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 $\mathrm{Irr}(a, \mathbb{F})$ (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 $\mathrm{Irr}(a, \mathbb{F})$,*
(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 $\mathrm{Im}\,\sigma = \mathbb{L}$ (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.*

$\sigma \in \mathrm{Mono}_{\mathbb{F}}(\mathbb{L}, \Omega) \Rightarrow \sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$

Extensão normal (parte II)

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ não é normal, pois $\mathbb{Q}(\sqrt[3]{2})$ não contém todas as raízes de X^3-2. Porém,

$$\mathbb{L} := \mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\,\xi, \sqrt[3]{2}\,\xi^2) \quad (\xi \neq \xi^3 = 1)$$

é tal que $\mathbb{L} \supseteq \mathbb{Q}(\sqrt[3]{2})$ e $\mathbb{L}/\mathbb{Q}$ é normal.

Def. Sejam $\mathbb{E}/\mathbb{F}$ uma extensão algébrica, e Ω um corpo algebricamente fechado contendo $\mathbb{E}$. O fecho normal da extensão $\mathbb{E}/\mathbb{F}$ (em Ω) é o menor corpo $\mathbb{L}$, com $\mathbb{E} \subseteq \mathbb{L} \subseteq \Omega$, tal que $\mathbb{L}/\mathbb{F}$ é normal. Denota-se $\mathbb{L} = N_\Omega(\mathbb{E}/\mathbb{F})$.

Proposição. Sejam $\mathbb{E}/\mathbb{F}$ uma ext. algébrica, e Ω um corpo alg. fechado contendo $\mathbb{E}$. Seja

$$\mathcal{N} = \{\mathbb{K} \text{ corpo} \mid \mathbb{E} \subseteq \mathbb{K} \subseteq \Omega \text{ e } \mathbb{K}/\mathbb{F} \text{ é normal}\}$$

Então $\mathbb{L} := \bigcap_{\mathbb{K} \in \mathcal{N}} \mathbb{K}$ é corpo, e $\mathbb{L}/\mathbb{F}$ é normal.

Dem.: A família $\mathcal{N}$ é não vazia, pois $\Omega/\mathbb{F}$ é

uma extensão normal (justifique).

Seja $\mathbb{L} = \bigcap_{\mathbb{K} \in \mathcal{N}} \mathbb{K}$. Então $\mathbb{L}$ é corpo (justifique).

Sejam $a \in \mathbb{L}$, e p_a seu polinômio minimal sobre $\mathbb{F}$.

Então $a \in \mathbb{K}$, $\forall\, \mathbb{K} \in \mathcal{N}$. Como $\mathbb{K}/\mathbb{F}$ é normal, $R(p_a) \subseteq \mathbb{K}$ ($R(p_a) = \{\text{raízes de } p_a\}$). Portanto, $R(p_a) \subseteq \mathbb{L}$. Daí $\mathbb{L}/\mathbb{F}$ é uma extensão normal. □

Obs (1) Por construção, na notação da proposição anterior, $\mathbb{E} \subseteq \mathbb{L}$. Além disso, se $\mathbb{K} \supseteq \mathbb{E}$ é tal que $\mathbb{K}/\mathbb{F}$ é normal, então $\mathbb{L} \subseteq \mathbb{K}$ (pois $\mathbb{K} \in \mathcal{N}$). Daí

$$N_\Omega(\mathbb{E}/\mathbb{F}) = \mathbb{L}.$$

(2) Vale que $\mathbb{E} \subseteq N_\Omega(\mathbb{E}/\mathbb{F})$, e

$$N_\Omega\big(N_\Omega(\mathbb{E}/\mathbb{F})/\mathbb{F}\big) = N_\Omega(\mathbb{E}/\mathbb{F}).$$

Proposição. Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica.

(i) Seja $S = \{\mathrm{Irr}(a, \mathbb{F}) \mid a \in \mathbb{E}\}$. Então $N_\Omega(\mathbb{E}/\mathbb{F})$ coincide com o corpo de raízes de S sobre $\mathbb{F}$.

(ii) Se $\mathbb{E} = \mathbb{F}(a_1, \dots, a_m)$ é finita, seja $S = \{\mathrm{Irr}(a_1, \mathbb{F}), \dots, \mathrm{Irr}(a_m, \mathbb{F})\}$. Então $N_\Omega(\mathbb{E}/\mathbb{F})$ é o corpo de raízes de $S/\mathbb{F}$.

