Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos e Ω um corpo algebricamente fechado contendo $\mathbb{E}$. Seja $\sigma : \mathbb{E} \to \Omega$ um $\mathbb{F}$-endomorfismo de modo que $\operatorname{Im}\sigma \subseteq \mathbb{E}$. Prove que $\operatorname{Im}\sigma = \mathbb{E}$, e portanto, σ é um $\mathbb{F}$-automorfismo de $\mathbb{E}$.

(9) Encontre o polinômio minimal sobre $\mathbb{Q}$ dos seguintes elementos de $\mathbb{C}$:

(a) $\dfrac{\sqrt{5}+1}{2}$,

(c) $\sqrt{2}+i$,

(12) Sejam $\mathbb{K}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ extensões de corpos e $a \in \mathbb{K}$. Mostre que se a é algébrico sobre $\mathbb{F}$, então a é algébrico sobre $\mathbb{E}$, e $[\mathbb{E}[a] : \mathbb{E}] \leq [\mathbb{F}[a] : \mathbb{F}]$.

(14) Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos finita. Assuma que vale a seguinte propriedade: dados $\mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{E}$ contendo $\mathbb{F}$, vale que $\mathbb{E}_1 \subseteq \mathbb{E}_2$ ou $\mathbb{E}_2 \subseteq \mathbb{E}_1$. Prove que $\mathbb{E}/\mathbb{F}$ é simples, ou seja, vale que $\mathbb{E} = \mathbb{F}(u)$, para algum $u \in \mathbb{E}$.

(16) Seja $\mathbb{F}$ um corpo e $p \in \mathbb{F}[X]$ irredutível sobre $\mathbb{F}$. Seja $\mathbb{E}$ uma extensão de $\mathbb{F}$. Mostre que, se $\operatorname{gr}(p)$ não divide $[\mathbb{E} : \mathbb{F}]$, então p não tem raízes em $\mathbb{E}$.

(19) Determine o grau da extensão $[\mathbb{F} : \mathbb{Q}]$, em que:

(a) $\mathbb{F} = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$

(15) Seja $\mathbb{F} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$ o subcorpo de $\mathbb{C}$ gerado por $\mathbb{Q}$ e as raízes quadradas de todos os números primos positivos.

(a) Prove que $\mathbb{F}/\mathbb{Q}$ é uma extensão algébrica.

(b) Mostre que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \cdots$ é uma cadeia ascendente própria de subcorpos de $\mathbb{C}$. Conclua que $\mathbb{F}/\mathbb{Q}$ é uma extensão infinita.

Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos e Ω um corpo algebricamente fechado contendo $\mathbb{E}$. Seja $\sigma : \mathbb{E} \to \Omega$ um $\mathbb{F}$-endomorfismo de modo que $\operatorname{Im}\sigma \subseteq \mathbb{E}$. Prove que $\operatorname{Im}\sigma = \mathbb{E}$, e portanto, σ é um $\mathbb{F}$-automorfismo de $\mathbb{E}$.

Sejam $a \in \mathbb{E}$ e p_a seu polinômio minimal sobre $\mathbb{F}$. Sejam $R(p_a)$ as raízes de p_a (em Ω). Dado $b \in R(p_a) \cap \mathbb{E}$, note que

$$0 = \sigma(p_a(b)) = p_a^{\sigma}(\sigma(b)) = p_a(\sigma(b)).$$

Daí $\sigma(b) \in R(p_a)$. Assim, como $\operatorname{Im}\sigma \subseteq \mathbb{E}$, vale que

$$\sigma(R(p_a) \cap \mathbb{E}) \subseteq R(p_a) \cap \mathbb{E}.$$

Mas $R(p_a)$ é finito, e portanto $R(p_a) \cap \mathbb{E}$ é finito. Como σ é injetora, segue que σ também é sobrejetora, quando restrito a $R(p_a) \cap \mathbb{E}$. Portanto, existe $b \in R(p_a) \cap \mathbb{E}$ tal que $\sigma(b) = a$, pois $a \in R(p_a) \cap \mathbb{E}$. Conclui-se que σ é sobrejetor. Então $\operatorname{Im}\sigma = \mathbb{E}$.

