Segunda prova **ÁLGEBRA 3** **Resolução**

Aqui n é um inteiro tal que $2 < n \equiv 2 \mod 4$.

1. (4 pontos) Determine as correspondências de Galois para $M/\mathbb{Q}$ onde M é corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ nos seguintes casos.

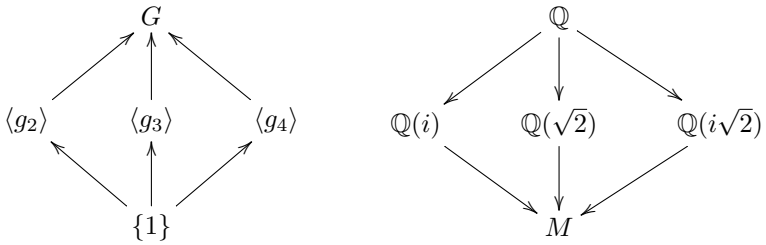
   (a) (1 ponto) $f(X) = X^3 + X^2 - n^2X - n^2$. [Redutível]
   Temos

   $$\begin{aligned} f(X) &= X^2(X+1) - n^2(X+1) = (X^2 - n^2)(X+1) \\ &= (X-n)(X+n)(X+1) \end{aligned}$$

   tem grupo de Galois trivial $\{1\}$ e o seu corpo de decomposição é $\mathbb{Q}$.

   (b) (1.5 ponto) $f(X) = X^4 - nX^2$. [Redutível]
   $f(X) = X^2(X^2 - n)$. O seu corpo de decomposição é $M = \mathbb{Q}(\sqrt{n})$, que tem grau 2 sobre $\mathbb{Q}$. Segue que o grupo de Galois G tem ordem 2, logo os seus subgrupos são $\{1\}$ e G, que correspondem aos subcorpos M e $\mathbb{Q}$ respectivamente.

   (c) (1.5 ponto) $f(X) = (X-n)(X^5 - 4X)$.
   $f(X) = (X-n)X(X^2-2)(X^2+2)$ tem corpo de decomposição $M = \mathbb{Q}(i, \sqrt{2})$, logo $|G| = |M : \mathbb{Q}| = 4$ e $G = \{g_1, g_2, g_3, g_4\}$. Temos $g_j(i) = \pm i$ e $g_j(\sqrt{2}) = \pm\sqrt{2}$, isso determina no máximo 4 possibilidades para cada g_j, por outro lado $|G| = 4$ logo cada possibilidade ocorre. Os elementos são determinados por $g_1(i) = i$, $g_1(\sqrt{2}) = \sqrt{2}$, $g_2(i) = i$, $g_2(\sqrt{2}) = -\sqrt{2}$, $g_3(i) = -i$, $g_3(\sqrt{2}) = \sqrt{2}$, $g_4(i) = -i$, $g_4(\sqrt{2}) = -\sqrt{2}$ e a situação é então a seguinte.



2. (3 pontos) Seja $\alpha \in \mathbb{C}$ uma raiz de $f(X) = X^3 - 7X + 7$.

   (a) (1 ponto) Mostre que $\mathbb{Q}(\alpha)/\mathbb{Q}$ é uma extensão de Galois.
   O discriminante é $-4(-7)^3 - 27 \cdot 7^2 = 7^2 \cdot (4 \cdot 7 - 27) = 7^2$, é um quadrado em $\mathbb{Q}$, logo o grupo de Galois de $f(X)$ é isomorfo a A_3 logo o corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ tem grau 3. Mas contém $\mathbb{Q}(\alpha)$, que tem grau 3, logo é igual a $\mathbb{Q}(\alpha)$, ou seja $\mathbb{Q}(\alpha)/\mathbb{Q}$ é extensão de Galois.

(b) (1 ponto) Seja $G = \mathscr{G}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{g_1, g_2, g_3\}$. Calcule

$$N(\alpha) = g_1(\alpha) \cdot g_2(\alpha) \cdot g_3(\alpha).$$

[Dica: avalie $(X - g_1(\alpha)) \cdot (X - g_2(\alpha)) \cdot (X - g_3(\alpha))$ em $X = 0$.]
Temos $f(X) = X^3 - 7X + 7 = (X - g_1(\alpha))(X - g_2(\alpha))(X - g_3(\alpha))$ logo $N(\alpha) = -f(0) = -7$.

(c) (1 ponto) Calcule $T(\alpha) = g_1(\alpha) + g_2(\alpha) + g_3(\alpha)$.
Sejam $\alpha_i := g_i(\alpha)$, $i = 1, 2, 3$. Temos

$$X^3 - 7X + 7 = f(X) = (X - \alpha_1) \cdot (X - \alpha_2) \cdot (X - \alpha_3)$$
$$= X^3 - (\alpha_1 + \alpha_2 + \alpha_3)X^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)X - \alpha_1\alpha_2\alpha_3,$$

e igualando os coeficientes obtemos $T(\alpha) = 0$.