Dem.: (ii) Sejam $\mathbb{E} = \mathbb{F}(a_1, \dots, a_m)$ e S, como no enunciado. Seja $\mathbb{L} = \mathbb{F}(R(S))$ o corpo de raízes de S sobre $\mathbb{F}$. Por um lado, como $N_\Omega(\mathbb{E}/\mathbb{F})/\mathbb{F}$ é normal e $a_1, \dots, a_m \in \mathbb{E} \subseteq N_\Omega(\mathbb{E}/\mathbb{F})$, segue que $R(\mathrm{Irr}(a_i, \mathbb{F})) \subseteq N_\Omega(\mathbb{E}/\mathbb{F})$, $\forall i = 1, \dots, m$. Portanto, $\mathbb{F}(R(S)) \subseteq N_\Omega(\mathbb{E}/\mathbb{F})$. Por outro lado, $\mathbb{F}(R(S)) \supseteq a_1, \dots, a_m$. Daí $\mathbb{F}(R(S)) \supseteq \mathbb{E}$. Além disso, $\mathbb{F}(R(S))/\mathbb{F}$ é uma extensão normal. Daí, por definição, $N_\Omega(\mathbb{E}/\mathbb{F}) \subseteq \mathbb{F}(R(S))$. Portanto, $N_\Omega(\mathbb{E}/\mathbb{F})$ é o corpo de raízes de S sobre $\mathbb{F}$. □

Definição. Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos, e Ω um corpo contendo $\mathbb{E}$. Denota-se

$$\mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega) = \{\mathbb{F}\text{-monomorfismo } \mathbb{E} \to \Omega\},$$

$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \{\mathbb{F}\text{-automorfismo de } \mathbb{E}\}.$$

Obs. (1) $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, munido da composição de funções, é um grupo.

(2) Podemos ver $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \subseteq \mathrm{Mono}_{\mathbb{F}}(\mathbb{E}, \Omega)$, do seguinte modo: como $\mathbb{E} \subseteq \Omega$, temos

aplicação identidade $\mathbb{E} \longrightarrow \Omega$. Então, dado $\sigma \in Aut(\mathbb{E}/\mathbb{F})$, temos um $\mathbb{F}$-monomorfismo dado pela composição $\mathbb{E} \xrightarrow{\sigma} \mathbb{E} \longrightarrow \Omega$.

Reciprocamente, se $\psi \in Mono_{\mathbb{F}}(\mathbb{E}, \Omega)$ é tal que $Im\,\psi = \mathbb{E}$, então $\psi \in Aut(\mathbb{E}/\mathbb{F})$.

(3) É comum denotar $Gal(\mathbb{E}/\mathbb{F}) = Aut(\mathbb{E}/\mathbb{F})$, e denominam de o grupo de Galois de $\mathbb{E}/\mathbb{F}$.

Teorema. Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica. Então $\mathbb{E}/\mathbb{F}$ é normal se, e somente se, $Mono_{\mathbb{F}}(\mathbb{E}, \Omega) = Aut(\mathbb{E}/\mathbb{F})$. □

Teorema. Sejam $\mathbb{L}/\mathbb{F}$ uma extensão normal e $\mathbb{K}$ um corpo intermediário $(\mathbb{L}/\mathbb{K}/\mathbb{F})$. As afirmações seguintes são equivalentes:

(i) $\mathbb{K}/\mathbb{F}$ é normal,

(ii) $\sigma(\mathbb{K}) = \mathbb{K}$, $\forall \sigma \in Aut(\mathbb{L}/\mathbb{F})$.

Neste caso, temos homomorfismo de grupos dado por restrição:

$$Aut(\mathbb{L}/\mathbb{F}) \longrightarrow Aut(\mathbb{K}, \mathbb{F}).$$

Seu núcleo é $Aut(\mathbb{L}/\mathbb{K})$.

$\sigma \in Aut(\mathbb{L}/\mathbb{F})$

$\sigma|_{\mathbb{K}} \in Aut(\mathbb{K}, \mathbb{F})$

Dem.: (i) $\Rightarrow$ (ii). Seja $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F}) \subseteq \mathrm{Mono}_{\mathbb{F}}(\mathbb{L}, \Omega)$. Então, $\sigma|_{\mathbb{K}} : \mathbb{K} \to \Omega$ é um $\mathbb{F}$-monomorfismo. Como $\mathbb{K}/\mathbb{F}$ é normal, vale $\mathrm{Im}\,\sigma|_{\mathbb{K}} = \mathbb{K}$. Ou seja,

$$\sigma(\mathbb{K}) = \mathbb{K}.$$

(ii) $\Rightarrow$ (i). Seja $\sigma_0 : \mathbb{K} \to \Omega$ um $\mathbb{F}$-monomorfismo. Como $\mathbb{L}/\mathbb{K}$ é algébrica, existe $\sigma : \mathbb{L} \to \Omega$ que estende σ_0. Como $\mathbb{L}/\mathbb{F}$ é normal, segue que $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$. De (ii), vale que $\sigma(\mathbb{K}) = \mathbb{K}$. Mas σ é extensão de σ_0, e portanto,

$$\mathrm{Im}\,\sigma = \mathrm{Im}\,\sigma_0 = \mathbb{K}.$$

Então $\mathbb{K}/\mathbb{F}$ é normal.

