10. Corpos finitos

Seja $p > 0$ um número primo. Denotaremos por $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ o corpo finito com p elementos. Se $\mathbb{F}$ é um corpo de característica $p > 0$, então $F : \mathbb{F} \to \mathbb{F}$ denota o *homomorfismo de Frobenius*, isto é, $F(a) = a^p$, para cada $a \in \mathbb{F}$. Já vimos que F é um monomorfismo de anéis. Denotaremos por $\bar{\mathbb{F}}_p$ um fecho algébrico de $\mathbb{F}_p$.

Teorema 10.1. *Seja $m \geq 1$. Então existe um corpo $\mathbb{E}$ com exatamente p^m elementos. Tal corpo é único, a menos de um isomorfismo. Ainda mais, as seguintes caracterizações de $\mathbb{E}$ são válidas:*

(1) *$\mathbb{E}$ é o corpo de raízes de $X^{p^m} - X$ sobre $\mathbb{F}_p$.*
(2) *$\mathbb{E}$ é o conjunto das raízes de $X^{p^m} - X$ em $\bar{\mathbb{F}}_p$.*

Demonstração. Seja $f(X) = X^{p^m} - X \in \mathbb{F}_p[X]$. Primeiramente, note que a derivada formal de f é $f' = -1$. Como $\mathrm{mdc}(f, f') = 1$, segue que todas as raízes de f são distintas.

Afirmação 1. Se $\mathbb{E} \subseteq \bar{\mathbb{F}}_p$ é um corpo que possui exatamente p^m elementos, então $\mathbb{E} = \{a \in \bar{\mathbb{F}}_p \mid f(a) = 0\}$.

De fato, o grupo multiplicativo de $\mathbb{E}$ possui exatamente $p^m - 1$ elementos. Portanto, cada $a \in \mathbb{E}^\times$ satisfaz $a^{p^m-1} = 1$. Assim, cada elemento de $\mathbb{E}$ satisfaz $X^{p^m} - X = 0$. Daí, $\mathbb{E}$ consiste das raízes de f.

Afirmação 2. O conjunto $\mathscr{R}(f) = \{a \in \bar{\mathbb{F}}_p \mid f(a) = 0\}$ é um corpo contendo $\mathbb{F}_p$.

De fato, dados $a, b \in \mathscr{R}(f)$, temos que:

- $f(a+b) = (a+b)^{p^m} - (a+b) = f(a) + f(b) = 0$,
- $f(ab) = (ab)^{p^m} - ab = (a^{p^m} - a + a)b^{p^m} - ab = f(a) + af(b) = 0$,
- como $\alpha^p = \alpha$, para cada $\alpha \in \mathbb{F}_p$, segue que $f(\alpha) = 0$. Assim, $\mathbb{F}_p \subseteq \mathscr{R}(f)$.

Portanto, $\mathscr{R}(f)$ é um anel contendo $\mathbb{F}_p$. Como $\mathscr{R}(f)$ é um domínio (pois é subanel do corpo $\bar{\mathbb{F}}_p$), segue que $\mathscr{R}(f)$ é corpo.

Afirmação 3. O corpo de raízes (em $\bar{\mathbb{F}}_p$) de f sobre $\mathbb{F}_p$ possui exatamente p^m elementos.

De fato, pela Afirmação 2, o conjunto $\mathscr{R}(f)$ é um corpo. Além disso, o mesmo é o menor corpo contendo $\mathbb{F}_p$ e as raízes de f. Portanto, $\mathscr{R}(f)$ é o corpo de raízes de f sobre $\mathbb{F}_p$

Portanto, existe um corpo com exatamente p^m elementos. Se $\mathbb{E}'$ é um outro corpo com p^m elementos, então, pela Afirmação 3, $\mathbb{E}'$ é o corpo de raízes de f sobre $\mathbb{F}_p$. Como o corpo de raízes é único, a menos de isomrfismo, segue que $\mathbb{E}'$ é isomorfo a $\mathbb{E}$. □

Se $q = p^m$, denote por $\mathbb{F}_q$ o corpo finito com q elementos. Note que, se m divide n, então $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ (assumindo que ambos são subcorpos de $\bar{\mathbb{F}}_p$).

A seguir, provaremos que o grupo multiplicativo de um corpo finito é cíclico (isto é, é gerado por um único elemento). Como consequência, obteremos a validade do Teorema do Elemento Primitivo para extensões de corpos envolvendo corpos finitos.

