12. Solubilidade via radicais

12.1. **Norma e traço.** Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos, e seja $\{a_1, \ldots, a_n\}$ uma $\mathbb{F}$-base de $\mathbb{E}$. Para cada $\alpha \in \mathbb{E}$, fica bem definido uma $\mathbb{F}$-transformação linear $\mathbb{E} \to \mathbb{E}$ via multiplicação por α. Mais precisamente, existem $\alpha_{ij} \in \mathbb{F}$ tais que

$$\alpha a_i = \sum_{j=1}^{n} \alpha_{ij} a_j, \quad i = 1, \ldots, n.$$

Seja $A = (\alpha_{ij})_{(i,j)}$. Define-se o *traço* e a *norma* do elemento α sobre $\mathbb{E}/\mathbb{F}$ pela fórmula:

$$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) := \mathrm{tr}(A) = \sum_{i=1}^{n} \alpha_{ii}, \quad \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \det A.$$

O *polinômio característico* do elemento α é, por definição, o polinômio característico da matriz A. Mais precisamente, define-se

$$F(\alpha, \mathbb{E}/\mathbb{F}) = \det(x\mathrm{Id} - A).$$

As seguintes propriedades ficam de exercício:

Lema 12.1. *Sejam $[\mathbb{E} : \mathbb{F}] = n$ e $\alpha \in \mathbb{E}$.*

(i) $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}$ *é $\mathbb{F}$-linear, e* $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha\beta) = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha)\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\beta)$.

(ii) *Se* $F(\alpha, \mathbb{E}/\mathbb{F}) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0$, *então*

$$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = -\alpha_{n-1}, \quad \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = (-1)^n \alpha_0.$$

(iii) α *é raiz de* $F(\alpha, \mathbb{E}/\mathbb{F})$.

(iv) $F(\alpha, \mathbb{F}(\alpha)/\mathbb{F}) = \mathrm{Irr}(\alpha, \mathbb{F})$.

(v) *Se* $\mathbb{L}/\mathbb{E}/\mathbb{F}$, *então* $F(\alpha, \mathbb{L}/\mathbb{F}) = F(\alpha, \mathbb{E}/\mathbb{F})^{[\mathbb{L}:\mathbb{E}]}$. *Ainda,*

$$\mathrm{tr}_{\mathbb{L}/\mathbb{F}}(\alpha) = [\mathbb{L} : \mathbb{E}]\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha), \quad e \quad \mathscr{N}_{\mathbb{L}/\mathbb{F}}(\alpha) = \left(\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha)\right)^{[\mathbb{L}:\mathbb{E}]}.$$

(vi) $F(\alpha, \mathbb{E}/\mathbb{F}) = \mathrm{Irr}(\alpha, \mathbb{F})^{[\mathbb{E}:\mathbb{F}(\alpha)]}$.

(vii) *Se* $\mathrm{Irr}(\alpha, \mathbb{F}) = \mathrm{Irr}(\beta, \mathbb{F})$, *então* $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = \mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\beta)$, *e* $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\beta)$.

(viii) *Se* $\mathbb{E}/\mathbb{F}$ *é separável e finita e* $\Omega \supseteq \mathbb{F}$ *é algebricamente fechado, então*

$$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\alpha) = \sum_{\sigma \in \mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)} \sigma(\alpha), \quad \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\alpha) = \prod_{\sigma \in \mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)} \sigma(\alpha).$$

Nomenclatura. Dizemos que uma extensão $\mathbb{E}/\mathbb{F}$ é *cíclica* se o mesmo é galoisiana finita e $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é um grupo cíclico. Da mesma forma, dizemos que $\mathbb{E}/\mathbb{F}$ é *abeliano*, *solúvel*, etc, se o grupo $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é abeliano, solúvel, etc.

12.2. **Extensão cíclica.** O objetivo desta seção é estudar as extensões da forma $X^n - a$, em que $a \in \mathbb{F}^\times$. Começamos com o seguinte:

Lema 12.2. *Assuma que $X^n - a = (X - a_1) \cdots (X - a_n)$ é a fatoração em polinômios de grau 1 em $\Omega[X]$. Então*

$$\{a_j a_1^{-1} \mid j = 1, 2, \ldots, n\} = W_n(\Omega).$$

Em adicional, se $\mathrm{car}\,\mathbb{F} = p \geq 0$ *não divide* n, *então* $X^n - a$ *é separável. Ainda mais, dados quaisquer* $\xi \in \mathcal{P}_n(\Omega)$ *e* $\alpha \in \mathscr{R}(X^n - a)$, *segue que*

$$X^n - a = (X - \alpha)(X - \xi\alpha)(X - \xi^2\alpha) \cdots (X - \xi^{n-1}\alpha).$$

Demonstração. Temos que $a_j^n = a$, para cada j. Portanto, $(a_j a_1^{-1})^n = a_j^n (a_1^n)^{-1} = aa^{-1} = 1$. Daí $a_j a_1^{-1} \in W_n(\Omega)$. Reciprocamente, dado $w \in W_n(\Omega)$, temos que $(a_1 w)^n = a_1^n w^n = a$. Ou seja, $a_1 w \in \mathscr{R}(X^n - a)$.

