# $3^{\underline{a}}$ Lista de Exercícios: Anéis e Corpos

**1.** Quais das seguintes extensões $F \subseteq K$ são separáveis :

a) um corpo de raízes $K$ de polinomio $X^7 + X^5 + X^2 + 1$ sobre o corpo $F$, onde $F$ tem 25 elementos;

b) um corpo de raízes $K$ de polinômio $X^5 + X + 5$ sobre o corpo $F$ de característica 0.

**2.** Decidir em cada caso abaixo se as extensões são normais sobre $\mathbb{Q}$ e em cada caso encontre $Aut_{\mathbb{Q}}(K)$.

a) $K = \mathbb{Q}(\sqrt[2]{2}, \sqrt[2]{3})$ b) $K = \mathbb{Q}(\sqrt[5]{7})$ c) $K = \mathbb{Q}(\sqrt[4]{2}, i)$

d) $K = \mathbb{Q}(\alpha)$ tal que $\alpha$ é raiz de um polinômio, de $\mathbb{Q}[X]$, de grau 2.

**3.** Encontrar um elemento primitivo para as extensões $\mathbb{Q} \subseteq K$:

a) $K = \mathbb{Q}(\alpha, \beta)$ onde $\alpha \neq \beta$ são raízes de $x^3 - 2$;

b) $K$ é o corpo de raízes de $f = x^4 - 2$ sobre $\mathbb{Q}$.

**4.** Mostrar que:

a) Se $p \in \mathbb{N}$ é número primo, $\mathbb{Z}_p$ é o corpo com $p$ elementos e $k$ é um corpo com $ch(k) = p$ então: $[k : \mathbb{Z}_p] = n$ com $n \in \mathbb{N}$ se e somente se $\sharp(k) = p^n$.

b) Se $k$ é corpo finito então existem $p$, $n \in \mathbb{N}$, com $p$ primo tais que $\sharp(k) = p^n$.

c) Se $k \subseteq L$ é uma extensão de corpos e $L$ é finito então existem $p$, $m$, $n \in \mathbb{N}$, com $p$ primo satisfazendo $\sharp(L) = p^m$, $\sharp(k) = p^n$ e $n$ divide $m$.

d) Exibir dois corpos $L$ e $k$ satisfazendo $\sharp(L) = 27$ e $\sharp(k) = 9$. Explicar porque $L$ não contem um corpo que é isomorfo a $k$.

**5.** Sejam $k$ um corpo finito com $q = p^n$ elementos e $L \mid k$ uma extensão de grau $m$.

a) $\sharp(L) =?$

b) Mostre que: $L \mid k$ é galoisiana e que $G = Gal(L/k)$ é cíclico gerado por $\sigma$ definido por: $\sigma(\alpha) = \alpha^q$ para todo $\alpha \in L$ (primeiro verifique que de fato $\sigma \in G$).

**6.** Sejam $k \subseteq K \subseteq \Omega$ extensões de corpos, com característica 0, $k \subseteq K$ extensão algébrica e $\Omega$ algebricamente fechado. Mostrar que:

a)Se $K = k(\alpha_1, \dots, \alpha_m)$ então $\sharp(Hom_k(K, \Omega)) = [K : k] = n$

b) Se $Hom_k(K, \Omega) = \{\sigma_1, \dots, \sigma_n\}$ e $\alpha \in K$ é tal que $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ se $i \neq j$ então $K = k(\alpha)$

c) Se $\Omega = \mathbb{C}$, $K = \mathbb{Q}(\alpha, \xi)$, onde $\alpha = \sqrt[3]{2}$ e $\xi = e^{\frac{2\pi i}{3}}$ e $\beta = \alpha + \xi$ então $K = \mathbb{Q}(\beta)$.

**7.** Seja $K$ um corpo de característica 0, $f$ um polinômio irredutível em $K[X]$ e $F$ um corpo de raízes de $f$ sobre $K$.

a) Mostrar que $G = Gal(F \mid K)$ age transitivamente sobre as raízes de $f$ isto é, para quaisquer duas raízes $\alpha$ e $\beta$ de $f$ em $F$ existe $\sigma \in G$ tal que $\sigma(\alpha) = \beta$.

b) Se $\deg f = n$, mostrar que podemos considerar $G \leq S_n$, o grupo simétrico de grau $n$.

c) Mostrar que o recíproco de (a) também vale: se $G \leq S_n$ age transitivamente sobre as raízes de $f$ então $f$ é irredutível sobre $K$.

d) Mostrar que se $f$ é irredutível sobre $K$ e $\deg f = n$, então $n$ divide $|G|$. (Já vimos em (b) que $|G|$ divide $n!$.)

**8.** Seja $p$ um primo, $f \in \mathbb{Q}[X]$ um polinômio irredutível sobre $\mathbb{Q}$ e $\deg f = p$. Seja $K$ o corpo de raízes de $f$ (como subcorpo de $\mathbb{C}$). Se $f$ tem duas raízes complexas não reais e $p-2$ raízes reais, mostrar que o grupo de Galois $G = Gal(K \mid \mathbb{Q}) \cong S_p$, o grupo simétrico de ordem $p$. (Dica: Mostrar que a conjugação complexa é um automorfismo não trivial e de ordem 2 de $K$, e que $G \leq S_p$ contém elementos de ordem $p$, isto é, $p$-ciclos.)

**9.** Seja $K$ o corpo de raízes de $f = x^3 - 2$ sobre $\mathbb{Q}$ e $G = Gal(K \mid \mathbb{Q})$. Calcular $G$, todos subgrupos de $G$ e todos subcorpos $\mathbb{Q} \subseteq F \subseteq K$.

**10.** Sejam $p_1, \ldots, p_n$ números primos positivos e distintos. Seja $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Mostrar que:

a) $\mathbb{Q} \subseteq L$ é uma extensão galoisiana.

b) Se $G = Gal(L/\mathbb{Q})$ então $G \simeq \mathbb{Z}_2^n$ (Dica: indução sobre $n$.)

c) Encontrar todos os subcorpos intermediários $K$ tais que $[K : \mathbb{Q}] = 2$

**11.** Sejam $F \subseteq L_1$ e $F \subseteq L_2$ duas extensões finitas e galosianas, com $L_1$ e $L_2$ subcorpos de um mesmo corpo algebricamente fechado $\Omega$. Consideramos $G_1 = Gal(L_1/F)$ e $G_2 = Gal(L_2/F)$. Mostrar que:

a) $L = L_1 \cdot L_2$ é extensão galoisiana de $F$.

b) Se $G = Gal(L/F)$ e $\varphi\colon G \longrightarrow G_1 \times G_2$ é dada por $\varphi(\sigma) = (\sigma_{L_1}, \sigma_{L_2})$ então:

$b_1$) $\varphi$ é um homomorfismo injetor de grupos.

$b_2$) Se $L_1 \cap L_2 = F$ então $\varphi$ é isomorfismo de grupos.

**12.** Seja $F \subseteq K$ uma extensão galoisiana de corpos com $G = Gal(K \mid F)$ um grupo finito abeliano. Mostrar que se $F \subseteq E \subseteq K$ é algum corpo intermediário então a extensão $F \subseteq E$ é galoisiana.