Lista de Álgebra 3 do dia 5 de abril de 2022.

Todos os corpos considerados contêm $\mathbb{Q}$ como subcorpo.

(1) Seja K um corpo e seja M um corpo de decomposição sobre K de um polinômio de $K[X]$, tal que $|M : K| = 21$. Seja L um corpo tal que $K \leq L \leq M$. Mostre que se $|L : K| = 3$ então L é corpo de decomposição sobre K de um polinômio de $K[X]$.

(2) Seja $f(X) \in \mathbb{Q}[X]$ um polinômio irredutível de grau 3, sejam v_1, v_2, v_3 as suas raízes complexas e seja $M = \mathbb{Q}(v_1, v_2, v_3) \subseteq \mathbb{C}$, corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).
   (a) Se $|M : \mathbb{Q}| = 3$ então $M \subseteq \mathbb{R}$.
   (b) Se $M \subseteq \mathbb{R}$ então $|M : \mathbb{Q}| = 3$.
   (c) Se $|M : \mathbb{Q}| = 6$ e $D = \Delta^2$ é o discriminante de $f(X)$ então uma base de M sobre $\mathbb{Q}$ é $\{1, v_1, v_1^2, \Delta, \Delta v_1, \Delta v_1^2\}$.

(3) Sejam M/K uma extensão de Galois finita, L_1, L_2 corpos com $K \leq L_i \leq M$ para $i = 1, 2$ e $H_1 = L_1'$, $H_2 = L_2'$ os correspondentes subgrupos de $G = \mathscr{G}(M/K)$ (pelas correspondências de Galois). Mostre que
   (a) $(L_1 \cap L_2)' = \langle H_1, H_2 \rangle$.
   (b) $\langle L_1, L_2 \rangle' = H_1 \cap H_2$.

   Aqui $\langle H_1, H_2 \rangle$ é o subgrupo de G gerado por H_1 e H_2 (a interseção dos subgrupos de G contendo H_1 e H_2), e $\langle L_1, L_2 \rangle$ é o subcorpo de M gerado por L_1 e L_2 (a interseção dos subcorpos de M contendo L_1 e L_2).

(4) Seja L/K uma extensão de corpos de grau finito. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).
   (a) Se os únicos subcorpos de L contendo K são L e K então $|L : K|$ é um número primo.
   (b) Se L/K é extensão de Galois e os únicos subcorpos de L contendo K são L e K então $|L : K|$ é um número primo.
   (c) Se L/K é extensão de Galois e existem exatamente 3 corpos F tais que $K \leq F \leq L$ então $|L : K| = p^2$ para algum primo p.

(5) O grupo de Galois $G_{f,K}$ de um polinômio $f(X) \in K[X]$ sobre K é o grupo de Galois de M_f/K onde M_f é um corpo de decomposição de $f(X)$ sobre K. Sejam $f(X), h(X) \in K[X]$. É claro que M_{fh}, corpo de decomposição de $f(X)h(X)$ sobre K, contém corpos de decomposição M_f, M_h de $f(X)$ e $h(X)$ respectivamente. Como M_f e M_h são extensões de Galois de K, são estáveis em M_{fh}/K, logo temos um homomorfismo canônico

$$\varphi : G_{fh,K} \to G_{f,K} \times G_{h,K}, \qquad \sigma \mapsto (\sigma|_{M_f}, \sigma|_{M_h}).$$

   (a) Mostre que $\ker(\varphi) = \{1\}$, ou seja φ é injetivo.
   (b) Mostre que em geral φ não é sobrejetivo.
   (c) Se $G_{f,K}$ e $G_{h,K}$ são abelianos, $G_{fh,K}$ é necessariamente abeliano?
   (d) Mostre que φ é um isomorfismo se e somente se $M_f \cap M_h = K$.

(6) Seja F/K extensão de corpos de grau finito e seja L um corpo tal que $K \leq L \leq F$. É verdade que para todo isomorfismo de aneis $\sigma : L \to L$ existe sempre um isomorfismo de aneis $g : F \to F$ tal que $\sigma = g|_L$?

Lista de Álgebra 3 do dia 5 de abril de 2022 - Resolução.

Todos os corpos considerados contêm $\mathbb{Q}$ como subcorpo.

(1) Seja K um corpo e seja M um corpo de decomposição sobre K de um polinômio de $K[X]$, tal que $|M : K| = 21$. Seja L um corpo tal que $K \leq L \leq M$. Mostre que se $|L : K| = 3$ então L é corpo de decomposição sobre K de um polinômio de $K[X]$.

Seja $N := L' \leq G$, então $|N : \{1\}| = |M : L| = 7$ logo $N \trianglelefteq G$ pois N é um 7-Sylow de G e $n_7(G) = 1$ pelo teorema de Sylow. Segue que $L = N'$ é estável em M/K, ou seja L/K é extensão de Galois.