Agora, assuma que $\operatorname{car}\mathbb{F}$ é zero ou $\operatorname{car}\mathbb{F} = p > 0$ não divide n. Então $(X^n - a)' = nX^{n-1} \neq 0$ possui somente o 0 como raiz. Segue que $\operatorname{mdc}(X^n - a, nX^{n-1}) = 1$, e então, $X^n - a$ é separável. A última afirmação segue de $W_n(\Omega) = \langle \xi \rangle$, para qualquer $\xi \in \mathcal{P}_n(\Omega)$. □

O próximo resultado diz que, se $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$, então a extensão $\mathbb{F}(\mathscr{R}(X^n - a))/\mathbb{F}$ é cíclica. Relembre que, a hipótese $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$ implica que $\operatorname{car}\mathbb{F}$ não divide n (ou é zero).

Teorema 12.3. *Sejam $\mathbb{F}$ um corpo tal que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$ e $a \in \mathbb{F}^\times$. Seja $\mathbb{E} = \mathbb{F}(\mathscr{R}(X^n - a))$. Então:*

(i) *$\mathbb{E} = \mathbb{F}(\alpha)$, para qualquer $\alpha \in \mathscr{R}(X^n - a)$.*
(ii) *$[\mathbb{E} : \mathbb{F}]$ divide n. Ainda, $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ é isomorfo a um subgrupo de $W_n(\mathbb{F})$.*
(iii) *$[\mathbb{E} : \mathbb{F}] = n$ se e só se $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) \cong W_n(\mathbb{F})$, e se e só se $X^n - a$ é irredutível em $\mathbb{F}[X]$.*

Demonstração. (i) Como $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$, o resultado segue do lema anterior.
(ii) Sejam $\xi \in \mathcal{P}_n(\mathbb{F})$ e $\alpha \in \mathscr{R}(X^n - a)$. Do lema anterior, temos então que $\mathscr{R}(X^n - a) = \{a, \xi a, \cdots, \xi^{n-1} a\}$. Para cada $\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$, temos que $\sigma(\mathscr{R}(X^n - a)) = \mathscr{R}(X^n - a)$. Portanto, $\sigma(\alpha) = \xi^j \alpha$, para algum j. Assim, temos um mapa

$$\psi : \sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F}) \mapsto \frac{\sigma(\alpha)}{\alpha} = \xi^j \in W_n(\mathbb{F}).$$

Provemos que ψ é um homomorfismo de grupos. Dados $\sigma_1, \sigma_2 \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$ tais que $\sigma_i(\alpha) = \xi^{j_i}\alpha$, temos que

$$(\sigma_1 \circ \sigma_2)(\alpha) = \sigma_1(\xi^{j_2}\alpha) = \xi^{j_2}\xi^{j_1}\alpha.$$

Portanto, $\psi(\sigma_1\sigma_2) = \psi(\sigma_1)\psi(\sigma_2)$. Agora, seja $\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$ tal que $\psi(\sigma) = 1$. Então $\sigma(\alpha) = \alpha$. Isso implica que $\sigma = \operatorname{Id}_{\mathbb{F}(\alpha)}$. Daí $\sigma = 1$. Concluí-se que ψ é injetora, e portanto, $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ é isomorfo a um subgrupo de $W_n(\mathbb{F})$. Por consequência, $[\mathbb{E} : \mathbb{F}] = |\operatorname{Aut}(\mathbb{E}/\mathbb{F})|$ divide $|W_n(\mathbb{F})| = n$.
(iii) Por (i), $\mathbb{L}$ é uma extensão simples de $\mathbb{F}$ por qualquer $\alpha \in \mathscr{R}(X^n - a)$. Assim, $[\mathbb{E}, \mathbb{F}] = n$ implica que $n = \operatorname{gr}(\operatorname{Irr}(\alpha, \mathbb{F}))$. Portanto, $\operatorname{Irr}(\alpha, \mathbb{F}) = X^n - a$. Reciprocamente, se $X^n - a$ é irredutível, então $X^n - a = \operatorname{Irr}(\alpha, \mathbb{F})$, e daí $[\mathbb{E} : \mathbb{F}] = n$.

