Алгоритмы в математике *(теория чисел)*

Михайлов Максим

19 июня 2022 г.

Оглавление

Лекция 1

3 марта

1 Алгебраические тела, обзор

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.

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

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

2 На пути к доказательству теоремы Фробениуса I

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

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. $\lessdot x \in T, \{x^0, x, x^2 \dots x^{n+1}\}$ — 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. $\exists \alpha, \beta, \gamma : \alpha + \beta u + \gamma v = 0$.

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

$$\lessdot uv + vu = -\frac{\gamma}{\beta} v^2 - \frac{\gamma}{\beta} v^2 = \frac{-2\gamma}{\beta} v^2 \in \mathbb{R}$$

$$-\frac{\alpha\gamma}{\beta} v + bv = \left(b - \frac{\alpha\gamma}{\beta}\right) v \in \mathbb{I}$$

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.

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

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

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

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

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:

$$u^2 = v^2 = w^2 = -1$$
$$uv = -vu = w$$
$$vw = -wv = u$$
$$wu = -uw = v$$

Доказательство. Дома. □

Лекция 3

18 марта

3 На пути к доказательству теоремы Фробениуса II

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.

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

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

□

Теорема 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 $il = -li, jl = -lj, kl = -lk$.

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

Примечание. Четвёртая лекция транслировалась в низком качестве, поэтому не была сохранена. Основной материал о кватернионах рассказан повторно в пятой лекции.

Лекция 5

2 апреля

4 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:

$$ij = k = -ji$$
$$jk = i = -kj$$
$$ki = j = -ik$$
$$i^2 = j^2 = k^2 = ijk = -1$$

Тогда умножение в явном виде:

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

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

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 $\sphericalangle \tilde{u} = \frac{\tilde{q}}{|\tilde{q}|}$. Тогда:

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

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

Лемма 7. $\forall v \in \mathbb{R}^3 \;\; |v| = |\mathcal{L}_q(v)|$ при $|q| = 1$

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

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

□

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

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

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

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

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

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

$$= (\cos^2\varphi - \sin^2\varphi)\vec{n} + 2\cos\varphi \cdot \sin\varphi \underbrace{[\tilde{u} \times \vec{n}]}_{\vec{n}_\perp}$$

$$= \cos 2\varphi \vec{n} + \sin 2\varphi \vec{n}_\perp$$

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

□

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):

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

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

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

Лекция 6

9 апреля

4.1 Напоминание о кватернионах

Кватернионы записываются как:

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

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

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

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.

5 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, $\det A = \det A^{\mathrm{T}}$ 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 $\det A = 1$

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

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

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 $a,b,c,d\in\mathbb{R}$.

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

$\cdot$	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 $\mathbb{R}^3$

6 $SU(2)$ 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, соттветствующих одной точке, называется **кратностью накрытия**. Кратность накрытия окружности — ∞.

Кратность накрытия для $SO(3)$ — 2.

Лекция 7

16 апреля

7 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.

$$T_0 \coloneqq \{z \in K \mid \left\|z - z_p\right\| < B\}, B \in \mathbb{R}_+$$

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

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

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

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.

Лекция 8

23 апреля

8 Топологические группы

8.1 Топология

Определение. Топология на множестве M — система подмножеств $\tau \subset 2^M$, $\tau = \{A_i\}_{i \in I}$, для которой выполнены **аксиомы топологии**:

1. $M, \varnothing \in \tau$
2. $\bigcup_i A_i \in \tau$
3. $\bigcap_i^{\text{кон.}} A_i \in \tau$

$T = (M, \tau)$ называется **топологическим пространством**.

Примечание. Множества A_i называются **открытыми**.

Пример.

- Дискретная топология τ_d — все подмножества открыты.
- Стандартная топология на прямой τ_s — топология открытых интервалов.
- Топология Зарисского на прямой τ_z — открытые множества суть открытые интервалы, из которых выкинуто конечно или счётное число точек.
- Топология окружности τ_c
- Антидискретная топология τ_a — открыто только M и $\varnothing$

Определение. Окрестность точки P — всякое открытое множество, содержащее точку P.

