Grupo de Galois de um polinómio

$f \in K[X]$ polinómio separável

Seja E_f / K uma extensão de decomposição. Então E_f / K é de Galois e diz-se que

$$G_f := \mathrm{Gal}(E_f / K)$$

é o grupo de Galois de f $/K$.

Se $f = \prod_{i=1}^{r} (X - \alpha_i)$ em E_f, então

$$\forall \sigma \in G_f \qquad \sigma \cdot f = \prod_{i=1}^{r} (X - \sigma(\alpha_i)) = f$$

$\therefore$ G_f permuta as raízes de f.

$\therefore$ G_f pode ser visto como um subgrupo S_r.

$\therefore$ $|G_f| \mid r!$

<u>Prop</u>: Seja $f \in K[X]$ um polinômio separável. Então f é irredutível se G_f age transitivamente nas raízes de f.

<u>Dem</u>: $\boxed{\Rightarrow}$ Seja f irredutível. Sejam $\alpha_1, \ldots, \alpha_r \in E_f$ as raízes de f. Então

$$f = \prod_{\mu \in \{\sigma(\alpha_1) \mid \sigma \in G_f\}} (X - \mu)$$

pois f (sendo irredutível) é o pol. mínimo de α_1.

$\boxed{\Leftarrow}$ Suponhamos que G_f age transitiv.

Seja $g \in K[X]$ um fator irred. de f e seja $\alpha \in E_f$ t.q. $g(\alpha) = 0$.

Temos
$$g = \prod_{\mu \in \{\sigma(\alpha) \mid \sigma \in G_f\}} (X - \mu).$$

Como G_f age transitivamente segue $f = g$, pois têm as mesmas raízes.

$\therefore f$ é irredutível.

$\blacksquare$

<u>Exemplo</u>: Calcular o grupo de Galois de $f = X^4 - 2 \in \mathbb{Q}[X]$.

Criterio Eisenstein $\Longrightarrow$ f irredutível.

Raízes: $\sqrt[4]{2}, \sqrt[4]{2}\,i, -\sqrt[4]{2}, -\sqrt[4]{2}\,i$

$$\Longrightarrow E_f = \mathbb{Q}(\sqrt[4]{2}, i)$$

$$\Longrightarrow$$

$$[E_f : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})]$$

$$= 4 \times 2 = 8$$

$$R := \{\sqrt[4]{2}, \sqrt[4]{2}\,i, -\sqrt[4]{2}, -\sqrt[4]{2}\,i\}$$

$$\Longrightarrow G_f < S_R = S_4$$

$\Longrightarrow G_f = D_4$ pois D_4 é o

único subgrupo de S_4 com 8 elementos
(a menos de isomorfismo!).

Diretamente: $\exists\ \sigma, \tau \in G_f$

$$\sigma(i) = -i \qquad \tau(i) = i$$
$$\sigma(\sqrt[4]{2}) = \sqrt[4]{2} \qquad \tau(\sqrt[4]{2}) = \sqrt[4]{2}\, i$$

pois $\sigma \equiv$ conjugação complexa e

τ existe pq

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$$

$= \deg f$

$\Rightarrow f$ é irred. em $\mathbb{Q}(i)[x]$

$\Rightarrow \exists \tau$.

Temos $\operatorname{ord} \sigma = 2$ $\operatorname{ord} \tau = 4$ e

$$\tau\sigma = \sigma\tau^3 \quad \text{(exerc.)}$$

<u>NB</u>: $\sigma = (2\ 4)$

$\tau = (1\ 2\ 3\ 4)$.

