Resolução Prova 2 de Álgebra 3 - 2019-2

(1) (3 pontos) Para cada um dos polinômios $f(X)$ seguintes seja M um corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ e seja $G := \mathscr{G}(M/\mathbb{Q})$ o grupo de Galois de $M/\mathbb{Q}$. Encontre a estrutura de G.

(a) (1 ponto) $f(X) = X^3 - 1$.

$f(X) = (X-1)(X^2+X+1)$ logo $M = \mathbb{Q}(\alpha)$ onde α é raiz de X^2+X+1, por exemplo podemos escolher $\alpha = -1/2 + i\sqrt{3}/2$. Segue que $M = \mathbb{Q}(i\sqrt{3})$ logo $|G| = |M:\mathbb{Q}| = 2$ e G é um grupo cíclico de ordem 2.

(b) (1 ponto) $f(X) = X^4 - 3X^2 + 2$.

Chamando $T = X^2$ e resolvendo a equação $T^2 - 3T + 2 = 0$ obtemos que as suas raizes são 1 e 2, logo $f(X) = (X^2-1)(X^2-2) = (X-1)(X+1)(X^2-2)$. Segue que $M = \mathbb{Q}(\sqrt{2})$ é um corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Sendo $|G| = |M:\mathbb{Q}| = 2$ obtemos que G é um grupo cíclico de ordem 2.

(c) (1 ponto) $f(X) = X^4 - 4X^2 + 2$.

$f(X)$ é irredutível pelo critério de Eisenstein aplicado ao primo 2. Chamando $T = X^2$ e resolvendo a equação $T^2 - 4T + 2 = 0$ obtemos que as suas raizes são $2 \pm \sqrt{2}$. Segue que as raizes de $f(X)$ são $\pm\alpha$, $\pm\beta$ onde $\alpha = \sqrt{2+\sqrt{2}}$ e $\beta = \sqrt{2-\sqrt{2}}$. Temos

$$\alpha\beta = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{2} = \alpha^2 - 2$$

logo $\beta = (\alpha^2-2)/\alpha \in \mathbb{Q}(\alpha)$, segue que $M = \mathbb{Q}(\alpha)$ logo $|G| = |M:\mathbb{Q}| = 4$ sendo $f(X)$ irredutível sobre $\mathbb{Q}$. Como $f(X)$ é irredutível a ação de G sobre o conjunto das 4 raizes de $f(X)$ é transitiva, logo existe $g \in G$ tal que $g(\alpha) = \beta$, daí $g(\sqrt{2}) = g(\alpha^2-2) = \beta^2 - 2 = -\sqrt{2}$ logo $g(\beta) = g(\sqrt{2}/\alpha) = -\sqrt{2}/\beta = -\alpha$, $g(-\alpha) = -g(\alpha) - \beta$, $g(-\beta) = -g(\beta) = -(-\alpha) = \alpha$ e g tem estrutura cíclica $(\alpha, \beta, -\alpha, -\beta)$. Como $|G| = 4$ segue que $G = \langle g \rangle$ é cíclico.

(2) (1 ponto) Descreva as correspondências de Galois para $M/\mathbb{Q}$ onde M é corpo de decomposição sobre $\mathbb{Q}$ para $f(X) = X^4 - 4X^2 + 2$.

Os subgrupos de $G = \langle g \rangle$ são $\{1\}$, $\langle g^2 \rangle = \{1, g^2\}$ e $G = \langle g \rangle$. Precisamos encontrar $\langle g^2 \rangle'$. Mas g^2 tem estrutura cíclica $(\alpha, -\alpha)(\beta, -\beta)$ logo é claro que $g^2(\alpha^2) = (-\alpha)^2 = \alpha^2$, ou seja $\alpha^2 \in \langle g^2 \rangle'$. Segue que $\mathbb{Q}(\alpha^2) \subseteq \langle g^2 \rangle'$. Por outro lado $\alpha^2 = 2 + \sqrt{2}$ logo $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$, e

$|\langle g^2\rangle' : \mathbb{Q}| = |G : \langle g^2\rangle| = 2$, logo $\langle g^2\rangle' = \mathbb{Q}(\alpha^2)$. As correspondências de Galois são então as seguintes (as setas são inclusões).

