Relembre:

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,* $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ *é isomorfo a um subgrupo de* $W_n(\mathbb{F})$.

Em particular, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é cíclico.

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

Teorema 8.6 (Teorema Fundamental da Teoria de Galois). *Seja* $\mathbb{E}/\mathbb{F}$ *uma extensão galoisiana finita. Denote por* $\mathcal{G}$ *o conjunto dos subgrpos de* $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, *e* $\mathcal{K}$ *o conjunto dos corpos* $\mathbb{K}$, *com* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$. *Então, os mapas* $\mathbb{K} \in \mathcal{K} \mapsto \mathrm{Aut}(\mathbb{E}/\mathbb{K}) \in \mathcal{G}$ *e* $H \in \mathcal{G} \mapsto \mathbb{E}^H \in \mathcal{K}$ *são inversas uma da outra. Além disso:*

(3) *Se* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$, *então* $\mathbb{K}/\mathbb{F}$ *é normal se, e somente se,* $\mathrm{Aut}(\mathbb{E}/\mathbb{K})$ *é um subgrupo normal de* $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$. *Neste caso,* $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{E}/\mathbb{F})/\mathrm{Aut}(\mathbb{E}/\mathbb{K})$.

Solubilidade via Radicais

Def. Seja $\mathbb{F}$ um corpo de característica zero. Uma extensão de corpos $\mathbb{E}/\mathbb{F}$ é dita ser radical se existe uma sequência de subcorpos

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

tal que, $\forall i = 0, 1, \dots, m-1$, existem $d_i \in \mathbb{F}_{i+1}$ e $n_i \in \mathbb{N}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$.

Def. Seja $f \in \mathbb{F}[X]$. Dizemos que f é solúvel por radicais se existe uma extensão de corpos radical $\mathbb{E}/\mathbb{F}$ tal que $\mathcal{R}(f) \subseteq \mathbb{E}$.

Def. Seja $f \in \mathbb{F}[X]$ separável. Definimos o grupo de Galois de f por $G_f = \mathrm{Aut}(\mathbb{F}(\mathcal{R}(f))/\mathbb{F})$.

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

Dem.: Pelo Teorema do Elemento Primitivo, existe $a \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(a)$. Seja $\mathbb{L} = \mathbb{F}(\mathcal{R}(\mathrm{Irr}(a, \mathbb{F})))$

$\mathbb{E}/\mathbb{F}$ é separável $\Rightarrow$ a é separável $\Rightarrow$ $\mathrm{Irr}(a, \mathbb{F})$ é sep.

$\Rightarrow \mathbb{L}/\mathbb{F}$ é galoisiana finita...

Denote $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) = \{\sigma_1, \dots, \sigma_s\}$. Então, como

$$\mathcal{R}(\mathrm{Irr}(a, \mathbb{F})) \subseteq \sigma_1(\mathbb{E}) \cdot \dots \cdot \sigma_s(\mathbb{E}) \subseteq \mathbb{L}$$

$$\Rightarrow \mathbb{L} = \sigma_1(\mathbb{E}) \cdot \dots \cdot \sigma_s(\mathbb{E}).$$

Sendo $\mathbb{E}/\mathbb{F}$ radical, podemos escrever

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

Sejam $d_i \in \mathbb{F}_{i+1}$, com $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$. Defina, para cada $j = 1, \dots, s$, o corpo

$$\mathbb{E}_j = \mathbb{E} \cdot \sigma_1(\mathbb{E}) \cdot \dots \cdot \sigma_j(\mathbb{E}).$$

Temos que

$$(*) \quad \mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{E}_1 \subseteq \dots \subseteq \mathbb{E}_s = \mathbb{L}.$$

Ainda, para cada $j = 0, \dots, s-1$, temos que (em que $\mathbb{E}_0 := \mathbb{E}$).

$$(**) \quad \mathbb{E}_j \subseteq \mathbb{E}_j(\sigma_{j+1}(d_1)) \subseteq \mathbb{E}_j(\sigma_{j+1}(d_1), \sigma_{j+1}(d_2)) \subseteq \dots \subseteq \mathbb{E}_j(\sigma_{j+1}(d_1), \dots, \sigma_{j+1}(d_m))$$

$$= \mathbb{E}_j \cdot \sigma_{j+1}(\mathbb{E}) = \mathbb{E}_{j+1},$$

além disso

$$\sigma_{j+1}(d_\ell)^{n_\ell} \in \sigma_{j+1}(\mathbb{F}_\ell) = \sigma_{j+1}(\mathbb{F}(d_1, \dots, d_{\ell-1})) \subseteq \mathbb{E}_j(\sigma_{j+1}(d_1), \dots, \sigma_{j+1}(d_{\ell-1})).$$

Portanto, concatenando as sequências $(**)$ em $(*)$, obtemos que $\mathbb{L}/\mathbb{F}$ é radical. $\square$

Lema. Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita de grau n. Assuma que $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel, e $P_n(\mathbb{F}) \neq \emptyset$. Então $\mathbb{E}/\mathbb{F}$ é radical.

Dem.: Existe sequência

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

tal que $H_{i+1} \triangleleft H_i$ e H_i/H_{i+1} é cíclico de ordem p.