Рассмотрим произвольное $S \subset M$. Мы можем классифицировать точку P относительно S:

1. Внутренняя точка — $\exists O_P : O_P \subset S$
2. Внешняя точка — $\exists O_P : O_P \cap S = \varnothing$
3. Граничная точка — $\forall O_P \;\; O_P \cap S \neq \varnothing, O_P \cap \overline{S} \neq \varnothing$

Определение. Множество внутренних точек $\mathrm{Int}(S)$ [1] — **открытое ядро** S.

∂S — **граница** S.

$$S = \langle S \rangle \cup \langle M \setminus S \rangle \cup \partial S$$

Примечание. $\partial \langle S \rangle = \varnothing$

Рассмотрим отображение $\sigma : M_1 \longrightarrow M_2$, где $2^{M_1} = \{A_i\}, 2^{M_2} = \{B_j\}$

$$\sigma(A_i \cup A_k) = \sigma(A_i) \cup \sigma(A_k) \quad \sigma(A_i \cap A_k) \neq \sigma(A_i) \cap \sigma(A_k)$$

$$\sigma^{-1}(B_j \cup B_l) = \sigma^{-1}(B_j) \cup \sigma^{-1}(B_l) \quad \sigma^{-1}(B_j \cap B_l) = \sigma^{-1}(B_j) \cap \sigma^{-1}(B_l)$$

Определение. Рассмотрим топологические пространства $T_1 = (M_1, \tau_1)$ и $T_2 = (M_2, \tau_2)$. Тогда $\sigma^{-1}(\tau_2)$ — топология на M_1. Но на M_1 уже есть топология τ_1. Если τ_1 сильнее, чем $\sigma^{-1}(\tau_2)$, то σ называется **непрерывным** отображением.

Определение. Отображение называется непрерывным в точке $P \in M$, если:

$$\forall O_{\sigma(P)} \;\; \exists O_P : \sigma(O_P) \subset O_{\sigma(P)}$$

Определение. σ непрерывно, если прообраз всякого открытого множества открыт:

$$\forall B \in \tau_2 \;\; \sigma^{-1}(B) \in \tau_1$$

Эти определения эквивалентны.

Определение. Предельная точка последовательности — точка, в любой окрестности которой содержатся все элементы последовательности, начиная с некоторого номера.

Определение. Точка прикосновения множества — точка, в каждой окрестности которой находится хотя бы одна точка из множества.

Точка прикосновения — не всегда предельная точка и наоборот. Эти понятия совпадают, если выполнены **аксиомы счётности**:

1. У каждой точки есть счётная система определяющих окрестностей, т.е. любое открытое множество, содержащее эту точку, лежит в такой окрестности.
2. База топологии счётна.

[1] Также обозначается $\langle S \rangle$

Аксиомы отделимости:

1. Для любых двух точек p и q существуют окрестности O_p и O_q такие, что $q \notin O_p, p \notin O_q$.
2. У любых двух точек есть непересекающиеся окрестности.

   Примечание. Из 2 следует 1, но не наоборот. Контрпример — τ_z.
3. Для любого замкнутого множества и точки, не лежащей в нём, существуют непересекающиеся окрестности.
4. Для любых двух замкнутых непересекающихся множеств существуют непересекающиеся окрестности.

Лекция 9

30 апреля

8.2 Топологические группы

Определение. Топологическая группа — множество G такое, что:

1. G — группа с операцией μ, отобажением обратного элемента inv и единицей e.
2. G — топологическое пространство с топологией τ.
3. Операции μ, inv непрерывны в топологии τ.

Примечание. Отображение топологических пространств $f : T_1 \to T_2$ непрерывно, если:

$$\forall W \subset T_2 - \text{откр. } \exists V \subset T_1 - \text{откр. } f(V) \subset W$$

Примечание. Здесь и далее W_t, U_t, V_t обозначает открытую окрестность точки t.

