(10) Seja $\mathbb{F}$ um corpo de característica $p > 0$. Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita, e assuma que p não divide $[\mathbb{E} : \mathbb{F}]$. Prove que $\mathbb{E}/\mathbb{F}$ é uma extensão separável.

(11) Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos, com $\operatorname{car}\mathbb{F} = p > 0$, e $a \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Mostre que a é separável sobre $\mathbb{F}$ se, e somente se, $\mathbb{F}(a) = \mathbb{F}(a^{p^m})$, para todo $m \in \mathbb{N}$.

(14) Sejam $\mathbb{F}$ um corpo, $f \in \mathbb{F}[X]$ irredutível sobre $\mathbb{F}$, e $\mathbb{E}/\mathbb{F}$ uma extensão normal e finita. Sejam $f_1, f_2 \in \mathbb{E}[X]$ componentes mônicos e irredutíveis de f. Prove que existe $\sigma \in \operatorname{Aut}(\mathbb{E}/\mathbb{F})$ tal que $f_2 = f_1^\sigma$.

(12) Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica. Prove:

(a) $\mathbb{F}$ é perfeito se, e somente se, $\mathbb{E}$ é perfeito e $\mathbb{E}/\mathbb{F}$ é separável.
(b) Suponha que $\mathbb{E}/\mathbb{F}$ é finita. Então $\mathbb{F}$ é perfeito se, e somente se, $\mathbb{E}$ é perfeito.
(c) Indique um corpo imperfeito $\mathbb{F}$ e uma extensão algébrica $\mathbb{E}/\mathbb{F}$ tal que $\mathbb{E}$ seja perfeito.

(6) Seja $\alpha \in \mathbb{R}$ tal que $\alpha^4 = 5$.

(a) Prove que $\mathbb{Q}(i\alpha^2)/\mathbb{Q}$ é normal.
(b) Prove que $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}(i\alpha^2)$ é normal.
(c) Prove que $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}$ não é normal.

(7) Para cada um dos polinômios abaixo, encontre $\mathbb{L}$, o seu corpo de raízes sobre $\mathbb{Q}$, e determine $[\mathbb{L} : \mathbb{F}]$.

(e) $X^6 + X^3 + 1$

Relembre:

Teorema 6.6. *Seja $f \in \mathbb{F}[X]$ irredutível. Então f é separável se, e somente se, $f' \neq 0$.*

Assim, se f é irredutível e vale um entre (i) ou $\operatorname{car}\mathbb{F} = 0$, (ii) ou $\operatorname{car}\mathbb{F} = p > 0$ e $f \notin \mathbb{F}[X^p]$, então f é separável.

Teorema 6.7. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$, e $f \in \mathbb{F}[X]$ irredutível. Então existem $m \geq 0$ e um polinômio irredutível e separável $g \in \mathbb{F}[X]$ tal que $f = g(X^{p^m})$.*

Teorema 5.5. *Sejam $\mathbb{L}/\mathbb{F}$ uma extensão algébrica de corpos, e Ω um corpo algebricamente fechado contendo $\mathbb{L}$. Então $\mathbb{L}/\mathbb{F}$ é normal se, e somente se, $\operatorname{Aut}(\mathbb{L}/\mathbb{F}) = \operatorname{Mono}_{\mathbb{F}}(\mathbb{L}, \Omega)$.*

Teorema 6.12. *Seja $\mathbb{F}$ um corpo. As seguintes afirmações são equivalentes:*

(i) *O corpo $\mathbb{F}$ é perfeito.*
(ii) *Todo polinômio irredutível em $\mathbb{F}[X]$ é separável.*
(iii) *Toda extensão algébrica $\mathbb{E}/\mathbb{F}$ é separável.*

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

$f \in \mathbb{F}[X^p]$

$\exists\ g(X^p) = a_0 + a_1 X^p + \cdots + a_m X^{mp}$

$\mathbb{F}(\alpha)/\mathbb{F}_p(\alpha)$

$\mathbb{E}/\mathbb{F}_p$

(10) Seja $\mathbb{F}$ um corpo de característica $p > 0$. Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita, e assuma que p não divide $[\mathbb{E} : \mathbb{F}]$. Prove que $\mathbb{E}/\mathbb{F}$ é uma extensão separável.

Assuma que $\mathbb{E}/\mathbb{F}$ não é separável. Então, existe $a \in \mathbb{E}$ que não é separável sobre $\mathbb{F}$. Ou seja, $\mathrm{Irr}(a, \mathbb{F})$ não é separável. Por Teorema 6.6, segue que $\mathrm{Irr}(a, \mathbb{F}) \in \mathbb{F}[X^p]$. Portanto,

$$\mathrm{gr}\ \mathrm{Irr}(a, \mathbb{F}) = pm = [\mathbb{F}(a) : \mathbb{F}].$$

Daí, como $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}(a)][\mathbb{F}(a) : \mathbb{F}]$, segue que p divide $[\mathbb{E} : \mathbb{F}]$.

