11. Extensão Ciclotômica

Seja $\mathbb{F}$ um corpo. Queremos estudar raízes da unidade, ou seja, raízes do polinômio $X^n - 1$. Se $\operatorname{car}\mathbb{F} = p > 0$ e p divide n, então a derivada de $X^n - 1$ é nula. Portanto, $X^n - 1$ terá raízes repetidas. De fato, neste caso, podemos escrever $X^n - 1 = \left(X^{n/p} - 1\right)^p$. Se $\operatorname{car}\mathbb{F} = p \geq 0$ e p não divide n, então $(X^n - 1)' = nX^{n-1}$ não possui raízes em comum com $X^n - 1$. Portanto, neste caso, $X^n - 1$ é um polinômio separável.

Denote por $W_n(\mathbb{F}) = \{a \in \mathbb{F}^\times \mid a^n = 1\}$. Note que $W_n(\mathbb{F})$ é um subgrupo cíclico e finito de $\mathbb{F}^\times$, de cardinalidade no máximo n. Seja $\mathscr{R}(X^n - 1)$ o conjunto de raízes de $X^n - 1$ num fecho algébrico de $\mathbb{F}$. Note que $W_n(\mathbb{F}) = \mathscr{R}(X^n - 1) \cap \mathbb{F}^\times$.

Denote por $\mathcal{P}_n(\mathbb{F}) = \{a \in \mathbb{F}^\times \mid o(a) = n\}$. Os elementos de $\mathcal{P}_n(\mathbb{F})$ são denominados de *n-raiz primitiva da unidade*. Note que, ou $\mathcal{P}_n(\mathbb{F})$ é vazio, ou possui exatamente $\phi(n)$ elementos.

Proposição 11.1. *Sejam $\mathbb{F}$ um corpo, com $\operatorname{car}\mathbb{F} = p \geq 0$, e $n \in \mathbb{N}$. As seguintes afirmações são equivalentes:*

(i) $|W_n(\mathbb{F})| = n$,
(ii) $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$,
(iii) *p não divide n, e $X^n - 1$ fatora-se completamente em $\mathbb{F}[X]$.*

Neste caso, temos que $W_n(\mathbb{F}) = \langle\xi\rangle$ se e só se $\xi \in \mathcal{P}_n(\mathbb{F})$. Mais ainda

$$W_n(\mathbb{F}) = \bigcup_{d|n} \mathcal{P}_d(\mathbb{F}).$$

Demonstração. $(i) \Rightarrow (ii)$: Seja $\xi \in W_n(\mathbb{F})$ um gerador do grupo. Então $o(\xi) = n$. Portanto, $\xi \in \mathcal{P}_n(\mathbb{F})$.
$(ii) \Rightarrow (iii)$: Se p divide n e existe $\xi \in \mathcal{P}_n(\mathbb{F})$, então $0 = \xi^{p(n/p)} - 1 = (\xi^{n/p} - 1)^p$. Portanto, $o(\xi) \leq n/p < n$, uma contradição. Segue que p não divide n. Por fim, se $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$, então $\langle\xi\rangle = W_n(\mathbb{F})$ possui ordem n. Daí, $\mathbb{F}$ contém todas as raízes de $X^n - 1$.
$(iii) \Rightarrow (i)$: Já vimos que, nesta situação, o polinômio $X^n - 1$ é separável. Se $X^n - 1$ se fatora completamente em $\mathbb{F}[X]$, então as n raízes de $X^n - 1$ estão em $\mathbb{F}$. Portanto, $|W_n(\mathbb{F})| = n$. □

Se $\mathbb{F}$ é algebricamente fechado, então o polinômio $X^n - 1$ se fatora em produto de polinômios de grau 1. Portanto, podemos enunciar o seguinte:

Corolário 11.2. *Sejam $\bar{\mathbb{F}}$ um corpo algebricamente fechado, e $n \in \mathbb{N}$. As seguintes afirmações são equivalentes:*

