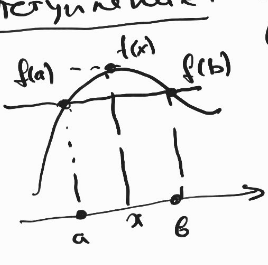
Лекция 8 октября (первая половина)

Теорема: Во всяком конечном поле p^n элементов (где $n \in \mathbb{N}$, $p \in \mathbb{N}$ - простое). Причём $\forall n, p$ такое поле существует и единственно с точностью до изоморфизма

Конструкция поля: расширение $\mathbb{F} \supset \mathbb{F}_p$ в котором многочлен $x^{p^n}-x$ полностью раскладывается на линейные множители; Все корни α многочлена $x^{p^n}-x$ в поле $\mathbb{F}$ образуют подполе $\mathbb{F}_q = \{\alpha \in \mathbb{F} \mid \alpha^{p^n} = \alpha\}$

- Почему у многочлена $x^{p^n}-x$ все корни разные?

Отступление: формальное дифф. исчисление в $\mathbb{k}[[x]]$.



Что такое производная от $f(x) = \underline{\text{наклон касат}}$

?

наклон секущей

$$\frac{f(b)-f(a)}{b-a} \in \mathbb{k}[[a,b]]$$

$$f(x) = x^n \qquad \frac{b^n-a^n}{b-a} = \underbrace{b^{n-1}+b^{n-2}a+\ldots+a^{n-1}}_{n}$$

многочлен

$$\frac{a^2-b^2}{a-b} \qquad \frac{a^3-b^3}{a-b}$$

$$f(x) = a_0 + a_1x + a_2x^2 + \dots$$

$$\frac{f(a)-f(b)}{a-b} = \underset{}{\overset{\frac{a-b}{a-b}}{a_1}} + a_2\underset{x+x}{(a+b)} + a_3\underset{x^2+x^2+x^2}{(a^2+ab+b^2)} + \dots$$

Опр. 1 Производная — это значение дроби $\dfrac{f(a)-f(b)}{a-b}$ при $a=b=x$

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \dots$$

сумма единиц в $\mathbb{k}$.

$$f(x) = a_0 + a_1x + a_2x^2 + \dots$$

Отображение дифференцирования:

$$\frac{d}{dx} : \mathbb{k}[[x]] \to \mathbb{k}[[x]]$$

$$f(x) \mapsto f'(x)$$

линейно над $\mathbb{k}$: $(\lambda f + \mu g)' = \lambda f' + \mu g'$

$\forall f, g \in \mathbb{k}[[x]] \quad \forall \lambda, \mu \in \mathbb{k}$

Опр. 2 $f(x+\delta) \in \mathbb{k}[x, \delta]$

$$\| \quad f(x) + \underline{\delta \cdot f'(x)} + \delta^2(\dots\dots)$$

члены делящиеся на δ^2

$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$

$f(x+\delta) = a_0 + a_1(x+\delta) + a_2\underset{2x\delta}{(x+\delta)^2} + a_3\underset{3x^2\delta}{(x+\delta)^3} + \dots$

$$\overset{\shortparallel}{f}(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

$$+$$

$$\delta f'(x) = \delta(\underbrace{a_1 + 2a_2 x + 3a_3 x^2 + \dots}_{f'(x)})$$

производная $f'(x)$ это такой ряд, что

$$f(x+\delta) = f(x) + f'(x)\cdot\delta + \delta^2 \underbrace{\cdots\cdots}_{k[x]}$$

члены, делимые на δ^2

Предупреждение: производная может обращаться в нуль, если char $k \neq 0$, даже когда ряд не константа!

$(x^p)' = \underbrace{p}_{=0} x^{p-1} = 0$ если char $k = p$

Упр. Доказать свойства дифф-я:

(1) правило Лейбница:

$$[fg]' = f'g + f\cdot g'$$

(2) производная композиции:

$$[f(g(x))]' = f'(g(x))\cdot g'(x)$$

$\forall f \in \Bbbk[[x]]$ $\forall g \in x\Bbbk[[x]]$

ряды без свободного члена

$$g = a_1x + a_2x^2 + \dots$$

$$f(x) = b_0 + b_1x + b_2x^2 + \dots$$

$$f(g(x)) = b_0 + b_1(a_1x + a_2x^2 + \dots) + b_2(a_1x + a_2x^2 + \dots)^2 + b_3(a_1x + a_2x^2 + \dots)^3$$

$$= b_0 + b_1a_1x + \dots$$

на коэффициент при x^k влияет лишь конечное число коэффициентов из первых k скобок.

(3) $\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}$ $\forall$ ряда g с ненулевым свободным членом

Упражнение на дом

(действовать по 2-му определению производной)

Пример:

$$f(x+\delta)g(x+\delta) = (f(x)+f'(x)\delta+\delta^2(\dots))\times$$
$$(g(x)+g'(x)\delta+\delta^2(\dots)) =$$
$$= f(x)g(x)+\delta\cdot(f(x)g'(x)+g(x)f'(x))+$$
$$+\delta^2(\dots\dots)$$

Факт: Корень α является кратным корнем многочлена f (т.е. $f(x)$ делится на $(x-\alpha)^2$) $\Leftrightarrow f'(\alpha)=0$

$$f(x)=(x-\alpha)^2 g(x)$$
$$f'(x)=\underline{2(x-\alpha)g(x)}+\underline{(x-\alpha)^2 g'(x)}$$
$$f'(\alpha)=0$$

если α - простой корень, т.е.