<u>Exemplo</u>: Correspondência de Galois

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}$

$f = (X^2-2)(X^2-3)$

Raízes : $\pm\sqrt{2}, \pm\sqrt{3}$

$|G| = 4$

$G = \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$

$$\begin{tikzcd}[column sep=small]
 & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
H_1 \arrow[dr, dash] & H_2 \arrow[d, dash] & H_3 \arrow[dl, dash] \\
 & \{1\} &
\end{tikzcd}$$

corresponde a

$G = \langle \sigma_1, \sigma_2 \rangle$

$\sigma_1(\sqrt{2}) = -\sqrt{2}, \quad \sigma_1(\sqrt{3}) = \sqrt{3}$

$$\sigma_2(\sqrt{2}) = \sqrt{2}, \quad \sigma_2(\sqrt{3}) = -\sqrt{3}$$

$$H_1 = \langle \sigma_1 \rangle \qquad H_2 = \langle \sigma_2 \rangle \qquad H_3 = \langle \sigma_1 \sigma_2 \rangle$$

$$\begin{tikzcd}
& \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
E^{\sigma_2} = \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) = E^{\sigma_1} \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) = E^{\sigma_1\sigma_2} \arrow[dl, dash] \\
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) &
\end{tikzcd}$$

Extensões ciclotômicas:

Exercício: Se E é um corpo e $G < E^\times$ é finito, então G é cíclico.

Exemplo: Se $G = U_n = \{\xi \in E \mid \xi^n = 1\}$, então G é cíclico.

Temos $|G| \leq n$.

NB: G tem n elementos se $f = X^n - 1$ (f decompõe em E e) só tem raízes simples, ou seja se $\operatorname{char} E = 0$ ou $\operatorname{char} E = p > 0$ e $(n, p) = 1$.

Notação: Se $|U_n| = n$, i.e.

E tem n raízes distintas de 1,

denotamos

$$\mu_n = U_n \simeq \mathbb{Z}/\langle n \rangle$$

Os geradores de μ_n, nesse caso, são denotados ξ_n (são as raízes-n primitivas de 1)

Neste caso, denota-se $K(\mu_n)/K$ a subextensão de decomposição de $f = X^n - 1$.

Temos $K(\mu_n)/K = K(\xi_n)/K$

Def: Uma extensão deste tipo diz-se ciclotómica.

NB: $K(\mu_n)|K$ é de Galois.

Q: $Gal(K(\mu_n)|K) = ?$

Prop: $Gal(K(\mu_n)|K) < \left(\mathbb{Z}/\langle n\rangle\right)^\times$

Dem: A restrição

$$Gal(K(\mu_n)|K) \ni \sigma \longmapsto \sigma|_{\mu_n} \in Aut(\mu_n) = \left(\mathbb{Z}/\langle n\rangle\right)^\times$$

($\mu_n = \mathbb{Z}/\langle n\rangle$)

é injetiva.

$\square$

Cor: $Gal(K(\mu_n)|K)$ é abeliano.

Cor: Se $n=p$ é primo, então

$Gal(K(\mu_n)|K)$ é cíclico.

<u>Exemplo</u>: 1. $Gal(\mathbb{Q}(\mu_3)|\mathbb{Q})$

$= \mathbb{Z}/\langle 2\rangle = (\mathbb{Z}/\langle 3\rangle)^\times$

2. $Gal(\mathbb{Q}(\mu_4)|\mathbb{Q})$

$= \mathbb{Z}/2 = (\mathbb{Z}/4)^\times$

$x^4-1 = (x^2-1)(x^2+1)$

3. $Gal(\mathbb{C}(\mu_n)/\mathbb{C}) = \{1\}$

Corpos Finitos :

Exemplo: $\mathbb{F}_p$, p primo

E é corpo finito $\Rightarrow$ $\operatorname{char} E = p > 0$

$\Rightarrow \mathbb{F}_p \subset E$

E finito $\Rightarrow [E : \mathbb{F}_p] < \infty$

Se $[E : \mathbb{F}_p] = n$, temos

$$|E| = p^n$$

<u>Teorema</u>: Seja $q = p^n$, então existe um corpo com q elementos $\mathbb{F}_q$.

$\mathbb{F}_q / \mathbb{F}_p$ é extensão de decomposição do polinômio separável $X^q - X$.

Em particular, $\mathbb{F}_q$ é único a menos de isomorfismo e $\mathbb{F}_q / \mathbb{F}_p$ é Galois.

Temos $\mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p) = \langle \sigma \rangle$
$\simeq \mathbb{Z}/\langle n \rangle$, onde $\sigma(a) := a^p$
é o automorfismo de Frobenius.