(i) $|W_n(\bar{\mathbb{F}})| = n$,
(ii) $\mathcal{P}_n(\bar{\mathbb{F}}) \neq \emptyset$,
(iii) *$X^n - 1 \in \bar{\mathbb{F}}[X]$ é um polinômio separável,*
(iv) *p não divide n.*

Em adicional, se $\operatorname{car}\bar{\mathbb{F}} = 0$, então todas as condições são válidas. □

Seja $\bar{\mathbb{F}}$ um fecho algébrico de $\mathbb{F}$, e seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. Considere o corpo $\mathbb{E} = \mathbb{F}(\xi)$. O grupo $W_n(\mathbb{E})$ é isomorfo ao grupo aditivo cíclico $\mathbb{Z}/n\mathbb{Z}$. Um isomorfismo pode ser dado por $\xi^i \in W_n(\mathbb{E}) \mapsto i + nZ \in \mathbb{Z}/n\mathbb{Z}$. Os elementos que geram $\mathbb{Z}/n\mathbb{Z}$ são exatamente as unidades do anel $\mathbb{Z}/n\mathbb{Z}$. Assim, existe bijeção entre $\mathcal{P}_n(\mathbb{E})$ e

$(\mathbb{Z}/n\mathbb{Z})^\times$. Note então que $\mathcal{P}_n(\mathbb{E}) = \{\xi^i \mid 1 \leq i \leq n, \text{mdc}(n,i) = 1\}$. Mais ainda, sabe-se que $\text{Aut}\,(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Por construção, $\mathbb{E}$ é o corpo de raízes de $X^n - 1$ sobre $\mathbb{F}$. Portanto, $\mathbb{E}/\mathbb{F}$ é galoisiana finita. Seja $\sigma \in \text{Aut}(\mathbb{E}/\mathbb{F})$. Então a restrição $\sigma|_{W_n(\mathbb{E})} : W_n(\mathbb{E}) \to W_n(\mathbb{E})$ é um isomorfismo de grupos. Isso significa que $\sigma(\xi) \in \mathcal{P}_n(\mathbb{E})$. Portanto, temos um mapa

$$\sigma \in \text{Aut}(\mathbb{E}/\mathbb{F}) \mapsto \sigma \in \text{Aut}(W_n(\mathbb{E})) \mapsto i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times,$$

em que $\sigma(\xi) = \xi^i$. Como $\sigma \in \text{Aut}(\mathbb{E}/\mathbb{F})$ é totalmente definido pelo elemento $\sigma(\xi)$, segue que o mapa $\text{Aut}(\mathbb{E}/\mathbb{F}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ é injetora.

Combinando essas observações, acabamos de provar o seguinte:

Teorema 11.3. *Seja $\mathbb{F}$ um corpo de característica $p \geq 0$, em que p não divide n. Seja $\xi \in \bar{\mathbb{F}}$ uma n-ésima raiz primitiva da unidade. Então:*

(1) *$\mathbb{F}(\xi)/\mathbb{F}$ é galoisiana finita,*
(2) *$\text{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ é isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^\times$, e portanto, $[\mathbb{F}(\xi) : \mathbb{F}]$ divide $\phi(n)$,*
(3) *$[\mathbb{F}(\xi) : \mathbb{F}] = \phi(n)$ se, e somente se, $\text{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

□

A extensão $\mathbb{F}(\xi)/\mathbb{F}$ é denominada de a *n-ésima extensão ciclotômica* de $\mathbb{F}$. Vamos estudar a extensão ciclotômica no caso de $\mathbb{F} = \mathbb{Q}$. Para isso, precisaremos do seguinte resultado elementar (demonstração fica de exercício):

Lema 11.4 (Lema de Gauss)**.** *Seja $f \in \mathbb{Z}[X]$ mônico, e assuma que $g, h \in \mathbb{Q}[X]$ sejam mônicos de modo que $f = gh$. Então $g, h \in \mathbb{Z}[X]$.* □