Além disso, de (ii), ocorre que $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) \cong W_n(\mathbb{F})$ se e só se $n = |\operatorname{Aut}(\mathbb{E}/\mathbb{F})| = [\mathbb{E} : \mathbb{F}]$. □

Em particular, temos o seguinte resultado:

Corolário 12.4. *Assuma que $\operatorname{car}\mathbb{F}$ é zero ou um primo que não divide n. Sejam $\bar{\mathbb{F}}$ um fecho algébrico de $\mathbb{F}$, e $a \in \mathbb{F}^\times$ e $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. Seja $\mathbb{L} = \mathbb{F}(\mathscr{R}(X^n - a))$. Então*

(i) *$\mathbb{L}/\mathbb{F}$ é galoisiana finita, e $\mathbb{L} = \mathbb{F}(\xi, \alpha)$, para qualquer $\alpha \in \mathscr{R}(X^n - a)$,*
(ii) *$\operatorname{Aut}(\mathbb{L}/\mathbb{F}(\xi))$ é cíclico, e sua ordem divide n,*
(iii) *$\mathbb{F}(\xi)/\mathbb{F}$ é galoisiana finita, e $\operatorname{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ é abeliano.*

Portanto, $\operatorname{Aut}(\mathbb{L}/\mathbb{F})$ é solúvel.

Demonstração. O corpo $\mathbb{E} = \mathbb{F}(\xi)$ é tal que $\mathcal{P}_n(\mathbb{E}) \neq \emptyset$. Portanto, (i) e (ii) seguem do teorema anterior. O item (iii) foi provado no Teorema 11.9. A conclusão final segue da correspondência de Galois (Teorema 8.6.(3)). □

Para provar a recíproca do Teorema 12.3, precisaremos do seguinte:

Teorema 12.5 (Artin)**.** *Seja S um grupo e $\sigma_1, \ldots, \sigma_m$ homomorfismos $S \to \mathbb{F}^\times$ dois a dois distintos. Então $\{\sigma_1, \ldots, \sigma_m\}$ é um conjunto $\mathbb{F}$-linearmente independente.*

Demonstração. Provaremos por indução em m, em que a base $m = 1$ é imediata. Sejam $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$ e considere a combinação linear $\alpha_1\sigma_1 + \cdots + \alpha_m\sigma_m = 0$. Portanto,

$$\alpha_1\sigma_1(a) + \cdots + \alpha_m\sigma_m(a) = 0, \quad \forall a \in S. \tag{12.2}$$

Como $\sigma_1 \neq \sigma_m$, existe $b \in S$ tal que $\sigma_1(b) \neq \sigma_m(b)$. Assim, por (12.2), temos que

$$0 = \alpha_1\sigma_1(ba) + \cdots + \alpha_m\sigma_m(ba) = \alpha_1\sigma_1(b)\sigma_1(a) + \cdots + \alpha_m\sigma_m(b)\sigma_m(a), \quad \forall a \in S$$

Multiplicando (12.2) por $\sigma_m(b)$ e subtraindo da equação acima, obtemos que

$$0 = \alpha_1(\sigma_1(b) - \sigma_m(b))\sigma_1(a) + \cdots + \alpha_{m-1}(\sigma_{m-1}(b) - \sigma_m(b))\sigma_{m-1}(a), \quad \forall a \in S$$

Isso implica que

$$\alpha_1(\sigma_1(b) - \sigma_m(b))\sigma_1 + \cdots + \alpha_{m-1}(\sigma_{m-1}(b) - \sigma_m(b))\sigma_{m-1} = 0,$$

em que cada $\alpha_i(\sigma_i(b) - \sigma_m(b)) \in \mathbb{F}$. Pela hipótese de indução, $\{\sigma_1, \ldots, \sigma_{m-1}\}$ é um conjunto $\mathbb{F}$-linearmente independente. Portanto, $\alpha_i(\sigma_i(b) - \sigma_m(b)) = 0$, para todo i. Como $\sigma_1(b) - \sigma_m(b) \neq 0$, temos que $\alpha_1 = 0$. Portanto, a hipótese de indução implica que $\alpha_2 = \cdots = \alpha_m = 0$. Daí, $\{\sigma_1, \ldots, \sigma_m\}$ é $\mathbb{F}$-linearmente independente. □

Corolário 12.6 (Dedekind)**.** *Sejam $\sigma_1, \ldots, \sigma_m \in \mathrm{Aut}(\mathbb{F})$ dois a dois distintos. Então $\{\sigma_1, \ldots, \sigma_m\}$ é um conjunto $\mathbb{F}$-linearmente independente.* □

Teorema 12.7 (90 de Hilbert)**.** *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita de corpos tal que $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$ é cíclica. Seja $a \in \mathbb{E}$.*