(11) Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos, com $\mathrm{car}\,\mathbb{F} = p > 0$, e $a \in \mathbb{E}$ algébrico sobre $\mathbb{F}$. Mostre que a é separável sobre $\mathbb{F}$ se, e somente se, $\mathbb{F}(a) = \mathbb{F}(a^{p^m})$, para todo $m \in \mathbb{N}$.

Assuma que a não é separável sobre $\mathbb{F}$. Então, do Teorema 6.7, existem $m > 0$ e $g \in \mathbb{F}[X]$ irredutível e separável tais que

$$\mathrm{Irr}(a, \mathbb{F}) = g(X^{p^m}).$$

Temos que $0 = g(a^{p^m})$. Daí g é o polinômio minimal de a^{p^m} sobre $\mathbb{F}$. Então

$$[\mathbb{F}(a) : \mathbb{F}] = p^m\, \mathrm{gr}(g) > \mathrm{gr}(g) = [\mathbb{F}(a^{p^m}) : \mathbb{F}].$$

Portanto, $\mathbb{F}(a) \neq \mathbb{F}(a^{p^m})$.

Reciprocamente, assuma que a é separável sobre $\mathbb{F}$, e seja $m \in \mathbb{N}$. Então a é separável

sobre $F(a^{p^m})$. Além disso, a é raiz de

$$F(a^{p^m})[X] \ni X^{p^m} - a^{p^m}.$$

Daí $\mathrm{Irr}(a, F(a^{p^m}))$ divide $X^{p^m} - a^{p^m}$.

Mas, $X^{p^m} - a^{p^m} = (X-a)^{p^m} \in F[X]$. Assim, todas as raízes de $\mathrm{Irr}(a, F(a^{p^m}))$ deve coincidir com a. Como $\mathrm{Irr}(a, F(a^{p^m}))$ é separável, temos que $\mathrm{Irr}(a, F(a^{p^m})) = X - a$.

Portanto, $a \in F(a^{p^m})$. Então, vale que $F(a) = F(a^{p^m})$.

$\Rightarrow F(a) \subseteq F(a^{p^m})$

Por outro lado, $a^{p^m} \in F(a) \Rightarrow F(a^{p^m}) \subseteq F(a)$.

$\sigma : \mathbb{E} \to \Omega$, $f = \alpha_0 + \cdots + \alpha_m X^m \in \mathbb{E}[X]$

$\Omega[X] \ni f^\sigma := \sigma(\alpha_0) + \sigma(\alpha_1) X + \cdots + \sigma(\alpha_m) X^m$.

(14) Sejam $\mathbb{F}$ um corpo, $f \in \mathbb{F}[X]$ irredutível sobre $\mathbb{F}$, e $\mathbb{E}/\mathbb{F}$ uma extensão normal e finita. Sejam $f_1, f_2 \in \mathbb{E}[X]$ componentes mônicos e irredutíveis de f. Prove que existe $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ tal que $f_2 = f_1^\sigma$.

Sejam $f_1, \ldots, f_s \in \mathbb{E}[X]$ mônicos e irredutíveis tais que

$$f = \alpha f_1 f_2 \cdots f_s, \quad \alpha \in \mathbb{F}.$$

Seja Ω um fecho algébrico de $\mathbb{E}$. Escolha $a_1, \ldots, a_s \in \Omega$ tais que $f_1(a_1) = \cdots = f_s(a_s) = 0$.

Afirmação. Se $f_i(a_j) = 0$, então $f_i = f_j$.

De fato, note que $f_j = \mathrm{Irr}(a_j, \mathbb{E})$. Se $f_i(a_j) = 0$, então f_j divide f_i. Como f_i é irredutível e mônico, segue que $f_i = f_j$

Fixe i. Vamos provar que existe $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ tal que $f_i = f_1^{\sigma}$. α $\mathrm{Irr}(a_1, \mathbb{F}) = f$, além disso, $f(a_2) = 0$.

$\mathbb{F}(a_1) \to \Omega$

Seja $\sigma_0 : \mathbb{F}(a_1) \longrightarrow \Omega$ um $\mathbb{F}$-monomorfismo tal que $\sigma_0(a_1) = a_2$. Como $\mathbb{E}/\mathbb{F}$ é algébrica, existe um $\mathbb{F}$-monomorfismo $\sigma : \mathbb{E} \to \Omega$ que estende σ_0. Como $\mathbb{E}/\mathbb{F}$ é normal, segue que $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$.