$$\begin{array}{ccc} \{1\} & & M \\ \downarrow 2 & & \uparrow 2 \\ \langle g^2\rangle & & \mathbb{Q}(\sqrt{2}) \\ \downarrow 2 & & \uparrow 2 \\ G & & \mathbb{Q} \end{array}$$

(3) (1 ponto) Seja $G = \mathscr{G}(M/\mathbb{Q})$ o grupo de Galois de $M/\mathbb{Q}$ onde M é corpo de decomposição de $f(X) = X^4 - 4X^2 + 2$ sobre $\mathbb{Q}$. Sejam α, β raizes de $f(X)$ em M tais que $\gamma := \alpha + \beta \neq 0$. Calcule a norma

$$N_{M/\mathbb{Q}}(\gamma) = \prod_{g\in G} g(\gamma).$$

Podemos escolher os mesmos α e β definidos acima. Segue que

$$\begin{aligned} N(\alpha+\beta) &= (\alpha+\beta)g(\alpha+\beta)g^2(\alpha+\beta)g^3(\alpha+\beta) \\ &= (\alpha+\beta)(\beta-\alpha)(-\alpha-\beta)(-\beta+\alpha) \\ &= (\alpha+\beta)^2(\alpha-\beta)^2 = (\alpha^2-\beta^2)^2 \\ &= (2+\sqrt{2}-(2-\sqrt{2}))^2 = (2\sqrt{2})^2 = 8. \end{aligned}$$

(4) (2 pontos) Seja M/K extensão de Galois com grupo de Galois $G = \langle\sigma\rangle \cong C_3$. Defina o traço de um elemento $\alpha \in M$ como sendo

$$T(\alpha) = T_{M/K}(\alpha) = \sum_{g\in G} g(\alpha).$$

Seja $a \in M$ e suponha $T(a) = 0$.

(a) (0.5 ponto) Calcule $T(1)$.
$T(1) = 1 + \sigma(1) + \sigma^2(1) = 1 + 1 + 1 = 3$.

(b) (0.5 ponto) Mostre que existe $c \in M$ tal que $T(c) = 1$.
$T(1/3) = 1/3 + \sigma(1/3) + \sigma^2(1/3) = 1/3 + 1/3 + 1/3 = 1$.

(c) (1 ponto) Seja $b := ac + a\sigma(c) + \sigma(ac)$. Mostre que $b - \sigma(b) = a$.

$$\begin{aligned} b - \sigma(b) &= ac + a\sigma(c) + \sigma(ac) - \sigma(a)\sigma(c) - \sigma(a)\sigma^2(c) - \sigma^2(ac) \\ &= ac + a\sigma(c) - \sigma(a)\sigma^2(c) - \sigma^2(a)\sigma^2(c) \\ &= a(T(c) - \sigma^2(c)) - \sigma^2(c)(T(a) - a) \\ &= a - a\sigma^2(c) + a\sigma^2(c) = a. \end{aligned}$$

(5) (3 pontos) Seja M/K uma extensão de Galois finita.

(a) (1 ponto) Se $M \neq K$ e os únicos subcorpos de M contendo K são M e K, $|M : K|$ é um número primo?

Sim. Seja $G := \mathscr{G}(M/K)$, de ordem $|G| = |M : K| > 1$, e seja $g \in G$ de ordem prima p (existe pelo teorema de Cauchy). Seja $L := \langle g \rangle'$. Então $|M : L| = |\langle g \rangle : \{1\}| = p \neq 1$ logo $L \neq M$. Pela hipótese segue que $L = K$ logo $|M : K| = |M : L| = p$.

(b) (1 ponto) Se $|M : K| = 15$, existe sempre um subcorpo L de M tal que $K < L < M$ e tal que L/K é extensão de Galois?

Sim. Seja $G := \mathscr{G}(M/K)$, então $|G| = |M : K| = 15$ logo o 5-Sylow P de G é normal em G, segue que $L := P' \leq M$ é extensão de Galois de K e $K < L < M$ sendo $5 = |P| = |P : \{1\}| = |M : L|$.

(c) (1 ponto) Se M é corpo de decomposição sobre K para um polinômio $f(X) \in K[X]$, o grau de $f(X)$ divide $|M : K|$?

Não, por exemplo $X^3 - 1 = (X - 1)(X^2 + X + 1)$ tem corpo de decomposição igual a $\mathbb{Q}(i\sqrt{3})$, de grau 2 sobre $\mathbb{Q}$.