(i) *$\mathscr{N}_{\mathbb{E}/\mathbb{F}}(a) = 1$ se, e somente se, existe $b \in \mathbb{E}$ tal que $a = b/\sigma(b)$.*
(ii) *$\mathrm{tr}_{\mathbb{E}/\mathbb{F}}\, a = 0$ se, e só se, existe $b \in \mathbb{E}$ tal que $a = b - \sigma(b)$.*

Demonstração. ($\Leftarrow$) Como $\sigma(b)$ e b possuem o mesmo polinômio minimal, segue que $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(b) = \mathrm{tr}_{\mathbb{E}/\mathbb{F}}(\sigma(b))$ e $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(b) = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(\sigma(b))$. Portanto, vale a volta.
(i)($\Rightarrow$): Seja $a \in \mathbb{E}$ tal que $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(a) = 1$. Do Teorema de Dedekind, $\sigma^0, \sigma^1, \ldots, \sigma^{m-1}$ são $\mathbb{E}$-linearmente independentes. Então, existe $c \in \mathbb{E}$ tal que

$$b := c + a\sigma(c) + (a\sigma(a))\sigma^2(c) + \cdots + (a\sigma(a)\cdots\sigma^{n-2}(a))\sigma^{n-1}(c) \neq 0.$$

Note que $\sigma(b) = b/a$, pois $1 = \mathscr{N}_{\mathbb{E}/\mathbb{F}}(a) = a\sigma(a)\cdots\sigma^{n-1}(a)$ e $\sigma^n = \mathrm{id}$. Portanto, $a = b/\sigma(b)$.
(ii)($\Rightarrow$): Pelo Teorema de Dedekind, existe $c \in \mathbb{E}$ tal que

$$0 \neq \sigma^0(c) + \sigma(c) + \cdots + \sigma^{n-1}(c) = \mathrm{tr}_{\mathbb{E}/\mathbb{F}}(c).$$

Seja

$$b := \frac{1}{\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(c)}\left(a\sigma(c) + (a + \sigma(a))\sigma^2(c) + \cdots + (a + \sigma(a) + \cdots + \sigma^{n-2}(a))\sigma^n(c)\right).$$

Note que $\sigma(b) = b - a$, pois $\sigma^n = \mathrm{Id}$ e $\mathrm{tr}_{\mathbb{E}/\mathbb{F}}(a) = a + \sigma(a) + \cdots + \sigma^{n-1}(a) = 0$. Portanto, $b - \sigma(b) = a$. □

Teorema 12.8. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana de grau n, $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$, e assuma que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Então, existe $a \in \mathbb{F}^\times$ tal que $X^n - a$ é irredutível em $\mathbb{F}[X]$ e $\mathbb{E} = \mathbb{F}(\mathscr{R}(X^n - a))$. Além disso, $\mathbb{E} = \mathbb{F}(\alpha)$, $\forall\alpha \in \mathscr{R}(X^n - a)$.*

Demonstração. Seja $\xi \in \mathcal{P}_n(\mathbb{F})$. Então $\mathscr{N}_{\mathbb{E}/\mathbb{F}}(\xi) = 1$. Do Teorema 90 de Hilbert, existe $\alpha \in \mathbb{E}$ tal que $\xi = \alpha/\sigma(\alpha)$. Portanto, $\sigma^j(\alpha) = \xi^{-j}\alpha$, para cada j. Segue que $\alpha, \xi^{-1}\alpha, \ldots, \xi^{n-1}\alpha$ são raízes distintas de $\operatorname{Irr}(\alpha, \mathbb{F})$. Daí, $n \leq \operatorname{gr}\operatorname{Irr}(\alpha, \mathbb{F}) \leq [\mathbb{E} : \mathbb{F}] = n$. Portanto, vale a igualdade. Por fim, $\sigma\alpha^n = \alpha^n$. Portanto, $a := \alpha^n \in \mathbb{E}^{\langle\sigma\rangle} = \mathbb{F}$. Agora, α é raiz de $X^n - a$, e $\operatorname{gr}(X^n - a) = n = \operatorname{gr}(\operatorname{Irr}(\alpha, \mathbb{F}))$. Segue que $X^n - a = \operatorname{Irr}(\alpha, \mathbb{F})$ é um polinômio irredutível.

As últimas consequências seguem dos fatos de que $\mathscr{R}(X^n - a) = \{\xi^j\alpha \mid j = 0, \ldots, n-1\} \subseteq \mathbb{E}$, e $[\mathbb{F}(\alpha) : \mathbb{F}] = \operatorname{gr}\operatorname{Irr}(\alpha, \mathbb{F}) = [\mathbb{E} : \mathbb{F}]$. □

Assim, temos uma caracterização de extensões cíclicas de grau n de um corpo $\mathbb{F}$, desde que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Portanto, excluímos o caso em que $\operatorname{car}\mathbb{F} = p > 0$ e p divide n.

