Лекция 12 мая (вторая половина)

Группы Галуа многочленов

$f \in \mathbb{k}[x]$, $\mathbb{L}_f$ – поле разложения f над $\mathbb{k}$

сепарабельный

$\mathbb{L}_f \supset \mathbb{k}$ – конечное расширение Галуа

$\mathrm{Gal}(\mathbb{L}_f/\mathbb{k}) := \mathrm{Gal}(f/\mathbb{k})$ наз. группой Галуа многочлена f.

Поле $\mathbb{L}_f$ порождается как алгебра корнями $\theta_1, \dots, \theta_m$ многочлена f.

$$\mathbb{L}_f = \mathbb{k}[\theta_1, \dots \theta_m] \circlearrowright \varphi$$

переставляет корни

$\exists$ каноническое вложение $\mathrm{Gal}(f) \hookrightarrow S_m$

группе перестано
всех корней.

$\mathrm{Gal}(f) < S_m$ – это подгруппа перестановок, сохраняющих все алгебраические соотношения между корнями $\underset{< \quad I}{\overrightarrow{\Bbbk[t_1,\dots,t_m]}}$

$$\Bbbk[t_1,\dots,t_m] \twoheadrightarrow \mathbb{L}_f = \Bbbk[\theta_1,\dots,\theta_m]$$

$$\mathrm{ev}_{\theta_1,\dots,\theta_m} : f(t_1,\dots,t_m) \mapsto f(\theta_1,\dots,\theta_m)$$

$\ker \mathrm{ev}_{\theta_1,\dots,\theta_m} = I$ – идеал полиномиальных соотношений между корнями

$\sigma \in S_m$ лежит в группе $\mathrm{Gal}(f) \Leftrightarrow$

$\forall\, f(t_1,\dots,t_m) \in I \quad f^{\sigma}(t_1,\dots,t_m) =$

$I \ni f(t_{\sigma(1)},\dots,t_{\sigma(m)})$

$\sigma : I \to I$

$V(I) \subset \Bbbk^m$ – множество всех точек вида $(\theta_{\sigma(1)},\dots,\theta_{\sigma(m)}) \in \Bbbk^m$

где σ пробегает $\mathrm{Gal}(f) < S_m$

все эти точки различны.

$(\theta_{\sigma(1)} \dots \theta_{\sigma_m}) = \sigma\theta$

S_m: k^m перестановками координат.

$\theta \leftarrow (\theta_1, \dots, \theta_m)$

$\boxed{\text{все корни } f.}$

$\alpha = (\alpha_1, \dots, \alpha_m) \in \boxed{V(I)} \Rightarrow e_i(\alpha_1 \dots \alpha_m) = (-1)^i a_i$

$f = x^m + a_1 x^{m-1} + \dots + a_m$

$$\boxed{\begin{array}{l} e_i(t_1, \dots, t_m) - (-1)^i a_i \in I \\ e_i(\theta_1, \dots, \theta_m) = (-1)^i a_i \text{ по Виета} \end{array}}$$

$\prod(t - \alpha_i) = f = \prod(t - \theta_i)$

координаты точки α получаются перестановкой из координат точки θ. Эта перестановка сохраняет все соотношения между корнями, иначе $\exists h \in I, h^\sigma \notin I$.

$$\begin{array}{l} h^\sigma(\theta_1 \dots \theta_m) \neq 0 \\ \quad \| \\ h(\theta_{\sigma(1)} \dots \theta_{\sigma(m)}) = h(\alpha_1, \dots, \alpha_m) = 0 \end{array}$$

Вычисление группы $\mathrm{Gal}(f)$ при помощи резольвенты Галуа.

Пусть: $\theta_1, \dots, \theta_m$ — корни f в $\mathbb{L}_f$.

$$\underset{\mathbb{L}_f[t_1,\dots,t_n]}{\boxed{\psi(t_1,\dots,t_m)=t_1\theta_1+\dots+t_m\theta_m}}$$

$$\underset{\underset{\boxed{\text{Резольвента Галуа}}}{\uparrow}}{F(t_1,\dots,t_m)}=\prod_{\sigma\in S_n}\psi^{\sigma}(t_1,\dots,t_m)=$$

$$=\prod_{\sigma\in S_m}\psi(t_{\sigma(1)},\dots,t_{\sigma(m)})=$$

$$=\prod_{\sigma\in S_m}(\theta_1 t_{\sigma(1)}+\dots+\theta_m t_{\sigma(m)})$$

многочлен степени $n!$ из $\mathbb{L}_f[t_1\dots t_n]$

Сгруппируем в произведении все множители, которые лежат в одном смежном классе $h\cdot\mathrm{Gal}(f) < S_m$