Agora, via restrição, o mapa $\mathrm{Aut}(\mathbb{L}/\mathbb{F}) \to \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ está bem definido. Dado $\sigma_0 \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$, vimos que existe extensão $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$ tal que $\sigma|_{\mathbb{K}} = \sigma_0$. Portanto, tal mapa é sobrejetor. Seja $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$ tal que $\sigma|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. Daí $\sigma(a) = a$, $\forall a \in \mathbb{K}$. Ou seja, σ é um $\mathbb{K}$-automorfismo. Daí $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{K})$. □

Exemplos. (1) $Aut(\mathbb{F}/\mathbb{F}) = \{Id_{\mathbb{F}}\}$.

(2) $Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \sigma\}$, tal que

$$\sigma(a+b\sqrt{2}) = a - b\sqrt{2}.$$

De fato, existem dois $\mathbb{Q}$-monomorfismos

$$\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}.$$

(pois $X^2 - 2$ tem 2 raízes distintas). Como $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ é normal, vale que

$$Mono_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) = Aut(\mathbb{Q}(\sqrt{2})/\mathbb{Q}).$$

(3) $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{Id_{\mathbb{Q}(\sqrt[3]{2})}\}$

Isso porque temos três $\mathbb{Q}$-monomorfismos

$$\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}.$$

(que leva $\sqrt[3]{2}$ em $\sqrt[3]{2}$, $\sqrt[3]{2}\xi$, ou $\sqrt[3]{2}\xi^2$). Porém, a imagem de $\psi: \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ é tal que $Im\,\psi = \mathbb{Q}(\sqrt[3]{2})$ se e só se $\psi(\sqrt[3]{2}) = \sqrt[3]{2}$, se e só se $\psi = Id_{\mathbb{Q}(\sqrt[3]{2})}$

(6) Seja $\mathbb{E} = \mathbb{F}(u)$, de modo que $[\mathbb{E} : \mathbb{F}]$ é ímpar. Prove que $\mathbb{E} = \mathbb{F}(u^2)$.

A extensão $\mathbb{F}(u)/\mathbb{F}(u^2)$ tem grau no máximo 2. Pois u satisfaz um polinômio de grau 2 com coeficientes em $\mathbb{F}(u^2)$ (isso, pois $u^2 \in \mathbb{F}(u^2)$).

Então, temos o seguinte:

$$[\mathbb{F}(u) : \mathbb{F}] = [\mathbb{F}(u) : \mathbb{F}(u^2)] \, [\mathbb{F}(u^2) : \mathbb{F}].$$

Mas $[\mathbb{F}(u) : \mathbb{F}]$ é ímpar. Então $[\mathbb{F}(u) : \mathbb{F}(u^2)]$ não pode ser par. Daí $[\mathbb{F}(u) : \mathbb{F}(u^2)] = 1$

Portanto, $\mathbb{F}(u^2) = \mathbb{F}(u) = \mathbb{E}$. □

(17) Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos finita e seja $f \in \mathbb{F}[X]$ um polinômio irredutível sobre $\mathbb{F}$. Mostre que se $\text{mdc}([\mathbb{E} : \mathbb{F}], \text{gr}(f)) = 1$, então f é irredutível sobre $\mathbb{E}$.

Seja Ω um corpo algebricamente fechado contendo $\mathbb{E}$. Seja $g \in \mathbb{E}[X]$ irredutível que divide f. Seja $a \in \Omega$ raiz de g, então a também é raiz de f. O polinômio minimal de a sobre $\mathbb{F}$ é múltiplo escalar de f, e o pol. min. de a sobre $\mathbb{E}$ é multiplo escalar de g. Então $[\mathbb{F}(a) : \mathbb{F}] = \text{gr } f$, e $[\mathbb{E}(a) : \mathbb{E}] = \text{gr}(g)$.

Temos que $\mathbb{F}(a) \subseteq \mathbb{E}(a)$. Portanto

$[E(a):F] = [E(a):E][E:F] = [E(a):F(a)][F(a):F]$.