(9) Encontre o polinômio minimal sobre $\mathbb{Q}$ dos seguintes elementos de $\mathbb{C}$:

(a) $\frac{\sqrt{5}+1}{2}$,

(c) $\sqrt{2}+i$,

(a) $\frac{\sqrt{5}+1}{2} \notin \mathbb{Q}$. Portanto, seu polinômio minimal tem grau > 1. Note que

$$\left(2\cdot\left(\frac{\sqrt{5}+1}{2}\right)-1\right)^2 = 5.$$

Portanto, $\frac{\sqrt{5}+1}{2}$ satisfaz $(2X-1)^2 = 5$. Ou seja, satisfaz o polinômio $g(X) = 4X^2 - 4X - 4$. Assim, $\frac{\sqrt{5}+1}{2}$ satisfaz $f(X) = X^2 - X - 1 \in \mathbb{Q}[X]$.

Como $\operatorname{gr} f = 2$ e f é mônico, então o polinômio minimal de $\frac{\sqrt{5}+1}{2}$ sobre $\mathbb{Q}$ é $X^2 - X - 1$.

(c) Note que $\mathbb{Q}(\sqrt{2}+i) = \mathbb{Q}(\sqrt{2}, i)$, e então,

$$[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})]\underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{2}.$$

Prova-se que $i \notin \mathbb{Q}(\sqrt{2})$, e portanto, X^2+1 é o pol. min. de i sobre $\mathbb{Q}(\sqrt{2})$. Daí $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$. Então $[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}] = 4 = \operatorname{gr}(\operatorname{Irr}(\sqrt{2}+i, \mathbb{Q}))$.

Agora, $((\sqrt{2}+i)^2 - 1)^2 = -8$.

Portanto, $\sqrt{2}+i$ satisfaz $f = (X^2-1)^2 + 8 =$
$= X^4 - 2X^2 + 9$. Com $\operatorname{gr} f = 4$ e f mônico,
Vale que o pol. min. de $\sqrt{2}+i$ sobre $\mathbb{Q}$ é $X^4 - 2X^2 + 9$.

(b) $\sqrt{3-\sqrt{6}}$

$$\left(\left(\sqrt{3-\sqrt{6}}\right)^2 - 3\right)^2 = 6$$

Então $\sqrt{3-\sqrt{6}}$ satisfaz $X^4 - 6X^2 + 3$. Por
critério de Eisenstein, $X^4 - 6X^2 + 3$ é irredutível
Portanto, $\operatorname{Irr}(\sqrt{3-\sqrt{6}}, \mathbb{Q}) = X^4 - 6X^2 + 3$.

"

$\sqrt{3-\sqrt{6}} \notin \mathbb{Q}(\sqrt{6})$. Assuma o contrário, então

$$\sqrt{3-\sqrt{6}} = a + b\sqrt{6}, \qquad a, b \in \mathbb{Q}$$

Daí $3 - \sqrt{6} = a^2 + 6b^2 + 2ab\sqrt{6}$.

Portanto

$$\begin{cases} 3 = a^2 + 6b^2 \\ -1 = 2ab \end{cases}, \quad a, b \in \mathbb{Q}.$$

Daí $12b^2 = \underbrace{4a^2b^2}_{1} + 24b^4$,

ou seja, $12b^2 = 1 + 24b^2$.

Portanto, $b \notin \mathbb{Q}$.

(12) Sejam $\mathbb{K}/\mathbb{E}$ e $\mathbb{E}/\mathbb{F}$ extensões de corpos e $a \in \mathbb{K}$. Mostre que se a é algébrico sobre $\mathbb{F}$, então a é algébrico sobre $\mathbb{E}$, e $[\mathbb{E}[a] : \mathbb{E}] \leq [\mathbb{F}[a] : \mathbb{F}]$.

