4. Extensão normal (Parte I)

Começaremos com a seguinte definição, cuja importância ficará clara em breve. Seja Ω um corpo algebricamente fechado contendo um corpo $\mathbb{F}$. Dado $f \in \mathbb{F}[X]$, denote por $\mathscr{R}(f) \subseteq \Omega$ o conjunto das raízes de f em Ω, isto é,

$$\mathscr{R}(f) = \{a \in \Omega \mid f(a) = 0\}.$$

Definição 4.1. Sejam $\mathbb{F}$ um corpo, Ω um corpo algebricamente fechado contendo $\mathbb{F}$, e $\mathscr{S} \subseteq \mathbb{F}[X]$ um conjunto de polinômios. Seja $\mathscr{R}(\mathscr{S}) = \bigcup_{f\in\mathscr{S}} \mathscr{R}(f) \subseteq \Omega$ o conjunto de todas as raízes de todos os $f \in \mathscr{S}$. Um *corpo de raízes* de $\mathscr{S}$ sobre $\mathbb{F}$ (em Ω) é o corpo $\mathbb{L} = \mathbb{F}(\mathscr{R}(\mathscr{S}))$.

No caso em que $\mathscr{S}$ contém um único elemento, digamos $\mathscr{S} = \{f\}$, então dizemos simplesmente que $\mathbb{L}$ é um corpo de raízes de f sobre $\mathbb{F}$.

Exemplo 4.1. (1) O corpo de raízes de $X^2 + 1$ sobre $\mathbb{Q}$ é $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$.

(2) Seja $f = (X^2 - 2)(X^2 - 3)$. Suas raízes são $\pm\sqrt{2}, \pm\sqrt{3}$. Então o corpo de raízes de f sobre $\mathbb{Q}$ é $\mathbb{L} = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note que o mesmo $\mathbb{L}$ também é o corpo de raízes de $\mathscr{S} = \{X^2 - 2, X^2 - 3\}$ sobre $\mathbb{Q}$.

(3) Sejam $\xi \in \mathbb{C}$ tal que $\xi \neq \xi^3 = 1$. Então um corpo de raízes de $X^3 - 2$ sobre $\mathbb{Q}$ é $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2)$. O mesmo coincide com $\mathbb{Q}(\sqrt[3]{2}, \xi)$. De fato, por um lado, $\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2 \in \mathbb{Q}(\sqrt[3]{2}, \xi)$. Mas,

$$\xi = \frac{\sqrt[3]{2}\xi}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2).$$

Portanto, vale a igualdade de corpos.

(4) Sejam p primo e $\zeta \in \mathbb{C}$ tal que $\zeta \neq \zeta^p = 1$. As raízes de $X^p - 1$ são $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$. Então, o corpo de raízes de $X^p - 1$ sobre $\mathbb{Q}$ é $\mathbb{Q}(1, \zeta, \zeta^2, \ldots, \zeta^{p-1})$. Como $1, \zeta^2, \ldots, \zeta^{p-1} \in \mathbb{Q}(\zeta)$, segue que o corpo de raízes coincide com $\mathbb{Q}(\zeta)$. Note que o tal corpo coincide com a extensão simples de $\mathbb{Q}$ por uma das raízes de $X^p - 1$.

Proposição 4.2. *Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio de grau $n \geq 1$. Seja $\mathbb{L}$ um corpo de raízes de f sobre $\mathbb{F}$. Então $\mathbb{L}/\mathbb{F}$ é finita e $[\mathbb{L} : \mathbb{F}] \leq n!$.*

Demonstração. Temos que $\mathbb{L} = \mathbb{F}(a_1, \ldots, a_m)$, em que $\mathscr{R}(f) = \{a_1, \ldots, a_m\}$ são as raízes de f, em algum corpo algebricamente fechado Ω. Temos que $[\mathbb{F}(a_1) : \mathbb{F}] \leq n$ (coincide com o grau da componente irredutível de f o qual a_1 é raiz). Então $g(X) := \frac{f(X)}{X - a_1} \in \mathbb{F}(a_1)[X]$ é um polinômio de grau $n - 1$. Além disso, o corpo de raízes de g sobre $\mathbb{F}(a_1)$ é o próprio $\mathbb{L}$, por construção. Por indução, $[\mathbb{L} : \mathbb{F}(a_1)] \leq (n - 1)!$. Portanto,

