1. An element $a \in K$ is reversible, if $\exists a^{-1} \in K$

◁ in the fiels, all elements except 0 are reversible.

Свойство 1.1.5. Let K be a ring with 1. Then, $\forall a \in K \exists$ no more than 1 reverse element for $\cdot$.

Доказательство. Let there be 2 reverse elements: b_1 & b_2. Then:

$$b_1 = b_1 \cdot 1 = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = 1 \cdot b_2 = b_2$$

□

Свойство 1.1.6. Let K be a ring with 1. Then, $\forall$ reversible $a \in K : (a^{-1})^{-1} = a$

Доказательство. $a = a \cdot 1 = a \cdot (a^{-1} \cdot (a^{-1})^{-1}) = (a \cdot a^{-1}) \cdot (a^{-1})^{-1} = 1 \cdot (a^{-1})^{-1} = (a^{-1})^{-1}$ □

Свойство 1.1.7. -0 = 0

Доказательство. Follows from the $0 + 0 = 0$. □

Свойство 1.1.8. If K is a ring with 1, then $1^{-1} = 1$

Доказательство. Follows from $1 \cdot 1 = 1$ □

Определение 1.2. ▷ Substraction – addition a reverse element for $+$:

$$a - b := a + (-b).$$

▷ Division on a reversible element b is a multiplication by b^{-1}:

$$\frac{a}{b} := a \cdot b^{-1}.$$

1.2 Sub-field and sub-ring

Определение 1.3.

- ▷ Let $K \subset L$ (both are rings with the same operations). Then K is a **sub-ring** of L, and L is an **supra-ring** of K.
- ▷ Let $K \subset L$ (both are fields with the same operations). Then K is a **sub-field** of L; L is a **supra-field** of K.

Лемма 1.1. *Let L be a ring, $K \subset L$. Conditions:*

1. *Closedness of* $+ : \forall a,b \in K : \quad a + b \in K$
2. *Closedness of* $\cdot : \forall a,b \in K \quad a \cdot b \in K$
3. *Existence of reverse element for* $+$
   $\forall a \in K \quad \exists - a \in K$
4. *Existence of reverse element for* $\cdot$
   $\forall a \in K, a \neq 0, \quad \exists a^{-1} \in K.$

Then K is a field, then, it's a sub-field of L.

Доказательство.

- ▷ By Lemma 1, K – commutative sub-ring of L.
- ▷ It remains to check the existence of 1 in K.
  Consider any non-zero element $a \in K$. Then $a^{-1} \in K$, and that means, that $a \cdot a^{-1} = 1 \in K$.

□

1.3 Homomorphism

Определение 1.4. ◁ Let K, L be a rings. Then a relation $f : K \mapsto L$ is called **homomorphism**, if $\forall a,b \in K$:

$$f(a + b) = f(a) + f(b) \ \& \ f(ab) = f(a)f(b)$$

A kernel of homomorphism f is denoted as $\operatorname{Ker} f = \{x \in K : f(x) = 0\}$ An image of homomorphism f is denoted as $\operatorname{Im} f = \{y \in L : \exists x \in K : f(x) = y\}$.

Свойство 1.3.1. If $f : K \mapsto L$ is homomorphism, then $f(0_K) = 0_L$.

Доказательство. $f(0_K) = f(0_K + 0_k) = f(0_K) + f(0_K)$. Substracting from left and right side $f(0_k)$, we get $f(0_K) = 0_L$ □

Лемма 1.2. *Let K, L be rings, $f : K \mapsto L$ – homomorphism of rings. Then:*

- ▷ $\operatorname{Ker} f$ *is a sub-ring of* K.
- ▷ $\operatorname{Im} f$ *is a sub-ring of* L.

Доказательство. It's enough to check conditions from Lemma 1.

1. ▷ Let $a,b \in \operatorname{Ker} f$. Then $f(a+b) = f(a) + f(b) = 0 + 0 = 0 \Rightarrow a + b \in \operatorname{Ker} f$.
   ▷ $f(ab) = f(a)f(b) = 0 \cdot 0 = 0 \Rightarrow ab \in \operatorname{Ker} f$.
   ▷ $f(-a) = -f(a) = -0_L = 0_L$.
2. ▷ Let $y, y' \in \operatorname{Im} f$, and $x, x' \in K$ are such that $f(x) = y$ & $f(x') = y'$.
   ▷ Then $y + y' = f(x) + f(x') = f(x + x') \in \operatorname{Im} f$ & $y \cdot y' = f(x) \cdot f(x') \in \operatorname{Im} f$.
   ▷ $-y = -f(x) = f(-x) \in \operatorname{Im} f$.