Непрерывность μ:

$$x, y \in G, W = W_{\mu(x,y)} \implies \exists U = U_x, V = V_y : UV \subset W$$

Непрерывность inv:

$$x \in G, W = W_{\text{inv}(x)} \implies \exists U = U_x : U^{-1} \subset W$$

$$x, y \in G, W = W_{\mu(x,\text{inv}(y))} \implies \exists U = U_x, V = V_y : UV^{-1} \subset W$$

Пример. $\mathbb{R}^2$ со операцией сложения и окрестностью $O_v, v \in \mathbb{R}^2$:

$$O_v \coloneqq \{u \in \mathbb{R}^2 \mid \|u - v\| < \alpha, \alpha \in \mathbb{R}_+\}$$

Пример. Группа $U(1)$ — группа поворотов окружности:

$$U(1) \coloneqq \{z \mid |z| = 1\}$$

Пример. Группа всех матриц $GL(n)$.

Норма порождена скалярным произведением $\langle A, B\rangle = \operatorname{tr} A^{\mathrm{T}}B$.

Свойства.

1. $\forall \{x_i\}_{i=1}^n$ — совокупность элементов G, $\{V_i\}$ — их окрестности.

   $\forall y = x_1^{m_1}x_2^{m_2}\dots x_n^{m_n}$ и W — окрестность y. Тогда $V_1^{m_1}V_2^{m_2}\dots V_n^{m_n} \subset W$

   Доказательство. По индукции. □

2. $\forall f_a, f_b', \varphi : G \to G, f_a(x) = xa, f_b'(x) = bx, \varphi(x) = \operatorname{inv}(x)$. Это гомеоморфизмы.

   Доказательство. f_a — биекция по свойствам группы.

   Непрерывность: пусть $f_a(x) = xa = y$. $\forall W = W_y$, тогда $\exists U = U_x, V = V_a : UV \subset W \implies Ua \subset W \implies f_a(U) \subset W$ □

3. $\forall P$ — подмножество G, F — замкнутое в G, U — открытое в G. Тогда $\forall a \in G\ aF, Fa, F^{-1}$ замкнутые и UP, PU, U^{-1} открыты.

   Доказательство. $Fa = f_a(F)$, но f_a гомеоморфизм.

   $UP = \bigcup_{x\in P} \underbrace{Ux}_{\text{откр.}}$ и объединение открытых множеств открыто. □

4. Однородность: $\forall p, q \in G\ \exists f \in \operatorname{homo}(G) : f(p) = q$

   Это значит, что топологические свойства группы однозначно определяются её свойствами в окрестности какой-либо точки.

5. Регулярность: $\forall x \in G, S \subset G$ — замкнутое, $x \notin S \implies \exists O_x, O_S : O_x \cap O_S = \{\varnothing\}$

   Доказательство. Пусть e — нейтральный элемент группы G, $V = V_e$.

   $$e^{-1}e = e \implies \exists U = U_e : U^{-1}U \subset V$$

   Покажем, что $\overline{U} \subset V$.

   $$\forall x \in \overline{U} \implies \exists O_x : O_x \cap U \neq \varnothing$$

   xU содержит точку x, т.к. $e \in U$, следовательно $\exists b \in U : xb = a \in U, x = ab^{-1} \in UU^{-1} \subset V \implies \overline{U} \subset V$ □

6. Пусть H — топологическая подгруппа G. Тогда:

   (a) gH открыто.

   (b) H замкнуто и H — компонента связности.

Теорема 8. Пусть G — связная топологическая группа, т.е. у нее нет подгрупп. Пусть e — нейтральный элемент $G, U = U_e$.

Тогда U индуцирует все G.

Доказательство. $\lessdot V = U \cap \mathrm{inv}(U)$. Тогда $V^{-1} = V$.

$\lessdot V_1 \subset V_2 \subset \ldots \subset V_n \subset \ldots \subset V_\infty$, где $V_i = V_{i-1}V$, а $V_1 = V$.

