Алгоритмы в математике *(теория чисел)*

Михайлов Максим

5 июня 2022 г.

Оглавление

Лекция 1

3 марта

1 Алгебраическое тело

Определение. Алгебраическое тело — множество T с бинарными операциями $+$ и $\cdot$, такими, что:

1. $(T, 0, +)$ — абелева группа:
    - $\forall \alpha, \beta, \gamma \quad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
    - $\exists 0 : \alpha + 0 = \alpha = 0 + \alpha$
    - $\forall \alpha \in T \ \exists (-\alpha) : \alpha + (-\alpha) = 0 = (-\alpha) + \alpha$
    - ⋆ $\forall \alpha, \beta \in T \quad \alpha + \beta = \beta + \alpha$
2. $((T \setminus \{0\}), 1, *)$ — группа:
    - $\alpha(\beta\gamma) = (\alpha\beta)\gamma$
    - $\exists 1 : \alpha \cdot 1 = \alpha = 1 \cdot \alpha$
    - $\forall \alpha \neq 0 \ \exists \alpha^{-1} : \alpha\alpha^{-1} = 1 = \alpha^{-1}\alpha$
    - ⋆ Если умножение не коммутативно, то T — тело, иначе — поле.
3. Дистрибутивность: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$

Пример. $\mathbb{F}_p$ — поле вычетов по модулю p.

$$\mathbb{F}_p = \{0, 1, 2 \ldots p - 1\}$$

1. $\mathbb{F}_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Таблица 1.1: Таблицы сложения и умножения в $\mathbb{F}_2$

Пусть есть поле $\mathbb{F}_k, k = n \cdot m, m \neq 0, n \neq 0$. Т.к. $n < k$ и $m < k$, то $n \cdot m = 0$. Таким образом, в поле есть делители нуля.

Примечание. Переход от $\mathbb{Q}$ к $\mathbb{R}$ — топологическая конструкция, поэтому будем рассматривать переход из $\mathbb{Q}$ в $\mathbb{C}$ над рациональными числами.

Определение. $\mathbb{C} \cong {}^{K[t]}\!/\!_{(t^2+1)K[t]}$

$\cdot$	1	i
1	1	i
i	i	-1

Теорема 1 (Фробениуса). Дано тело T, такое что $T \supset \mathbb{R}$. Тогда:

1. Каждый элемент $\mathbb{R}$ коммутирует с каждым элементом T.
2. Каждый элемент T представим как:

$$x = x_0 + x_1 i_1 + x_2 i_2 + \cdots + x_n i_n$$

Из этого следует, что выполнено одно из:

1. T это $\mathbb{R}$
2. T это $\mathbb{C}$
3. T это $\mathbb{K}$

Если $i_1, i_2 \ldots i_n$ — базис $\mathbb{I}$, то $\dim \mathbb{I} \in \{0, 1, 3\}$

Лекция 2

11 марта

$\lhd \mathbb{I} = \{z \mid z^2 \in \mathbb{R}, z^2 \leq 0\}$

Примечание. $\mathbb{R} \cap \mathbb{I} = \{0\}$

Теорема 2. $\mathbb{R} \oplus \mathbb{I} = T$

Лемма 1. Если $z \in \mathbb{I}$, то $\forall \alpha \in \mathbb{R} \ \ \alpha z \in \mathbb{I}$.

Доказательство.

$$(\alpha z)^2 = \alpha^2 z^2 \leq 0 \Rightarrow \alpha z \in \mathbb{I}$$

□

Лемма 2. Если $z \in \mathbb{I}$ и z^{-1} существует, то $z^{-1} \in \mathbb{I}$, где z^{-1} это такой элемент $\mathbb{I}$, что $zz^{-1} = 1$.