Teorema 11.5. *Seja $\xi \in \mathcal{P}_n(\mathbb{C})$. Então $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$. Além disso, vale o isomorfismo $\text{Aut}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Demonstração. Seja p um número primo que não divide n. Sejam $f_1 = \text{Irr}(\xi, \mathbb{Q})$, e $f_2 = \text{Irr}(\xi^p, \mathbb{Q})$. Vamos provar que $f_1 = f_2$. Caso contrário, como ambos dividem $X^n - 1$, temos que $X^n - 1 = f_1(X)f_2(X)g(X)$. Do Lema de Gauss, segue que $g(X) \in \mathbb{Z}[X]$. Como ξ é raiz de $f_2(X^p)$, temos que $f_2(X^p) = f_1(X)h(X)$, para algum $h(X) \in \mathbb{Q}[X]$. Novamente do Lema de Gauss, vale que $h \in \mathbb{Z}[X]$.

Seja $\pi : \mathbb{Z} \to \mathbb{F}_p$ o homomorfismo canônico. Além disso, para cada $z \in \mathbb{Z}$, temos que $\pi(z^p) = \pi(z)^p = \pi(z)$. Portanto, temos que

$$f_1^\pi(X)h^\pi(X) = \pi(f_2(X^p)) = (f_2^\pi(X))^p.$$

Isso significa que $d(X) := \text{mdc}(f_1^\pi, f_2^\pi) \neq 1$. Portanto, $(d(X))^2$ divide $f_1^\pi f_2^\pi g^\pi = \pi(X^n - 1)$. Mas $\pi(X^n - 1)$ é separável, uma contradição. Conclui-se então que $f_1 = f_2$.

Como $\text{mdc}(p, n) = 1$, segue que $\xi^p \in \mathcal{P}_n(\mathbb{C})$. Repetindo o argumento para outros primos não dividindo n, obtemos que $\text{Irr}(\zeta, \mathbb{Q}) = \text{Irr}(\xi, \mathbb{Q})$, para qualquer $\zeta \in \mathcal{P}_n(\mathbb{C})$. Portanto, $\text{gr}(\text{Irr}(\xi, \mathbb{Q})) \geq \phi(n)$. Do teorema anterior, segue que $\text{gr}(\text{Irr}(\xi, \mathbb{Q})) = \phi(n)$. □

Seja $\Phi_n(X) = \text{Irr}(\xi, \mathbb{Q})$. Então, a demonstração do teorema anterior garante que $\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n(\mathbb{C})}(X - \zeta)$ é um polinômio de grau $\phi(n)$. Denominamos $\Phi_n(X)$ de

o *n-ésimo polinômio ciclotômico*. Mais ainda, temos que

$$X^n - 1 = \prod_{\zeta \in W_n(\mathbb{C})} (X - \zeta) = \prod_{d|n} \left(\prod_{\zeta \in \mathcal{P}_d(\mathbb{C})} (X - \zeta) \right) = \prod_{d|n} \Phi_d(X).$$

Como $X^n - 1$ e cada $\Phi_d(X)$ é um polinômio mônico em $\mathbb{Q}[X]$, o Lema de Gauss garante que cada $\Phi_d(X) \in \mathbb{Z}[X]$. Mais ainda, a fórmula anterior permite calcular $\Phi_n(X)$ recursivamente. De fato,

$$\Phi_n(X) = \frac{X^n - 1}{\prod\limits_{\substack{d|n \\ d \neq n}} \Phi_d(X)}.$$

Exemplo 11.1.

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

(2) Se p é primo, então

$$\Phi_p = \frac{X^p - 1}{\Phi_1(X)} = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

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

A construção dos polinômios $\Phi_n(X)$ podem ser feitas sobre qualquer corpo. O que pode ocorrer é que os mesmos não necessariamente são irredutíveis sobre um corpo qualquer.

