Лекция 19 мая (первая половина)

Круговые поля $\mathbb{K}_n \supset \mathbb{Q}$

$\xi_n = e^{2\pi i/n} \in \mathbb{C}$ – примитивный $\sqrt[n]{1} \in \mathbb{C}$

$R_n \subset \mathbb{C}$ – множество всех примитивных корней из 1 степени n, $\xi_n \in R_n$

$\Phi_n(x) = \prod\limits_{\xi \in R_n} (x - \xi)$ – многочлен корнями которого являются все примитивные корни из 1 и только они.

$\mathbb{K}_n$ – поле разложения Φ_n над $\mathbb{Q}$ наз. n-тым круговым полем.

$Gal(\Phi_n) = ?$

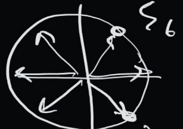
$n = p$ – простое

$\Phi_n = \frac{x^p - 1}{x - 1} = 1 + x + \ldots + x^{p-1}$

$\deg \Phi_n = \varphi(n)$

https://us02web.zoom.us/j/83841293804?
pwd=NGdaNjc2alY1Zk9heTZEbDlLQmY2UT09

$n = 6$



$g \in Gal(\Phi_n/\mathbb{Q})$

Φ_6 – квадратичный

$g: \xi_n \longmapsto \xi_n^{m(g)}$ $m(g)$ взаимно просто с n

$g \mapsto m(g)$ вложение групп

$\mathrm{Gal}(\Phi_n) \hookrightarrow (\mathbb{Z}/(n))^*$

обратим mod n

Все корни Φ_n - целы над $\mathbb{Z}$: $\Phi_n \mid x^n - 1$

$\Downarrow$

Все коэф-ты $\Phi_n \in \mathbb{Z}$ $\boxed{\Phi_n \in \mathbb{Z}[x]}$

Возьмём простое $p \in \mathbb{N} : p \mid n$

$\boxed{x^n - 1 \text{ сепарабелен над } \mathbb{F}_p}$

$\overline{\Phi}_n \in \mathbb{F}_p[x]$ - редукция коэффициентов по mod p.

сепарабельный? многочлен.

$\mathrm{Gal}(\overline{\Phi}_n / \mathbb{F}_p) \hookrightarrow \mathrm{Gal}(\Phi_n/\mathbb{Q})$.

$\mathbb{K}_n$ корни $\xi \in R_n$ многочлена Φ_n целые над $\mathbb{Z}$, $\xi \in \mathcal{O}$

$\overline{\xi} = [\xi]_p \in \mathcal{O}/(p)$ корни $\overline{\Phi}_n$ над $\mathbb{F}_p$

они порождают поле разложения $\overline{\Phi}_n$ над $\mathbb{F}_p$

$= \overline{\mathbb{K}}_{n,p}$

$\mathrm{Gal}(\mathbb{K}_{n,p}/\mathbb{F}_p)$ - циклическая группа, порожденная Фробениусом. $F: \alpha \to \alpha^p$.

$$F: [\xi]_p \longmapsto [\xi]_p^{\,p} = [\xi^p]_p.$$

$$\Downarrow$$

перестановки примитивных корней $\xi \in R_n$ заданная правилом $\xi \longmapsto \xi^p$ $p \nmid n$

лежит в группе $\mathrm{Gal}(\Phi_n/\mathbb{Q})$

т.е. отображение $\xi \longmapsto \xi^p$ продолжается до автоморфизма кругового поля $\mathbb{K}_n$ над $\mathbb{Q}$.

$g: \xi \longrightarrow \xi^p$ для $\xi \in R_n$

наз. Элементом p-Фробениуса в $\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})$

$\zeta_n \longrightarrow \zeta_n^m$ с любым $m \in (\mathbb{Z}/(n))^n$

$m = p_1^{s_1} \cdots p_k^{s_k}$ $p_i \nmid n$

$$\zeta_n \longrightarrow \zeta_n^{p_1^{s_1} \cdots p_k^{s_k}} = \underbrace{F_{p_1}^{s_1} F_{p_2}^{s_2} \cdots F_{p_k}^{s_k}} \zeta_n$$

$\Downarrow$ m

Gal

$$\mathrm{Gal}(\Phi_n) \hookrightarrow \underbrace{(\mathbb{Z}/(n))^*}$$ это изоморфизм.

Поэтому: Группа Галуа транзитивно действует на корнях

$\Downarrow$

Φ_n неприводим, и является минимальным многочленом для ζ_n

$$\mathrm{Gal}(\Phi_n) = (\mathbb{Z}/(n))^*$$

Приложение: $n=p$ — простое.

$(\mathbb{Z}/(n))^* = \mathbb{F}_p^\times$ — обратимые элементы $\mathbb{F}_p$.

в $\mathbb{F}_p^\times$ есть ровно одна подгруппа индекса 2

— а именно группа квадратов.

$H < \mathbb{F}_p^\times \quad \forall \xi \in \mathbb{F}_p^\times \quad \xi H \cdot \xi H = H$

$\boxed{\mathbb{F}_p^\times / H = \mathbb{Z}/(2)} \longrightarrow \quad \xi H \cdot \xi H = \xi^2 H \Rightarrow \xi^2 \in H$

H — содержит $(\mathbb{F}_p^\times)^2 \quad H = (\mathbb{F}_p^\times)^2$

$\mathrm{Gal}(\Phi_p) = \mathbb{F}_p^\times$

в $\mathbb{K}_p = \mathbb{Q}[\sqrt[p]{1}] = \mathbb{Q}[\zeta_p]$ есть ровно поле $\mathbb{K}_p \supset \mathbb{L} \supset \mathbb{Q}$ степени 2 над $\mathbb{Q}$. Оно порождается

$$\theta = \sum_{g \in (\mathbb{F}_p^\times)^2} g(\zeta_p) - \sum_{g \notin (\mathbb{F}_p^\times)^2} g(\zeta_p) =$$

гауссова сумма

$$g : \zeta_p \mapsto \zeta_p^m \qquad = \sum_{m=1}^{p-1} \zeta_p^m \begin{bmatrix} m \\ p \end{bmatrix}$$

символ Лежандра

$$\begin{bmatrix} m \\ p \end{bmatrix} = \begin{cases} +1 & \text{если } m \text{ квадрат} \\ -1 & \text{если } m \text{ не квадр.,} \end{cases}$$

θ - квадратичная иррациональность.