Então, até o fim desta subseção, vamos direcionar os nossos estudos para o caso faltante. A conclusão será que, essencialmente, o polinômio $X^p - X - a$ terá as propriedades que queremos, e por isso, será um substituto do polinômio $X^p - a$.

Vamos estudarmos as extensões cíclicas de grau p, em que $\operatorname{car}\mathbb{F} = p > 0$. Da caracterização de grupos solúveis finitos (veja abaixo), seguirá que esse caso é suficiente para os nossos propósitos.

Neste sentido, temos o seguinte:

Teorema 12.9 (Artin-Schreier)**.** *Seja* $\operatorname{car}\mathbb{F} = p > 0$. *Para todo* $a \in \mathbb{F}$, *o polinômio* $f = X^p - X - a$ *é separável e* $\mathscr{R}(f) = \{\alpha, \alpha + 1, \ldots, \alpha + p - 1\}$, *para qualquer* $\alpha \in \mathscr{R}(f)$. *Além disso, as seguintes afirmações são equivalentes:*

(i) f *é irredutível em* $\mathbb{F}[X]$,
(ii) $a \notin \{b^p - b \mid b \in \mathbb{F}\}$,
(iii) $\mathscr{R}(f) \cap \mathbb{F} = \emptyset$.

Nestas condições, seja $\mathbb{E} = \mathbb{F}(\mathscr{R}(f))$. *Então* $\mathbb{E}/\mathbb{F}$ *é uma extensão galoisiana de grau* p, *e* $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ *é cíclico de ordem* p. *Além disso,* $\mathbb{E} = \mathbb{F}(\alpha)$, $\forall \alpha \in \mathscr{R}(f)$.

Demonstração. Assuma que $\alpha \in \mathscr{R}(f)$. Então, para qualquer $i \in \{0, 1, \ldots, p-1\}$, temos que

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) - a = \alpha^p + i^p - \alpha - i - a = f(\alpha) + i - i = 0.$$

Portanto, $\{\alpha, \alpha + 1, \ldots, \alpha + p - 1\} \subseteq \mathscr{R}(f)$. Como f possui grau p, segue que os dois conjuntos coincidem. Em particular, f é separável.
$(i) \Rightarrow (ii)$: se $a = b^p - b$, para algum $b \in \mathbb{F}$, então $f(b) = b^p - b - a = 0$. Portanto, f não é irredutível em $\mathbb{F}[X]$.
$(ii) \Rightarrow (iii)$: Se existe $b \in \mathscr{R}(f) \cap \mathbb{F}$, então $0 = f(b) = b^p - b - a$. Portanto, $a = b^p - b$ está no conjunto definido em (ii).
$(iii) \Rightarrow (i)$: Assuma que $f = gh$, com $g \in \mathbb{F}[X]$ mônico e $1 \leq \operatorname{gr}(g) < p$. Escreva $g(X) = X^q + b_{q-1}X^{q-1} + \cdots + b_1X + b_0$. Então, existem $1 \leq j_1 < j_2 < \cdots < j_q \leq p - 1$ tais que $g(X) = (X - \alpha - j_1)\cdots(X - \alpha - j_q)$. Portanto, $b_{q-1} = -\sum_{\ell=1}^{q}(\alpha + j_\ell) = -q\alpha - r \in \mathbb{F}$. Daí, $\alpha = -q^{-1}(b_{q-1} + r) \in \mathbb{F} \cap \mathscr{R}(f)$.

Para finalizar, da caracterização de $\mathscr{R}(f)$, segue que $\mathbb{E} = \mathbb{F}(\alpha)$ para qualquer $\alpha \in \mathscr{R}(f)$. Da Proposição 3.6, temos que $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) = \{\sigma_0, \sigma_1, \ldots, \sigma_{p-1}\}$, em que $\sigma_i(\alpha) = \alpha + i$. Além disso, note que $\sigma_0 = \operatorname{Id}_{\mathbb{E}}$ e $\sigma_i = \sigma_1^i$. Portanto, $\operatorname{Aut}(\mathbb{E}/\mathbb{F})$ é cíclico, e gerado por σ_1. □

A recíproca do Teorema 12.3, na situação em que grau da extensão coincide com a característica do corpo, pode ser enunciada da seguinte forma:

Teorema 12.10. *Seja* $\operatorname{car}\mathbb{F} = p > 0$*, e assuma que* $\mathbb{E}/\mathbb{F}$ *é uma extensão cíclica de grau* p*. Denote* $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$*. Então, existe* $a \in \mathbb{F}$ *tal que* $f = X^p - X - a$ *é irredutível em* $\mathbb{F}[X]$ *e* $\mathbb{E} = \mathbb{F}(\mathscr{R}(f))$*. Neste caso,* $\mathbb{E} = \mathbb{F}(\alpha)$*,* $\forall \alpha \in \mathscr{R}(f)$*.*

Demonstração. Temos que $\operatorname{tr}_{\mathbb{E}/\mathbb{F}}(-1) = p(-1) = 0$. Portanto, do Teorema 90 de Hilbert, existe $\alpha \in \mathbb{E}$ tal que $-1 = \alpha - \sigma(\alpha)$. Ou seja, $\sigma(\alpha) = \alpha + 1$. Daí $\sigma^j(\alpha) = \alpha + j$, para cada j. Os elementos $\alpha, \alpha+1, \ldots, \alpha+p-1$ são dois a dois distintos, e são raízes de $\operatorname{Irr}(\alpha, \mathbb{F})$. Portanto,

$$n \leq \operatorname{gr}(\operatorname{Irr}(\alpha, \mathbb{F})) \leq [\mathbb{E} : \mathbb{F}] = n.$$

Segue que $\operatorname{gr}(\operatorname{Irr}(\alpha, \mathbb{F})) = n$. Seja $a = \alpha(\alpha+1)\cdots(\alpha+p-1) = \prod_{j=0}^{n-1} \sigma^j(\alpha)$. Então, $\sigma(a) = a$. Daí $a \in \mathbb{E}^{\langle\sigma\rangle} = \mathbb{F}$. Segue que

$$\operatorname{Irr}(\alpha, \mathbb{F}) = \prod_{i=0}^{p-1} (X - \alpha - i) = X^p - X - a \in \mathbb{F}[X],$$

e portanto, $X^p - X - a$ é irredutível. As demais conclusões seguem do Teorema de Artin-Schreier. □

12.3. **Revisão: Grupos solúveis.** Nesta subseção vamos relembrar a definição e algumas propriedades envolvendo grupos solúveis. Enunciaremos os resultados sem prová-los.

Definição 12.11. Seja G um grupo. Então G é *solúvel* se existe uma sequência de subgrupos

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = 1,$$

tal que, para todo $i = 1, \ldots, m$, $G_i \lhd G_{i-1}$ (ou seja, G_i é um subgrupo normal de G_{i-1}), e G_{i-1}/G_i é abeliano.

Teorema 12.12. *Seja* G *um grupo finito. Então* G *é solúvel se, e somente se, existe uma sequência de subgrupos*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = 1,$$

tal que, para todo $i = 1, \ldots, m$*,* $G_i \lhd G_{i-1}$*, e* G_{i-1}/G_i *é cíclico de ordem prima.*

Teorema 12.13. *Sejam* G *um grupo e* $H \subseteq G$ *um subgrupo.*

(i) *Se* G *é solúvel, então* H *é solúvel.*
(ii) *Assuma que* H *é normal. Então* G *é solúvel se, e somente se,* H *e* G/H *são solúveis.*

Teorema 12.14. *Para* $n \geq 5$*, o grupo simétrico* $\mathcal{S}_n$ *não é solúvel.*

12.4. **Solubilidade via radicais em característica zero.** Vamos descrever formalmente o significado de ser possível caracterizar as raízes de um polinômio via operações do corpo e "extração de raízes".

Definição 12.15. Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos de característica zero. Dizemos que a extensão $\mathbb{E}/\mathbb{F}$ é *radical* se existe uma sequência de subcorpos

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{E}$$

satisfazendo a seguinte condição. Para cada $i = 0, 1, \ldots, m-1$, $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$, para algum $d_i \in \mathbb{F}_{i+1}$ tal que existe $n_i \in \mathbb{N}$ com $d_i^{n_i} \in \mathbb{F}_i$.

Definição 12.16. Seja $f \in \mathbb{F}[X]$ um polinômio separável. Dizemos que f é *solúvel por radicais* se existe uma extensão radical $\mathbb{E}/\mathbb{F}$ tal que $\mathbb{E} \supseteq \mathscr{R}(f)$.

A seguir, vamos definir o grupo de Galois de um polinômio separável:

Definição 12.17. Seja $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio separável. O *Grupo de Galois* do polinômio f é o grupo $G_f = \mathrm{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F})$.