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{F}(a_1)][\mathbb{F}(a_1) : \mathbb{F}] \leq n!$$

□

Proposição 4.3. *Sejam $\mathbb{F}$ corpo, $\mathscr{S} \subseteq \mathbb{F}[X]$ e Ω um corpo algebricamente fechado contendo $\mathbb{F}$. O corpo de raízes $\mathbb{L} \subseteq \Omega$ de $\mathscr{S}$ sobre $\mathbb{F}$ é o menor subcorpo de Ω contendo $\mathbb{F}$, e de tal forma todo $f \in \mathscr{S}$ se decompõe como produto de polinômios de grau 1 em $\mathbb{L}[X]$.*

Demonstração. Seja $\mathbb{E} \subseteq \Omega$ um corpo de modo que todo polinômio em $\mathscr{S}$ se fatora como produto de polinômios de grau 1. Então, dado $f \in \mathscr{S}$, podemos escrever

$$f = \alpha(X - a_1) \cdots (X - a_m) \in \mathbb{E}[X].$$

Então $a_1, \ldots, a_m \in \mathbb{E}$, ou seja, $\mathscr{R}(f) \subseteq \mathbb{E}$. Portanto, $\mathscr{R}(\mathscr{S}) \subseteq \mathbb{E}$. Isso implica que $\mathbb{E} \supseteq \mathbb{F}(\mathscr{S}) = \mathbb{L}$. □

Definição 4.4. Sejam $\mathbb{E}_1$ e $\mathbb{E}_2$ corpos contendo um mesmo corpo $\mathbb{F}$. Um $\mathbb{F}$-*homomorfismo* (ou $\mathbb{F}$-monomorfismo) é um mapa $\eta : \mathbb{E}_1 \to \mathbb{E}_2$ tal que $\eta(\alpha) = \alpha$, $\forall \alpha \in \mathbb{F}$. Da mesma forma define-se $\mathbb{F}$-isomorfismo, $\mathbb{F}$-endomorfismo e $\mathbb{F}$-automorfismo.

Notação. Dado um homomorfismo de corpos $\eta : \mathbb{F} \to \mathbb{E}$, e $f \in \mathbb{F}[X]$, denote por $f^\eta = \eta(f)$ (relembre que η induz um homomorfismo de anéis $\mathbb{F}[X] \to \mathbb{E}[X]$).

O próximo resultado mostra que um corpo de raízes não depende do corpo maior em que o mesmo é construído:

Teorema 4.5. *Sejam Ω e Ω' dois corpos algebricamente fechados contendo $\mathbb{F}$, e seja $\mathscr{S} \subseteq \mathbb{F}[X]$. Sejam $\mathscr{R}$ e $\mathscr{R}'$ o conjunto das raízes de todos os $f \in \mathscr{S}$ em Ω e Ω', respectivamente. Sejam $\mathbb{L} = \mathbb{F}(\mathscr{R}) \subseteq \Omega$ e $\mathbb{L}' = \mathbb{F}(\mathscr{R}') \subseteq \Omega'$. Então, existe um $\mathbb{F}$-isomorfismo $\mathbb{L} \to \mathbb{L}'$.*

Demonstração. Por construção, a extensão de corpos $\mathbb{L}/\mathbb{F}$ é algébrica. Então, da Proposição 3.7, a aplicação identidade $\mathbb{F} \to \Omega'$ admite uma extensão $\eta : \mathbb{L} \to \Omega'$. Dado $f \in \mathscr{S}$, temos que $f^\eta = f$, pois η é um $\mathbb{F}$-monomorfismo. Como $\mathbb{L}$ é um corpo de raízes para todos os polinômios em $\mathscr{S}$, segue que

$$f = \alpha(X - a_1) \cdots (X - a_m), \quad a_1, \ldots, a_m \in \mathbb{L}.$$

Assim,

$$f = f^\eta = \alpha(X - \eta(a_1)) \cdots (X - \eta(a_m)).$$

Por um lado, da Proposição 4.3, vale que $\mathbb{L}' \subseteq \operatorname{Im}\eta$. Por outro lado, a mesma conta mostra que $\eta(\mathscr{R}) \subseteq \mathscr{R}'$. Daí $\operatorname{Im}\eta \subseteq \mathbb{F}(\mathscr{R}') = \mathbb{L}'$. Segue que $\operatorname{Im}\eta = \mathbb{L}'$. Conclui-se que $\eta : \mathbb{L} \to \mathbb{L}'$ é um $\mathbb{F}$-isomorfismo. □