Agora, note que

$$f = f^{\sigma} = \alpha f_1^{\sigma} \cdots f_s^{\sigma}.$$

Se ocorresse $f_i^{\sigma} = g_1 g_2$, então teríamos que

$$f_i = (f_i^{\sigma})^{\sigma^{-1}} = g_1^{\sigma^{-1}} g_2^{\sigma^{-1}}.$$

Portanto, como f_i é irredutível, temos que cada f_i^{σ} é irredutível em $\mathbb{E}[X]$. Além disso,

$$0 = \sigma(f_1(a_1)) = f_1^{\sigma}(\sigma(a_1)) = f_1^{\sigma}(a_2).$$

Assim, da afirmação, obtemos que $f_1^{\sigma} = f_2$.

(12) Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica. Prove:

(a) $\mathbb{F}$ é perfeito se, e somente se, $\mathbb{E}$ é perfeito e $\mathbb{E}/\mathbb{F}$ é separável.

(b) Suponha que $\mathbb{E}/\mathbb{F}$ é finita. Então $\mathbb{F}$ é perfeito se, e somente se, $\mathbb{E}$ é perfeito.

(c) Indique um corpo imperfeito $\mathbb{F}$ e uma extensão algébrica $\mathbb{E}/\mathbb{F}$ tal que $\mathbb{E}$ seja perfeito.

(c) Sejam $\mathbb{F}$ um corpo não perfeito e $\Omega = \overline{\mathbb{F}}$ o seu fecho algébrico. Como Ω é algebricamente fechado, Ω é perfeito. Além disso, por definição, $\Omega/\mathbb{F}$ é algébrica.

(a) Assuma que $\mathbb{F}$ é perfeito. Então, por $\mathbb{E}/\mathbb{F}$ ser algébrica segue que a mesma é separável.

Seja $\mathbb{L}/\mathbb{E}$ uma extensão algébrica. Então, $\mathbb{L}/\mathbb{F}$ é algébrica. Como $\mathbb{F}$ é perfeito, $\mathbb{L}/\mathbb{F}$ é separável. Portanto, $\mathbb{L}/\mathbb{E}$ é separável. Assim, da equivalência (i) e (iii) do Teorema 6.12, temos que $\mathbb{E}$ é perfeito.

Reciprocamente, assuma que $\mathbb{E}$ é perfeito e $\mathbb{E}/\mathbb{F}$ é separável. Seja $f \in \mathbb{F}[X]$ um polinômio mônico e irredutível. Seja $\Omega = \overline{\mathbb{E}}$ um fecho algébrico de $\mathbb{E}$, e seja $a \in \Omega$ tal que $f(a) = 0$. Então $f = \mathrm{Irr}(a, \mathbb{F})$. Além disso, a é algébrico sobre $\mathbb{E}$. Daí $\mathbb{E}(a)/\mathbb{E}$ é algébrica. Como $\mathbb{E}$ é perfeito, $\mathbb{E}(a)/\mathbb{E}$ é separável. Como $\mathbb{E}/\mathbb{F}$ é separável, segue que $\mathbb{E}(a)/\mathbb{F}$ é separável. Em particular, a é separável sobre $\mathbb{F}$. Portanto seu

polinômio minimal sobre $\mathbb{F}$ é separável. Daí f é separável. Da equivalência (i)$\Leftrightarrow$(ii) do Teorema 6.12, obtemos que $\mathbb{F}$ é perfeito.

(b) (Ideia) segue de (a) que $\mathbb{F}$ perfeito $\Rightarrow$ $\mathbb{E}$ perfeito.

Se $\mathbb{E}$ é perfeito, seja $F: \mathbb{E} \to \mathbb{E}$, $F(a) = a^p$. Como $\mathbb{E}$ é perfeito, vale que $F(\mathbb{E}) = \mathbb{E}$. Considere

$$\mathbb{F} \subseteq F^{-1}(\mathbb{F}) \subseteq \underbrace{F^{-2}(\mathbb{F})}_{F^{-1}(F^{-1}(\mathbb{F}))} \subseteq \cdots$$

(verifique que são corpos)

Como $[\mathbb{E}:\mathbb{F}] < \infty$, a sequência estabiliza, ou seja, existe $m \in \mathbb{N}$ tal que $F^{-m}(\mathbb{F}) = F^{-m-s}(\mathbb{F})$, $\forall s > 0$. Em particular, $F^{-m}(\mathbb{F}) = F^{-m-1}(\mathbb{F})$. Assim, como F é sobre, dado $a \in \mathbb{F}$, existe $b \in \mathbb{E}$ tal que $F^{m+1}(b) = a$. Daí

$$b \in F^{-m-1}(\mathbb{F}) = F^{-m}(\mathbb{F}) \Rightarrow F^m(b) \in \mathbb{F}$$

Daí $a = F^{m+1}(b) = F(\underbrace{F^m(b)}_{\in \mathbb{F}}) = (F^m(b))^p$. Ou seja, $a \in \mathbb{F}^p$. Daí $\mathbb{F}^p = \mathbb{F}$ e $\mathbb{F}$ é perfeito.