Assim, temos

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

em que $\mathbb{F}_i = \mathbb{E}^{H_i}$. Além disso,

$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}_{i+1}) = H_{i+1} \triangleleft H_i = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_i).$$

Portanto, $\mathbb{F}_{i+1}/\mathbb{F}_i$ é galoisiana finita. Ainda,

$$\mathrm{Aut}(\mathbb{F}_{i+1}/\mathbb{F}_i) \cong H_{i+1}/H_i \text{ é cíclico.}$$

Como $p \mid |\mathrm{Aut}(\mathbb{E}/\mathbb{F})| = n$, então $P_p(\mathbb{F}_i) \neq \emptyset$. Daí, existe $d_i \in \mathbb{F}_{i+1}$ tal que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^p \in \mathbb{F}_i$.

Segue que $\mathbb{E}/\mathbb{F}$ é radical. $\square$

Lema. 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 $n_i \in \mathbb{N}$ com $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$.

Seja $n = n_1 \cdots n_m$ e assuma que $P_n(\mathbb{F}) \neq \emptyset$. Então $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel.

Dem.: Existe sequência
$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_m = \{1\}.$$
tal que $H_i = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_i)$. Fixe i. Então, n_i divide n. Portanto $\emptyset \neq P_{n_i}(\mathbb{F}) = P_{n_i}(\mathbb{F}_i)$. Ainda, $\mathbb{F}_{i+1} = \mathbb{F}_i(\mathcal{R}(X^{n_i} - d_i^{n_i}))$. Assim, $\mathbb{F}_{i+1}/\mathbb{F}_i$ é galoisiana finita cíclica. Portanto,
$$H_{i+1} = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_{i+1}) \lhd \mathrm{Aut}(\mathbb{E}/\mathbb{F}_i) = H_i.$$
Além disso, $H_i/_{H_{i+1}} = \mathrm{Aut}(\mathbb{E}/\mathbb{F}_i)/\mathrm{Aut}(\mathbb{E}/\mathbb{F}_{i+1}) \cong \mathrm{Aut}(\mathbb{F}_{i+1}/\mathbb{F}_i)$ é cíclico (em particular, abeliano). Assim, $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é solúvel. $\square$

Teorema. Sejam $\mathbb{F}$ um corpo de característica zero e $f \in \mathbb{F}[X]$ separável. Então f é solúvel por radicais se, e somente se, G_f é solúvel.

Dem.: Assuma que f é solúvel por radicais. Então, existe $\mathbb{F}/\mathbb{F}$ radical e finita tal que $\mathcal{R}(f) \subseteq \mathbb{E}$. Existe $\mathbb{L}/\mathbb{E}$ tal que $\mathbb{L}/\mathbb{F}$ é radical e galoisiana finita. Sejam
$$\mathbb{F} = \mathbb{F}_0 \subseteq \ldots \subseteq \mathbb{F}_m = \mathbb{L},$$
e $d_i \in \mathbb{L}$, $n_i \in \mathbb{N}$ tais que $\mathbb{F}_{i+1} = \mathbb{F}_i(d_i)$ e $d_i^{n_i} \in \mathbb{F}_i$.
Sejam $n = n_1 \ldots n_m$, $\overline{\mathbb{F}}$ um fecho algébrico de $\mathbb{F}$ e $\xi \in P_n(\overline{\mathbb{F}})$. Temos que $\mathbb{L}(\xi)/\mathbb{F}(\xi)$ é radical, pois
$$\mathbb{F}(\xi) = \mathbb{F}_0(\xi) \subseteq \mathbb{F}_1(\xi) \subseteq \cdots \subseteq \mathbb{F}_m(\xi) = \mathbb{L}(\xi).$$

Além disso, $P_n(\mathbb{F}(\xi)) \neq \emptyset$. Portanto, $\mathrm{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\xi))$ é solúvel. Sabemos que $\mathbb{F}(\xi)/\mathbb{F}$ é galoisiana finita e abeliana. (isto é, $\mathrm{Aut}(\mathbb{F}(\xi)/\mathbb{F})$ é abeliano)
Além disso,

$$\mathrm{Aut}(\mathbb{F}(\xi)/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{L}(\xi)/\mathbb{F}) \big/ \mathrm{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\xi)).$$

Segue que $\mathrm{Aut}(\mathbb{L}(\xi)/\mathbb{F})$ é solúvel. Daí

$$G_f = \mathrm{Aut}(\mathbb{F}(\mathcal{R}(f))/\mathbb{F}) \cong \mathrm{Aut}(\mathbb{L}(\xi)/\mathbb{F}) \big/ \mathrm{Aut}(\mathbb{L}(\xi)/\mathbb{F}(\mathcal{R}(f)))$$

e portanto, G_f é solúvel.

Reciprocamente, assuma que G_f é solúvel. Seja $\mu \in P_{|G_f|}(\mathbb{F})$. Então, seja $\mathbb{E} = \mathbb{F}(\mu)$. Temos que

$$\mathrm{Aut}(\mathbb{E}(\mathcal{R}(f))/\mathbb{E}) \cong \mathrm{Aut}(\mathbb{F}(\mathcal{R}(f))/\mathbb{E} \cap \mathbb{F}(\mathcal{R}(f))) \subseteq G_f$$

Daí $\mathrm{Aut}(\mathbb{E}(\mathcal{R}(f))/\mathbb{E})$ é solúvel. Como $P_{|G_f|}(\mathbb{E}) \neq \emptyset$, segue que $\mathbb{E}(\mathcal{R}(f))/\mathbb{E}$ é radical. Como $\mathbb{E} = \mathbb{F}(\mu)$ e $\mu^{|G_f|} \in \mathbb{F}$, segue que $\mathbb{E}(\mathcal{R}(f))/\mathbb{F}$ é radical. Portanto, f é solúvel por radicais. $\square$