Доказательство.

$$z^2(z^{-1})^2 = \underbrace{zz}_{<0} z^{-1}z^{-1} = 1 \Rightarrow z^{-1}z^{-1} < 0 \Rightarrow z^{-1} \in \mathbb{I}$$

□

Лемма 3. Всякий элемент x из T представим единственным образом в виде:

$$x \stackrel{!}{=} a + z, \quad a \in \mathbb{R}, z \in \mathbb{I}$$

Доказательство. $\lhd x \in T, \{x^0, x, x^2 \dots x^{n+1}\}$ — линейно зависимые, т.к. пространство размерности $n+1$, а элементов $n+2$. Тогда по определению линейной зависимости $\exists \{\alpha_i\}_{i=0}^{n+1} \subset \mathbb{R}$, такие что:

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_{n+1} x^{n+1} = 0$$

Тогда x является корнем многочлена вида $x - a = 0$ и тогда $x = a$, либо x является корнем многочлена вида $x^2 + 2\alpha x + \beta = 0$ и тогда x можно представить в виде $a + z$.

Покажем единственность. Пусть $x = a + y$ и $x = b + z$, где $a, b \in \mathbb{R},\ y, z \in \mathbb{I}$.

$$a + y - b - z = 0$$
$$a + y - b = z$$
$$\underbrace{(a-b)^2}_{\in\mathbb{R}} + 2(a-b)y + \underbrace{y^2}_{\in\mathbb{R}} = \underbrace{z^2}_{\in\mathbb{R}}$$
$$2(a-b)y = 0$$

Таким образом, либо $a = b$, а следовательно $y = z$, либо $y = 0 \implies x \in \mathbb{R} \implies z = 0$ $\square$

Лемма 4. Пусть $u, v \in \mathbb{I}, a, b \in \mathbb{R}$. Тогда $uv + vu = \xi \in \mathbb{R}$ и $au + bv = \eta \in \mathbb{I}$.

Доказательство. Положим, что $\{1, u, v\}$ линейно зависим, т.е. $\exists \alpha, \beta, \gamma : \alpha + \beta u + \gamma v = 0$.

$$\beta u = -\alpha - \gamma v \Rightarrow \alpha = 0 \Rightarrow u = -\frac{\gamma}{\beta} v$$

$$\lhd uv + vu = -\frac{\gamma}{\beta} v^2 - \frac{\gamma}{\beta} v^2 = \frac{-2\gamma}{\beta} v^2 \in \mathbb{R}$$
$$-\frac{\alpha\gamma}{\beta} v + bv = \left(b - \frac{\alpha\gamma}{\beta}\right) v \in \mathbb{I}$$

Положим, что $\{1, u, v\}$ линейно независим.

$$\eta^2 = (\beta + z)^2 = (au + bv)^2 = a^2u^2 + b^2v^2 + ab(uv + vu)$$

$$(\beta + z)^2 = a^2u^2 + b^2v^2 + ab(\alpha + y)$$
$$\beta^2 + 2\beta z + z^2 = a^2u^2 + b^2v^2 + ab(\alpha + y)$$
$$2\beta z = ab(\alpha + y)$$

Если $z = 0$, то $\{1, u, v\}$ линейно зависим ($\beta = au + bv$) — противоречие.

$\lhd z \neq 0, z = \frac{ab}{2\beta} y$

$$au + bv = \beta + \frac{ab}{2\beta} y$$

$$a'u + b'v = \beta' + \frac{a'b'}{2\beta'} y$$

$$(a - a')u + (b - b')v = (\beta - \beta') + \left(\frac{ab}{2\beta} - \frac{a'b'}{2\beta'}\right) y$$

Тогда мы можем выбором a и b занулить $\frac{ab}{2\beta} - \frac{a'b'}{2\beta'}$, поэтому $\{1, u, v\}$ линейно зависимы.
Не дописано $\square$

Лемма 5.

- $u, v \in \mathbb{I}$
- $u^2 = -1$
- $v^2 = -1$
- $w = u \cdot v$

Тогда:

$$\begin{aligned} u^2 = v^2 = w^2 &= -1 \\ uv = -vu &= w \\ vw = -wv &= u \\ wu = -uw &= v \end{aligned}$$

Доказательство. Дома. □

Лекция 3

18 марта

Пример (split complex number). Это не тело.