$h\sigma$

$$F(t_1,\dots,t_m) = \prod_{h\in S_m/Gal(f)} \underbrace{\prod_{\sigma\in Gal(f)} \varphi}_{F_h(t_1,\dots,t_n)}$$

$$F_h(t_1,\dots,t_n) = \prod_{\sigma\in Gal(f)} (\theta_1 t_{h\sigma(1)} + \dots + \theta_m t_{h\sigma(m)})$$

$$= \prod_{\sigma\in Gal(f)} (\underbrace{\theta_{\sigma^{-1}(1)}}_{} t_{h(1)} + \dots + \underbrace{\theta_{\sigma^{-1}(m)}}_{} t_{h(m)})$$

$$= \prod_{\sigma\in Gal(f)} \sigma\varphi^h$$

φ^h получается из φ перестановкой h переменных $t_1, \dots, t_n$

$\sigma(\varphi^h)$ – результат действия автоморфизма $\sigma : \mathbb{L}_f \longrightarrow \mathbb{L}_f$ на

Коэффициенты формы $\varphi^h \in \mathbb{L}_f[t_1,\dots,t_n]$

когда $\sigma \in Gal(f)$ формы $\sigma\varphi^h$ все различны и составляют одну орбиту группы Галуа $(\theta_{\sigma(1)}, \dots, \theta_{\sigma(m)})$

$\mathbb{F}_h(t_1,\dots t_m)$ имеет $\mathbb{K}^m$

Галуа-инвариантные коэффициенты.

$$F_h(t_1,\dots,t_m) \in \mathbb{K}[t_1,\dots,t_m]$$

неприводим т.к. группа Галуа транзитивно действует на линейных множителях кольцо разложение F_h над $\mathbb{L}_f$

$$F(t_1,\dots,t_m) = \prod_{h \in S_m / Gal(f)} F_h(t_1,\dots t_m)$$

разложение F на неприводимы множители над $\mathbb{K}$

$Gal(f) < S_m$ состоит из всех перестановок переменных $t_1,\dots,t_m$, которые оставляют на месте какой-нибудь неприводимый множитель.

Оно реально позволяет вычислять группы многочленов над $\mathbb{Q}$.

$$f(x) = \underline{x^n + a_1 x^{n-1} + \ldots + a_n} \in \mathbb{Z}[x]$$

$\mathbb{K} = \mathbb{Q}$

$$\Big\downarrow \text{ редуцирую по модулю } p.$$

$$\bar{f}(x) \in \mathbb{F}_p[x]$$

$$\bar{f}(x) = x^n + [a_1]_p x^{n-1} + \ldots + [a_n]_p$$

если многочлен $\bar{f}$ сепарабелен над $\mathbb{F}_p$

то $\mathrm{Gal}(\bar{f}/\mathbb{F}_p) \hookrightarrow \mathrm{Gal}(f/\mathbb{Q})$.

Док-во: $\theta_1, \ldots, \theta_n$ – корни f в $\mathbb{L}_f \supset \mathbb{Q}$

$\nearrow$ целые над $\mathbb{Z}$

F_h – целые над $\mathbb{Z}$ и лежат в $\mathbb{Q}$

$$\Downarrow$$

$$F_h \in \mathbb{Z}[t_1, \ldots, t_n]$$

$F = \prod F_h$ — разложение на неприводимые в $\mathbb{Z}[t_1, \dots, t_m]$

$$\begin{tikzcd} F = \prod F_h \arrow[d, "h \in S_m/\mathrm{Gal}(f)", "\text{редукция mod } p"'] \\ \overline{F} = \prod \overline{F}_h \end{tikzcd}$$

$$\begin{tikzcd} I_f \supset \mathcal{O} \arrow[d, "\text{mod } p"] \\ \mathcal{O}/(p). \end{tikzcd}$$

$\mathcal{O}$ — кольцо целых над $\mathbb{Z}$ элементов

классы $[\theta_1]_p, \dots, [\theta_m]_p$ порождают поле разложения $\overline{f}$ над $\mathbb{F}_p$

$\overline{F}$ — резольвента Галуа $\overline{f}$

$\overline{F} = \overline{F}_h$ дофакторизовываются до разложения над $\mathbb{F}_p$
некоторые $\overline{F}_h$ дополнительно но могут разложиться над $\mathbb{F}_p$.

$\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subset S_m$ стабилизатор неприводимого множителя мн-на $\overline{F}$ над $\mathbb{F}_p$, если этот множитель пришёл из F_h.

Следствие: если $\bar f$ над $\mathbb{F}_p$ сепарабелен и раскладывается на неприводимые множители степеней $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_m$

То тогда $Gal(f/\mathbb{Q})$ содержит перестановку циклового типа $\underline{\lambda}$.

Док-во: Группа автоморфизмов конечного поля циклическая и порождена Фробениусом.

$\mathbb{L}_{\bar f} \supset \mathbb{F}_p$ — циклическая группа, порожденная фробениусом

$\bar f_1 \, \bar f_2 \ldots \bar f_m$

$\theta_1 \ldots \theta_k$

$\theta_1 \to \theta_2 \to \ldots \to \theta_k$

транзитивно действует на корнях каждого неприводимого множителя

$\Downarrow$

что каждое $\lambda_i = \deg \bar f_i$ должен быть цикл длины λ_i из $\underline{Gal(\bar f/\mathbb{F}_p)} \hookrightarrow \underline{Gal(f/\mathbb{Q})}$