(6) Seja $\alpha \in \mathbb{R}$ tal que $\alpha^4 = 5$.

(a) Prove que $\mathbb{Q}(i\alpha^2)/\mathbb{Q}$ é normal.

(b) Prove que $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}(i\alpha^2)$ é normal.

(c) Prove que $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}$ não é normal.

(a) Como $(i\alpha^2)^2 = -\alpha^4 = -5 \in \mathbb{Q}$. Daí $[\mathbb{Q}(i\alpha^2) : \mathbb{Q}] \leq 2$. Da Proposição 4.8, $\mathbb{Q}(i\alpha^2)/\mathbb{Q}$ é normal.

(b) Argumento parecido: vale que $(\alpha + i\alpha)^2 \in \mathbb{Q}(i\alpha^2)$.

(verifique e conclua)

(c) Note que

$$(\alpha + i\alpha)^2 = \alpha^2 + 2i\alpha^2 - \alpha^2 = 2i\alpha^2,$$

$$(\alpha + i\alpha)^4 = (2i\alpha^2)^2 = -4\alpha^4 = -20.$$

Então $\mathrm{Irr}(\alpha + i\alpha, \mathbb{Q}) = x^4 + 20$. As raízes de $x^4 + 20$ são: ($\Rightarrow [\mathbb{Q}(\alpha + i\alpha) : \mathbb{Q}] = 4$).

$$\mathcal{R}(x^4 + 20) = \{\alpha + i\alpha, \alpha - i\alpha, -\alpha + i\alpha, -\alpha - i\alpha\}$$

(verifique)

Se $\mathbb{Q}(i\alpha + \alpha)/\mathbb{Q}$ fosse normal, então

$$\mathcal{R}(x^4 + 20) \subseteq \mathbb{Q}(i\alpha + \alpha).$$

Em particular,

$$\mathbb{Q}(i\alpha + \alpha) \ni \frac{1}{2}\left((\alpha + i\alpha) + (\alpha - i\alpha)\right) = \alpha,$$

$$\ni \frac{1}{\alpha}\left((\alpha + i\alpha) - \alpha\right) = i.$$

Daí $\mathbb{Q}(i\alpha+\alpha) \supseteq \mathbb{Q}(\alpha, i)$.

Por um lado, $\mathrm{Irr}(\alpha, \mathbb{Q}) = X^4 - 5$, daí $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$.

Mas, $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Daí $i \notin \mathbb{Q}(\alpha)$. Portanto,

$\mathrm{Irr}(i, \mathbb{Q}(\alpha)) = X^2 + 1$. Assim

$$[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 8.$$

Isso contradiz o fato de $[\mathbb{Q}(i\alpha+\alpha):\mathbb{Q}] = 4$.

Portanto, $\mathbb{Q}(i\alpha+\alpha)/\mathbb{Q}$ não é normal.

(7) Para cada um dos polinômios abaixo, encontre $\mathbb{L}$, o seu corpo de raízes sobre $\mathbb{Q}$, e determine $[\mathbb{L} : \mathbb{F}]$.

(e) $X^6 + X^3 + 1$

Vale que

$$R(X^6+X^3+1) = \left\{ e^{\frac{2\pi i}{9}}, e^{\frac{4\pi i}{9}}, e^{\frac{8\pi i}{9}}, e^{\frac{10\pi i}{9}}, e^{\frac{14\pi i}{9}}, e^{\frac{16\pi i}{9}} \right\}.$$

Daí $\mathbb{Q}(R(X^6+X^3+1)) = \mathbb{Q}(e^{\frac{2\pi i}{9}})$. Daí basta mostrar que $f(X) = X^6 + X^3 + 1$ é irredutível. Defina

$$g(X) := f(X+1).$$

Se $f = h_1 h_2$ então $g(X) = h_1(X+1)\, h_2(X+1)$. Daí, basta mostrar que g é irredutível. Temos que

$$g(X) = (X+1)^6 + (X+1)^3 + 1 = \left(\sum_{i=0}^{6} \binom{6}{i} X^i\right) + \left(\sum_{i=0}^{3} \binom{3}{i} X^i\right) + 1$$

$$= X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3.$$

Do critério de Eisenstein com $p = 3$, g é irredutível.

Dai $[\mathbb{Q}(e^{\frac{2\pi i}{9}}) : \mathbb{Q}] = 6.$