По определению $V_i = \bigcup_{p \in V} V_{i-1}p$ и объединение открытых открыто. Тогда по индукции V_∞ открыто, но при этом оно содержит все элементы группы, т.е. замкнуто. Таким образом, V_∞ открыто и замкнуто, т.е. является компонентой связности, и т.к. G связна, $V_\infty = G$. □

Лекция 10

7 мая

9 p-адические числа

9.1 Модули

Определение. Модуль — функция $|\cdot| : \mathbb{K} \to \mathbb{R}_+$ такая, что:

1. $|x| = 0 \iff x = \mathbb{0}$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

Определение. Модуль **неархимедов**, если $|x + y| \leq \max(|x|, |y|)$

Примечание. Из неархимедовости следует третье свойство модуля.

Определение. Тривиальный модуль: $|x| := \begin{cases} 0, & x = \mathbb{0} \\ 1, & x \neq \mathbb{0} \end{cases}$

Определение. p-адическая оценка[1], где p — простое число:

$$v_p(x) := \begin{cases} +\infty, & x = 0 \\ n, & x \in \mathbb{Z} \wedge x = p^n \cdot \tilde{x} \wedge \tilde{x} \not\vdots p \\ v_p(m) - v_p(k), & x = \frac{m}{k} \end{cases}$$

Определение (p-модуль). $|x|_p := p^{-v_p(x)}$

Лемма 10.

$$v_p(xy) = v_p(x) + v_p(y)$$

[1] Modulation

$$v_p(x+y) \geq \min(v_p(x), v_p(y))$$

Доказательство. Пусть $x = p^k\tilde{x}, y = p^l\tilde{y}$ и $\tilde{x}, \tilde{y} \not\vdots p$.

$$xy = p^k\tilde{x} \cdot p^l\tilde{y} = p^{k+l}\tilde{x}\tilde{y}$$

Пусть $k > l$.

$$x + y = p^k\tilde{x} + p^l\tilde{y} = p^l(p^{u-l}\tilde{x} + \tilde{y})$$

□

Лемма 11. Определение $|\cdot|_p$ корректно, т.е. $|\cdot|_p$ — модуль.

Доказательство.

$$|xy|_p \overset{\text{def}}{=} p^{-v_p(xy)} \overset{(2)}{=} p^{-v_p(x)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} \overset{\text{def}}{=} |x|_p|y|_p$$

$$|x+y|_p \overset{\text{def}}{=} p^{-v_p(x+y)} \overset{(3)}{\leq} p^{-\min(v_p(x),v_p(y))} = \max(p^{v_p(x)}, p^{v_p(y)}) \overset{\text{def}}{=} |x|_p|y|_p$$

□

Забавный факт: $\lim_{n\to+\infty} |p^n|_p \to 0$

Лемма 12. Свойства модуля в произвольном $\mathbb{K}$:

1. $|e| = 1$
2. $\exists n : x^n = e \implies |x| = 1$
3. $|-e| = 1$
4. $|-x| = x$

Доказательство.

1. $|e| = |e \cdot e| = |e| \cdot |e| = 1$
2. $1 = |e| = |x^n| = |x|^n$
3. $|-e \cdot -e| = |e^2| = 1$
4. Из предыдущего пункта.

□

Лемма 13. $x \neq |y| \implies |x+y| = \max(|x|, |y|)$

Доказательство. Пусть $|x| > |y|$.

$$|x + y| \leq \max(|x|, |y|) = x$$

$$|x| = |(x + y) - y| \leq \max(|x + y|, |y|) = |x + y|$$

$$\left.\begin{matrix} |x + y| \leq |x| \\ |x| \leq |x + y| \end{matrix}\right\} \implies |x + y| = |x|$$

□

Лемма 14.

$$|x + y| \leq \max(|x|, |y|) \iff |z + 1| \leq \max(|z|, 1)$$

Доказательство.

$\implies$ очевидно

$\impliedby$ Рассмотрим случай $y = \mathbb{0}$. Тогда $\forall x \;\; |x| \leq \max(|x|, 0) = |x|$ очевидно верно.