Isso significa que

$[F(a):F]$ divide $[E(a):E][E:F]$.

Mas $[F(a):F] = \operatorname{gr} f$ e $\operatorname{mdc}(\operatorname{gr} f, [E:F]) = 1$.

Daí $\operatorname{gr} f \mid [E(a):E] = \operatorname{gr}(g)$.

Por outro lado, g divide f. Portanto, $\operatorname{gr}(f) = \operatorname{gr}(g)$

Daí f é irredutível em $E[X]$. □

$f \in (g) \subseteq E[x]$

algébrico sobre $\mathbb{F}$

(2) Sejam $\mathbb{L}/\mathbb{E}/\mathbb{F}$ extensão de corpos e $a \in \mathbb{L}$. Prove que $\mathrm{Irr}(a,\mathbb{E})$ divide $\mathrm{Irr}(a,\mathbb{F})$.

Sejam $\psi_a : \mathbb{E}[X] \longrightarrow \mathbb{L}$ dado por $\psi_a(X) = a$. Então, $\ker \psi_a = (\mathrm{Irr}(a,\mathbb{E}))$. Além disso, $\mathrm{Irr}(a,\mathbb{F}) \in \mathbb{F}[X] \subseteq \mathbb{E}[X]$. Ainda

$$\psi_a(\mathrm{Irr}(a,\mathbb{F})) = \mathrm{Irr}(a,\mathbb{F})(a) = 0.$$

Portanto, $\mathrm{Irr}(a,\mathbb{F}) \in \ker \psi_a = (\mathrm{Irr}(a,\mathbb{E}))$.

Então $\mathrm{Irr}(a,\mathbb{F}) = g(X)\,\mathrm{Irr}(a,\mathbb{E})$, para algum $g(X) \in \mathbb{E}[X]$. Daí $\mathrm{Irr}(a,\mathbb{E})$ divide $\mathrm{Irr}(a,\mathbb{F})$. □

(10) Determine o polinômio minimal de $\alpha = \sqrt{3} + i \in \mathbb{C}$ sobre $\mathbb{F}$, em que:
(a) $\mathbb{F} = \mathbb{Q}$,
(b) $\mathbb{F} = \mathbb{Q}[\sqrt{3}]$,
(c) $\mathbb{F} = \mathbb{Q}[i\sqrt{3}]$,
(d) $\mathbb{F} = \mathbb{Q}[i]$.

Usaremos que $\mathbb{Q}(\sqrt{3}+i) = \mathbb{Q}(\sqrt{3}, i)$, e $[\mathbb{Q}(\sqrt{3}+i) : \mathbb{Q}] = 4$.

Portanto, $\mathrm{gr}(\mathrm{Irr}(\sqrt{3}+i, \mathbb{Q}) = 4$. Temos que

$$\left((\sqrt{3}+i)^2 - 2\right)^2 = -12$$

Portanto, $\sqrt{3}+i$ satisfaz $(X^2-2)^2 = -12$. Ou seja, $\sqrt{3}+i$ satisfaz $X^4 - 4X^2 + 16 \in \mathbb{Q}[X]$. Como, o grau do pol. min. de $\sqrt{3}+i$ sobre $\mathbb{Q}$ é 4, segue que seu pol. min. é $X^4 - 4x^2 + 16$.

$\text{Irr}(\sqrt{3}+i, \mathbb{Q}) = x^4 - 4x^2 + 16$.

(b) Temos que

$$[\mathbb{Q}[\sqrt{3}+i] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}+i] : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

4 $\qquad$ 2

Portanto, $[\mathbb{Q}(\sqrt{3}+i) : \mathbb{Q}(\sqrt{3})] = 2$.

$$\left((\sqrt{3}+i) - \sqrt{3}\right)^2 = -1.$$

Portanto $\sqrt{3}+i$ satisfaz $(x - \sqrt{3})^2 = -1$, ou seja, $\sqrt{3}+i$ satisfaz $x^2 - 2\sqrt{3}x + 4 \in \mathbb{Q}(\sqrt{3})[x]$.

Portanto, $\text{Irr}(\sqrt{3}+i, \mathbb{Q}(\sqrt{3})) = x^2 - 2\sqrt{3}x + 4$.

(c) $(\sqrt{3}+i)^2 = 2 + 2\sqrt{3}i \in \mathbb{Q}(i\sqrt{3})$.

Então $\sqrt{3}+i$ satisfaz $x^2 - (2 + 2\sqrt{3}i) \in \mathbb{Q}(i\sqrt{3})$.

$\therefore$ (Completar).