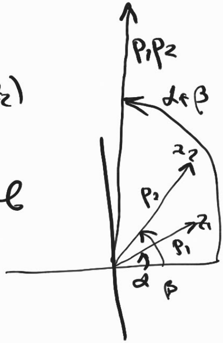
Лекция 1 октября (вторая половина)

Умножение радиус-векторов на плоскости:



$$|z_1z_2| = |z_1||z_2|$$
$$\mathrm{Arg}(z_1z_2) = \mathrm{Arg}(z_1) + \mathrm{Arg}(z_2)$$

Факт: Так определённое умножение радиус-векторов превращает векторы из евклидова $\mathbb{R}^2$ в **поле**.

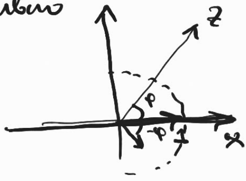
векторы – абелева группа по сложению

умножение – коммутативно

имеет единицу $= 1$

у каждого $z \neq 0$ есть z^{-1}

$$|z^{-1}| = \frac{1}{|z|}$$
$$\mathrm{Arg}\, z^{-1} = -\mathrm{Arg}\, z.$$



$\boxed{(a+b)c = ac+bc} \Leftrightarrow$ преобразование

$\mu_c : \mathbb{R}^2 \to \mathbb{R}$

умножение на c

$z \longmapsto zc$

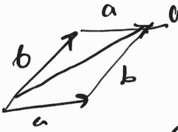
сохраняет суммы

$\mu_c(a+b) = \mu_c(a) + \mu_c(b)$

$|z| \mapsto |z|\cdot|c|$ растягивает длины в $|c|$ раз отн. нуля

$\operatorname{Arg} z \mapsto \operatorname{Arg} z + \operatorname{Arg} c$ поворачивает всё на угол $\operatorname{Arg} c$

M_c – поворотная гомотетия.



повор и гомотетии пар-мы ⟶ пар-мы

$\mathbb{R}^2$ – это поле

$\mathbb{C} \longrightarrow \mathbb{R}^2$

$[x+iy] \longmapsto z=(x,y)$

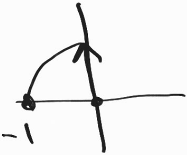
изоморфизм полей? Линейный изоморфизм?

векторных пространств

$(x_1+iy_1)(x_2+iy_2) =$

$= x_1x_2 + \underbrace{i\,i\,y_1y_2} +$

$+ (x_1y_2 + x_2y_1)i$

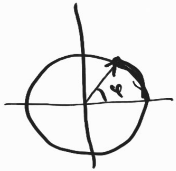


$i^2 = -1$

$i \in \mathbb{R}^2$
ведёт себя
как класс $[t] = \sqrt{-1} \in \mathbb{C}$

$\sin 3\varphi = ?$

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



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

$$= \cos^n\varphi + n i \cos^{n-1}\varphi \sin\varphi + \ldots =$$

$$= \underbrace{\sum \binom{n}{k} \cos^{n-k}\varphi \cdot i^k \cdot \sin^k\varphi}$$

$$\| \quad \underbrace{\cos n\varphi + i \sin n\varphi}$$

$$\cos n\varphi = \binom{n}{0}\cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi \sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi$$

$$\sin n\varphi = \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \ldots$$

Конечные поля!

$\mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/(2)$

$x^2 + 1 = (x+1)^2$

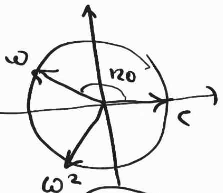
$x^2 + x + 1$ — неприводим

$x^2 + x = x(x+1)$

нет корней в $\mathbb{F}_2$ $\longrightarrow$ x^2+x+1

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[x]}{(x^2+x+1)} = \left\{ a + b\omega \;\middle|\; \begin{array}{l} a, b \in \mathbb{F}_2 \\ \omega : \omega^2 + \omega + 1 = 0 \end{array} \right\}$$

(похоже на $\mathbb{C}$



роль "комплексного сопряжения" играет Фробениус $x \longmapsto x^2$

$(\omega^2)^2 = \omega^4 = \omega$

$\boxed{z^3 = 1}$

$z^3 - 1 = (z-1)(z^2+z+1)$

$\mathbb{F}_3 = \{0, 1, -1\} = \mathbb{Z}/3$ $\qquad$ $(\omega^2+\omega+1=0)$

$\omega^2 = \overline{\omega}$

$$\mathbb{F}_9 = \frac{\mathbb{F}_3[x]}{(x^2+1)}$$

x^2+1 - неприводим в $\mathbb{F}_3[x]$

$$\| $$

$$\left\{ a+bi \;\middle|\; \begin{matrix} a,b\in\mathbb{F}_3 \\ i^2=-1 \end{matrix} \right\}$$