Definição 4.6. Seja $\mathbb{L}/\mathbb{F}$ uma extensão algébrica de corpos. A extensão é dita ser *normal* se, para todo $a \in \mathbb{L}$, todas as raízes de $\operatorname{Irr}(a, \mathbb{F})$ (polinômio minimal de a sobre $\mathbb{F}$) estão em $\mathbb{L}$.

Teorema 4.7. *Sejam $\mathbb{L}/\mathbb{F}$ uma extensão de corpos algébrica, e Ω um corpo algebricamente fechado contendo $\mathbb{L}$. As seguintes afirmações são equivalentes:*

(i) *$\mathbb{L}/\mathbb{F}$ é uma extensão normal,*
(ii) *existe $S \subseteq \mathbb{L}$ de modo que $\mathbb{L} = \mathbb{F}(S)$, e, para todo $a \in S$, $\mathbb{L}$ contém todas as raízes de $\operatorname{Irr}(a, \mathbb{F})$,*
(iii) *$\mathbb{L}$ é o corpo de raízes sobre $\mathbb{F}$ de algum conjunto de polinômios em $\mathbb{F}[X]$,*
(iv) *Se $\sigma : \mathbb{L} \to \Omega$ é um $\mathbb{F}$-monomorfismo, então $\operatorname{Im}\sigma = \mathbb{L}$ (portanto, σ é um $\mathbb{F}$-automorfismo de $\mathbb{L}$),*
(v) *se $f \in \mathbb{F}[X]$ é irredutível sobre $\mathbb{F}$, e $\mathbb{L}$ contém uma raiz de f, então $\mathbb{L}$ contém todas as raízes de f.*

Demonstração. $(i) \Rightarrow (ii)$: Pode-se tomar $S = \mathbb{L}$. Por definição, $\mathbb{L}$ contém todas as raízes de todo $a \in \mathbb{L}$. Além disso, $\mathbb{L} = \mathbb{F}(S)$.
$(ii) \Rightarrow (iii)$: Por (ii), $\mathbb{L} = \mathbb{F}(S)$, em que, para todo $a \in S$, $\mathscr{R}(\operatorname{Irr}(a, \mathbb{F})) \subseteq \mathbb{L}$. Seja $\mathscr{S} = \{\operatorname{Irr}(a, \mathbb{F}) \mid a \in S\}$. Defina $\mathscr{R}(\mathscr{S}) \subseteq \Omega$. Como todo elemento de $\mathscr{R}(\mathscr{S})$ pertence a $\mathbb{L}$, obtemos que $\mathscr{R}(\mathscr{S}) \subseteq \mathbb{L}$. Por outro lado, $S \subseteq \mathscr{R}(\mathscr{S})$. Então $\mathbb{L} = \mathbb{F}(S) \subseteq \mathbb{F}(\mathscr{R}(\mathscr{S}))$. Portanto, vale a igualdade e $\mathbb{L}$ é o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{F}$.

