Алгоритмы в математике *(теория чисел)*

Михайлов Максим

11 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:
   - $\forall \alpha, \beta, \gamma \quad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
   - $\exists 0 : \alpha + 0 = \alpha = 0 + \alpha$
   - $\forall \alpha \in T \;\; \exists (-\alpha) : \alpha + (-\alpha) = 0 = (-\alpha) + \alpha$
   - $\star$ $\forall \alpha, \beta \in T \quad \alpha + \beta = \beta + \alpha$
2. $((T \setminus \{0\}), 1, *)$ — группа:
   - $\alpha(\beta\gamma) = (\alpha\beta)\gamma$
   - $\exists 1 : \alpha \cdot 1 = \alpha = 1 \cdot \alpha$
   - $\forall \alpha \neq 0 \;\; \exists \alpha^{-1} : \alpha\alpha^{-1} = 1 = \alpha^{-1}\alpha$
   - $\star$ 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:

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

Из этого следует, что выполнено одно из:

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

Если $i_1, i_2 \dots i_n$ — 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:

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

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 $y = 0 \implies x \in \mathbb{R} \implies z = 0$ □

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 □

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. $\square$

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.

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

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

  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 4

29 марта

Лемма 7. – $u^2 =$

???

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 $uv = -vu$.

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

Остальная часть лекции рассказана повторно на пятой лекции.

Лекция 5

2 апреля

2 Введение в 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:

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

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

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**.

$\vartriangleleft q \in \mathbb{K}$ 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 8. $\forall v \in \mathbb{R}^3 \;\; |v| = |\mathcal{L}_q(v)|$ 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 9. $\forall q \in \mathbb{K} : \|q\| = 1 \;\; \forall \alpha \in \mathbb{R} \quad \mathcal{L}_q(\alpha p + s) = \alpha\mathcal{L}_q(p) + \mathcal{L}_q(s)$

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

Доказательство. С помощью расписывания определения через координаты:

$$\mathcal{L}_q(v) = (q_0^2 - |\tilde{q}|^2)v + 2\langle \tilde{q}, \tilde{v}\rangle \tilde{v} - 2q_0[\tilde{q} \times \tilde{v}] \tag{1}$$

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

□

Теорема 4. $\lhd q \in \mathbb{K} : |q| = 1$. 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 $\vec{n} \perp \vec{u}$

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

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

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

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

□

Теорема 5 (∗). $\lhd q \in \mathbb{K} : \|q\| = 1, q = \cos\frac{\varphi}{2} + \tilde{u}\sin\frac{\varphi}{2}$

$\mathcal{L}_{q^*}$ — это поворот либо вектора на угол $-\varphi$, либо координатной сетки на угол φ.

Доказательство. Т.к. $\|q\| = 1, q^* = q^{-1}$.

$$\mathcal{L}_{q^{-1}}(\mathcal{L}_q(v)) = q^{-1}(qvq^{-1})q = eve = v$$

□

Теорема 6. $\lhd p, q \in \mathbb{K} : \|p\| = \|q\| = 1$. Тогда $\mathcal{L}_q \circ \mathcal{L}_p = \mathcal{L}_{q\cdot p}$.

Доказательство. Фиксируем $p, q \in \mathbb{K}, v \in \mathbb{R}^3$.

$$\mathcal{L}_q(\mathcal{L}_p(v)) = q(pvp^*)q^* = qpv(qp)^* = \mathcal{L}_{q\cdot p}(v)$$

□

$$q = q_0 + \tilde{q} = \cos\frac{\varphi}{2} + \tilde{u}\sin\frac{\varphi}{2}$$

Подставим в (1):

$$
\begin{aligned}
\mathcal{L}_q(v) &= \left(\cos^2\frac{\varphi}{2} - \sin^2\frac{\varphi}{2}\right)\tilde{v} + 2\sin\frac{\varphi}{2}\langle\tilde{u}, \tilde{v}\rangle \cdot \tilde{u} - 2\cos^2\frac{\varphi}{2}[\tilde{u} \times \tilde{v}] \\
&= \cos\varphi\tilde{v} + (1 - \cos\varphi)\langle\tilde{u}, \tilde{v}\rangle\tilde{u} - \sin\varphi[\tilde{u} \times \tilde{v}]
\end{aligned}
$$