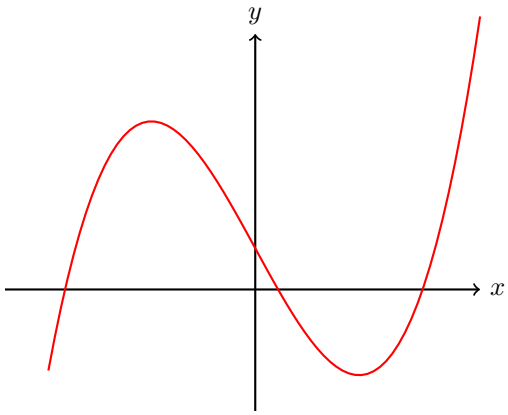
(2) Seja $f(X) \in \mathbb{Q}[X]$ um polinômio irredutível de grau 3, sejam v_1, v_2, v_3 as suas raízes complexas e seja $M = \mathbb{Q}(v_1, v_2, v_3) \subseteq \mathbb{C}$, corpo de decomposição de $f(X)$ sobre $\mathbb{Q}$. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).

(a) Se $|M : \mathbb{Q}| = 3$ então $M \subseteq \mathbb{R}$. Verdadeiro, pois se $\sigma : \mathbb{C} \to \mathbb{C}$ é a conjugação complexa então $\tau := \sigma|_M \in G = \mathscr{G}(M/K)$ e $\tau^2 = 1$, por outro lado $|G| = |M : \mathbb{Q}| = 3$ logo $\tau = 1$, ou seja $M \subseteq \mathbb{R}$.

(b) Se $M \subseteq \mathbb{R}$ então $|M : \mathbb{Q}| = 3$. Falso, por exemplo seja

$$f(X) = X^3 - 4X + 1 \in \mathbb{Q}[X],$$

irredutível em $\mathbb{Q}[X]$, tem discriminante igual a $-4(-4)^3 - 27 = 229$ é um número primo, logo não é um quadrado em $\mathbb{Q}$. Além disso $f(X)$ tem 3 raízes reais, como mostrado por um simples esboço de gráfico.



(c) Se $|M : \mathbb{Q}| = 6$ e $D = \Delta^2$ é o discriminante de $f(X)$ então uma base de M sobre $\mathbb{Q}$ é $\{1, v_1, v_1^2, \Delta, \Delta v_1, \Delta v_1^2\}$. Temos que $\Delta \notin \mathbb{Q}$, logo $|\mathbb{Q}(\Delta) : \mathbb{Q}| = 2$ e o polinômio minimal de Δ sobre $\mathbb{Q}$ é $X^2 - D = X^2 - \Delta^2$, por outro lado $|\mathbb{Q}(v_1) : \mathbb{Q}| = 3$ pois o polinômio minimal de v_1 sobre $\mathbb{Q}$ é (um múltiplo escalar de) $f(X)$, pois $f(X)$ é irredutível em $\mathbb{Q}[X]$ e $f(v_1) = 0$. Como $|\mathbb{Q}(\Delta) : \mathbb{Q}| = 2$ não divide $|\mathbb{Q}(v_1) : \mathbb{Q}|$, temos que $\Delta \notin \mathbb{Q}(v_1)$, logo

$$|\mathbb{Q}(v_1, \Delta) : \mathbb{Q}| = |\mathbb{Q}(v_1)(\Delta) : \mathbb{Q}(v_1)| \cdot |\mathbb{Q}(v_1) : \mathbb{Q}| = 2 \cdot 3 = 6.$$

Como $\mathbb{Q}(v_1, \Delta) \subseteq M$ têm o mesmo grau sobre $\mathbb{Q}$, segue que $M = \mathbb{Q}(v_1, \Delta)$. Como $1, v_1, v_1^2, \Delta, \Delta v_1, \Delta v_1^2$ são 6 elementos, para mostrar que formam uma base de M sobre $\mathbb{Q}$ basta mostrar que são linearmente independentes sobre $\mathbb{Q}$. Como $|\mathbb{Q}(v_1)(\Delta) : \mathbb{Q}(v_1)| = 2$, temos

que $\{1, \Delta\}$ é uma base de $\mathbb{Q}(v_1, \Delta)$ sobre $\mathbb{Q}(v_1)$, logo se $a_1, \ldots, a_6 \in \mathbb{Q}$ são tais que

$$a_1 + a_2 v_1 + a_3 v_1^2 + a_4 \Delta + a_5 \Delta v_1 + a_6 \Delta v_1^2 = 0$$

então $a_1 + a_2 b_1 + a_3 v_1^2 = 0$ e $a_4 + a_5 v_1 + a_6 v_1^2 = 0$, logo $a_i = 0$ para todo i pois $\{1, v_1, v_1^2\}$ é uma base de $\mathbb{Q}(v_1)$ sobre $\mathbb{Q}$.