Рассмотрим случай $y \neq \mathbb{0}$. Тогда пусть $z = \frac{x}{y}$.

$$\left|\frac{x}{y} + 1\right| \leq \max\left(\left|\frac{x}{y}\right|, 1\right) \implies |x + y| \leq \max(|x|, |y|)$$

□

Утверждение. $|x| \leq 1 \implies |x - 1| \leq 1$

Определение. Метрика, порожденная модулем: $d(x, y) \coloneqq |x - y|$

Лемма 15. Если модуль неархимедов, то $d(x, y) \leq \max(d(x, z), d(z, y))$

Утверждение. Все треугольники в $\mathbb{K}$ с неархимедовым модулем равнобедренные.

Пример. $x = p^k\tilde{x}, y = p^l\tilde{y}, \tilde{x}, \tilde{y} \not\vdots p$ Если $k > l$:

$$p^k\tilde{x} + p^l\tilde{y} = p^l \underbrace{(p^{k-l}\tilde{x} + \tilde{y})}_{\not\vdots p}$$

Если $k = l$:

$$p^k\tilde{x} + p^k\tilde{y} = p^k \underbrace{(\tilde{x} + \tilde{y})}_{\text{может } \vdots p}$$

Пример. $p_1 = 5, p_2 = 3$

$$|50|_5 = |5^2 \cdot 2|_5 = 5^{-2} = \frac{1}{25} \quad |50|_3 = 1$$

$$|17|_5 = 5^{-0} = 1 \quad |17|_3 = 1$$

$$|15|_5 = 5^{-1} = \frac{1}{5} \quad |15|_3 = 3^{-1} = \frac{1}{3}$$

$$\left|\frac{3}{25}\right|_5 = 5^{-(0-2)} = 25 \quad \left|\frac{3}{25}\right|_3 = 3^{-(1-0)} = \frac{1}{3}$$

Пример. $x = \frac{2}{15}, y = \frac{3}{15}, z = \frac{7}{15}$

$$|x-y|_5 = \left|\frac{1}{15}\right|_5 = 5^{-(0-1)} = 5 \quad |x-y|_3 = \left|\frac{1}{15}\right|_3 = 3$$

$$|x-z|_5 = \left|\frac{1}{3}\right|_5 = 1 \quad |x-z|_3 = \left|\frac{1}{3}\right|_3 = 3$$

$$|y-z|_5 = \left|\frac{4}{15}\right|_5 = 5 \quad |y-z|_3 = \left|\frac{4}{15}\right|_3 = 3$$

Мы получили равносторонний треугольник при $|\cdot|_3$.

Определение.

$$B := \{x \mid d(x, x_0) < r\}$$
$$\overline{B} := \{x \mid d(x, x_0) \le r\}$$

Лемма 16.

1. $b \in B(a,r) \implies B(b,r) = B(a,r)$, аналогичное верно для $\overline{B}$
2. $B(a,r)$ — открытое и замкнутое. Если $r \neq 0$, то $\overline{B}(a,r)$ — тоже открытое и замкнутое.
3. $r > s, B(a,r) \cap B(b,s) \neq \varnothing \implies B(b,s) \subset B(a,r)$

Доказательство.

1. $|b-a| < r$.

   $\forall x \in B(a,r) \quad |x-b| \le \max(|x-a|, |b-a|) < r \implies x \in B(b,r) \implies B(a,r) \subset B(b,r)$

2. Рассмотрим точку вне шара, она принадлежит с некоторой окрестностью дополнению шара, следовательно дополнение открыто, следовательно шар замкнут.
3. $B(a,s) = B(c,s) \subset B(c,r) = B(b,r)$

□

Лекция 11

14 мая

9.2 Теорема Островского

Примечание. Аксиома Архимеда:

$$\forall \varepsilon, M \ \ \exists n \in \mathbb{N} : n\varepsilon > M$$

У архимедовости поля есть связь с аксиомой Архимеда, сейчас мы её найдём.