Пример. $\lhd u = \frac{1}{\sqrt{3}}(1, 1, 1)$, поворот на $\frac{2\pi}{3}$.

$$
\begin{aligned}
\mathcal{L}_q((1,0,0)) &= \cos\frac{2\pi}{3} \cdot i + \left(1 - \cos\frac{2\pi}{3}\right) \cdot \frac{1}{\sqrt{3}}\langle(1,1,1),(1,0,0)\rangle \cdot \frac{1}{\sqrt{3}}(i + j + k) \\
&\quad - \sin\frac{2\pi}{3}\left[\frac{1}{\sqrt{3}}(i + j + k) \times i\right] \\
&= \frac{i}{2} + \frac{3}{2} \cdot \frac{i + j + k}{3} + \frac{\sqrt{3}}{2} \cdot \frac{1}{\sqrt{3}}\begin{vmatrix} i & j & k \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{vmatrix} \\
&= -\frac{i}{2} + \frac{i + j + k}{2} + \frac{j - k}{2} = \frac{2j}{2} = j
\end{aligned}
$$

Лекция 6

9 марта

2.1 Напоминание о кватернионах

Кватернионы записываются как:

$$q = q_0 + q_1 i + q_2 j + q_3 k \overset{\text{def}}{=} q_0 + \tilde{q}$$

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Таблица 6.1: Таблица Кэли для кватернионов

Пространство кватернионов есть прямое произведение действительных чисел и чистых кватернионов:

$$\mathbb{K} = \mathbb{R} \oplus \underbrace{\mathbb{P}_E}_{\cong\mathbb{R}^3}$$

$\langle\cdot,\cdot\rangle$	i	j	k
i	1	0	0
k	0	1	0
j	0	0	1

Таблица 6.2: Скалярное произведение кватернионов

Пусть $q \in \mathbb{K}, \vec{v} \in \{0\} \oplus \mathbb{P}_E$. $\triangleleft \mathcal{L}_q(v) = qvq^{-1}$.

$|q| \coloneqq \sqrt{\|q\|}, \|q\| \coloneqq qq^*, q^{-1} \coloneqq \frac{q^*}{\|q\|}$

Если $|q| = 1$, то $q = \cos\frac{\varphi}{2} + \tilde{u}\sin\frac{\varphi}{2}$, где $\tilde{u} = \frac{\tilde{q}}{|\tilde{q}|}$. В этом случае qvq^{-1} есть поворот на угол φ.

3 Кватернионы и $SU(2)$

Рассмотрим матрицы $A \in \mathbb{C}^{2\times 2}$, которым соответствуют операторы $\hat{A} : \mathbb{C}^2 \to \mathbb{C}^2$.

Тогда $AA^* = E$, где A^* – **эрмитово сопряжение**, т.е. транспонируем матрицу и каждый элемент комплексно сопрягаем.

Т.к. $\det(AB) = \det A \cdot \det B$, следовательно $1 = \det E = \det(AA^*) = \det A \cdot \det A^* \implies \det A = \frac{1}{\det A^*}$. Кроме того, $\det A = \det A^\intercal$ и $\prod_i a_i^* = (\prod_i a_i)^*$ и $\sum_i b_i^* = (\sum_i b_i)^*$ и тогда:

$$\sum_j \prod_i a_{ij}^k = \sum_j \left(\prod_i a_{ij}\right)^* = \left(\sum_j \prod_i a_{ij}^*\right)$$