(3) Sejam M/K uma extensão de Galois finita, L_1, L_2 corpos com $K \leq L_i \leq M$ para $i = 1, 2$ e $H_1 = L_1'$, $H_2 = L_2'$ os correspondentes subgrupos de $G = \mathscr{G}(M/K)$ (pelas correspondências de Galois). Mostre que

(a) $(L_1 \cap L_2)' = \langle H_1, H_2 \rangle$. Observe que um elemento $m \in M$ pertence a $\langle H_1, H_2 \rangle'$ se e somente se $h(m) = m$ para todo $h \in H_1 \cup H_2$, logo $\langle H_1, H_2 \rangle' = H_1' \cap H_2' = L_1 \cap L_2$. Segue que

$$(L_1 \cap L_2)' = \langle H_1, H_2 \rangle'' = \langle H_1, H_2 \rangle.$$

(b) $\langle L_1, L_2 \rangle' = H_1 \cap H_2$. Um elemento $g \in G$ pertence a $\langle L_1, L_2 \rangle'$ se e somente se $g(\ell) = \ell$ para todo $\ell \in L_1 \cup L_2$, logo $\langle L_1, L_2 \rangle' = L_1' \cap L_2' = H_1 \cap H_2$.

Aqui $\langle H_1, H_2 \rangle$ é o subgrupo de G gerado por H_1 e H_2 (a interseção dos subgrupos de G contendo H_1 e H_2), e $\langle L_1, L_2 \rangle$ é o subcorpo de M gerado por L_1 e L_2 (a interseção dos subcorpos de M contendo L_1 e L_2).

(4) Seja L/K uma extensão de corpos de grau finito. Para cada uma das seguintes frases, diga se é verdadeira (demonstrando) ou falsa (dando um contra-exemplo).

(a) Se os únicos subcorpos de L contendo K são L e K então $|L : K|$ é um número primo. Falso, por exemplo seja $f(X) = X^4 + X + 1$, que é irredutível em $\mathbb{Q}[X]$ e tem grupo de Galois sobre $\mathbb{Q}$ isomorfo a S_4. Seja $\alpha \in \mathbb{C}$ uma raiz de $f(X)$ e sejam $L = \mathbb{Q}(\alpha)$, $K = \mathbb{Q}$, M o corpo de decomposição de $f(X)$ contido em $\mathbb{C}$. O corpo intermediário L corresponde a um estabilizador de ponto em $G = \mathscr{M}/K \cong S_4$ pelas correspondências de Galois. Em particular L' é um subgrupo maximal de G, logo não existem subgrupos $H \leq G$ tais que $L' < H < G$. Segue que não existem corpos intermediários entre $G' = K$ e $L'' = L$.

(b) Se L/K é extensão de Galois e os únicos subcorpos de L contendo K são L e K então $|L : K|$ é um número primo. Verdadeiro, pois definindo $G = \mathscr{G}(L/K)$, se os únicos subcorpos de L contendo K são L e K então os únicos subgrupos de G são $L' = \{1\}$ e $K' = G$. Segue que G é cíclico de ordem prima. De fato, se $g \in G$ é diferente de 1 então $\{1\} \neq \langle g \rangle \leq G$ implica $\langle g \rangle = G$, logo g tem ordem prima.

(c) Se L/K é extensão de Galois e existem exatamente 3 corpos F tais que $K \leq F \leq L$ então $|L : K| = p^2$ para algum primo p. Verdadeiro. Seguindo o procedimento do item acima, precisamos mostrar que se um grupo finito G admite exatamente 3 subgrupos então a sua ordem é p^2 para algum primo p. Sejam $\{1\}$, H e G os três subgrupos de G. Se $g \in G - H$ então $\langle g \rangle \neq \{1\}, H$ logo $\langle g \rangle = G$. Segue que G é cíclico de ordem finita n, e sabemos que G contém tantos subgrupos quantos são os divisores da sua ordem. Segue que n tem exatamente 3 divisores, e isso implica que $n = p^2$ para algum primo p.

