Extensão Ciclotômica (parte II)

$W_n(F) = \{x \in F \mid x^n = 1\}$, $P_n(F) = \{x \in F \mid o(x) = n\}$.

$W_n(F) = \bigcup_{d \mid n} P_n(F)$

$\xi \in P_n(\mathbb{C})$

$$\Phi_n(X) = \mathrm{Irr}(\xi, \mathbb{Q}) = \prod_{\zeta \in P_n(\mathbb{C})} (X - \zeta).$$

Temos também que

$$X^n - 1 = \prod_{\xi \in W_n(\mathbb{C})} (X - \xi) = \prod_{d \mid n} \prod_{\xi \in P_d(\mathbb{C})} (X - \xi) = \prod_{d \mid n} \Phi_d(X).$$

Além disso, $X^n - 1 \in \mathbb{Z}[X]$, e cada $\Phi_d(X) \in \mathbb{Q}[X]$.

Do Lema de Gauss, segue que cada $\Phi_d(X) \in \mathbb{Z}[X]$.

Note que podemos calcular Φ_n de forma recursiva:

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(X)}.$$

Exemplos.

(i) $\Phi_1(X) = X - 1$

(ii) Se p é primo, então

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

(iii) $\Phi_6(X) = \dfrac{X^6-1}{\Phi_1\cdot\Phi_2\cdot\Phi_3} = \dfrac{X^6-1}{(X-1)(X+1)(X^2+X+1)} = X^2-X+1.$

Teorema. Sejam $n\in\mathbb{N}$ e p um primo, $p\nmid n$. Seja $\overline{\mathbb{F}_p}$ um fecho algébrico de $\mathbb{F}_p$, e seja $\xi\in P_n(\overline{\mathbb{F}_p})$. Então

$$[\mathbb{F}_p(\xi):\mathbb{F}_p] = o(p+n\mathbb{Z}),$$

sendo $o(p+n\mathbb{Z})$ a ordem do elemento $(p+n\mathbb{Z})$ no grupo $(\mathbb{Z}/n\mathbb{Z})^\times$.

Dem.: Como ξ é algébrico sobre $\mathbb{F}_p$, o corpo $\mathbb{F}_p(\xi)$ é finito. Assim, seja $F: a\in\mathbb{F}_p(\xi)\longmapsto a^p\in\mathbb{F}_p(\xi)$. Então

$$[\mathbb{F}_p(\xi):\mathbb{F}_p] = |Aut(\mathbb{F}_p(\xi)/\mathbb{F}_p)| = o(F).$$

Temos ainda:

$$\begin{aligned} o(F) &= \min\{r>0 \mid F^r = Id\} \\ &= \min\{r>0 \mid \xi = F^r(\xi) = \xi^{p^r}\} \\ &= \min\{r>0 \mid p^r\equiv 1 \pmod n\} = o(p+n\mathbb{Z}). \end{aligned}$$ □

Para cada n, não múltiplo de p, defina

$$\Psi_n(X) = \prod_{\xi\in P_n(\overline{\mathbb{F}_p})} (X-\xi).$$

Temos que

$$\mathbb{F}_p[X]\ni X^n-1 = \prod_{d\mid n}\Psi_d(X).$$

Proposição. Seja $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ o homomorfismo canônico. Então:

(i) $\overline{\Phi}_n^{\pi}(X) = \overline{\Psi}_n(X)$

(ii) Seja $r = \frac{\varphi(n)}{o(p+n\mathbb{Z})}$. Então $\overline{\Psi}_n(X)$ é o produto de r polinômios mônicas e irredutíveis de grau $o(p+n\mathbb{Z})$ em $\mathbb{F}_p[X]$.