И следовательно $\det A^* = (\det A)^*$

Определение. $SU(2)$ – группа A таких, что $AA^* = E$ и $\det A = 1$

$\sphericalangle A \in SU(2), A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

$$\det A = 1 \implies \alpha\delta - \beta\gamma = 1$$

Тогда:

$$\begin{cases} E_{11} = \alpha\overline{\alpha} + \beta\overline{\beta} = 1 \\ E_{12} = \alpha\overline{\gamma} + \beta\overline{\delta} = 0 \\ E_{21} = \gamma\overline{\alpha} + \delta\overline{\beta} = 0 \\ E_{22} = \gamma\overline{\gamma} + \delta\overline{\delta} = 1 \end{cases}$$

Из условий для E_{11} и E_{22}:

$$|\alpha|^2 + |\beta|^2 = 1 \implies \begin{cases} \alpha = e^{i\varphi_1}\cos\theta \\ \beta = e^{i\varphi_2}\sin\theta \end{cases}$$

$$|\gamma|^2 + |\delta|^2 = 1 \implies \begin{cases} \gamma = e^{i\psi_1}\cos\chi \\ \delta = e^{i\psi_2}\sin\chi \end{cases}$$

Из E_{12} и E_{21}:

$$e^{i\varphi_1}\cos\theta e^{-i\psi_1}\cos\chi + e^{i\varphi_2}\sin\theta e^{-i\psi_2}\sin\chi = 0$$

$$e^{i(\varphi_1-\psi_1)}\cos\theta\cos\chi + e^{i(\varphi_2-\psi_2)}\sin\theta\sin\chi = 0$$

$$2\cos(\varphi_1-\psi_1)\cos\theta\cos\chi + 2i\sin(\varphi_2-\chi_2)\sin\theta\sin\chi = 0$$

$$\begin{cases}\cos(\varphi_1-\psi_1)\cos\theta\cos\chi = 0\\ \sin(\varphi_2-\psi_2)\sin\theta\sin\chi = 0\end{cases}$$

$$A^{-1} = \begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix} = \begin{pmatrix}\overline{\alpha} & \overline{\gamma}\\ \overline{\beta} & \overline{\delta}\end{pmatrix} \implies \delta = \overline{\alpha}, \gamma = -\overline{\beta}$$

Пусть $\alpha = a + ic, \beta = b + id$, где $a, b, c, d \in \mathbb{R}$.

$$\begin{aligned}A &= \begin{pmatrix}a+ic & b+id\\ -b+id & a-ic\end{pmatrix}\\ &= a\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}ic & b+id\\ -b+id & -ic\end{pmatrix}\\ &= a\underbrace{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}}_{\Xi_0} + b\underbrace{\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}}_{\Xi_1} + c\underbrace{\begin{pmatrix}i & 0\\ 0 & i\end{pmatrix}}_{\Xi_2} + d\underbrace{\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}}_{\Xi_3}\end{aligned}$$

$\cdot$	Ξ_0	Ξ_1	Ξ_2	Ξ_3
Ξ_0	Ξ_0	Ξ_1	Ξ_2	Ξ_3
Ξ_1	Ξ_1	$-\Xi_0$	Ξ_3	$-\Xi_2$
Ξ_2	Ξ_2	$-\Xi_3$	$-\Xi_0$	Ξ_1
Ξ_3	Ξ_3	Ξ_2	$-\Xi_1$	$-\Xi_0$

Таблица 6.3: Таблица Кэли для матриц Ξ_i

Таким образом, у нас есть соответствие $SU(2)$ и $\mathbb{K}$: $\Xi_0 \Leftrightarrow 1, \Xi_1 \Leftrightarrow i, \Xi_2 \Leftrightarrow j, \Xi_3 \Leftrightarrow k$. Но это не изоморфизм — ограничение на $\det A = 1$ не позволяет любому кватерниону сопоставить элемент $SU(2)$. Найдем, чему $SU(2)$ изоморфно.