(5) O grupo de Galois $G_{f,K}$ de um polinômio $f(X) \in K[X]$ sobre K é o grupo de Galois de M_f/K onde M_f é um corpo de decomposição de $f(X)$ sobre K. Sejam $f(X), h(X) \in K[X]$. É claro que M_{fh}, corpo de decomposição de $f(X)h(X)$ sobre K, contém corpos de decomposição M_f, M_h de $f(X)$ e $h(X)$ respectivamente. Como M_f e M_h são extensões de Galois de K, são estáveis em M_{fh}/K, logo temos um homomorfismo canônico

$$\varphi : G_{fh,K} \to G_{f,K} \times G_{h,K}, \qquad \sigma \mapsto (\sigma|_{M_f}, \sigma|_{M_h}).$$

(a) Mostre que $\ker(\varphi) = \{1\}$, ou seja φ é injetivo. Um elemento $g \in G_{fh,K}$ pertence ao núcleo de φ se e somente se fixa todo elemento de M_f e todo elemento de M_h, segue que o núcleo de φ é dado por

$$\ker(\varphi) = {M_f}' \cap {M_h}' = \langle M_f, M_h \rangle' = {M_{fh}}' = \{1\}.$$

(b) Mostre que em geral φ não é sobrejetivo. Por exemplo, se $f = h$ então obviamente $G_{fh} = G_{f^2} = G_f$ e tomando f de grau 2 obtemos que G_f tem ordem 2, logo não é isomorfo a $G_f \times G_f$.

(c) Se $G_{f,K}$ e $G_{h,K}$ são abelianos, $G_{fh,K}$ é necessariamente abeliano? Sim, pois pelo item (a) $G_{fh,K}$ é isomorfo a um subgrupo de $G_{f,K} \times G_{h,K}$, que é abeliano se $G_{f,K}$ e $G_{h,K}$ são abelianos.

(d) Mostre que φ é um isomorfismo se e somente se $M_f \cap M_h = K$. Observe que a condição $M_f \cap M_h = K$ é equivalente a ${M_f}'{M_h}' = G$. De fato ${M_f}'$ e ${M_h}'$ são normais em G (sendo M_f/K e M_h/K extensões de Galois) logo se $M_f \cap M_h = K$ então

$$G = K' = (M_f \cap M_h)' = \langle {M_f}', {M_h}' \rangle = {M_f}'{M_h}'$$

e se ${M_f}'{M_h}' = G$ então

$$K = G' = ({M_f}'{M_h}')' = \langle {M_f}', {M_h}' \rangle' = (M_f \cap M_h)'' = M_f \cap M_h.$$

Logo basta mostrar que φ é sobrejetiva se e somente se ${M_f}'{M_h}' = G$. Isso segue do fato seguinte.

Sejam $f_i : G \to G_i$, $i = 1, 2$, dois homomorfismos sobrejetivos e sejam $A_i := \ker(f_i)$, $i = 1, 2$. Então

$$f : G \to G_1 \times G_2, \qquad f(x) := (f_1(x), f_2(x))$$

é sobrejetivo se e somente se $A_1 A_2 = G$.

De fato se $A_1 A_2 = G$ e $(g_1, g_2) \in G_1 \times G_2$ então existem $x_1, x_2 \in G$ tais que $f_i(x_i) = g_i$ para $i = 1, 2$, e podemos escrever $x_1 = a_1 a_2$, $x_2 = a_1' a_2'$ com $a_1, a_1' \in A_1$, $a_2, a_2' \in A_2$, assim $g_1 = f_1(x_1) = f_1(a_2)$ e $g_2 = f_2(x_2) = f_2(a_1')$. Seja $g := a_1' a_2$. Temos

$$\begin{aligned} f(g) &= (f_1(a_1' a_2), f_2(a_1' a_2)) = (f_1(a_2), f_2(a_1')) \\ &= (f_1(a_1) f_1(a_2), f_2(a_1') f_2(a_2')) \\ &= (f_1(a_1 a_2), f_2(a_1' a_2')) \\ &= (f_1(x_1), f_2(x_2)) = (g_1, g_2). \end{aligned}$$

Se f é sobrejetivo e $x \in G$ então existem $a_1, a_2 \in G$ tais que $f(a_1) = (1, f_2(x))$ e $f(a_2) = (f_1(x), 1)$, assim $a_i \in A_i$ para $i = 1, 2$ e $f(x) = (f_1(x), f_2(x)) = f(a_1) f(a_2) = f(a_1 a_2)$. Segue que $x(a_1 a_2)^{-1} = a \in \ker(f) = A_1 \cap A_2$ logo $x = a a_1 \cdot a_2 \in A_1 A_2$.

(6) Seja F/K extensão de corpos de grau finito e seja L um corpo tal que $K \leq L \leq F$. É verdade que para todo isomorfismo de aneis $\sigma : L \to L$ existe sempre um isomorfismo de aneis $g : F \to F$ tal que $\sigma = g|_L$? Não, tome por exemplo $F = \mathbb{Q}(\sqrt[4]{2})$, $L = \mathbb{Q}(\sqrt{2})$ e $K = \mathbb{Q}$. O único automorfismo não trivial de F é dado por $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, logo fixa todo elemento de L, por outro lado L admite o automorfismo não trivial que leva $\sqrt{2}$ para $-\sqrt{2}$.