$(iii) \Rightarrow (iv)$: Seja $\mathbb{L}$ o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{F}$. Seja $\sigma : \mathbb{L} \to \Omega$ um $\mathbb{F}$-monomorfismo. Para cada $f \in \mathbb{F}[X]$, podemos escrever $f = \alpha(X-a_1)\cdots(X-a_m)$, com $a_1, \ldots, a_m \in \mathbb{L}$. Portanto, $f = f^\eta = \alpha(X-\eta(a_1))\cdots(X-\eta(a_m))$. Repetindo o argumento na demonstração do Teorema 4.5, obtemos que $\operatorname{Im}\sigma = \mathbb{L}$.
$(iv) \Rightarrow (v)$: Seja $f \in \mathbb{F}[X]$ irredutível e seja $a \in \mathbb{L}$ com $f(a) = 0$. Seja $b \in \Omega$ com $f(b) = 0$. Daí, da Proposição 3.6, existe um $\mathbb{F}$-monomorfismo $\eta_0 : \mathbb{F}(a) \to \Omega$ tal que $\eta_0(a) = b$. Da Proposição 3.7, segue que η_0 admite extensão $\eta : \mathbb{L} \to \Omega$, tal que $\eta(a) = b$. De (iv), segue que $\operatorname{Im}\eta = \mathbb{L}$. Portanto, $b = f(a) \in \mathbb{L}$. Conclui-se que $\mathscr{R}(f) \subseteq \mathbb{L}$.
$(v) \Rightarrow (i)$: Sejam $a \in \mathbb{L}$ e $p_a \in \mathbb{F}[X]$ seu polinômio minimal sobre $\mathbb{F}$. Então p_a é um polinômio irredutível que possui uma raiz em $\mathbb{L}$ (o próprio elemento a). De (v), segue que $\mathscr{R}(p_a) \subseteq \mathbb{L}$. Portanto, $\mathbb{L}/\mathbb{F}$ é extensão normal. □

A seguir, mostraremos exemplos e contra-exemplos de extensões normais.

Proposição 4.8. *Se $[\mathbb{E} : \mathbb{F}] = 2$, então $\mathbb{E}/\mathbb{F}$ é uma extensão normal.*

Demonstração. Seja $a \in \mathbb{E}$. Se $a \in \mathbb{F}$, então seu polinômio minimal é $X - a$. Daí $\mathbb{E}$ contém todas as raízes desse polinômio (que é somente o elemento a). Assuma então que $a \notin \mathbb{F}$. Então, seu polinômio minimal p_a possui grau 2. Daí $p_a = (X-a)g(X)$, com $\operatorname{gr}(g) = 1$. Assim, $\mathbb{E}$ possui a única raiz de g. Daí $\mathbb{E}$ possui todas as raízes de p_a. Conclui-se que $\mathbb{E}/\mathbb{F}$ é normal. □

Exemplo 4.2. A propriedade da extensão ser normal não é boa, no seguinte sentido. Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões de corpos. Então, se duas das extensões são normais, não necessariamente a terceira será normal também. Os exemplos seguintes ilustram tal fato:

(1) $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ são extensões normais (pois ambos possuem grau 2). Porém, $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ não é uma extensão normal (pois $X^4 - 2$ possui raízes complexas, enquanto que $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathbb{R}$, por exemplo).
(2) São normais as seguintes extensões: $\mathbb{Q}[\sqrt[3]{2}, \xi]/\mathbb{Q}[\sqrt[3]{2}]$ (pois o grau é 2) e $\mathbb{Q}[\sqrt[3]{2}, \xi]/\mathbb{Q}$ (pois é o corpo de raízes de $X^3 - 2$ sobre $\mathbb{Q}$, conforme exemplo anterior). Porém, $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ não é normal (por que?).

Entretanto, temos o seguinte resultado:

Proposição 4.9. *Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensões de corpos. Se $\mathbb{L}/\mathbb{F}$ é normal, então $\mathbb{L}/\mathbb{E}$ é normal.*

Demonstração. Como $\mathbb{L}/\mathbb{F}$ é normal, do Teorema 4.7.(iii), $\mathbb{L}$ é o corpo de raízes sobre $\mathbb{F}$ de algum conjunto $\mathscr{S} \subseteq \mathbb{F}[X]$. Porém, $\mathscr{S} \subseteq \mathbb{F}[X] \subseteq \mathbb{E}[X]$. Por um lado, $\mathbb{L} = \mathbb{F}(\mathscr{R}(\mathscr{S})) \subseteq \mathbb{E}(\mathscr{R}(\mathscr{S}))$. Por outro, $\mathscr{R}(\mathscr{S}) \subseteq \mathbb{L}$, e daí $\mathbb{E}(\mathscr{R}(\mathscr{S})) \subseteq \mathbb{L}$. Portanto, $\mathbb{L}$ é o corpo de raízes de $\mathscr{S}$ sobre $\mathbb{E}$. Daí $\mathbb{L}/\mathbb{E}$ é normal. □