(1) Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos. Mostre que as afirmações seguintes são equivalentes:
   (a) $\mathbb{E}/\mathbb{F}$ é normal e separável,
   (b) existe $S \subseteq \mathbb{F}[X]$ um conjunto de polinômios *separáveis* tal que $\mathbb{E}$ é o corpo de raízes de S sobre $\mathbb{F}$.

(2) Seja $\mathbb{L}/\mathbb{F}$ uma extensão normal. Seja $f \in \mathbb{F}[X]$ um polinômio mônico e irredutível em $\mathbb{F}[X]$, e seja $f = f_1 \cdots f_m$, com $f_1, \ldots, f_m \in \mathbb{L}[X]$, a sua decomposição em produto de polinômios mônicos e irredutíveis em $\mathbb{L}[X]$. Então

$$\{f_1, \ldots, f_m\} = \{f_1^\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})\}.$$

(3) Prove que existem corpos $\mathbb{F}$ e $\mathbb{E}$, com $\mathbb{F} \subseteq \mathbb{E}$, satisfazendo:
   (a) a extensão $\mathbb{E}/\mathbb{F}$ é finita,
   (b) existem infinitos corpos entre $\mathbb{F}$ e $\mathbb{E}$.

(3) Prove que existem corpos $\mathbb{F}$ e $\mathbb{E}$, com $\mathbb{F} \subseteq \mathbb{E}$, satisfazendo:
   (a) a extensão $\mathbb{E}/\mathbb{F}$ é finita,
   (b) existem infinitos corpos entre $\mathbb{F}$ e $\mathbb{E}$.

Teorema 7.13. *Seja $\mathbb{E}/\mathbb{F}$ uma extensão finita de corpos. Então $\mathbb{E}/\mathbb{F}$ é simples se, e só se, existe um número finito de corpos entre $\mathbb{F}$ e $\mathbb{E}$.*

(13) Sejam $\mathbb{F}$ um corpo de característica $p > 0$, e $\mathbb{L} = \mathbb{F}(X, Y)$ o corpo de frações do anel de polinômios sobre $\mathbb{F}$ em duas variáveis. Seja $\mathbb{E} = \mathbb{F}(X^p, Y^p) \subseteq \mathbb{L}$, a extensão de $\mathbb{F}$ pelos elementos X^p e Y^p. Prove que:
   (a) $\mathbb{L}/\mathbb{E}$ é uma extensão de grau p^2,
   (b) $[\mathbb{E}(\zeta) : \mathbb{E}] = p$, para qualquer $\zeta \in \mathbb{L}$.
   (c) Conclua que $\mathbb{L}/\mathbb{E}$ não possui nenhum elemento primitivo.

(1) Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos. Mostre que as afirmações seguintes são equivalentes:
   (a) $\mathbb{E}/\mathbb{F}$ é normal e separável,
   (b) existe $S \subseteq \mathbb{F}[X]$ um conjunto de polinômios *separáveis* tal que $\mathbb{E}$ é o corpo de raízes de S sobre $\mathbb{F}$.

(b) $\Rightarrow$ (a) Se $\mathbb{E} = \mathbb{F}(\mathcal{R}(S))$, daí $\mathbb{E}/\mathbb{F}$ é normal.
Todo $\alpha \in \mathcal{R}(S)$ é raiz de um polinômio separável $f \in \mathbb{F}[X]$ (*) Portanto, α é separável sobre $\mathbb{F}$.
Do Corolário 7.7, segue que $\mathbb{E}/\mathbb{F}$ é separável.

(*) $\mathrm{Irr}(\alpha, \mathbb{F}) \mid f \Rightarrow$ daí $\mathrm{Irr}(\alpha, \mathbb{F})$ é separável.

(a) $\Rightarrow$ (b). Como $\mathbb{E}/\mathbb{F}$ é normal, vale que

$$\mathbb{E} = \mathbb{F}(\mathcal{R}(S))$$

para algum $S \subseteq \mathbb{F}[X]$. Seja

$$S' = \{ f \text{ irred.} \mid f \text{ é comp. irr. de algum } g \in S \}.$$

Assim, $\mathbb{E} = \mathbb{F}(\mathcal{R}(S'))$. Se $f \in S'$ não é separável, seja $\alpha \in$ raiz de f. Então

$$\mathrm{Irr}(\alpha, \mathbb{F}) = \alpha f$$

não é separável. Isso contradiz o fato de $\mathbb{E}/\mathbb{F}$ ser separável.

Corolário 7.7. *Sejam $\mathbb{E} = \mathbb{F}(S)$ uma extensão de corpos. Então $\mathbb{E}/\mathbb{F}$ é separável se, e somente se, todo $a \in S$ é separável sobre $\mathbb{F}$.*

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.*

Seja $a \in \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \dots)$. Então, vale que existem $\sqrt{2}, \sqrt{3}, \dots, \sqrt{p_m}$ tais que

$$a \in \mathbb{Q}(\sqrt{2}, \sqrt{3}, \dots, \sqrt{p_m}).$$

Como $\mathbb{Q}(\sqrt{2}, \dots, \sqrt{p_m})/\mathbb{Q}$ é algébrica, segue que a é alg. sobre $\mathbb{Q}$.

Exemplos.

(1) $\mathbb{C}/\mathbb{R}$. Temos que

$$\mathbb{R} = \{x \in \mathbb{C} \mid \overline{x} = x\}$$

A conj. complexa é um $\mathbb{R}$-automorfismo de $\mathbb{C}$.

$\mathbb{E}/\mathbb{F}$ gal. e fin $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, $\mathbb{F} = \{x \in \mathbb{E} \mid \sigma(x) = x, \forall \sigma\}$

(2) $a \in \mathbb{C}$. Se $a \notin \mathbb{R}$, então, defina

$$f(X) = (X - a)(X - \bar{a}) =$$

$$= X^2 - (a + \bar{a})X + a \cdot \bar{a} \in \mathbb{R}[X]$$

$$\overline{a + \bar{a}} = \bar{a} + \bar{\bar{a}} = \bar{a} + a = a + \bar{a} \in \mathbb{R}$$

$$\overline{a \cdot \bar{a}} = \bar{a} \cdot \bar{\bar{a}} = \bar{a} \cdot a = a \cdot \bar{a} \in \mathbb{R}$$