O resultado principal desta subseção é o seguinte:

Teorema 12.18. *Seja $\mathbb{F}$ um corpo de característica zero e $f \in \mathbb{F}[X]$ um polinômio separável. Então f é solúvel por radicais se, e somente se, o grupo de Galois G_f é solúvel.*

Antes de demonstrarmos o tal teorema, precisaremos dos seguintes resultados:

Lema 12.19. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão separável finita e radical. Então existe uma extensão $\mathbb{L}/\mathbb{E}$ tal que $\mathbb{L}/\mathbb{F}$ é galoisiana finita e radical.*

Demonstração. Do Teorema do Elemento Primitivo (Corolário 7.15.(i)), existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$. Seja $\mathbb{L} = \mathbb{F}(\mathrm{Irr}(a, \mathbb{F}))$. Então $\mathbb{L}/\mathbb{F}$ é galoisiana finita, e $\mathbb{L}$ é uma extensão de $\mathbb{E}$ ($\mathbb{L}$ é o fecho normal da extensão $\mathbb{E}/\mathbb{F}$).

Da definição de extensão radical, denote

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \mathbb{F}_m = \mathbb{E},$$

e sejam $d_i \in \mathbb{E}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$, com $d_i^{n_i} \in \mathbb{F}_i$. Denote $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) = \{\sigma_1, \ldots, \sigma_s\}$, e assuma que $\sigma_1 = \mathrm{Id}_{\mathbb{L}}$. Defina indutivamente:

$$\mathbb{E}_0 = \mathbb{E},$$
$$\mathbb{E}_j = \sigma_j(\mathbb{E}) \cdot \mathbb{E}_{j-1}, \quad j \geq 1.$$

Note que $\mathscr{R}(\mathrm{Irr}(a, \mathbb{F})) \subseteq \mathbb{E}_s$. Portanto, $\mathbb{E}_s = \mathbb{L}$. Ainda, por construção, temos que

$$\mathbb{F} \subseteq \mathbb{E}_0 \subseteq \mathbb{E}_1 \subseteq \cdots \subseteq \mathbb{E}_s = \mathbb{L}.$$

Note que, para $i \geq 1$, temos

$$\begin{aligned} \mathbb{E}_{i-1} \subseteq \mathbb{E}_{i-1}(\sigma_i(d_1)) \subseteq \cdots \subseteq \mathbb{E}_{i-1}(\sigma_i(d_1), \sigma_i(d_2), \ldots, \sigma_i(d_m)) \\ = \mathbb{E}_{i-1} \cdot \sigma_i(\mathbb{E}) = \mathbb{E}_i. \end{aligned} \tag{12.3}$$

Além disso, $\sigma_i(d_j)^{n_j} \in \sigma_i(\mathbb{F}_j) = \sigma_i(\mathbb{F}(d_1, \ldots, d_{j-1})) \subseteq \mathbb{E}_{i-1}(\sigma_i(d_1), \ldots, \sigma_i(d_{j-1}))$. Portanto, a extensão $\mathbb{E}_i/\mathbb{E}_{i-1}$ é radical. Concatenando as torres dadas por (12.3), para cada $i = 1, \ldots, s$, e a torre de $\mathbb{E}/\mathbb{F}$, obtemos que $\mathbb{L}/\mathbb{F}$ é radical. □

Lema 12.20. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita e solúvel de grau n. Assuma que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Então $\mathbb{E}/\mathbb{F}$ é uma extensão radical.*

Demonstração. Como $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel e finito, existe uma sequência de subgrupos

$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m = \{1\}$$

tal que $H_i \triangleleft H_{i-1}$ e H_{i-1}/H_i é cíclico de ordem prima. Da correspondência de Galois, obtemos sequência de corpos

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{E},$$

em que $\mathbb{F}_i = \mathbb{E}^{H_i}$. Como $\mathrm{Aut}(\mathbb{E}/\mathbb{F}_i) = H_i \triangleleft H_{i-1} = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_{i-1})$, temos que $\mathbb{F}_i/\mathbb{F}_{i-1}$ é galoisiana finita. Ainda, $\mathrm{Aut}(\mathbb{F}_i/\mathbb{F}_{i-1}) \cong H_{i-1}/H_i$ é cíclico de ordem prima p. Como $\emptyset \neq \mathcal{P}_n(\mathbb{F}) \subseteq \mathcal{P}_n(\mathbb{F}_{i-1})$ e p divide n, segue que $\mathcal{P}_p(\mathbb{F}_{i-1}) \neq \emptyset$. Portanto, do

Teorema 12.8, segue que existe $d_{i-1} \in \mathbb{F}_i$ tal que $\mathbb{F}_i = \mathbb{F}_{i-1}(d_{i-1})$, e $d_{i-1}^{n_{i-1}} \in \mathbb{F}_{i-1}$. Assim, $\mathbb{E}/\mathbb{F}$ é radical. □

Lema 12.21. *Seja $\mathbb{E}/\mathbb{F}$ galoisiana finita e radical, e escreva*

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{E}.$$

Sejam $d_i \in \mathbb{E}$ e $n_i \in \mathbb{N}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$. Seja $n = \text{mmc}(n_1, \ldots, n_m)$, e assuma que $\mathcal{P}_n(\mathbb{F}) \neq \emptyset$. Então $\text{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel.

