$M(x) = \underbrace{p_1(x)}_{\alpha} \underbrace{p_2(x)}_{\alpha_1}$ – ЛОЖЬ!

γ

$\alpha_0 = \alpha$

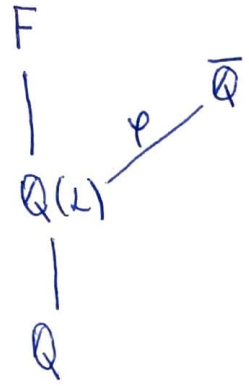
$\gamma(\alpha_0) = \alpha_1$ – противоречие, т.к. $\alpha = \alpha_0$ не высекает из вагона $p_1(x)$

II способ

F | Q

$m_\alpha(\alpha) = 0$ $\quad m(\beta) = 0$

$\alpha \neq \beta$



$\varphi \in \mathrm{Hom}(Q(\alpha), \bar{Q})$

$\varphi(\alpha) = \beta$ теорема Кронекера

φ продолжить до $\tilde{\varphi} \in \mathrm{Aut}(\bar{Q}, \bar{Q})$

$\tilde{\varphi}|_{Q(\alpha)} = \varphi$

$\tilde{\varphi}(F) = F$

$\tilde{\varphi}(\alpha) \in F \Rightarrow \varphi(\alpha) = \beta \in F$

Семинар 19.

9) K – коммут. кольцо с 1, без делителей 0

Док-ть: $\forall$ конечная подгруппа мультипликативной группы обратимых элементов кольца явл-ся циклической.

$K \subset F$ – поле (частных) отношений кольца K $= \mathrm{Frac}\, K$

$\frac{k_1}{k_2} \quad k_1, k_2 \in K$

$\frac{k_1}{k_2} + \frac{l_1}{l_2} = \frac{k_1 l_2 + k_2 l_1}{k_2 l_2}$

$\frac{k_1}{k_2} \cdot \frac{l_1}{l_2} = \frac{k_1 l_1}{k_2 l_2}$

$G < K \subset F$ $\quad G < F$ частн.

Пример. $\mathbb{C} \supset G \ni g$, G – конечная группа

$g^n = 1 \quad n = |\mathrm{ord}\, G| < \infty$

$g = e^{\frac{2\pi i}{n}} \Rightarrow G = \mathbb{Z}_n$.

Пройденная теорема: конечная подгруппа поля – цикл. группа.
Ссылка на нее завершает док-во.

① Сколько неприводимых многочленов второй степени над $\mathbb{F}_5$?

$x^2 + ax + b \quad a, b \in \mathbb{F}_5$

Всего: $5 \times 5 = 25$

$(x - \alpha)(x - \beta) \quad \alpha, \beta \in \mathbb{F}_5 \Rightarrow$ #неприводимых: $25 - 15 = 10$

Приводимых: $10 + 5 = 15$

$\frac{-a \pm \sqrt{a^2 - 4b^2}}{2}$ $\quad a^2 - 4b$ неявл-ся эл-том $\mathbb{F}_5^2$

↑ квадраты $\mathbb{F}_5$

$\mathbb{F}_5$:

$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{4}$	$\bar{1}$

$a^2 - 4b = \bar{2}$

$\bar{0}\ \bar{1}\ \bar{4}$ ↑ $\bar{3}$

- если $\bar{a} = \bar{0}$, то $\bar{b} = 2 \longrightarrow x^2 + \bar{2}$
- если $a^2 = \bar{1}$, то $\bar{b} = 1 \longrightarrow x^2 + x + \bar{1}$, $x^2 + \bar{4}x + \bar{1}$
- если $a^2 = 4$, то $\bar{b} = 3 \longrightarrow x^2 + \bar{2}x + \bar{3}$, $x^2 + \bar{3}x + \bar{3}$

$x^{5^2 - 1} - 1 = x^{24} - 1 = (x^{12})^2 - 1 = (x^{12} + 1)(x^{12} - 1) = ((x^4)^3 + 1)(x^{12} - 1) =$

$= (x^4 + 1)(x^8 - x + 1)(x^6 - 1)(x^6 + 1) = (x^4 + 1)(x^8 - x + 1)(x^3 - 1)(x^3 + 1)(x^3 - 1) \times$

$\times (x^4 + x^2 + 1) = \ldots$

Семинар № 19

(2) $\mathbb{F}_{p^m} < \mathbb{F}_{p^n} \iff m \mid n.$

($\Rightarrow$) $p^n - 1 = |F^*_{p^n}|$

$p^m - 1 = |F^*_{p^m}|$ $\Rightarrow (p^m-1) \mid (p^n-1)$

Задача. $НОД(p^n-1, p^m-1) = p^{(n,m)} - 1.$ (1)

$НОД(x^n-1, x^m-1) = x^{(n,m)} - 1$ (2)

(1) $\Rightarrow$ $p^m - 1 \mid p^{(n,m)} - 1 \Rightarrow m = (n,m)$, т.е. $m \mid n$.