□

1.4 Homomorphism types

- ▷ Let $f : K \mapsto L$ – homomorphism of rings.
- ▷ If f is an injection, then f is **monomorphism**
- ▷ If f is a surjection ($\operatorname{Im} f = L$), then f is an **epimorphism**
- ▷ **If f is a biection, then f is isomorphism**
- ▷ **Isomorphism = monomorphism + epimorphism.**

Лемма 1.3. *Let $f : K \mapsto L$ be a homomorphism of rings. Then f is monomorphism if and only if* $\operatorname{Ker} f = \{0\}$.

Доказательство. $\Rightarrow$

- ▷ If f is monomorphism, then f is an injection.
- ▷ Let $a \in \operatorname{Ker} f$. From $f(a) = 0 = f(0)$ implies, that $a = 0$ (because of the injection f).

$\Leftarrow$

- ▷ Let $f(a) = f(b)$. Then $f(a - b) = f(a) - f(b) = 0$.

- ▷ That means that $a - b \in \operatorname{Ker} f = \{0\}$, from this $a = b$. In conclusion, f is an injection, and that means f is monomorphism.

□

Лемма 1.4. *Let $f : K \mapsto L$ be an isomorphism of rings. Then $f^{-1} : L \mapsto K$ is an isomorphism of rings.*

Доказательство.

- ▷ It's enough to proof that f^{-1} is homomorphism (because relation that is reverse to biection is a biection).
- ▷ Consider any a,$b \in L$.
- ▷ Let $w = f^{-1}(a + b) - f^{-1}(a) - f^{-1}(b)$. Because of f is a biection, we have:

$$f(w) = f(f^{-1}(a + b)) - f(f^{-1}(a)) - f(f^{-1}(b)) = a + b - a - b = 0$$

- ▷ From $(f(w) = 0 = f(0)\ )$ and because of f is a biection, we implie that $w = 0$.
- ▷ Therefore, $f^{-1}(a + b) = f^{-1}(a) + f^{-1}(b)$
- ▷ Let $z = f^{-1}(ab) - f(f^{-1}(a)) \cdot f(f^{-1}(b)) = ab - ab = 0$.
- ▷ From $f(z) = 0 = f(0)$ and because of f is a biection, we implie that $z = 0$

Therefore, $f^{-1}(ab) = f^{-1}(a) \cdot f^{-1}(b)$. □

1.5 Isomorphic rings

Определение 1.5. If $\exists f : K \mapsto L$ (f – isomorphism), then we say that K, L are isomorphic. Denotion: $K \simeq L$.

Теорема 1.1. *$\simeq$ is a relation of equality on the set of all rings.*

Доказательство.

- ▷ Reflexivity is obvious: $\mathrm{id} : K \mapsto K$ $(\mathrm{id}(x) = x \quad \forall x \in K)$ is obviously an isomorphism
- ▷ Symmetry is proven in Lemma 5.
- ▷ Let's prove transitivity: let K,L,M be rings, $K \simeq L$ & $L \simeq M$.
- ▷ Then there are isomorphisms $f : K \mapsto L$ & $g : L \mapsto M$. Let's prove that $g \cdot f : K \mapsto M$ (set up by rule $gf(a) := g(f(a))$) is also an isomorphism.

- ▷ Composition of these biections is obviously a biection.
- ▷ Checking that gf is homomorphism of rings:

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

$$gf(ab) = g(f(ab)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = gf(a) \cdot gf(b)$$

□

2 2023-09-08 – 2

2.1 Complex numbers

Определение 2.1.

- ▷ A set of *complex numbers* contains sorted pairs of real numbers:

$$\mathbb{C} = \{(a,b) : a,b \in \mathbb{R}\}$$

- ▷ Addition: $(a,b) + (a',b') := (a+a', b+b')$
- ▷ Multiplication: $(a,b) \cdot (a',b') := (aa' - bb', ab' + ba')$.

Определение 2.2.

