**Resolução da segunda prova de álgebra 3 - 2018-2**

1. Descreva as correspondências de Galois entre $M/\mathbb{Q}$ e o seu grupo de Galois $G = \mathscr{G}(M/\mathbb{Q})$ onde $M$ é o corpo de decomposição contido em $\mathbb{C}$ de $f(X)$ nos casos seguintes.

   (a) (1.5 ponto) $f(X) = X^2 + 2$ (é irredutível). As raízes são $\alpha = i\sqrt{2}$ e $-\alpha$, logo o corpo de decomposição é $\mathbb{Q}(\alpha)$, tem grau 2 sobre $\mathbb{Q}$ sendo $f(X)$ irredutível logo $|G| = 2$. Os subgrupos de $G$ são $\{1\}$ e $G$ e temos $\{1\}' = \mathbb{Q}(\alpha)$, $G' = \mathbb{Q}$.

   (b) (1.5 ponto) $f(X) = X^3 - 8$ (não é irredutível). As raízes são 2, $2t$, $2t^2$ onde $t = e^{i2\pi/3}$ logo o corpo de decomposição é $\mathbb{Q}(t)$, tem grau 2 sobre $\mathbb{Q}$ logo $|G| = 2$. Os subgrupos de $G$ são $\{1\}$ e $G$ e temos $\{1\}' = \mathbb{Q}(t)$, $G' = \mathbb{Q}$.

   (c) (2 pontos) $f(X) = X^3 - 4$ (é irredutível).
   $\alpha = \sqrt[3]{4}$, $t = e^{2\pi i/3} = -1/2 + i\sqrt{3}/2$. Sejam $K = \mathbb{Q}$, $M = \mathbb{Q}(\alpha, t)$ o corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ e $G = \mathcal{G}(M/K)$. Se $g \in G$ temos que $g(\alpha)$ é uma raiz de $f(X)$ logo as possibilidades são

   - $g(\alpha) = \alpha$. Neste caso se $g(\alpha t) = \alpha t$ então $\alpha t = g(\alpha t) = g(\alpha)g(t) = \alpha g(t)$ logo $g(t) = t$ e $g$ é a identidade. Se $g(\alpha t) = \alpha t^2$ então $\alpha t^2 = g(\alpha t) = g(\alpha)g(t) = \alpha g(t)$ logo $g(t) = t^2$.
   - $g(\alpha) = \alpha t$. Neste caso se $g(\alpha t) = \alpha$ então $\alpha = g(\alpha t) = g(\alpha)g(t) = \alpha t g(t)$ logo $g(t) = t^2$. Se $g(\alpha t) = \alpha t^2$ então $\alpha t^2 = g(\alpha t) = g(\alpha)g(t) = \alpha t g(t)$ logo $g(t) = t$.
   - $g(\alpha) = \alpha t^2$. Neste caso se $g(\alpha t^2) = \alpha$ então $\alpha = g(\alpha t^2) = g(\alpha)g(t)^2 = \alpha t^2 g(t)^2$ logo $g(t) = t^2$. Se $g(\alpha t^2) = \alpha t$ então $\alpha t = g(\alpha t^2) = g(\alpha)g(t)^2 = \alpha t^2 g(t)^2$ logo $g(t) = t$.

   Segue que os elementos de $G$ são (determinados pela ação nas três raizes e) dados por

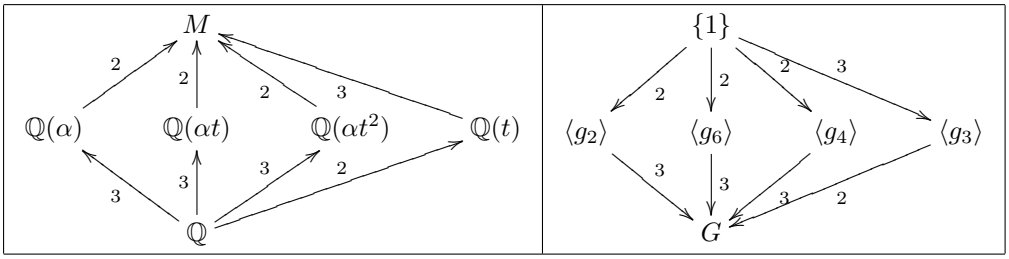
| Elemento | Imagem de $\alpha$ | Imagem de $t$ | Estrutura |
|---|---|---|---|
| $g_1$ | $\alpha$ | $t$ | Identidade |
| $g_2$ | $\alpha$ | $t^2$ | 2-cíclo $(\alpha t, \alpha t^2)$ |
| $g_3$ | $\alpha t$ | $t$ | 3-cíclo $(\alpha, \alpha t, \alpha t^2)$ |
| $g_4$ | $\alpha t$ | $t^2$ | 2-cíclo $(\alpha, \alpha t)$ |
| $g_5$ | $\alpha t^2$ | $t$ | 3-cíclo $(\alpha, \alpha t^2, \alpha t)$ |
| $g_6$ | $\alpha t^2$ | $t^2$ | 2-cíclo $(\alpha, \alpha t^2)$ |

   Como $G \cong S_3$, cada possibilidade ocorre. Observe que $g_1 = 1$. Deduzimos que

   - $\mathbb{Q}' = G$
   - $\mathbb{Q}(\alpha)' = \{g_1, g_2\} = \langle g_2 \rangle$,
   - $\mathbb{Q}(\alpha t)' = \{g_1, g_6\} = \langle g_6 \rangle$,
   - $\mathbb{Q}(\alpha t^2)' = \{g_1, g_4\} = \langle g_4 \rangle$,

