MAT0364/MAT6643 - Teoria de Galois (2021)

Lista 3

(1) Determine $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$, em que:
   (a) $\mathbb{E} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{F} = \mathbb{Q}$.
   (b) $\mathbb{F} = \mathbb{Q}$ e $\mathbb{E}$ é o corpo de raízes de $X^n - 2$ sobre $\mathbb{Q}$.

(2) Sejam $p_1, \ldots, p_n \in \mathbb{Z}_{>0}$ primos distintos. Prove que

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong \underbrace{C_2 \times \cdots \times C_2}_{n \text{ vezes}},$$

   em que C_2 denota o grupo cíclico de ordem 2

(3) Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita em que $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é um grupo abeliano. Prove que, dado qualquer corpo $\mathbb{K}$, com $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$, a extensão $\mathbb{K}/\mathbb{F}$ é galoisiana.

(4) Seja $\mathbb{E}/\mathbb{F}$ uma extensão separável de modo que existe n tal que $[\mathbb{F}(a) : \mathbb{F}] \leq n$, $\forall a \in \mathbb{E}$. Prove que $\mathbb{E}/\mathbb{F}$ é uma extensão finita, e que $[\mathbb{E} : \mathbb{F}] \leq n$.

(5) Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana finita tal que $[\mathbb{E} : \mathbb{F}] = p^n m$, em que p não divide m. Mostre que existe um corpo $\mathbb{K}$, com $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$, tal que $[\mathbb{K} : \mathbb{F}] = m$.

(6) Seja $\mathbb{E}/\mathbb{F}$ uma extensão galoisiana tal que $[\mathbb{E} : \mathbb{F}] = p^2 q$, em que p e q são primos, $q < p$ e q não divide $p^2 - 1$. Mostre que:
   (a) Existem subcorpos intermediários $\mathbb{K}_1, \mathbb{K}_2$, tais que $\mathbb{K}_1/\mathbb{F}$ e $\mathbb{K}_2/\mathbb{F}$ são galoisianas, $[\mathbb{K}_1 : \mathbb{F}] = p^2$ e $[\mathbb{K}_2 : \mathbb{F}] = q$.
   (b) Prove que $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ é abeliano.

(7) Sejam $\mathbb{F}$ um corpo, $f \in \mathbb{F}[X]$ de grau positivo, e $\mathbb{L} = \mathbb{F}(\mathscr{R}(f))$. Dizemos que $\mathrm{Aut}(\mathbb{L}/\mathbb{F})$ age transitivamente nas raízes de f se, para quaisquer $u, v \in \mathscr{R}(f)$, existe $\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F})$ tal que $\sigma(u) = v$. Prove que as seguintes afirmações são equivalentes:
   (a) $\mathrm{Aut}(\mathbb{E}/\mathbb{F})$ age transitivamente no conjunto das raízes de f,
   (b) Existem $\alpha \in \mathbb{F}$, $m \in \mathbb{N}$ e $g \in \mathbb{F}[X]$ irredutível tais que $f = \alpha g^m$.

(8) Seja $\mathbb{F}$ um corpo finito e $n \in \mathbb{N}$. Prove que existe $f \in \mathbb{F}[X]$ irredutível de grau n.

(9) Sejam $\mathbb{F}_q$ e $\mathbb{F}_{q'}$ subcorpos do fecho algébrico de $\mathbb{F}_p$, em que $q = p^m$, $q' = p^{m'}$. Prove que $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ se, e somente se, q divide q'.

(10) Fixe p um primo e $n \in \mathbb{N}$, e seja $S = \{f(X) \in \mathbb{F}_p[X]$ mônico e irredutível, $\mathrm{gr}(f)$ divide $n\}$. Prove que

$$\prod_{f(X) \in S} f(X) = X^{p^n} - X.$$

(11) Seja $\mathbb{F}$ um corpo. Prove que um subgrupo finito $H \subseteq \mathbb{F}^\times$ é cíclico.