① em (i) $\overline{\Psi}_1(X) = X - 1 = \pi(X-1) = \overline{\Phi}_1^{\pi}(X)$. Assumindo que $\overline{\Psi}_d(X) = \overline{\Phi}_d^{\pi}(X)$, $\forall\, d \mid n$, temos que

$$X^n - 1 = \pi(X^n - 1) = \pi\left(\prod_{d\mid n} \Phi_d(X)\right) = \prod_{d\mid n} \overline{\Phi}_d^{\pi}(X) = \overline{\Phi}_n^{\pi} \cdot \prod_{\substack{d\mid n \\ d\neq n}} \overline{\Psi}_d$$

$$\prod_{d\mid n} \overline{\Psi}_d(X)$$

Como $\overline{\mathbb{F}}_p[X]$ é domínio, segue que $\overline{\Psi}_n(X) = \overline{\Phi}_n^{\pi}(X)$.

(ii) Podemos escrever $\overline{\Psi}_n(X)$ como produto de alguns $\mathrm{Irr}(\xi, \mathbb{F}_p)$, $\xi \in P_n(\overline{\mathbb{F}}_p)$. Do teorema anterior, $gr(\mathrm{Irr}(\xi, \mathbb{F}_p)) = o(p + n\mathbb{Z})$. □

Corolário. (i) $\overline{\Psi}_n(X)$ se fatora como produto de polinômios de grau 1 se e só se $p \equiv 1 \pmod n$.

(ii) $(\mathbb{Z}/n\mathbb{Z})^{\times} = \langle p + n\mathbb{Z} \rangle$ se, e somente se, $\overline{\Psi}_n(X)$ é irredutível em $\mathbb{F}_p[X]$. □

Teorema. Seja $\mathbb{F}$ um corpo, $\mathbb{F}_0 \subseteq \mathbb{F}$ seu corpo primo, e $\overline{\mathbb{F}}$ seu fecho algébrico. Assuma que $\operatorname{car}\mathbb{F}$ é 0 ou não divide n, e seja $\xi \in P_n(\overline{\mathbb{F}})$. Então

$$\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong \operatorname{Aut}(\mathbb{F}_0(\xi)/\mathbb{F}_0(\xi)\cap\mathbb{F}) \subseteq \operatorname{Aut}(\mathbb{F}_0(\xi)/\mathbb{F}_0).$$

Em particular, $\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ é um grupo abeliano. □

Extensões Cíclicas

Lema. Seja Ω um corpo algebricamente fechado e $a \in \Omega^\times$. Então

(i) Se $R(X^n - a) = \{a_1, \dots, a_n\}$, então

$$\{a_1 a_1^{-1}, a_2 a_1^{-1}, \dots, a_n a_1^{-1}\} = W_n(\Omega).$$

(ii) Se $\operatorname{car}\Omega = 0$ ou $\operatorname{car}\Omega$ não divide n, então $X^n - a$ é separável. Além disso

$$X^n - a = \prod_{i=1}^{n} (X - \xi^i \alpha),$$

para qualquer $\xi \in P_n(\Omega)$ e $\alpha \in R(X^n - a)$.

Dem.: (i) Temos que $a_j^n = a_1^n = a$. Daí

$$(a_j a_1^{-1})^n = a_j^n \cdot (a_1^n)^{-1} = a \cdot a^{-1} = 1 \Rightarrow a_j a_1^{-1} \in W_n(\Omega).$$

Reciprocamente, se $\zeta \in W_n(\Omega)$, então $(\zeta a_1)^n = \zeta^n \cdot a_1^n = a$.

(ii) Segue de (i) e do fato de que $W_n(\Omega) = \langle \xi \rangle$, para qualquer $\xi \in P_n(\Omega)$. Ainda $(X^n - a)' = nX^{n-1}$, daí $\mathrm{mdc}(nX^{n-1}, X^n - a) = 1$. □

(Relembre que $P_n(\mathbb{F}) \neq \emptyset \Rightarrow \mathrm{car}\,\mathbb{F} \nmid n$)

Teorema. Sejam $\mathbb{F}$ um corpo tal que $P_n(\mathbb{F}) \neq \emptyset$, e $a \in \mathbb{F}^\times$. Seja $\mathbb{L} = \mathbb{F}(R(X^n - a))$. Então

(i) $\mathbb{L} = \mathbb{F}(\alpha)$, para qualquer $\alpha \in R(X^n - a)$.

