MAT0364/MAT6643 - Teoria de Galois (2021)

Lista 1

(1) Prove que $\mathbb{Q}[\sqrt{3}, i] = \mathbb{Q}[\sqrt{3} + i]$. Calcule $[\mathbb{Q}[\sqrt{3}, i] : \mathbb{Q}]$.

(2) Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $\alpha_1, \ldots, \alpha_m \in \mathbb{E}$. Prove que

$$\mathbb{F}[\alpha_1, \ldots, \alpha_m] = \{f(\alpha_1, \ldots, \alpha_m) \mid f(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]\}.$$

(3) Sejam $\mathbb{E}/\mathbb{F}$ extensão de corpos e $S \subseteq \mathbb{E}$. Prove que a intersecção de uma família arbitrária de subcorpos de $\mathbb{E}$ é corpo. Prove que

$$\mathbb{F}(S) = \bigcap_{\substack{\mathbb{L} \subseteq \mathbb{E} \text{ corpo} \\ \mathbb{F}, S \subseteq \mathbb{L}}} \mathbb{L}.$$

(4) Considere o subcorpo $\mathbb{Q}(u) \subseteq \mathbb{C}$, em que $u^3 - u^2 + u + 2 = 0$. Expresse $(u^2 + u + 1)(u^2 - u)$ e $(u - 1)^{-1}$ na forma $au^2 + bu + c$, com $a, b, c \in \mathbb{Q}$.

(5) Seja $\mathbb{F}$ um corpo finito. Prove que existem $p, m \in \mathbb{N}$, com p primo, de modo que $\mathbb{F}$ tem exatamente p^m elementos.

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

(7) Seja $\mathbb{F}/\mathbb{Q}$ uma extensão de corpos com $[\mathbb{F} : \mathbb{Q}] = 2$. Prove que existe $d \in \mathbb{Z}$ de modo que $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$.

(8) Sejam $\mathbb{K}/\mathbb{F}$ uma extensão de corpos, e $\mathbb{E}_1, \mathbb{E}_2$ corpos de modo que $\mathbb{F} \subseteq \mathbb{E}_i \subseteq \mathbb{K}$. Assuma que $[\mathbb{E}_i : \mathbb{F}] < \infty$, para $i = 1, 2$. Seja $\mathbb{E}$ o subcorpo de $\mathbb{K}$ gerado por $\mathbb{E}_1$ e $\mathbb{E}_2$ (isto é, o menor subcorpo de $\mathbb{K}$ contendo $\mathbb{E}_1$ e $\mathbb{E}_2$). Prove que $[\mathbb{E} : \mathbb{F}] \leq [\mathbb{E}_1 : \mathbb{F}][\mathbb{E}_2 : \mathbb{F}]$.

(9) Encontre o polinômio minimal sobre $\mathbb{Q}$ dos seguintes elementos de $\mathbb{C}$:
   (a) $\dfrac{\sqrt{5} + 1}{2}$,
   (b) $\sqrt{3 - \sqrt{6}}$,
   (c) $\sqrt{2} + i$,
   (d) $\sqrt{p}$, em que $p \in \mathbb{Z}$, $p > 0$, é um número primo.

(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) $\mathbb{F} = \mathbb{Q}[i]$.

(11) Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica. Seja $\mathcal{R}$ um anel com $\mathbb{F} \subseteq \mathcal{R} \subseteq \mathbb{E}$. Prove que $\mathcal{R}$ é um corpo.

(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 $[\mathbb{E}[a] : \mathbb{E}] \leq [\mathbb{F}[a] : \mathbb{F}]$.

(13) Seja $\mathbb{K} = \mathbb{F}(u)$, em que u é transcendental sobre $\mathbb{F}$. Seja $\mathbb{E} \subseteq \mathbb{K}$ um subcorpo, com $\mathbb{F} \neq \mathbb{E}$. Prove que u é algébrico sobre $\mathbb{E}$.

(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 $u \in \mathbb{E}$.

(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.

(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 $\mathbb{E}$.

(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 $\operatorname{mdc}([\mathbb{E} : \mathbb{F}], \operatorname{gr}(f)) = 1$, então f é irredutível sobre $\mathbb{E}$.

(18) Sejam $\mathbb{E}/\mathbb{F}$ uma extensão de corpos, e $u, v \in \mathbb{E}$ elementos algébricos sobre $\mathbb{F}$. Denote por $m = [\mathbb{F}[u] : \mathbb{F}]$ e $n = [\mathbb{F}[v] : \mathbb{F}]$.
 (a) Mostre que, se $\operatorname{mdc}(m, n) = 1$, então $\operatorname{Irr}(v, \mathbb{F})$ (o polinômio minimal de v sobre $\mathbb{F}$) é irredutível sobre $\mathbb{F}[u]$. Conclua que, se $\operatorname{mdc}(m, n) = 1$, então $[\mathbb{F}[u, v] : \mathbb{F}] = mn$.
 (b) Calcule $[\mathbb{Q}[\sqrt{2}, \sqrt[3]{5}] : \mathbb{Q}]$.

(19) Determine o grau da extensão $[\mathbb{F} : \mathbb{Q}]$, em que:
 (a) $\mathbb{F} = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$,
 (b) $\mathbb{F} = \mathbb{Q}(\sqrt{18}, \sqrt[4]{2})$,
 (c) $\mathbb{F} = \mathbb{Q}(\sqrt{8}, 3 + \sqrt{50})$,
 (d) $\mathbb{F} = \mathbb{Q}(\sqrt[3]{2}, u)$, em que $u^4 + 6u + 2 = 0$.

(20) Determine se o polinômio $f \in \mathbb{F}[X]$ é irredutível sobre $\mathbb{F}$, em que:
 (a) $f = X^2 + 3$, e $\mathbb{F} = \mathbb{Q}[\sqrt{5}]$,
 (b) $f = X^3 + 8X - 2$, e $\mathbb{F} = \mathbb{Q}[\sqrt{2}]$,
 (c) $f = X^5 + 3X^3 - 9X - 6$, e $\mathbb{F} = \mathbb{Q}[\sqrt{7}, \sqrt{5}, i]$.