(12) Seja $f \in \mathbb{F}[X]$ um polinômio mônico e $\bar{\mathbb{F}}$ o fecho algébrico de $\mathbb{F}$. Assuma que o conjunto $\mathscr{R}(f) = \{a \in \bar{\mathbb{F}} \mid f(a) = 0\}$ constitui um corpo. Prove que $\operatorname{char}\mathbb{F} = p > 0$, e existe $m \in \mathbb{N}$ tal que $f(X) = X^{p^m} - X$.

(13) Prove as seguintes formulas envolvendo o polinômio ciclotômico:
   (a) Seja p primo e $r \geq 1$. Então $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.
   (b) Escreva $n = p_1^{r_1} \cdots p_s^{r_s}$ a decomposição de n em produto de primos, em que $p_i \neq p_j$ se $i \neq j$. Então
   $$\Phi_n(X) = \Phi_{p_1 \cdots p_s}\left(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}}\right).$$
   (c) Se $n > 1$ é ímpar, então $\Phi_{2n}(X) = \Phi_n(-X)$.
   (d) Sejam p primo e $n \in \mathbb{N}$. Se p não divide n, então
   $$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}.$$
   Se p divide n, então $\Phi_{pn}(X) = \Phi_n(X^p)$.

(14) Seja Φ_n o n-ésimo polinômio ciclotômico, para $n > 1$. Prove que
$$\Phi_n(1) = \begin{cases} p, & \text{se } n \text{ é uma potência de um primo } p, \\ 1, & \text{caso contrário} \end{cases}$$

(15) Sejam $n, m \in \mathbb{N}$ primos entre si, e $\xi_n \in \mathcal{P}_n(\mathbb{C})$ e $\xi_m \in \mathcal{P}_m(\mathbb{C})$ uma n-raiz e uma m-raiz primitiva da unidade, respectivamente. Prove que $\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}$. Prove que $\mathbb{Q}(\xi_n) \cdot \mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_{mn})$, em que $\xi_{mn} \in \mathcal{P}_{mn}(\mathbb{C})$.

(16) Sejam $p \in \mathbb{N}$ primo e $\mathbb{L} = \mathbb{Q}(\mathscr{R}(X^p - 2))$. Prove que:
   (a) $[\mathbb{L} : \mathbb{Q}] = p(p-1)$.
   (b) Existe exatamente um subcorpo $\mathbb{E} \subseteq \mathbb{L}$ tal que $[\mathbb{E} : \mathbb{Q}] = p-1$, e de modo que $\mathbb{E}/\mathbb{Q}$ é galoisiana.

(17) Fixe $n \in \mathbb{N}$, e seja $\mathbb{E} = \mathbb{Q}(X_1, \ldots, X_n)$. Para cada $\pi \in \mathcal{S}_n$, defina $\pi : \mathbb{E} \to \mathbb{E}$ via $\pi(X_i) = X_{\pi(i)}$.
   (a) Prove que π está bem definida, e que $\pi \in \operatorname{Aut}(\mathbb{E})$. Portanto, temos um mapa $\mathcal{S}_n \to \operatorname{Aut}(\mathbb{E})$.
   (b) Prove que o mapa $\mathcal{S}_n \to \operatorname{Aut}(\mathbb{E})$ é injetiva. Portanto, podemos identificar $\mathcal{S}_n \subseteq \operatorname{Aut}(\mathbb{E})$.
   (c) Conclua que, se $\mathbb{F} = \mathbb{E}^{\mathcal{S}_n}$, então $\operatorname{Aut}(\mathbb{E}/\mathbb{F}) \cong \mathcal{S}_n$. Conclua que, para todo grupo finito G, existe uma extensão de corpos galoisiana finita $\mathbb{L}/\mathbb{K}$ tal que $G \cong \operatorname{Aut}(\mathbb{L}/\mathbb{K})$.

(18) Seja $p \geq 5$ um número primo e $f(X) \in \mathbb{Q}[X]$ irredutível de grau p. Assuma que f tenha exatamente duas raízes não reais em $\mathbb{C}$. Seja $\mathbb{L}$ o corpo de raízes de f sobre $\mathbb{Q}$. Prove que $\operatorname{Aut}(\mathbb{L}/\mathbb{Q}) \cong \mathcal{S}_p$. Conclua que f não é solúvel por radicais.