(Как сосчитать явно?)

Пример! $p = 1 + x + \dots + x^{p-1}\Big|_{x=1} = \Phi_p(1)$

$p-1$

$$\Phi_p(1) = \prod_{k=1}^{p-1}(1-\zeta^k) = \prod_{k=1}^{\frac{p-1}{2}}(1-\zeta^k)(1-\zeta^{-k}) =$$

$$\boxed{1-\zeta^{-k} = (\zeta^k-1)\zeta^{-k}}$$

$$= \prod_{k=1}^{\frac{p-1}{2}}(-1)(1-\zeta^k)^2\zeta^{-k} =$$

$$= (-1)^{\frac{p-1}{2}} \underbrace{\prod_{k=1}^{\frac{p-1}{2}}(1-\zeta^k)^2}_{\text{квадрат}} \cdot \underbrace{\zeta^l}_{\text{тоже полный квадрат}} \qquad l = -\sum_{k=1}^{\frac{p-1}{2}} k \pmod p$$

$$\zeta^l = (\zeta^m)^2$$

$$2m \equiv l \mod p.$$

$$\sqrt{\underset{p^*}{\underset{\parallel}{(-1)^{\frac{p-1}{2}}p}}} \in \mathbb{K}_p \qquad \mathbb{Q}[\sqrt{p^*}] = \mathbb{Q}[\text{гаусс}]$$

Трудная задача:

гаусс. сумма $\overset{?}{=} \sqrt{p^*}$

Циклические расширения

$\Bbbk$ — любое поле, содержащее все корни $\sqrt[n]{1}$

x^n-1 полностью разлагается над $\mathbb{k}$ на n различных линейных множителей.
(автоматом char $\mathbb{k} \nmid n$)

$\mu_n(\mathbb{k})$ - группа корней $\sqrt[n]{1}$

$a \in \mathbb{k}^\times$

Факт! многочлен $x^n - a$ всегда раскладывается над $\mathbb{k}$ на неприводимые множители $g_1 \dots g_s$, где $s \mid n$ и каждый

$$g_i = x^{n/s} - b_i, \quad b_i \in \mathbb{k}$$

и в этом случае $a = b^k$ для $b \in \mathbb{k}^\times$

В частности неприводимость $x^n - a$ означает что $|\mathrm{Gal}(x^n-a)| = n$, является циклической группой, $\mathbb{k}[x]/(x^n-a)$ - это поле разложения многочлена x^n-a

Док-во: Пусть $\overline{\mathbb{k}} \supset \mathbb{k}$ - алгебраическое замыкание, α - корень многочлена $x^n - a := f(x)$

множество всех корней - это $\xi \cdot \alpha$

где $\xi \in \mu_n(\mathbb{k})$

$$g \in Gal(f/\mathbb{k}) \qquad \alpha \longmapsto \overset{\mu_n(\mathbb{k})}{\overset{\Downarrow}{\xi_g}} \alpha$$

$$\xi\alpha \longmapsto g(\xi\alpha) = \xi g(\alpha) = \xi_g \xi \alpha$$

любой корень умножается на ξ_g

$$g \longmapsto \xi_g \qquad Gal(f/\mathbb{k}) \hookrightarrow \mu_n(\mathbb{k}),$$

цикличная

$\Downarrow$

$Gal(f/\mathbb{k})$ циклична

$$\boxed{|G| = m}$$

$$f = x^n - a = \prod_{\xi \in \mu_n/Gal} \underbrace{\prod_{g \in Gal} (x - \xi \xi_g \alpha)}$$

Пусть Gal порождается элементом

$$\alpha \longmapsto \zeta\alpha$$

$\zeta \in \mu_n(\mathbb{k})$, порядка m

ζ - примитивный корень степени $m | n$ из единиц

$$f = \prod_{\xi \in \mu_n/Gal} \underset{\substack{\shortparallel \\ g_\xi}}{\prod_{i=0}^{m-1} (x - \xi \zeta^i \alpha)}$$

$f = \prod g_\xi \qquad g_\xi \in \Bbbk[x] \quad \deg g_\xi = m$

$$g_\xi = \prod_{i=0}^{m-1} (x - \xi \underline{\zeta}^i \alpha) = \qquad \zeta^m - 1 = 0$$

$$\underline{e_i(1, \dots, \zeta^{m-1}) =} \; = \begin{cases} 1 & i = m \\ 0 \end{cases}$$

$$= x^m - \xi^m \alpha^m \in \underline{\Bbbk}[x]$$

неприводим

$f = g_1 \cdots g_{n/m} \qquad \deg g_i = m$

$g_e \Rightarrow \alpha^m = c \in \Bbbk$

$(x^n - b) = \prod g_i \Rightarrow \boxed{b = c^{n/m}}$

если $x^n - b$ неприводим $\Rightarrow$

$\Bbbk[x]/_{x^n - b} = \Bbbk[\sqrt[n]{b}]$ — это

расширение Галуа с циклической группой порядка n, совпадающее с полем разложения для $x^n - b$

$\Bbbk \ni \sqrt[n]{1}$

!