$$f(x)=(x-\alpha)g(x) \text{ и } g(\alpha)\neq 0$$
$$f'(x)=g(x)+(x-\alpha)g'(x)$$
$$f'(\alpha)=g(\alpha)\neq 0$$

У многочлена $\underbrace{x^{p^n}-x}_{f}$ нет кратных корней, т.к.

$$f'=-1 \qquad (x^{p^n})'=0$$

Единственность в теореме

"любое" поле $\mathbb{F}$ из $q = p^n$ элементов изоморфно построенному нами полю $\mathbb{F}_q$ из корней многочлена $f(x) = x^{p^n} - x$

Мультипликативная группа $\mathbb{F}^* = \mathbb{F} \setminus 0$ циклическая : $\exists \xi \in \mathbb{F} \setminus 0$:

$$\mathbb{F} \setminus 0 = \{1, \xi, \xi^2, \dots, \xi^{q-1}\}$$

Теорема: Конечная мультипликативная подгруппа в поле всегда циклическая.

Док-во: $G \ni a \quad |G| < \infty$

$a^k = a^m$ для $k, m \in \mathbb{N}$

$k \geq m$

$a^{k-m} = 1$

т.е. $\exists r \in \mathbb{N} : a^r = 1$ наименьшее такое r наз. порядком элемента a.

все степени элемента порядка r - это

$1, a, a^2, \dots, a^{r-1}$

$a^n = a^{rd+s} = a^s \quad 0 \leq s \leq r-1$

Надо найти элемент a, порядок которого равен порядку группы.

Возьмём в качестве a элемент максимального в G порядка пусть это $\underline{r}$.

Достаточно показать, что порядок любого элемента является делителем r

В этом случае все элементы удовл. уравнению $\boxed{x^r = 1}$

в поле имеется не более r таких элементов

и таких элементов имеется $|G|$

$\Rightarrow r = |G|$

$$\{G = 1, a, a^2, \ldots, a^{r-1}\}$$

Почему порядок любого элемента делит максимальный из порядков?

Достаточно $\forall\, a, b \in G$ порядков α и β построить элемент с порядком НОК(α, β)

если α и β взаимно просты, то

$c = ab$ имеет порядок $\alpha\beta$

$$(ab)^s = \underset{b^\beta}{\underset{\shortparallel}{1}} \qquad \underline{a^s = b^{\beta-s}}$$

$$\downarrow$$

$$b^{\alpha(\beta-s)} = a^{s\alpha} = 1$$

$$\underline{\alpha(\beta-s) \vdots \beta \Rightarrow \beta - s \vdots \beta \Rightarrow s \vdots \beta}$$

по тем же причинам $s \vdots \alpha \Rightarrow s \vdots \alpha\beta$

$(ab)^{\alpha\beta} = 1$ $\quad$ $\alpha\beta$ - порядок c.

если α и β не взаимно просты

$\alpha = p_1^{n_1} \cdots p_s^{n_s}$ $\quad$ $p_1, \ldots, p_s$ - все различные простые делители α и β.

$\beta = p_1^{m_1} \cdots p_s^{m_s}$

$\text{НОК} = A \cdot B \leftarrow p_i^{m_i}$ у которых $m_i < n_i$

$\uparrow$

те $p_i^{n_i}$ у которых $n_i \geq m_i$

$\boxed{\text{НОД}(A, B) = 1}$ $\quad$ $\left.\begin{array}{l} \alpha = A \cdot k \\ \beta = B \cdot m \end{array}\right]$

a^k и b^m у них порядки A и B,

$c = a^k b^m$ имеет порядок $AB = \text{НОК}(a,b)$

$$\begin{tikzcd}
 & \mathbb{F}^* = \{1, \xi, \ldots, \xi^{q-1}\} \arrow[d, phantom, "\parallel"] \\
\mathbb{K} \arrow[ur, "\sim"] \arrow[r, "\sim"'] & \mathbb{F}_q
\end{tikzcd}$$

построим некое новое поле $\mathbb{K}$, изоморфное обоим.

Элемент ξ – корень некоторого многочлена из $\mathbb{F}_p[x]$ например $\underline{\underline{\xi^q = 1}}$

Пусть $g \overset{\in \mathbb{F}_p[x]}{-}$ многочлен $\overset{?}{\text{наименьшей}}$ степени, $\overset{?}{\text{приведённый}}$, с корнем ξ.

Тогда он неприводим. $g(x) = g_1(x) \cdot g_2(x)$

$$0 = g(\xi) = \underline{g_1(\xi)}\, \underline{g_2(\xi)}$$

Поэтому $\dfrac{\mathbb{F}_p[x]}{(g)}$ – это поле.

$$\frac{\mathbb{F}_p[x]}{(g)} \xhookrightarrow{\sim} \mathbb{F}$$

$$[x] \longmapsto \xi$$

$$[h] \longmapsto h(\xi)$$

корректно определено:

$[h_1] = [h_2]$ $\quad h_1 = h_2 + g\cdot q$

$$h_1(\xi) = h_2(\xi) + \overset{0}{\cancel{g(\xi)}}\cdot q(\xi)$$

Это вложение.

Это наложение, т.к. $\mathbb{F} = \{1, \xi, \xi^2, \dots\}$

$[1][x][x^2]\dots x^{q-1}$

$\frac{\mathbb{F}_p[x]}{(g)}$ и $\mathbb{F}_q$ — корни многочлена $x^{p^n} - x$.

- многочлен g имеет корень в поле $\mathbb{F}_q$ (Упр. на дом)

если этот корень α.

$$\frac{\mathbb{F}_p[x]}{(g)} \longrightarrow \mathbb{F}_q$$

$$[h] \longmapsto h(\alpha).$$

вложение: Доделать док-во