- ▷ Let $z = (a,b) \in \mathbb{C}$
- ▷ A **real part** of z is denoted as $\operatorname{Re}(z) := a$.
- ▷ An **imaginary parst** of z is denoted as $\operatorname{Im}(z)$
- ▷ Complex conjugation: $\overline{z} := (a, -b)$
- ▷ Norm of z is denoted as $N(z) := a^2 + b^2$
- ▷ Module of z is denoted as $|z| := \sqrt{N(z)} = \sqrt{a^2+b^2}$
- ▷ Obviously, $\overline{\overline{z}} = z$.

Теорема 2.1. $\mathbb{C}$ *is a field.*

Доказательство. ▷ (1) and (2) because addition in $\mathbb{C}$ is componented, so associativity and commutativity are inherited from $\mathbb{R}$.

- ▷ (3) Zero in $\mathbb{C}$ is $0 := (0,0)$.

- (4) Reverse element for $+$. For $z = (a,b)$ set $-z := (-a, -b)$.
- (7) Commutativity of multiplication:

$$(a,b) \cdot (a',b') = (aa' - bb', ab' + ba') = (a'a - b'b, a'b + b'a) = (a', b') \cdot (a,b)$$

- (5) It's enough to check one distributivity (because multiplication is commutative):

$$\begin{aligned}(a,b) \cdot ((c_1, d_1) + (c_2, d_2)) = (a,b) \cdot (c_1 + c_2, d_1 + d_2) = \\ (ac_1 + ac_2 - bd_1 - bd_2, ad_1 + ad_2 + bc_1 + bc_2) = \\ (ac_1 - bd_1, ad_1 + bc_1) + (ac_2 - bd_2, ad_2 + bc_2) = (a,b) \cdot (c_1, d_1) + (a,b) \cdot (c_2, d_2)\end{aligned}$$

-

□

Замечание (Незавершённый конспект)**.** Данный конспект не завершён.

3 2023-09-15

3.1 root of complex number

- let $a \in \mathbb{C}, n \in \mathbb{N}$. Solve $z^n = a$
- $a = (r, \varphi), z = (\rho, \psi)$.
- By Moaur formula, $\rho = \sqrt[n]{r}$
- $n\psi = \varphi + 2\pi k, k \in \mathbb{Z}$. Dividing by n, we get:

$$\psi = \frac{\varphi}{n} + \frac{2\pi k}{n}$$

- For $k \in \{0,1, \ldots, n-1\}$, we get n different arguments.
- Every k can be factorized as $k = qn + r$. Then $\frac{2\pi k}{n} = \frac{2\pi r}{n} + 2\pi q$

3.2 root of n for 1

- Consider $z^n = 1$
- From last section we get: $\psi_k = \frac{2\pi k}{n}$, where $k \in \{0,1, \ldots, n-1\}$
- Using Moaur formula $\varepsilon_k = \varepsilon_1^k$. Then, all roots of 1 is powers ε_1

Замечание. $e^{i\varphi} = (\cos\alpha, \sin\alpha)$

Materials

3.3 Integers

3.4 divisibility

Определение 3.1. Let $a,b \in \mathbb{Z}, b \neq 0$. Then $a \vdots b$ or $b|a$, if $a = bc$, where $c \in \mathbb{Z}$

Свойство 3.4.1. If $a \vdots b, b \vdots c \Rightarrow a \vdots c$

Доказательство. Then $a = kb, b = nc (k,n \in \mathbb{Z}) \Rightarrow a = knc$. □

Свойство 3.4.2. Let $a,b \vdots d, x,y \in \mathbb{Z}$. Then $ax + by \vdots d$

Доказательство. Then $a = kd, b = nd \Rightarrow ax + by = (kx + ny)d$ □

Свойство 3.4.3. Let $a,b \in \mathbb{N}, a \vdots d \Rightarrow a \geqslant d$.

Теорема 3.1. *Let* $a \in \mathbb{Z}, b \in \mathbb{N} \Rightarrow \exists! q,r \in \mathbb{Z} : 0 \leqslant r < b \ \& \ a = bq + r$

Доказательство.
- ▷ $\exists$. Let q be an integer that $bq \leqslant a < b(q+1)$ and $r = a - bq$. Then $0 \leqslant r < b$
- ▷ !. Let $a = bq_1 + r_1 = bq_2 + r_2$, where $0 \leqslant r_1, r_2 < b$
- ▷ Не умаляя общности $r_1 > r_2 \Rightarrow 0 < r_1 - r_2 < b$
- ▷ From other side, $r_1 - r_2 = b(q_2 - q_1) \geqslant b$!?