Определение.

$$Z : \mathbb{Z} \to \mathbb{K} \quad Z(n) := \begin{cases} \mathbb{0}, & n = 0 \\ \mathbb{1} + \mathbb{1} + \ldots + \mathbb{1}, & n \in \mathbb{N} \\ -(\mathbb{1} + \mathbb{1} + \ldots + \mathbb{1}), & n < 0 \end{cases}$$

Теорема 9. Модуль неархимедов $\iff \forall n \in \mathbb{Z} \ \ |Z(n)| \leq 1$

Доказательство.

$\Longrightarrow$ $|\mathbb{0}| = 0$, поэтому $|Z(0)| \leq 1$ выполнено, для отрицательных n будет верно, если докажем для положительных n. Докажем по индукции:

База. $|1| = 1 \leq 1$

Индукция. Пусть $|k| \leq 1$, тогда $|k+1| \leq \max(|k|, 1) \leq 1$

$\Longleftarrow$ $\lessdot m \in \mathbb{N}$

$$|x+1|^m = |(x+1)^m|$$

$$\overset{\text{бином Ньютона}}{=} \left| \sum_{i=0}^{m} z\left(C_m^i\right) x^i \right| \leq \sum_{i=0}^{m} |z(C_m^i)||x|^i$$

$$\leq \sum_{i=0}^{m} |x|^i = 1 + |x| + |x|^2 + \ldots + |x|^m$$
$$\leq (m+1)\max(|x|^m, 1)$$

$$\forall m \in \mathbb{N} \quad |x+1|^m \leq \max(|x|^m, 1) \implies |x+1| \leq \max(|x|, 1)$$
$$\implies \lim_{m\to+\infty} |x+1| \leq \lim_{m\to\infty} \sqrt[m]{m+1}\max(|x|, 1)$$
$$\implies |x+1| \leq \max(|x|, 1)$$

□

Определение. Модуль $|\cdot|_1$ **эквивалентен** $|\cdot|_2$, если $\exists \alpha \in \mathbb{R} : \forall x \in \mathbb{K} \ \ |x|_1 = |x|_2^\alpha$

Теорема 10 (Островский)**.** Любой нетривиальный модуль над $\mathbb{Q}$ эквивалентен либо $|\cdot|_p$, либо $|\cdot|_\infty$

Доказательство. Рассмотрим архимедов модуль $|\cdot|$.

Тогда по определению $\exists n \in \mathbb{Z} : |Z(n)| > 1$. Пусть n_0 — минимальный такой n, $|n_0| =: x$.

$\exists \alpha : x = n_0^\alpha$, $\alpha = \log_{n_0} x$. Будем доказывать, что это α подходит как коэффициент эквивалентности рассматриемого модуля и $|\cdot|_\infty$, т.е. рассмотрим произвольное $n \in Z(\mathbb{N})$ и покажем, что $|n| = |n|_\infty^\alpha$.

Выпишем n в системе счисления с основанием n_0:

$$n = \sum_{i=0}^{k} a_i n_0^i, \quad 0 \leq a_i < n_0, a_k \neq 0, n_0^k \leq n < n_0^{k+1}$$

$$|n| = \left|\sum_{i=0}^{k} a_i n_0^i\right| \leq \sum_{i=0}^{k} |a_i| n_0^{i\alpha} \leq \sum_{i=0}^{k} n_0^{i\alpha} = n_0^{k\alpha} \sum_{i=0}^{k} n_0^{-i\alpha} \leq n_0^{k\alpha} \sum_{i=0}^{\infty} n_0^{i\alpha} = n_0^{k\alpha} \underbrace{\left(\frac{n_0^\alpha}{n_0^\alpha - 1}\right)}_{C} \leq n^\alpha C$$

Подставим n вместо $n^N, N \in \mathbb{N}$.

$$|n|^N = |n^N| \leq C \cdot n^{N\alpha} \implies \lim_{N\to\infty} |n| \leq \overbrace{\lim_{N\to\infty} \sqrt[N]{C}}^{\to 1} n^\alpha \implies |n| \leq n^\alpha \tag{4}$$

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|$$

$$|n| \geq n_0^{(k+1)\alpha} - |n_0^{k+1} - n|$$

$$
\begin{aligned}
&\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha \\
&\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha \\
&= n_0^{(k+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\
&=: n_0^{(k+1)\alpha} \tilde{C} \\
&> \tilde{C} n^\alpha
\end{aligned}
$$

По предельному переходу как в (4) получается $|n| \geq n^\alpha$. Но из (4) $|n| \leq n^\alpha$, следовательно $|n| = n^\alpha$ и архимедов модуль эквивалентен $|\cdot|_\infty$.