Определение. Множество **нормированных кватернионов** $\mathbb{NK} = \{|q| = 1 \mid q \in \mathbb{K}\}$

Определение. $\mathbb{NK}$ — подгруппа (по умножению) $\mathbb{K}$

$$S^3 \sim \mathbb{NK} \subset \mathbb{K}$$

Здесь и далее $\overset{G}{\cong}$ обозначает групповой изоморфизм.

$$\mathbb{NK} \overset{G}{\cong} SU(2) \quad \{0\} \oplus \mathbb{P}_E \overset{G}{\cong} SO(3)$$

Резюмируя: мы взяли подгруппу кватернионов $\mathbb{NK}$ и построили изоморфизм между этой подгруппой и $SU(2)$. На прошлом занятии мы построили изоморфизм между группой вращений $SO(3)$ и $\{0\} \oplus \mathbb{P}_E$. Эти изоморфизмы по умножению. Также есть изоморфизм по сложению между $\mathbb{P}_E$ и $\mathbb{R}^3$

4 $SU(2)$ и $SO(3)$

Любое вращение трёхмерного пространства можно рассматривать как переход произвольной точки сферы в другую произвольную точку сферы. Спроектируем сферу на плоскость, которую будем считать $\mathbb{C}$ с осями ξ и η. Оси сферы - xyz.

Упражнение читателю — показать, что:

$$\xi = \frac{x}{\frac{1}{2} - z} \quad \eta = \frac{y}{\frac{1}{2} - z}$$

Тогда введём комплексное число $\zeta = \xi + i\eta$. Не более сложно заметить, что:

$$\zeta = \frac{\frac{1}{2} + z}{x - iy}$$

, что следует из $x^2 + y^2 + z^2 = 1$

Нам надо научиться вращать вокруг оси z и x, тогда композицией этих двух действий мы сможем получить любое вращение.

Вращение вокруг оси z, т.е. в комплексной плоскости тривиально:

$$\zeta' = e^{i\theta}\zeta$$

Поворот вокруг оси x на угол χ (без доказательства):

$$\zeta'' = \frac{\zeta \cos\frac{\chi}{2} + i \sin\frac{\chi}{2}}{i\xi \sin\frac{\chi}{2} + \cos\frac{\chi}{2}}$$

Тогда композиция этих преобразований имеет вид:

$$A = \frac{a\xi + b}{c\xi + d}$$

Будем кодировать вращения как вектора $\vec{K}$, где направление определяет ось, относительно которой происходит вращение, и модуль определяет угол поворота ($|K| \leq \pi$).

Тогда мы можем рассмотреть многообразие таких векторов. В нём отождествлены противоположные точки. Есть проблема: оно связно, но оно не односвязно, т.е. у него нетривиальна фундаментальная группа. По теореме каждое многообразие можно достроить до односвязного, такое многообразие называется **накрытием**. Для $SO(3)$ такое многообразие это $SU(2)$.

Пример. Рассмотрим накрытие для окружности. Т.к. единственное другое многообразие с размерностью 1 это прямая, то будем строить накрытие из прямой. С помощью преобразования e^{it} будем накручивать прямую на окружность. Если в какой-либо точке прекратить накручивать, то точка конца помешает. Число слоев в накрытии, сотответствующих одной точке, называется **кратностью накрытия**. Кратность накрытия окружности $-\ \infty$.

Кратность накрытия для $SO(3) - 2$.

Лекция 7

16 марта

5 Алгебраические топологические тела

Что общего у поля вещественных чисел, поля комплексных чисел и тела кватернионов? Разумеется, много чего, но нас интересует тот факт, что они являются евклидовыми пространствами. Для удобства будем обозначать $\mathbb{R}, \mathbb{C}, \mathbb{K}$ как K.

Определение. Элементы последовательности $a_1, a_2 \dots a_n \dots$, где $a_i \in K$, **сходятся** к $a \in K$, если $\rho(a_n, a) \to 0$. Тогда обозначаем $\lim_{n\to\infty} a_n = a$.