Числа представимы в виде $z = a + bj$, есть дополнение $z^* = a - bj$ и тогда $zz^* = a^2 - b^2$. Изотропные элементы $e_1 = \frac{1+j}{2}$ и $e_2 = \frac{1-j}{2}$ образуют базис в этих числах. Кроме того, $e_1 e_1^* = e_2 e_2^* = 0$

Таблица 3.1: Таблица Кэли

	1	j
1	1	j
j	j	1

Пример. $\mathbb{R}[t] / t^2\mathbb{R}[t], z = a + bd$

Лемма 6. Пусть $u^2 = -1, v^2 = -1, w = uv$. Тогда $w = uv \in \mathbb{I}, w^2 = -1, uv = -vu = \omega, v\omega = -\omega v = u$ и т.д.

Доказательство.

$$\lhd (uv)(vu) = -vu = 1 \Rightarrow vu = (uv)^{-1}$$

$$\mathbb{R} \ni uv + vu = uv + (uv)^{-1} \in \mathbb{I} \implies uv - vu = 0 \implies uv = -vu$$

$\square$

Теорема 3.

- $\mathbb{I} = \{0\} \implies T = \mathbb{R}$
- $\mathbb{I} = \{x\}$

Лекция 4

18 марта

Пример (split complex number). Это не тело.

Числа представимы в виде $z = a + bj$, есть дополнение $z^* = a - bj$ и тогда $zz^* = a^2 - b^2$. Изотропные элементы $e_1 = \frac{1+j}{2}$ и $e_2 = \frac{1-j}{2}$ образуют базис в этих числах. Кроме того, $e_1e_1^* = e_2e_2^* = 0$

Таблица 4.1: Таблица Кэли

	1	j
1	1	j
j	j	1

Пример. ${}^{\mathbb{R}[t]}\!\diagup_{t^2\mathbb{R}[t]}, z = a + bd$

Лемма 7. Пусть $u^2 = -1, v^2 = -1, w = uv$. Тогда $w = uv \in \mathbb{I}, w^2 = -1, uv = -vu = \omega, v\omega = -\omega v = u$ и т.д.

Доказательство.

$$\lessdot(uv)(vu) = -vu = 1 \Rightarrow vu = (uv)^{-1}$$

$$\mathbb{R} \ni uv + vu = uv + (uv)^{-1} \in \mathbb{I} \implies uv - vu = 0 \implies uv = -vu$$

□

Теорема 4.

- $\mathbb{I} = \{0\} \implies T \cong \mathbb{R}$
- $\mathbb{I} = \{x\}, i \coloneqq \frac{x}{\sqrt{-x^2}}, i^2 = -1 \implies T \cong \mathbb{C}$

- $\mathbb{I} = \{x, y\}, i \coloneqq \frac{x}{\sqrt{-x^2}}, iy =: b + z, j_0 \coloneqq iy - b = z, j = \frac{j_0}{\sqrt{-j_0^2}} \implies \exists k = ij \implies q = \alpha + i\beta + j\gamma + k\delta \implies T \cong \mathbb{K}$
- $\{i, j, k, m\} \in \mathbb{I}$.

  Тогда пусть $im = a + x, jm = b + y, km = c + z$, где $a, b, c \in \mathbb{R}, x, y, z \in \mathbb{I}$. Рассмотрим $l_0 = m + ai + bj + ck \in \mathbb{I}$, при этом $l_0 \neq 0$ и $il_0, jl_0, kl_0 \in \mathbb{I}$. Тогда $il = -li, jl = -lj, kl = -lk$.

$$\left.\begin{aligned} ilj = -ijl = -kl \\ jli = -lji = lk \end{aligned}\right\} \implies kl = -kl = 0$$

Лекция 5

29 марта

Лемма 8. – $u^2 =$

???

Доказательство.

$$\mathbb{R} \ni uv + vu \in \mathbb{I}$$

Мы доказывали, что ???

Мы доказывали, что $z \in \mathbb{I} \Rightarrow z^{-1} \in \mathbb{I}$

По другой лемме $ab \in \mathbb{R},\ u, v \in \mathbb{I} \Rightarrow au + bv \in \mathbb{I}$

Тогда $uv + vu = 0$ и $uv = -vu$.

$\lhd \omega^2 = uvuv = uv(-vu) = -u^2 = -1$ □

Остальная часть лекции рассказана повторно на пятой лекции.

Лекция 6

2 июня

2 Кватернионы

Будем обозначать $q = q_0 + \tilde{q}$, где q_0 — вещественная часть, а $\tilde{q}$ — мнимая. Также можно неформально говорить, что $q_0 \in \mathbb{R}$, а $\tilde{q} \in \mathbb{R}^3$.