Sobre um corpo primo finito, temos os seguintes resultados:

Teorema 11.6. *Sejam $n \in \mathbb{N}$ e p um primo não dividindo n. Seja $\bar{\mathbb{F}}_p$ um fecho algébrico de $\mathbb{F}_p$, e seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}}_p)$. Então $[\mathbb{F}_p(\xi) : \mathbb{F}_p] = o(p + n\mathbb{Z})$, a ordem do elemento $p + n\mathbb{Z}$ em $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Demonstração. Da estrutura de corpos finitos, sabemos que $|\mathbb{F}_p(\xi)| = p^m$, em que $m = [\mathbb{F}_p(\xi) : \mathbb{F}_p] = |\mathrm{Aut}(\mathbb{F}_p(\xi))|$. Além disso, $\mathrm{Aut}(\mathbb{F}_p(\xi)/\mathbb{F}_p) = \langle F \rangle$, em que $F : a \in \mathbb{F}_p(\xi) \mapsto a^p \in \mathbb{F}_p(\xi)$. Temos ainda

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

□

Para cada n não múltiplo de p, seja

$$\Psi_n(X) = \prod_{\xi \in \mathcal{P}_n(\bar{\mathbb{F}}_p)} (X - \xi).$$

Note que $\mathbb{F}_p[X] \ni X^n - 1 = \prod_{d|n} \Psi_d(X)$. Além disso, vale o seguinte:

Corolário 11.7. *Seja $\pi : \mathbb{Z} \to \mathbb{F}_p$ a projeção canônica. Então*

(i) *$\Psi_n = \Phi_n^\pi$, para cada n não múltiplo de p,*

(ii) *Seja $r = \phi(n)/o(p + n\mathbb{Z})$. Então Ψ_n é o produto de r polinômios mônicos e irredutíveis de grau $o(p + n\mathbb{Z})$, distintos dois a dois em $\mathbb{F}_p[X]$.*

Demonstração. (i) Temos que $\Psi_1(X) = X - 1 = \pi(X-1) = \Phi_1^\pi(X)$. Assumindo, por indução, que $\Psi_d(X) = \Phi_d^\pi(X)$, para todo $d < n$, temos que

$$\prod_{d|n} \Psi_d(X) = X^n - 1 = \pi(X^n - 1) = \pi\left(\prod_{d|n} \Phi_d(X)\right) = \Phi_n^\pi\left(\prod_{\substack{d|n \\ d\neq n}} \Psi_d(X)\right).$$

Portanto, $\Phi_n^\pi(X) = \Psi_n(X)$.
(ii) Seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}}_p)$. Então, do teorema anterior, $\operatorname{gr}\operatorname{Irr}(\xi, \mathbb{F}_p) = o(p + n\mathbb{Z})$. Como Ψ_n é um polinômio separável e é o produto de alguns $\operatorname{Irr}(\xi, \mathbb{F}_p)$, o resultado segue. □

Olhando para os casos extremos no item (ii) do corolário anterior, obtemos o seguinte:

Corolário 11.8. *Seja n não múltiplo do primo p. Então*

(i) *$\Psi_n(X)$ se fatora completamente como produto de polinômios de grau 1 em $\mathbb{F}_p[X]$ se, e somente se, $p \equiv 1 \pmod{n}$.*
(ii) *$\Psi_n(X)$ é irredutível em $\mathbb{F}_p[X]$ se, e somente se, $(\mathbb{Z}/n\mathbb{Z})^\times = \langle p + n\mathbb{Z}\rangle$.*

□

Finalmente, para um corpo qualquer, podemos combinar a Proposição 9.3 e os resultados para $\mathbb{Q}$ e $\mathbb{F}_p$ para descrever o grupo de Galois de uma extensão ciclotômica:

Teorema 11.9. *Seja $\mathbb{F}$ um corpo, $\mathbb{F}_0 \subseteq \mathbb{F}$ seu corpo primo, e $\bar{\mathbb{F}} \supseteq \mathbb{F}$ um fecho algébrico. Assuma que $\operatorname{car}\mathbb{F}$ é zero ou não divida $n \in \mathbb{N}$. Seja $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. Então*

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

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