3. (2 pontos) Seja m um inteiro positivo impar e sejam

$$f(X) = X^4 + mX + m, \qquad R(X) = X^3 - 4mX - m^2.$$

O polinômio $f(X)$ é irredutível em $\mathbb{Q}[X]$ (sendo a sua redução módulo 2 irredutível em $\mathbb{F}_2[X]$) e $R(X)$ é a sua resolvente cúbica. Seja $\alpha \in \mathbb{C}$ uma raiz de $f(X)$. 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 $M/\mathbb{Q}$.

(a) (1 ponto) Mostre que se $m = 5$ a extensão $\mathbb{Q}(\alpha)/\mathbb{Q}$ é de Galois.
[Procure uma fatoração $f(X) = (X^2 + \sqrt{5}X + r)(X^2 - \sqrt{5}X + s)$.]
Temos $R(5) = 0$ e $R(X) = (X-5)(X^2+5X+5)$. As raízes de $R(X)$ são 5, $(-5 \pm \sqrt{5})/2$. Segue que $\mathbb{Q}(\sqrt{5})$ é um corpo de decomposição de $R(X)$ sobre $\mathbb{Q}$. Seguindo a dica, temos as condições $s - 5 + r = 0$, $\sqrt{5}(s - r) = 5$, $rs = 5$. Segue que $r(5 - r) = 5$ ou seja $r^2 - 5r + 5 = 0$ e resolvendo $r = (5 \pm \sqrt{5})/2$. Obtemos a solução $r = (5 - \sqrt{5})/2$, $s = (5 + \sqrt{5})/2$ e

$$f(X) = (X^2 + \sqrt{5}X + (5 - \sqrt{5})/2) \cdot (X^2 - \sqrt{5}X + (5 + \sqrt{5})/2).$$

Logo $G \cong C_4$. Segue que $|G| = 4 = |\mathbb{Q}(\alpha) : \mathbb{Q}|$, logo $\mathbb{Q}(\alpha)$ é corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ e $\mathbb{Q}(\alpha)/\mathbb{Q}$ é Galois.

(b) (1 ponto) Se $m = 7$, $R(X)$ é irredutível em $\mathbb{Q}[X]$. Neste caso, a extensão $\mathbb{Q}(\alpha)/\mathbb{Q}$ é de Galois?
O polinômio $R(X) = X^3 - 28X - 49$ é irredutível em $\mathbb{Q}[X]$, logo o grupo de Galois de $f(X)$ é A_4 ou S_4. Segue que $|M : \mathbb{Q}| = |G| \in \{|A_4|, |S_4|\} = \{12, 24\}$ logo $|M : \mathbb{Q}| \neq 4 = |\mathbb{Q}(\alpha) : \mathbb{Q}|$. Segue que $\mathbb{Q}(\alpha)$ não é corpo de decomposição sobre $\mathbb{Q}$ do polinômio minimal de α, logo $\mathbb{Q}(\alpha)/\mathbb{Q}$ não é extensão de Galois.

4. (1 ponto) Seja M um corpo de decomposição sobre $\mathbb{Q}$ do polinômio $f(X) \in \mathbb{Q}[X]$, irredutível em $\mathbb{Q}[X]$. Seja n o grau de $f(X)$ e sejam $\alpha_1, \ldots, \alpha_n$ as raízes de $f(X)$ em M. Diga se a seguinte frase é sempre verdadeira: "se $\mathbb{Q}(\alpha_1), \ldots, \mathbb{Q}(\alpha_n)$ são dois a dois distintos então $|M : \mathbb{Q}| = n!$".

   [Dica: considere os subgrupos correspondentes $\mathbb{Q}(\alpha_i)'$.]

   Aplicando as correspondências, a pergunta é se o fato que os estabilizadores das n raízes em $G = \mathscr{G}(M/\mathbb{Q})$ (que é isomorfo a um subgrupo de S_n) são dois a dois distintos implica que $|G| = n!$, ou seja $G \cong S_n$. A resposta é não, por exemplo vimos que existem polinômios irredutíveis de grau 4 com grupo de Galois isomorfo a A_4. Os estabilizadores dos 4 pontos em A_4 são $\mathrm{Stab}_{A_4}(1) = \langle(234)\rangle$, $\mathrm{Stab}_{A_4}(2) = \langle(134)\rangle$, $\mathrm{Stab}_{A_4}(3) = \langle(124)\rangle$, $\mathrm{Stab}_{A_4}(4) = \langle(123)\rangle$, dois a dois distintos, mas $|A_4| = 12 \neq 4! = 24$.