Seja p_a o polinômio minimal de a sobre $\mathbb{F}$. Então $p_a \in \mathbb{F}[X] \subseteq \mathbb{E}[X]$. Além disso, $p_a(a) = 0$, e portanto, a é algébrico sobre $\mathbb{E}$. Ainda,

$$\operatorname{gr}(\operatorname{Irr}(a, \mathbb{E})) \leq \operatorname{gr} p_a.$$

Portanto

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

(14) Seja $\mathbb{E}/\mathbb{F}$ uma extensão de corpos finita. Assuma que vale a seguinte propriedade: dados $\mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{E}$ contendo $\mathbb{F}$, vale que $\mathbb{E}_1 \subseteq \mathbb{E}_2$ ou $\mathbb{E}_2 \subseteq \mathbb{E}_1$. Prove que $\mathbb{E}/\mathbb{F}$ é simples, ou seja, vale que $\mathbb{E} = \mathbb{F}(u)$, para algum $u \in \mathbb{E}$.

Temos que $\mathbb{E} = \mathbb{F}(a_1, \ldots, a_m)$, em que $a_1, \ldots, a_m \in \mathbb{E}$.

Temos que $\mathbb{F}(a_1)$ e $\mathbb{F}(a_2)$ são corpos intermediários

Da propriedade, vale que $\mathbb{F}(a_1) \subseteq \mathbb{F}(a_2)$, ou $\mathbb{F}(a_2) \subseteq \mathbb{F}(a_1)$. Assuma, sem perda de generalidade, que $\mathbb{F}(a_1) \subseteq \mathbb{F}(a_2)$. Por um lado, $\mathbb{F}(a_2) \subseteq \mathbb{F}(a_1, a_2)$. Reciprocamente, $a_2 \in \mathbb{F}(a_2)$, e $a_1 \in \mathbb{F}(a_1) \subseteq \mathbb{F}(a_2)$. Daí $\mathbb{F}(a_1, a_2) \subseteq \mathbb{F}(a_2)$. Portanto, vale que $\mathbb{F}(a_1, a_2) = \mathbb{F}(a_2)$. Então

$$\mathbb{E} = \mathbb{F}(a_2, \ldots, a_m).$$

Por indução, conclui-se que $\mathbb{E} = \mathbb{F}[a]$. Daí, a extensão $\mathbb{E}/\mathbb{F}$ é simples.

(16) Seja $\mathbb{F}$ um corpo e $p \in \mathbb{F}[X]$ irredutível sobre $\mathbb{F}$. Seja $\mathbb{E}$ uma extensão de $\mathbb{F}$. Mostre que, se $\mathrm{gr}(p)$ não divide $[\mathbb{E} : \mathbb{F}]$, então p não tem raízes em $\mathbb{E}$.

Assuma que existe $a \in \mathbb{E}$ tal que $p(a) = 0$. Como p é irredutível sobre $\mathbb{F}$, vale que

$$\mathrm{gr}(p) = \mathrm{gr}\left(\mathrm{Irr}(a, \mathbb{F})\right) = [\mathbb{F}(a) : \mathbb{F}],$$

Como $a \in \mathbb{E}$, vale que $\mathbb{E} / \mathbb{F}(a) / \mathbb{F}$. Então

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}(a)]\,[\mathbb{F}(a) : \mathbb{F}] = [\mathbb{E} : \mathbb{F}(a)] \cdot \mathrm{gr}(p).$$

Portanto, $\mathrm{gr}(p)$ divide $[\mathbb{E} : \mathbb{F}]$.

(19) Determine o grau da extensão $[\mathbb{F} : \mathbb{Q}]$, em que:

(a) $\mathbb{F} = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$

Temos que

$$[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5})(\sqrt{-2}) : \mathbb{Q}(\sqrt[3]{5})]\,[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}].$$

Temos que $X^3 - 5 \in \mathbb{Q}[X]$ é irredutível (por critério de Eisenstein), e $\sqrt[3]{5}$ é uma de suas raízes. Portanto $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$.