(ii) $\mathbb{L}/\mathbb{F}$ é galoisiana finita, e $\mathrm{Aut}(\mathbb{L}/\mathbb{F})$ é isomorfo a um subgrupo de $W_n(\mathbb{F})$. Portanto, $[\mathbb{L}:\mathbb{F}] \mid n$.

(iii) $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \cong W_n(\mathbb{F}) \Leftrightarrow [\mathbb{L}:\mathbb{F}] = n$.

Dem.: (i) Do lema anterior, $R(X^n - a) = \{\alpha \xi^i \mid i = 0, \dots, n-1\}$, para qualquer $\alpha \in R(X^n - a)$, em que $\xi \in P_n(\mathbb{F})$. Portanto,

$$R(X^n - a) \subseteq \mathbb{F}(\alpha), \quad \forall \alpha \in R(X^n - a).$$

Por outro lado, $\alpha \in R(X^n - a) \subseteq \mathbb{L} \Rightarrow \mathbb{F}(\alpha) \subseteq \mathbb{L}$. Assim

$$\mathbb{L} = \mathbb{F}(R(X^n - a)) = \mathbb{F}(\alpha), \quad \forall \alpha \in R(X^n - a).$$

(ii) Como $X^n - a$ é separável, segue que $\mathbb{L}/\mathbb{F}$ é galoisiana finita. Fixe $\alpha \in R(X^n - a)$. Dado $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$, temos que $\sigma(\alpha) \in R(X^n - a)$. Assim, $\sigma(\alpha) = \alpha\xi^i$, para algum i. Portanto, $\frac{\sigma(\alpha)}{\alpha} = \xi^i \in W_n(\mathbb{F})$. Defina

$$\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F}) \longmapsto \frac{\sigma(\alpha)}{\alpha} \in W_n(\mathbb{F}).$$

Sejam $\tau, \sigma \in \mathrm{Aut}(L/F)$ tais que $\tau(\alpha) = \alpha\xi^i$, $\sigma(\alpha) = \alpha\xi^j$. Então ($\xi^i \in F$)

$$\frac{(\tau\circ\sigma)(\alpha)}{\alpha} = \frac{\tau(\alpha\xi^j)}{\alpha} = \frac{\xi^i\cdot\tau(\alpha)}{\alpha} = \frac{\xi^i\cdot\alpha\cdot\xi^j}{\alpha} =$$

$$= \xi^j\xi^i = \frac{\tau(\alpha)}{\alpha}\cdot\frac{\sigma(\alpha)}{\alpha}.$$

Assim, $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$ é hom. de grupos. Assuma que $\sigma \mapsto 1 = \frac{\sigma(\alpha)}{\alpha}$. Daí $\sigma(\alpha) = \alpha$. Mas σ é um F-monomorfismo de $F(\alpha)$ tal que $\sigma(\alpha) = \alpha$. Portanto, $\sigma = \mathrm{Id}$. Conclui-se que $\mathrm{Aut}(L/F)$ é isomorfo a um subgrupo de $W_n(F)$. Assim,

$$[L:F] = |\mathrm{Aut}(L/F)| \,/\, |W_n(F)| = n.$$

(iii) detalhes ficam de exercício. □

Corolário. Assuma que $\mathrm{car}\, F = 0$ ou não divide n. Sejam $\overline{F}$ um fecho algébrico de F, $\xi \in P_n(F)$ e $a \in F^\times$. Seja $L = F(\mathcal{R}(X^n - a))$. Então:

(i) L/F é galoisiana finita e $L = F(\xi, \alpha)$, para qualquer $\alpha \in \mathcal{R}(X^n - a)$.

(ii) $\mathrm{Aut}(L/F(\xi))$ é cíclico, e sua ordem divide n.

(iii) $F(\xi)/F$ é galoisiana finita, e $\mathrm{Aut}(F(\xi)/F)$ é abeliano. □