Demonstração. Da correspondência de Galois, temos

$$\text{Aut}(\mathbb{E}/\mathbb{F}) = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\},$$

em que $H_i = \text{Aut}(\mathbb{E}/\mathbb{F}_i)$. Como n_i divide n, segue que $\mathcal{P}_{n_i}(\mathbb{F}_i) = \mathcal{P}_{n_i}(\mathbb{F}) \neq \emptyset$. Portanto, do Teorema 12.3, temos que $\mathbb{F}_{i+1} = \mathbb{F}_i(\mathscr{R}(X^{n_i} - d_i^{n_i}))$, $\mathbb{F}_{i+1}/\mathbb{F}_i$ é galoisiana finita e $\text{Aut}(\mathbb{F}_{i+1}/\mathbb{F}_i)$ é cíclica. Portanto, da correspondência de Galois, segue que $H_{i+1} \lhd H_i$ e $H_i/H_{i+1} \cong \text{Aut}(\mathbb{F}_{i+1}/\mathbb{F}_i)$ é abeliana (de fato, é cíclica). Portanto, $\text{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel. □

Agora temos todos os passos para demonstrarmos o Teorema 12.18.

Demonstração do Teorema 12.18. Assuma que $G_f = \text{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F})$ é solúvel. Sejam $\bar{\mathbb{F}}$ um fecho algébrico de $\mathbb{F}$, $n = [\mathbb{F}(\mathscr{R}(f)) : \mathbb{F}]$, $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$ e $\mathbb{E} = \mathbb{F}[\xi]$. Da Proposição 9.3, temos que

$$\text{Aut}(\mathbb{E}(\mathscr{R}(f))/\mathbb{E}) \cong \text{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{E} \cap \mathbb{F}(\mathscr{R}(f))) \subseteq \text{Aut}(\mathbb{F}(\mathscr{R}(f))/\mathbb{F}).$$

Portanto, $\text{Aut}(\mathbb{E}(\mathscr{R}(f))/\mathbb{E})$ é solúvel. Do Lema 12.20, temos que $\mathbb{E}(\mathscr{R}(f))/\mathbb{E}$ é radical. Como $\mathbb{E} = \mathbb{F}(\xi)$ e $\xi^n \in \mathbb{F}$, segue que $\mathbb{E}(\mathscr{R}(f))/\mathbb{F}$ é radical. Portanto, f é solúvel via radicais.

Reciprocamente, assuma que f é solúvel via radicais. Então, existe $\mathbb{E}/\mathbb{F}$ finita e radical tal que $\mathscr{R}(f) \subseteq \mathbb{E}$. Do Lema 12.19, existe uma extensão $\mathbb{L}/\mathbb{E}$ tal que $\mathbb{L}/\mathbb{F}$ é galoisiana finita e radical. Da definição de extensão radical, escreva

$$\mathbb{F} = \mathbb{F}_0 \subseteq \mathbb{F}_1 \subseteq \cdots \subseteq \mathbb{F}_m = \mathbb{L},$$

e sejam $d_i \in \mathbb{L}$ e $n_i \in \mathbb{N}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$. Sejam $n = \text{mmc}(n_1, \ldots, n_m)$, $\bar{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$, e $\xi \in \mathcal{P}_n(\bar{\mathbb{F}})$. A extensão $\mathbb{L}(\xi)/\mathbb{F}(\xi)$ é radical, pois a torre seguinte satisfaz a definição:

$$\mathbb{F}(\xi) = \mathbb{F}_0(\xi) \subseteq \mathbb{F}_1(\xi) \subseteq \cdots \subseteq \mathbb{F}_m(\xi) = \mathbb{L}(\xi).$$

Então, segue do Lema 12.21, que $\text{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\xi))$ é solúvel. Por Teorema 11.9, $\mathbb{F}(\xi)/\mathbb{F}$ é galoisiana e $\text{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ é abeliano (e, portanto, solúvel). Daí, da correspondência de galois (Teorema 8.6.(3)), $\text{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong \text{Aut}(\mathbb{L}(\xi)/\mathbb{F})/\text{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\xi))$. Assim, $\text{Aut}(\mathbb{L}(\xi)/\mathbb{F})$ é solúvel (Teorema 12.13.(ii)).

Por fim, como $G_f \cong \text{Aut}(\mathbb{L}(\xi)/\mathbb{F})/\text{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\mathscr{R}(f)))$, segue que G_f é solúvel. □