Lema 10.2. *Seja G um grupo abeliano finito de ordem n. Assuma que, para todo m dividindo n, $\#\{x \in G \mid x^m = 1\} \leq m$. Então G é cíclico.*

Demonstração. Seja $G_m = \{x \in G \mid o(x) = m\}$ (em que $o(g)$ denota a ordem de g). Se $G_m \neq \emptyset$, então existe $g_m \in G_m$. Daí $\langle g_m \rangle$ é um subgrupo de ordem m. Todos os seus elementos satisfazem $g^m = 1$. Assim, por hipótese, segue que

$$\langle g_m \rangle = \{x \in G \mid x^m = 1\} \supseteq G_m.$$

Obtemos então

$$n = |G| = \sum_{m/n} \#G_m \leq \sum_{m/n} \phi(m) = n,$$

em que $\phi(m) = \#\{1 \leq r \leq m \mid \mathrm{mdc}(r, m) = 1\}$ é a função de Euler. Portanto, todo G_m é não vazio. Em particular, $G_n \neq \emptyset$, ou seja, G é cíclico. $\square$

Teorema 10.3. *Seja $\mathbb{F}$ um corpo finito. Então, seu corpo multiplicativo $(\mathbb{F}^\times, \cdot)$ é um grupo cíclico.*

Demonstração. Seja $G = \mathbb{F}^\times$ o grupo multiplicativo do corpo. Então, para cada m dividindo $|G|$, $\{x \in G \mid x^m = 1\}$ é o conjunto das raízes do polinômio $X^m - 1$. O último possui no máximo m raízes. Portanto, pelo lema anterior, $\mathbb{F}^\times$ é cíclico. $\square$

Corolário 10.4. *Sejam $\mathbb{F}$ um corpo finito e $\mathbb{E}/\mathbb{F}$ uma extensão finita. Então a extensão $\mathbb{E}/\mathbb{F}$ é simples, isto é, existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$.*

Demonstração. Pelo teorema anterior, $\mathbb{E}^\times = \langle a \rangle$. Portanto, obtemos que $\mathbb{E} = \mathbb{F}(a)$. $\square$

Por fim, vamos calcular o grupo de automorfismos de uma extensão de corpos envolvendo corpos finitos. Começamos com o seguinte:

Teorema 10.5. *Seja $q = p^m$. Então $\mathrm{Aut}(\mathbb{F}_q) = \langle F \rangle$ é um grupo de ordem m, gerado pelo homomorfismo de Frobenius.*

Demonstração. Como $\mathbb{F}_p$ é perfeito, a extensão $\mathbb{F}_q/\mathbb{F}_p$ é separável. Além disso, do Teorema 10.1, a extensão também é normal. Portanto, $\mathbb{F}_q/\mathbb{F}_p$ é galoisiana finita de grau m. Assim, $|\mathrm{Aut}(\mathbb{F}_q)| = |\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = m$.

Como o homomorfismo de Frobenius é um homomorfismo de anéis $F : \mathbb{F}_q \to \mathbb{F}_q$, segue que $F \in \mathrm{Aut}(\mathbb{F}_q)$. Ainda, para cada $x \in \mathbb{F}_q$, temos que $F^m(x) = x^{p^m} = x$. Portanto, $F^m = 1$. Assuma que $1 < s \leq m$ é tal que $F^s = 1$. Então todo $x \in \mathbb{F}_q$ satisfaz $0 = F^s(x) - x = x^{p^s} - x$. Isso implica que $\mathbb{F}_q \subseteq \mathbb{F}_{p^s}$. Mas $p^s \leq q$, e portanto, vale a igualdade. Obtemos então que $q = p^s$, ou seja, $s = m$. Segue que $\langle F \rangle$ é um subgrupo com m elementos. Assim, conclui-se que $\mathrm{Aut}(\mathbb{F}_q) = \langle F \rangle$. $\square$

Colecionando os resultados provados, enunciamos o seguinte:

Corolário 10.6. *Seja $\mathbb{E}/\mathbb{F}$ em que $\mathbb{E}$ é finito e de característica $p > 0$. Então $\mathbb{E}/\mathbb{F}$ é galoisiana finita. Ainda mais, se $|\mathbb{F}| = p^m$ e $|\mathbb{E}| = p^n$, então m divide n. O grupo de automorfismos da extensão é $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle F^m \rangle$, e sua ordem é $n/m = [\mathbb{E} : \mathbb{F}]$.*

Demonstração. Do teorema anterior, $\mathrm{Aut}(\mathbb{E}) = \langle F \rangle$ possui ordem n. Ainda,

$$\mathbb{E}^{\langle F^m \rangle} = \{x \in \mathbb{E} \mid F^m(x) = x^{p^m} = x\} = \mathbb{F}.$$

Portanto, da correspondência de Galois, $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle F^m \rangle$. A ordem do subgrupo é $n/m = [\mathbb{E} : \mathbb{F}]$. $\square$