□

3.5 GCD

Определение 3.2. Let $a_1, \ldots, a_n \in \mathbb{Z}$. Denote $OD(a_1, \ldots, a_n)$ as a set of every divisors of these numbers. GCD is denoted as $(a_1, \ldots, a_n)$

Свойство 3.5.1. If $b \in \mathbb{N}, a \vdots b \Rightarrow OD(a,b)$ is all divisors of b and $(a,b) = b$

Доказательство.
- ▷ If d is common divisor of a,b, then $d|b$.
- ▷ If $d|b$, then $a \vdots d$ using property 1 of divisibility. That means that $(a,b) = d$.

□

Свойство 3.5.2. let $a,b,c,k \in \mathbb{Z}, c = a + kb$. Then $OD(a,b) = OD(c,b) \Rightarrow (a,b) = (c,b)$

Доказательство.
- ▷ Let $d \in OD(a,b)$. Then $c \vdots d \Rightarrow d \in OD(c,b)$
- ▷ If $d \in OD(c,b)$, then $a = c - kb \vdots d \Rightarrow d \in OD(a,b)$

□

3.6 Euclid algorithm

- ▷ Let $a{,}b \in \mathbb{N}, a > b$

  1 $a = bq_1 + r_1$

  2 $b = r_1 q_2 + r_2$

  3 $r_1 = r_2 q_3 + r_3$

  1. $\ldots$

  n r_{n-2}

- ▷ $b > r_1 > r_2 > \ldots$ and algorithm will stop.

Теорема 3.2. $(a{,}b) = r_n$ *&* $OD(a{,}b)$ *are all* r_n *divisors*

Доказательство. Using Euclid algorithm □

Теорема 3.3. *Let* $a{,}b{,}m \in \mathbb{N}$*. Then*

1. $(am, bm) = m(a{,}b)$
2. *if* $d \in OD(a{,}b)$*, then* $(\frac{a}{d}, \frac{b}{d}) = \frac{(a{,}b)}{d}$

Замечание. Using Euclid algorithm, basing on 1st line of algorithm.

Упражнение. *Proof the theorem above.*

3.7 Linear GCD representation

Теорема 3.4. *Let* $a{,}b \in \mathbb{Z}$*. Then* $\exists x{,}y \in \mathbb{Z} : (a{,}b) = ax + by$

- ▷ *It's called linear representation of GCD.*

Доказательство. ▷ $GD(y) = GD(-y) \Rightarrow (a{,}b) = (a, -b)$. Then we assume that $a{,}b \in \mathbb{N}$.

- ▷ HYO $a \geqslant b$. Using Euclid algorithm, let $r_0 = b, r_{-1} = a$
- ▷ Prove that $(a{,}b) = x_k r_k + y_k r_{k-1} \forall k = \{n, \ldots, 0\}$ (where $(a{,}b) = r_n$) by induction
- ▷ $k = n$ is obvious.
- ▷ $k \mapsto k - 1$. We know that $r_k = r_{k-2} + r_{k-1} q_k$:

□

3.8 GCD of n numbers

Теорема 3.5. *Let $n \geqslant 2, a_1, \ldots, a_n \in \mathbb{Z}$. Puts $m_2 = (a_1, a_2), m_3 = (m_2, a_3), \ldots, m_n = (m_{n-1}, a_n)$. Then $m_n = (a_1, a_2, \ldots, a_n)$, and $OD(a_1, \ldots, a_n)$ are all m_n divisors.*

Доказательство. Using induction (trivial) □

Следствие. for $a_1, \ldots, a_n \in \mathbb{Z}\exists$ linear representation of GCD $: x_1, \ldots, x_n \in \mathbb{Z} : (a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n$

Доказательство. Trivial proof using induction. □

3.9 relatively prime numbers

Определение 3.3.

- ▷ $a_1, \ldots, a_n \in \mathbb{Z} : (a_1, \ldots, a_n) = 1 \Rightarrow$ these are relatively prime
- ▷ Попарно взаимно простые

Свойство 3.9.1. If $a{,}b{,}c \in \mathbb{Z}$ & $(a{,}b) = 1 \Rightarrow (ac, b) = (c, b)$

Доказательство.