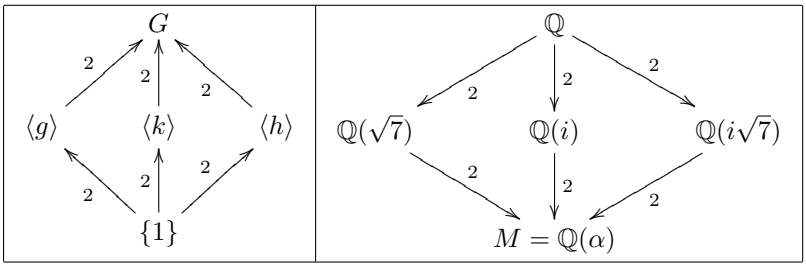
- $\mathbb{Q}(t)' = \{g_1, g_3, g_5\} = \langle g_3 \rangle$.
- $M' = \{1\}$.

Observe que $g_3 g_5 = 1$.




(d) (2 pontos) $f(X) = X^4 - 3X^2 + 4$ (é irredutível).

Sejam $\alpha = \sqrt{\frac{3+\sqrt{-7}}{2}}$, $\beta = \sqrt{\frac{3-\sqrt{-7}}{2}}$. $\alpha\beta = 2$ logo $\beta = 2/\alpha$ e $M = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$ é o corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Segue que $|G| = |M : \mathbb{Q}| = 4$. Existe $g \in G$ que leva $\alpha$ para $\beta$. Temos $g(\beta) = 2/\beta = \alpha$ e $g = (\alpha, \beta)(-\alpha, -\beta)$. Existe $k \in G$ que leva $\alpha$ para $-\beta$. Temos $k(-\beta) = 2\beta = \alpha$ e $k = (\alpha, -\beta)(-\alpha, \beta)$. Existe $h \in G$ que leva $\alpha$ para $-\alpha$. Temos $k(\beta) = -2/\alpha = -\beta$ e $k = (\alpha, -\alpha)(\beta, -\beta)$. Uma conta mostra que $\alpha^{-1} = -\frac{1}{4}(\alpha^3 - 3\alpha)$, $\alpha^{-2} = \frac{1}{4}(3 - \alpha^2)$, $\alpha^{-3} = \frac{1}{16}\alpha(-3\alpha^2 + 5)$. Observe que $(\alpha^3 - \alpha)^2 = -4$ e $(\alpha^3 - 5\alpha)^2 = 28$. Segue que $\langle g \rangle' = \mathbb{Q}(\alpha^3 - 5\alpha) = \mathbb{Q}(i)$, $\langle k \rangle' = \mathbb{Q}(\alpha^3 - \alpha) = \mathbb{Q}(\sqrt{7})$ e $\langle h \rangle' = \mathbb{Q}(\alpha^2) = \mathbb{Q}(i\sqrt{7})$.




2. Seja $M$ o corpo de decomposição contido em $\mathbb{C}$ de $f(X) = X^4 - 3X^2 + 4$ e seja $\alpha \in M$ uma raíz de $f(X)$. Lembre-se que chamando de $G$ o grupo de Galois $\mathscr{G}(M/\mathbb{Q})$ a norma de um elemento $m \in M$ é

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

(a) (1 ponto) Calcule a norma de $\alpha$. $N(\alpha) = \alpha(2/\alpha)(-\alpha)(-2/\alpha) = 4$.

(b) (1 ponto) Calcule a norma de $\alpha + 2/\alpha$. A igualdade $\alpha^4 = 3\alpha^2 - 4$ pode ser escrita $\alpha^2 + 4/\alpha^2 = 3$.

$$\begin{aligned} N(\alpha + 2/\alpha) &= (\alpha + 2/\alpha)(2/\alpha + \alpha)(-\alpha - 2/\alpha)(-2/\alpha - \alpha) \\ &= (\alpha + 2/\alpha)^4 = (\alpha^2 + 4/\alpha^2 + 4)^2 = (3 + 4)^2 = 49. \end{aligned}$$

3. (1 ponto) Seja $f(X)$ um polinômio irredutível de grau 4 e sejam $M$ o corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$ e $\alpha \in M$ uma raíz de $f(X)$. Mostre que se $\mathscr{G}(M/\mathbb{Q}) \cong S_4$ então os únicos subcorpos de $\mathbb{Q}(\alpha)$ são $\mathbb{Q}$ e $\mathbb{Q}(\alpha)$.

   Por contradição seja $\mathbb{Q} < L < \mathbb{Q}(\alpha)$ um subcorpo diferente de $\mathbb{Q}$ e $\mathbb{Q}(\alpha)$. Como $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 4$ segue que $|L : \mathbb{Q}| = 2$. O subgrupo $L'$ correspondente a $L$ na extensão de Galois $M/\mathbb{Q}$ tem então indice 2 em $G \cong S_4$ e contem $H = \mathbb{Q}(\alpha)'$. Mas $H$ tem índice 4 em $G$ logo é isomorfo a um estabilizador $S_3$ em $S_4$. Sendo $|G : L'| = 2$ segue que $L' \cong A_4$ (o único subgrupo de $S_4$ de índice 2 é $A_4$) logo em $S_4$ obtemos que $A_4$ contem um estabilizador $S_3$, o que é um absurdo (os estabilizadores contêm elementos ímpares, por exemplo eles contêm 2-cíclos).