II способ. $F_{p^n} > F_{p^m}$

F_{p^n} – мин. пр-во размерности d над F_{p^m}

$p^n = (p^m)^d = p^{md}$

($\Leftarrow$) $X^{p^d} - X - Roots \simeq \mathbb{F}_{p^d}$

$\underbrace{X^{p^m} - X}_{Roots} \subset \underbrace{X^{p^{md}} - X}_{Roots}$ $\iff$ $X^{p^m} - x \mid X^{p^{md}} - x$

$\Updownarrow$

$X^{p^m - 1} - 1 \mid X^{p^{md} - 1} - 1$

$НОД(x^{p^m-1} - 1, x^{p^{md}-1} - 1) = x^e - 1$, $e = НОД(p^m-1, p^{md}-1) =$

$= p^{(m,md)} - 1 = p^m - 1$

③ Пусть p – нечетн. число, ПРОСТОЕ.

X^2+1 неприводим над $F_p \Leftrightarrow p \equiv 3 \pmod 4$

Пример. $F_3 = \{0,1,-1\} \xrightarrow{\text{возв. в кв.}} \{0,1\}$ $\sqrt{-1}$ не сущ-ет

$F_5 = \{0,1,-1,2,-2\} \longrightarrow \{0,1,-1\}$ $\sqrt{-1} = 2$

$3 \equiv 3 \pmod 4$ $5 \equiv 1 \pmod 4$

Гипотеза. $\sqrt{-1}$ в F_p сущ-ет, если $p \equiv 1 \pmod 4$

$X^2+1=0$

$X^2=-1$

$X^4=1$

F_p^* – циклическая группа.

- Для $\forall$ делителя порядка цикл. группы $\exists!$ подгруппа этого порядка d.

$|F_p|^* \vdots 4 \Leftrightarrow |F_p| \equiv 1 \pmod 4$

$(-1)^{\frac{p-1}{4}}$ – корень $X^2+1=0$.

⑤ Док-тб: $Gal(\mathbb{F}_{p^{nd}} | \mathbb{F}_{p^d}) = \langle \Phi_{p^d} \rangle$,

$\Phi_{p^d} : \overline{F}_p \to \overline{F}_p$

$\Phi_{p^d}(x) = x^{p^d}$.

$\mathbb{F}_{p^n} | \mathbb{F}_p$ – всегда расширение Галуа

$X^{p^n} - X$ – сепарабельный многочлен

F_{p^n} – поле разложения $X^{p^n} - X$.

09.03.21

Семинар №20

1) G – группа

$\chi : G \to F^*$

$\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ характер

$\chi_1, \dots, \chi_r$ – различные характеры

Док-во: $\sum \alpha_i \chi_i = 0 \quad \forall g \in G \Rightarrow \alpha_i = 0$, $\alpha_i \in F$

Применение факта: F – расширение Галуа $F|K$ с группой $Gal(F|K) = H$

$\sigma \in H$

G

$=$

$F^* \to F^*$

$\alpha \in F^* \to \alpha^\sigma$

- Каждый эл-т группы Галуа H можно интерпретировать как характер F^*.

$\alpha_1 \chi_1 + \dots + \alpha_s \chi_s = 0$ Док-во по индукции.

Все $\alpha_i \neq 0$.

$\chi_1(g_0) \neq \chi_2(g_0)$, $g_0 \in G$

$\alpha_1 \chi_1(g) + \dots + \alpha_s \chi_s(g) = 0 \quad \forall g \in G$ – по предположению (*)

$\alpha_1 \chi_1(g_0 g) + \dots + \alpha_s \chi_s(g_0 g) = 0$

$\alpha_1 \chi_1(g_0)\chi_1(g) + \dots + \alpha_s \chi_s(g_0)\chi_s(g) = 0$ (**)

Домножим (*) на $\chi_1(g_0)$ => вычтем из (**)

$\alpha_2 \chi_1(g_0) \neq \alpha_2 \chi_2(g_0)$ $\sum_{j=2}^{s} \beta_j \chi_j(g) = 0$, $\beta_2 \neq 0$