Пространство кватернионов $\mathbb{K}$ в неком смысле изоморфно $\mathbb{R}^4$. В этом пространстве можно выделить подпространство мнимых кватернионов, изоморфное $\mathbb{R}^3$. Распишем $\tilde{q}$:

$$q = q_0 + q_1 i + q_2 j + q_3 k$$

Операция сложения работает "поэлементно":

$$p + q = (p_0 + q_0) + (\tilde{p} + \tilde{q}) = (p_0 + q_0) + (p_1 + q_1)i + (p_2 + q_2)j + (p_3 + q_3)k$$

Умножение более интересно и определяется следующими правилами:

$$\begin{aligned} ij &= k = -ji \\ jk &= i = -kj \\ ki &= j = -ik \\ i^2 = j^2 &= k^2 = ijk = -1 \end{aligned}$$

Тогда умножение в явном виде:

$$\begin{aligned} (p_0 + p_1 i + p_2 j + p_3 k)(q_0 + q_1 i + q_2 j + q_3 k) = \\ p_0 q_0 - \langle \tilde{p}, \tilde{q} \rangle + p_0 \tilde{q} + q_0 \tilde{p} + [\tilde{p} \times \tilde{q}] \end{aligned}$$

$$[p \times q] \coloneqq \det \begin{vmatrix} i & j & k \\ p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \end{vmatrix}$$

Нейтральные элементы:

- По сложению: $0 = 0 + \tilde{0}$
- По умножению: $1 = 1 + \tilde{0}$

Определение. Сопряженным к кватерниону $q = q_0 + \tilde{q}$ называется кватернион:

$$q^* = q_0 - \tilde{q}$$

Определение (норма кватерниона).

$$\|q\| = qq^* \quad |q| = \sqrt{\|q\|} = \sqrt{q_0^2 + q_1^2 + q_2^2 + q_3^2}$$

Определение.

$$q^{-1} = \frac{q^*}{\|q\|}$$

Определение (единичная сфера).

$$S = \{q \in \mathbb{K} \mid \|q\| = |q| = 1\}$$

Примечание. Если $|q| = 1$, то $q^{-1} = q^*$

Свойства.

1. $(q^*)^* = (q_0 - \tilde{q})^* = q_0 + \tilde{q} = q$
2. $q + q^* = 2q_0$ — "след"
3. $(pq)^* = q^* p^*$
4. $qq^* = (q_0 + \tilde{q})(q_0 - \tilde{q}) = q_0^2 - \tilde{q}\tilde{q} = q_0^2 - \overbrace{[\tilde{q} \times \tilde{q}]}^{0} + \langle \tilde{q}, \tilde{q} \rangle = q^* q = \|q\| = \|q^*\|$
5. $||pq|| = (pq)(pq)^* = (pq)(q^*p^*) = p(qq^*)p^* = p\|q\|p^* = \|q\|pp^* = \|q\|\|p\| = \|p\|\|q\|$
6. $\|q\| = 1$ — **единичный кватернион**.

$\lhd q \in \mathbb{K}$ такое, что $\|q\| = 1$, т.е. $q_0^2 + |\tilde{q}|^2_{\mathbb{R}^3} = 1$

$$\exists \varphi \in \mathbb{R} : \begin{cases} \cos^2 \varphi = q_0^2 \\ \sin^2 \varphi = |\tilde{q}|^2_{\mathbb{R}^3} \end{cases}$$

$$\exists! \varphi \in [0, \pi] : \begin{cases} \cos^2 \varphi = q_0^2 \\ \sin^2 \varphi = |\tilde{q}|^2_{\mathbb{R}^3} \end{cases}$$

Очевидно, не любой кватернион так можно представить. Поэтому $\lhd \tilde{u} = \frac{\tilde{q}}{|\tilde{q}|}$. Тогда:

$$q = q_0 + |\tilde{q}| \cdot \tilde{u} = \cos\varphi + \tilde{u}\sin\varphi$$

$$\lhd \mathcal{L}(v) \quad \mathcal{L} : \mathbb{K} \times \mathbb{R}^3 \to \mathbb{K} \quad \mathcal{L}_q(v) = q\tilde{v}q^*$$