Рассмотрим неархимедов модуль $|\cdot|$, тогда по определению $\forall n \in \mathbb{N} \;\; |Z(n)| \leq 1$.

$\exists \tilde{n} : |Z(\tilde{n})| < 1$, т.к. иначе модуль был бы тривиальным.

$$n_0 \coloneqq \min\{\tilde{n} : |Z(\tilde{n}) < 1\}$$

Утверждение. n_0 простой.

Доказательство. Пусть $n_0 = a \cdot b, \;\; a, b > 1$. Т.к. $a, b < n_0$, то $|a| = |b| = 1 \implies |n_0| = |ab| = |a| \cdot |b| = 1$, но $|n_0| < 1$ — противоречие. □

Обозначим тогда n_0 за p.

$\lhd n = pq + s, s \neq 0, s < p$ и $|s| = 1$.

$$\left.\begin{aligned} |p| < 1 \\ |q| \leq 1 \end{aligned}\right\} \implies |pq| = |p||q| < 1 \implies |n| = 1$$

$$n = p^v n', n' \not\vdots p \implies |n| = |p^v| \cdot |n'| = |p|^v = c^{-v}, c = |p|^{-1}$$

α, которое даст нам эквивалентность, это $\log_{|p|^{-1}} p$, т.к. $(|p|^{-1})^{-v\alpha} = p^{-v}$. □

Примечание. Это доказательство — для $\mathbb{N}$, но переход к $\mathbb{Q}$ очевиден. Зная, что $\forall n \in \mathbb{N} \;\; |n| = n^\alpha$ мы можем показать, что $\left|\frac{a}{b}\right| = \left(\frac{a}{b}\right)^\alpha$:

$$\left|\frac{a}{b}\right| = \left(\frac{a}{b}\right)^\alpha \iff |a| = \left(\frac{a}{b}\right)^\alpha b^\alpha \iff |a| = a^\alpha$$

Утверждение.

$$\forall n \in \mathbb{Q} \qquad \prod_{p \in \mathbb{P} \cup \{\infty\}} |n|_p = 1$$

Доказательство. Разложим n на простые множители:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$|n|_\infty = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$p \neq p_i \implies |n_p| = 1$$

$$p = p_i \implies |n|_p = p^{-\alpha_i}$$

□

Определение. (x_n) — **последовательность Коши**[1], если

$$\forall \varepsilon > 0 \;\; \exists M \in \mathbb{N} : \forall m, n \geq M \;\; |x_m - x_n| < \varepsilon$$

Определение. Поле $\mathbb{K}$ **полное**, если любая последовательность Коши имеет предел в $\mathbb{K}$.

Определение. $S \subset \mathbb{K}$ **плотно** в $\mathbb{K}$, если

$$\forall \alpha \in \mathbb{K} \;\; \forall U_x \;\; \exists s \in S : s \in U_x$$

Поле рациональных чисел $\mathbb{Q}$ не полное, поэтому мы его пополнили до $\mathbb{R}$. Мы сделаем аналогично: рассмотрим множество последовательностей Коши $\mathrm{CS}(\mathbb{K})$ и факторизуем его: $\mathrm{CS}(\mathbb{K})/N$, где $N := \{(x_n) : x_n \xrightarrow[n \to +\infty]{} 0\}$. Таким образом (с p–адическим модулем) мы получим p–адические числа.

Примечание. Рациональные числа плотны в p–адических числах.

p–адические числа записываются как:

$$\sum_{i=-k}^{+\infty} a_i p^i$$

в противопоставление $\mathbb{R}$, которые записываются как:

$$\sum_{i=-\infty}^{k} a_i 10^i$$

[1] Или фундаментальная последовательность.