$F|k$ $\quad \mathrm{Hom}_k(F, \overline{K})$

расш. Галуа $\quad \sigma_1, \dots, \sigma_s \qquad s = \deg F|K$

$$\mathrm{tr} f = \sigma_1(f) + \dots + \sigma_s(f)$$

$f \in F$

$$N(f) = \sigma_1(f)\,\sigma_2(f) \dots \sigma_s(f)$$

Пример. 1) $k \in K$

$$\mathrm{tr} k = k + \dots + k = (\deg F|K) \cdot k$$

2) $\mathbb{Q}(\sqrt[3]{2})$

$\sqrt[3]{2} \to \sqrt[3]{2}$, $\sqrt[3]{2} \to \omega\sqrt[3]{2}$, $\sqrt[3]{2} \to \omega^2\sqrt[3]{2}$, $\omega = e^{\frac{2\pi i}{3}}$

$$\mathrm{tr}(\sqrt[3]{2}) = \sqrt[3]{2} + \omega\sqrt[3]{2} + \omega^2\sqrt[3]{2} = 0$$

$$N(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega\sqrt[3]{2}\,\omega^2\sqrt[3]{2} = 2$$

3) $F = \mathbb{Q}(\sqrt{5})$

$$\mathrm{tr}(2+3\sqrt{5}) = 2+3\sqrt{5}+2-3\sqrt{5} = 4$$

$$N(2+3\sqrt{5}) = (2+3\sqrt{5})(2-3\sqrt{5}) = -41$$

$\mathbb{F}_4$ $\quad \mathbb{F}_2(\alpha)$ $\quad \alpha$ - корень $x^2 + x + 1$

$$\alpha^2 = \alpha + 1$$

$\mathrm{tr}\,\alpha = ?$ $\quad N(\alpha) = ?$

- Автоморфизм $\mathrm{Frob}: \alpha \mapsto \alpha^2$

$$\mathrm{tr}\,\alpha = \alpha + \alpha^2 = \alpha + \alpha + 1 = 1$$

$$N(\alpha) = \alpha \cdot \alpha^2 = \alpha^3 = \alpha(\alpha+1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$$

Напоминание $\quad \mathrm{Gal}(\mathbb{F}_{p^d}|\mathbb{F}_p) = \langle \sigma \rangle$ $\quad \alpha^{p^d} = \alpha$ $\quad x^{p^d} - x = 0$

$\sigma: \alpha \to \alpha^p$

$\sigma^2: \alpha \to \alpha^{p^2}$ $\dots$ $\sigma^{d-1}: \alpha \to \alpha^{p^{d-1}}$

(2) Док-ть

• Норма – голоморфна $F^* \to K^*$

▽ $\sigma_1, \dots, \sigma_s$

a, b

$N(a \cdot b) = \sigma_1(a \cdot b) \dots \sigma_s(a \cdot b) = \sigma_1(a) \dots \sigma_s(a)\, \sigma_1(b) \dots \sigma_s(b) = N(a) N(b)$

$N(a) \overset{?}{\in} K^*$, т.к. $N(a)$ инвариантна отн. Gal △

• След – линейный функционал на F над K

▽ $tr(a+b) = \sigma_1(a+b) + \dots + \sigma_s(a+b) = \sigma_1(a) + \dots + \sigma_s(a) + \sigma_1(b) + \dots + \sigma_s(b) =$

$= tr(a) + tr(b)$

$tr(a) \overset{?}{\in} K$, т.к. $tr(a)$ инвариантна отн. Gal

$tr(ka) = \sigma_1(ka) + \dots + \sigma_s(ka) = k(\sigma_1(a) + \dots + \sigma_s(a)) = k\, tr(a)$

Предположим, $\sigma_1(a) + \sigma_2(a) + \dots + \sigma_s(a) = 0 \quad \forall a \in F^*$

Это противоречит лемме Артина.

$\sigma_i : F^* \longrightarrow F^*$

элемент группы Галуа $Gal(F|K)$

можно (и нужно) понимать как характер F^*

Почему эл-ты Gal опр-ют различные характеры?

$f^{\sigma_1} = f^{\sigma_2} \quad \forall f \in F^* \Rightarrow \sigma_1 \sigma_2^{-1}\big|_F = id \Rightarrow \sigma_1 \sigma_2^{-1} = e \Rightarrow \sigma_1 = \sigma_2$ △

$\sigma_1 \neq \sigma_2$