Лемма 9. $\forall v \in \mathbb{R}^3 \;\; |v| = |\mathcal{L}_q(v)|$ при $|q| = 1$

Доказательство. Фиксируем $v \in \mathbb{R}^3, q \in \mathbb{K}$ такой, что $\|q\| = 1$.

$$\|\mathcal{L}_q(v)\| = \|q\tilde{v}q^*\| = \|q\| \cdot \|\tilde{v}\| \cdot \|q^*\| = \|\tilde{v}\| = \|v\|_{\mathbb{R}^3}$$

□

Лемма 10. $\forall q \in \mathbb{K} : \|q\| = 1 \;\; \forall \alpha \in \mathbb{R} \quad \mathcal{L}_q(\alpha p + s) = \alpha\mathcal{L}_q(p) + \mathcal{L}_q(s)$

Доказательство.

$$\mathcal{L}_q(\alpha p + s) = q(\alpha p + s)q^* = \alpha qpq^* + qsq^* = \alpha\mathcal{L}_q(p) + \mathcal{L}_q(s)$$

□

Лемма 11. $\forall \alpha \in \mathbb{R} \setminus \{0\} \;\; \forall q \in \mathbb{K} : \|q\| = 1 \quad |\alpha\tilde{q}| = |\mathcal{L}_q(\alpha\tilde{q})|$

Доказательство. С помощью расписывания определения через координаты:

$$\mathcal{L}_q(v) = (q_0^2 - |\tilde{q}|^2)v + 2\langle\tilde{v}, \tilde{q}\rangle\tilde{v} - 2[\tilde{q} \times \tilde{v}]$$

$$\mathcal{L}_q(\alpha\tilde{q}) = \alpha\mathcal{L}_q(\tilde{q}) = \alpha((q_0^2 - |\tilde{q}|^2)\tilde{q} + 2\langle\tilde{q}, \tilde{q}\rangle\tilde{q} - 2q_0[\tilde{q} \times \tilde{q}]) = \alpha(q_0^2 + |\tilde{q}|^2)\tilde{q} = \alpha\tilde{q}$$

□

Теорема 5. $\lhd q \in \mathbb{K} : |q| = 1$. Тогда q можно представить как $q = \cos\varphi + \tilde{u}\sin\varphi$. Кроме того, $\mathcal{L}_q(v) = q\tilde{v}q^* = q\tilde{v}q^{-1}$.

Тогда действие $\mathcal{L}_q$ на $\mathbb{R}^3$ — поворот на угол 2φ относительно оси u.

Доказательство. Зафиксируем $v \in \mathbb{R}^3$. Разложим v как $v = \vec{a} + \vec{b}$, где $\vec{a} \parallel \vec{u}$, а $\vec{n} \perp \vec{u}$

$$\mathcal{L}_q(v) = \mathcal{L}_q(\vec{a} + \vec{n}) = \mathcal{L}_q(\vec{a}) + \mathcal{L}_q(\vec{n})$$

$$\mathcal{L}_q(\vec{a}) \overset{\exists K \in \mathbb{R}: a = k\tilde{q}}{=} \vec{a}$$

$$\mathcal{L}_q(\vec{n}) = (q_0^2 - |\tilde{q}|^2)\vec{n} + 2\langle\vec{n}, \vec{q}\rangle\vec{n} - 2q_0[\tilde{n} \times \vec{q}]$$

$$
\begin{aligned}
&= (q_0^2 - |\tilde{q}|^2)\vec{n} - 2q_0[\tilde{n} \times \vec{q}] \\
&= (\cos^2\varphi - \sin^2\varphi)\vec{n} + 2\cos\varphi \cdot \sin\varphi \underbrace{[\tilde{u} \times \vec{n}]}_{\vec{n}_\perp} \\
&= \cos 2\varphi\vec{n} + \sin 2\varphi\vec{n}_\perp
\end{aligned}
$$

$$
|\vec{n}_\perp| = |[\tilde{u} \times \vec{n}]| = |\tilde{u}| \cdot |\vec{n}| \cdot \sin\frac{\pi}{2} = |\vec{n}|
$$

□

Не дописано