Теорема: Во всяком конечном поле $\mathbb{F}$ должно быть p^n элементов, где $p=\mathrm{char}\,\mathbb{F}$ а $n=\dim\mathbb{F}$ как векторного пр-ва над простым подполем.

$$|\mathbb{F}|<\infty \Rightarrow \mathrm{char}\,\mathbb{F}=p>0$$ - простое число

$$(\underbrace{1+\dots+1}_{p}=0)$$

$\mathbb{F}\supset\mathbb{F}_p$ - простое подполе = наименьшее по включению подполе в $\mathbb{F}$

$\mathbb{F}$ - векторное пр-во над $\mathbb{F}_p$ конечномерное, допускает базис $e_1,\dots,e_n$: любой $\xi\in\mathbb{F}$ однозначно записывается как $x_1e_1+x_2e_2+\dots+x_ne_n$, с $x_i\in\mathbb{F}_p$.

$\xi\mapsto(x_1,\dots,x_n)\in\mathbb{F}_p^n$ - это биекция

$n = \dim_{\mathbb{F}_p}\mathbb{F}$

$|\mathbb{E}| = p^n = p^{\quad\ _{\mathbb{F}_p}}.$

Теорема 3 Для каждого простого $p \in \mathbb{N}$ и каждого $n \in \mathbb{N}$ имеется единственное с точностью до изоморфизма поле $\mathbb{F}_q$, состоящее из $q = p^n$ элементов.

Док-во: Построим конкретное поле $\mathbb{F}_q$ из $q = p^n$ элементов.

Отступление: $\forall$ кольца с единицей? без делителей нуля K и любого приведённого многочлена $f \in K[t]$ можно построить такое кольцо $L \supset K$, что $f(t)$ будет в $L[t] \supset K[t]$ многочлен полностью разлагаться в произведение линейных множителей $(t-\alpha_1)\cdot\ldots\cdot(t-\alpha_n)$ где $n = \deg f$.

Индукция по $\deg f$. Пусть для всех $h \in K[t]$ с $\deg h < \deg f$ факт верен.

① $f = h_1 h_2$ – приводим.

$\exists L_1 \supset K$: h_1 полностью разложится

$\exists L_2 \supset L_1$: h_2 полностью разложится

в L_2 $f = h_1 h_2$ полностью разложится

② f – неприводим.

$$\boxed{L_1 = \frac{K[x]}{(f)}} \supset K \leftarrow \text{константы}$$

если K – поле, то и L получится полем.

$K \hookrightarrow K[x]$ – вложение

$c_1 - c_2 \not\vdots\, (f)$ $\quad \deg f > 0$

в $L_1[x]$ f становится приводим

т.к. $[x] = \theta$ – это корень f $\rightarrow$

$f = (x - \theta)\, q(x)$ в $L_1[x]$

Дальше как в ①

Построим кольцо $\mathbb{K} \supset \underline{\underline{\mathbb{F}_p}}$: многочлен

$f(x) = x^{p^n} - x$ полностью разложится в

$\mathbb{K}[x]$ на линейные множители.

можно считать $\mathbb{K}$ полем

Корни многочлена f в поле $\mathbb{K}$

$\boxed{\alpha_1, \dots, \alpha_{p^n}}$ составляют поле.

$$\alpha^{p^n} - \alpha = 0 \Leftrightarrow \alpha^p = \alpha \quad \beta^{p^n} = \beta \Rightarrow$$

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$$

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha+\beta$$

$\underbrace{(\alpha+\beta)^p = \alpha^p + \beta^p}$ в поле характеристики p

построим поле $\mathbb{F}_q$ из p^n элементов = = корней? многочлена $\underline{x^{p^n}-x}$ в некотором расширении $\mathbb{K}$ поля $\mathbb{F}_p$.

Почему все корни у этого многочлена разные? и почему их ровно p^n штук?

Внимание!

в листок 3 добавилась задача 13.5 (г): перечислить все квадраты в полях $\mathbb{F}_4$, $\mathbb{F}_8$ и $\mathbb{F}_9$