<u>Dem</u>: 1. Seja E um corpo com $|E| = q$. Temos

$$E^\times = \mathbb{Z}/\langle q-1 \rangle \text{ (exer. ant.)}$$

logo $X^{q-1}-1$ tem $q-1$ raízes distintas

e f tem q raízes distintas.

$\therefore$ $E/\mathbb{F}_p$ é ext. de decomp. de f.

2. Recíproca/ dado $f = X^q - X$,

temos $f' = 1$ logo f é separável.

Sejam

- $E/\mathbb{F}_p$ extensão de decomp. de f
- $E' := \{ r \in E \mid f(r) = 0 \} \subset E$

Temos

- $|E'| = q$ ($=$ # raízes de E)
- E' é subcorpo:

$r_1, r_2 \in E$

$$\Rightarrow \begin{cases} r_1 r_2^{\pm 1} \in E' \\ r_1 \pm r_2 \in E' \end{cases}.$$

$$f(X) = X^q - X$$

$$f(r_1+r_2) = (r_1+r_2)^q - (r_1+r_2)$$
$$= r_1^q + r_2^q - r_1 - r_2$$

$\therefore \; E = E'$, logo $|E| = q$.

3. Seja $G = \mathrm{Gal}(E/\mathbb{F}_p)$, então

$$|G| = [E : \mathbb{F}_p] = n.$$

Seja $\sigma \in G$ o aut. de Frobenius.

Temos

$$n = \min \{ m \mid \forall_{x \in \mathbb{F}_q^\times} \ x^{p^m - 1} = 1 \}$$

$$= \min \{ m \mid \forall_{x \in \mathbb{F}_q} \ x^{p^m} = x \}$$

$$= \min \{ m \mid \forall_{x \in \mathbb{F}_q} \ \sigma^m = \sigma \}$$

$$= \operatorname{ord}(\sigma)$$

$$\therefore \ G = \langle \sigma \rangle = \mathbb{Z}/\langle n \rangle .$$

$\blacksquare$

<u>Cor</u>: $\mathbb{F}_{p^n}$ tem um só subcorpo com p^d elementos $\forall_{d \mid n}$

<u>Dem</u>: Seja $F \subset \mathbb{F}_{p^n}$ subcorpo

$G = Gal(\mathbb{F}_{p^n} / \mathbb{F}_p)$ e $H = Gal(\mathbb{F}_{p^n}/F)$.

Temos

$$|F| = p^{[F:\mathbb{F}_p]} = p^{(G:H)}$$

o resultado segue pq $\mathbb{Z}/\langle n\rangle$ tem exata/ um subgrupo de ordem d para cada $d|n$.

$\square$

<u>Cor</u>: Seja E/k uma extensão de corpos finitos. E/k é simples, i.e., $\exists \alpha : E = k(\alpha)$, E/k é de Galois e $\mathrm{Gal}(E/k)$ é cíclico.

<u>Dem</u>: Seja $n = [E : \mathbb{F}_p]$.

Então $E^\times = E^\times = \mathbb{Z}/\langle p^n - 1\rangle$.

Seja $\zeta \in E^\times$ um gerador.

Temos $E = k(\xi)$.

$E/\mathbb{F}_p$ é de Galois $\Longrightarrow$

E/k é de Galois

$\mathrm{Gal}(E/k) < \mathrm{Gal}(E/\mathbb{F}_p)$

$\Longrightarrow \mathrm{Gal}(E/k)$ é cíclico.

$\square$

<u>Exemplo</u>: Calcular $Gal(\mathbb{F}_2(\mu_7)/\mathbb{F}_2)$

Temos $\mathbb{F}_2(\mu_7) = \mathbb{F}_{2^n}$ para algum n,

onde $n =$ a ordem $\sigma: \zeta \longmapsto \zeta^2$

em $Gal(\mathbb{F}_2(\mu_7)|\mathbb{F}_2)$

$$\sigma(\zeta_7) = \zeta_7^2$$

$$\sigma^2(\zeta_7) = \zeta_7^4$$

$$\sigma^3(\zeta_7) = \zeta_7^8 = \zeta_7$$

$$\therefore Gal(\mathbb{F}_2(\mu_7)/\mathbb{F}_2) = \mathbb{Z}/\langle 3\rangle$$

$\boxed{\xi}$