Por outro lado, $f = X^2 + 2 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$. Ainda, $\sqrt{-2}$ é raiz de f. Como $\operatorname{gr} f = 2$ não divide $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$, segue que f não possui raiz em $\mathbb{Q}(\sqrt[3]{5})$. Como $\operatorname{gr} f = 2$, segue que f é irredutível sobre $\mathbb{Q}(\sqrt[3]{5})$. Daí

$$\operatorname{Irr}(\sqrt{-2}, \mathbb{Q}(\sqrt[3]{5})) = X^2 + 2.$$

Daí $[\mathbb{Q}(\sqrt[3]{5})(\sqrt{-2}) : \mathbb{Q}(\sqrt[3]{5})] = 2$. Segue que

$$[\mathbb{Q}(\sqrt[3]{5}, \sqrt{-2}) : \mathbb{Q}] = 6.$$

(15) Seja $\mathbb{F} = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots)$ o subcorpo de $\mathbb{C}$ gerado por $\mathbb{Q}$ e as raízes quadradas de todos os números primos positivos.

(a) Prove que $\mathbb{F}/\mathbb{Q}$ é uma extensão algébrica.

(b) Mostre que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \cdots$ é uma cadeia ascendente própria de subcorpos de $\mathbb{C}$. Conclua que $\mathbb{F}/\mathbb{Q}$ é uma extensão infinita.

(a) Seja $a \in \mathbb{F}$. Temos que existe $m \in \mathbb{N}$ e $f \in \mathbb{Q}[X_1, \ldots, X_m]$ de modo que

$$a = f(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_m}),$$ em que $p_1, \ldots, p_m$ são primos.

Daí $a \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})$. Como $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})/\mathbb{Q}$ é algébrica, segue que a é algébrico sobre $\mathbb{Q}$.

Portanto, $\mathbb{F}/\mathbb{Q}$ é algébrica.

(b) Considere $p_1, p_2, \ldots$ a sequência dos números primos. Ideia: provar por indução em m que

$$\sqrt{p_m} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{m-1}}).$$

Extra. Sejam F corpo, $f \in F[X]$ irredutível e L um corpo de raízes de f sobre F. Assuma que $f = (X-a_1)\dots(X-a_m)$.

Prove que são equivalentes:

(i) $[L:F] = m$

(ii) $L = F(a_j)$, para algum $j \in \{1,\dots,m\}$

(iii) $L = F(a_j)$, $\forall j \in \{1,\dots,m\}$.

(i) $\Rightarrow$ (iii). Temos que $L = F(a_1,\dots,a_m)$. Dado $j \in \{1,\dots,m\}$, temos que $[F(a_j):F] = \operatorname{gr} f = m$, pois f é irredutível. Ainda,

$$[L:F] = [L:F(a_j)][F(a_j):F],$$

Como $[L:F] = m$ (por (i)), vale que $[L:F(a_j)] = 1$.

Daí $L = F(a_j)$.

(iii) $\Rightarrow$ (ii) OK.

(ii) $\Rightarrow$ (i) De (ii), temos que $L = F(a_j)$, p/ algum j.

Portanto, $[L:F] = \operatorname{gr} f = m$.

$j: \overline{F}_1 \to \overline{F}_2$, $\overline{F}_1$ é alg. fech. $F \subset F_1 \subset \overline{F}_1 / F$

$(\overline{F}_2 / \overline{F}_1) / F$

$\overline{F}_2 / F$ é alg.

$\overline{F}_2 \supseteq j(\overline{F}_1)$

$\overline{F}_1 / F$

$\overline{F}_2 / \overline{F}_1 / F$

($\overline{F}_1$ é fech. alg. de F

e $\overline{F}_2 / \overline{F}_1$ e $\overline{F}_2 / F$ é alg.

é alg.

(i) F é alg. fech.

(ii) E/F é alg., então $E \cong F$.

$(i(F) = E)$

$X^3 - 2$

$\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ $\quad |Aut(\mathbb{Q}\sqrt[3]{2}/\mathbb{Q})| \neq 3.$

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ não é normal

+ Separável

$[L:\mathbb{Q}] = |\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})|$ $\quad \mathrm{char}\,F = p > 0$

$X^p - a$

$\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \subseteq \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$

$\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sigma} \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$

(fecho alg. de F em L

$\overline{F}^{L} = \{\text{elem. alg. } / F\}$

(fecho alg. de F : c/ fecho alg. fech. $\overline{F}$ t.q. $\overline{F}/F$ é alg.

p irr. $\Rightarrow^{a}$ $F(a)/F$