Определение. Если на теле введено понятие сходимости, то такое тело называется **топологическим**.

На топологическом теле операции непрерывны, т.е. если $\lim_{n\to\infty} a_n = a$ и $\lim_{n\to\infty} b_n = b$, то:

$$\lim_{n\to\infty} a_n + b_n = a + b \qquad \lim_{n\to\infty} a_n b_n = ab$$

Из этих двух равенств также следует непрерывность вычитания и умножения, т.к. $\lim_{n\to\infty} -a_n = -a$ и $\lim_{n\to\infty} a_n^{-1} = a^{-1}$.

Определение. Топологическое тело с операциями $+, \cdot, -, ^{-1}$ называется **алгебраически-топологическим**

Норма для K:

1. $\mathbb{R} : \|r\| = \sqrt{r \cdot r}$
2. $\mathbb{C} : \|z\| = \sqrt{z \cdot z^*}$
3. $\mathbb{K} : \|q\| = \sqrt{q \cdot q^*}$

Тогда метрика на K это $\rho(z_1, z_2) = \|z_1 - z_2\|$.

Определение. **Топология** на K это $\tau \subset 2^K$ такое, что:

1. $\{0\}, K \in \tau$
2. $\bigcup_i T_i \in \tau$
3. $\bigcap_{\text{кон.}} T_i \in \tau$

Элементы τ называются **открытыми**.

Пример.

$$T_0 := \{z \in K \mid \|z - z_p\| < B\}, B \in \mathbb{R}_+$$

О непрерывности некоторого отображения $f : A \to B$ можно говорить только если $A, B \in \mathrm{Top}$[1]

Обозначение. Для тела L и $X, Y \subset L$:

- $X + Y := \{x + y \mid x \in X, y \in Y\}$
- $X - Y := \{x - y \mid x \in X, y \in Y\}$
- $XY := \{xy \mid x \in X, y \in Y\}$
- $XY^{-1} := \{xy^{-1} \mid x \in X, y \in Y\}$

Определение. Последовательность $U_1, U_2 \ldots U_n \ldots$, где $U_n \subset L$ и $0 \in U_{n+1} \subset U_n$ называется **системой окрестностей нуля топологического тела** L, если $\forall n \in \mathbb{N}\ \exists p$:

1. $(U_p + U_p) \subset U_n$
2. $U_p U_p \subset U_n$
3. $-U_p \subset U_n$
4. $(e + U_p)^{-1} \subset e + U_n$, где e — единица тела L.
5. $\forall a \in L\ \ aU_p \subset U_n, U_p a \subset U_n$

Определение. Последовательность $a_1, a_2 \ldots a_n \ldots$, где $\forall i\ \ a_i \in L$, сходится к $a \in L$, если:

$$\forall n\ \ \exists r\ \ \forall p > n\ \ (a_p - a) \in U_n$$

Теорема 7. Если на теле[2] L определена сходимость и $\lim_{n\to\infty} a_n = a, \lim_{n\to\infty} b_n = b$, то:

$$\lim_{n\to\infty} a_n + b_n = a + b$$
$$\lim_{n\to\infty} a_n \cdot b_n = a \cdot b$$
$$\lim_{n\to\infty} -a_n = -a$$
$$\lim_{n\to\infty} a_n^{-1} = a^{-1}$$

[1] Категория топологических пространств
[2] Не обязательно топологическом

Доказательство. По условию теоремы $\exists p_1 : a_{p_1} \in a + U_n, \exists p_2 : b_{p_2} \in b + U_n$. Пусть $p = \max(p_1, p_2)$.[3]

$$a_p + b_p \in a + b + U_n + U_n$$

По определению системы окрестностей нуля:

$$\exists p_3 : U_{p_3} + U_{p_3} \subset U_n$$

$$(a_p + b_p) - (a + b) \in U_n$$

Аналогично остальные пункты. □

[3] На лекции этого не было, но мне кажется это необходимым.