- ▷ Let $d = (c{,}b)$ & $f = (ac, b)$
- ▷ $c \vdots d \Rightarrow ac \vdots d \Rightarrow d \in OD(ac, b) \Rightarrow f \vdots d$
- ▷ $b \vdots f \Rightarrow bc \vdots f \Rightarrow f \in OD(ac, bc)$
- ▷ $\Rightarrow^{\text{th 2, 3}} c = c(a{,}b) = (ac, bc) \vdots f$
- ▷ $\Rightarrow, f \in OD(c{,}b) \Rightarrow^{\text{th. 2}} d \vdots f$
- ▷ From $d{,}f \in \mathbb{N}, d \vdots f, f \vdots d \Rightarrow d = f$

□

Свойство 3.9.2. If $a{,}b{,}c \in \mathbb{Z}, (a{,}b) = 1$ & $ac \vdots b \Rightarrow c \vdots b$

Доказательство. Using corollary above (trivial). □

Свойство 3.9.3. Let $a_1, \ldots, a_n; b_1, \ldots, b_m \in \mathbb{Z}$ & $(a_i, b_j) = 1 \Rightarrow (a_1 \ldots a_n, b_1 \ldots b_m)$

Доказательство. Using doubled induction. □

3.10 Prime numbers

Определение 3.4. ▷ Number that has 2 divisors.

- ▷ Else: factorizable
- ▷ P – a set of all primes.
- ▷ If $p \in P$, then $1|P, P|P$
- ▷ $1 \notin P$

Определение 3.5. Let $a \in \mathbb{N}$. Itself divisor of a is any it's divisor, not equal to 1 and a. (Intrivial divisort)

Свойство 3.10.1. If $a \in \mathbb{N}$ is factorizable, then $\exists a = bc : b,c \in \mathbb{N}, a > b, c > 1$

Свойство 3.10.2. Let $a \in \mathbb{N}, a \neq 1, d$ – minimal Intrivial divisor of a. Then $d \in P$.

Доказательство. ▷ using definition, $d > 1$

- ▷ Let d be factorizable. Using corl. 1 $d = bc$, where $d > b > 1$
- ▷ From $a \vdots d, d \vdots b \Rightarrow a \vdots b$!?. Then $b < d$ is itself divisor of a

□

Теорема 3.6. *There is infinite number of primes.*

Доказательство. ▷ Let $m = p_1 p_2 \dots p_n + 1$, q is minimal itself divisor.

□

Свойство 3.10.3. Let $a \in \mathbb{Z}, p \in P$. Then $a \vdots p \vee (a,p) = 1$.

Свойство 3.10.4. Let $a_1, \dots, a_n \in \mathbb{Z}, p \in P$ such that $a_1 \dots a_n \vdots p \Rightarrow \exists i \in \{1, \dots, n\}$, such that $a_i \vdots p$

Доказательство. Let not $a_i \vdots p$. Then $(a_i, p) = 1$.

Using corl. 4, $(a_1, \dots, a_n, p) = 1$!? □

Теорема 3.7 (OTA)**.** *$\forall a > 1$ can be factorized into multiplication of primes. This factorization is the only one.*

Доказательство. $\exists$. Base $n \in P$ is obvious. $\mapsto$.

- ▷ Let $a \notin P$, and for all $b < a$ theorem is proven.
- ▷ Then $a = bc$, where $1 < b, c < a \Rightarrow b = p_1 \dots p_n$ and $c = q_1 \dots q_m$
- ▷ Then $a = p_1 \dots p_n q_1 \dots q_n$ is what we wanted.

!. Let $a = p_1 \dots p_n = q_1 \dots q_m$ – two factorizations a into prime factorizations, and a is minimal integer, for which factorization is the only one.

- ▷ from $a = p_1 \dots p_n \vdots q_i \Rightarrow p_i \vdots q_1$ for some $i \in \{1, \dots, n\}$. НУО $i = 1$.
- ▷ From $p_1, q_1 \in P$ & $p_1 \vdots q_1 \Rightarrow p_1 = q_1$
- ▷ Then $a' = \frac{a}{p_1} = p_2 \dots p_n = q_2 \dots q_n$. But factorization a' into multiplication of primes is the only one with the precision of permutations of elements of multiplication.

  Замечание. In particular, $n = m$.

□

3.11 Canonic factorization

Определение 3.6. $n = p_1^k{}_1 p_2^k{}_2 \dots p_s^k{}_s$