Resolução da terceira prova de Introdução à Álgebra (2019-1).

(1) Seja $f(X) \in \mathbb{F}_3[X]$ irredutível de grau 3.

(a) (1 ponto) Seja F uma extensão de $\mathbb{F}_3$ tal que $|F| = 81$. Diga se existe $\alpha \in F$ tal que $f(\alpha) = 0$. [Dica: qual é o grau $|\mathbb{F}_3(\alpha) : \mathbb{F}_3|$?]

Se existe $\alpha \in F$ tal que $f(\alpha) = 0$ então $|\mathbb{F}_3(\alpha) : \mathbb{F}_3| = 3$ (o grau de $f(X)$), por outro lado $|F : \mathbb{F}_3| = 4$ (pois $|F| = 81 = 3^4$). Se $\alpha \in F$ pela formula do grau

$$4 = |F : \mathbb{F}_3| = |F : \mathbb{F}_3(\alpha)| \cdot |\mathbb{F}_3(\alpha) : \mathbb{F}_3| = |F : \mathbb{F}_3(\alpha)| \cdot 3,$$

contradição, sendo $|F : \mathbb{F}_3(\alpha)|$ um inteiro.

(b) (1 ponto) Mostre que $f(X)$ divide $X^{27} - X$ em $\mathbb{F}_3[X]$. [Dica: considere um corpo $\mathbb{F}_3(\alpha)$ onde $f(\alpha) = 0$.]

Seja α uma raiz de $f(X)$ em uma oportuna extensão de $\mathbb{F}_3$ (por exemplo $\alpha = \overline{X} \in \mathbb{F}_3[X]/(f(X))$). Temos $|\mathbb{F}_3(\alpha) : \mathbb{F}_3| = 3$ logo $|\mathbb{F}_3(\alpha)| = 3^3 = 27$, ou seja $F = \mathbb{F}_3(\alpha)$ é um corpo com 27 elementos. Sabemos que isso implica $\alpha^{27} = \alpha$. De fato $\alpha \neq 0$ sendo $f(X)$ irredutível, logo $\alpha \in F^*$ que é um grupo multiplicativo de ordem 26 logo $\alpha^{26} = 1$ que implica $\alpha^{27} = \alpha$. Segue que α é raiz de $X^{27} - X$, logo o polinômio minimal de α sobre $\mathbb{F}_3$ divide $X^{27} - X$. Mas o polinômio minimal de α, a menos de uma constante multiplicativa, é o próprio $f(X)$. Logo $f(X)$ divide $X^{27} - X$.

(2) Sejam $\alpha = \sqrt{2 + \sqrt{6}} \in \mathbb{R}$, $\beta = \sqrt{10 + \sqrt{10}} \in \mathbb{R}$.

(a) (1 ponto) $\mathbb{Q}(\alpha)/\mathbb{Q}$ é extensão de Galois?

Temos

$$0 = (\alpha^2 - 2)^2 - 6 = \alpha^4 - 4\alpha^2 - 2,$$

logo o polinômio minimal de α sobre $\mathbb{Q}$ é $X^4 - 4X^2 - 2$, irredutível pelo critério de Eisenstein. As raízes de $f(X)$ são $\pm\alpha$ e $\pm\gamma$ onde $\gamma = i\sqrt{\sqrt{6} - 2} \in \mathbb{C} - \mathbb{R}$. Segue que $\mathbb{Q}(\alpha)/\mathbb{Q}$ não é extensão de Galois pois contem α mas não contem todas as raízes do polinômio minimal de α, de fato não contem γ pois $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ mas $\gamma \notin \mathbb{R}$.

Importante: estou usando o fato seguinte, visto nas aulas teóricas:
Seja M/K extensão de Galois finita com grupo de Galois G. Se $f(X) \in_{irr} K[X]$, de grau $n \geq 1$, tem uma raiz em M então $f(X)$ pode ser decomposto em fatores lineares em $M[X]$ e admite exatamente n raizes distintas.

(b) (1 ponto) $\mathbb{Q}(\beta)/\mathbb{Q}$ é extensão de Galois?

Temos

$$0 = (\beta^2 - 10)^2 - 10 = \beta^4 - 20\beta^2 + 90,$$

logo o polinômio minimal de β sobre $\mathbb{Q}$ é $X^4 - 20X^2 + 90$, irredutível pelo critério de Eisenstein aplicado ao primo 5. As suas raízes são β, $-\beta$, γ, $-\gamma$ onde $\gamma = \sqrt{10 - \sqrt{10}} \in \mathbb{R}$. Sendo $\beta\gamma = \sqrt{90} = 3\sqrt{10}$ obtemos $\gamma = 3\sqrt{10}/\beta = 3(\beta^2 - 10)/\beta \in \mathbb{Q}(\beta)$ logo $\mathbb{Q}(\beta)$ contem todas as raízes de $f(X) = X^4 - 20X^2 + 90$ e além disso é gerado por elas. Segue que $\mathbb{Q}(\beta)/\mathbb{Q}$ é extensão de Galois sendo $\mathbb{Q}(\beta)$ corpo de decomposição do polinômio $f(X)$ sobre $\mathbb{Q}$.

(3) Sejam $\alpha = i + \sqrt{5}$, $M = \mathbb{Q}(\alpha)$, $G = \mathscr{G}(M/\mathbb{Q}) = \{g_1, \ldots, g_m\}$.

(a) (1 ponto) Mostre que M é corpo de decomposição do polinômio $f(X) = (X^2 + 1)(X^2 - 5)$ sobre $\mathbb{Q}$.

Temos $\alpha^2 = 4 + 2i\sqrt{5}$ logo $i\sqrt{5} \in M$, e $\beta = i\sqrt{5}\alpha = -\sqrt{5} + 5i$. Segue que $6i = \alpha + \beta \in M$ logo $i \in M$, logo $\sqrt{5} = \alpha - i \in M$. Deduzimos que M contem $\mathbb{Q}(i, \sqrt{5})$ e a outra inclusão é imediata, logo $M = \mathbb{Q}(i, \sqrt{5})$ é corpo de decomposição de $f(X)$ sendo $\mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5})$.

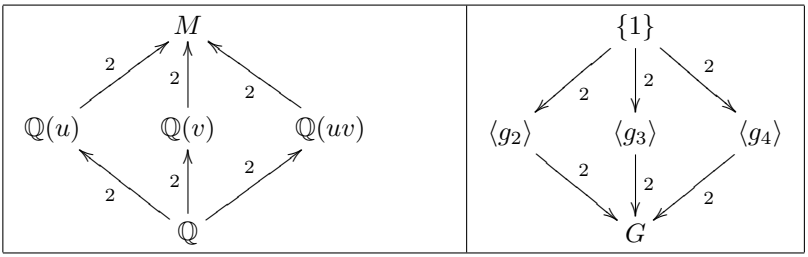
(b) (1 ponto) Descreva as correspondências de Galois de $M/\mathbb{Q}$.

Sejam $G = \mathscr{G}(M/\mathbb{Q})$, $u = \sqrt{5}$, $v = i$. Se $g \in G$ não é a identidade então $g(u) \neq u$ ou $g(v) \neq v$. No primeiro caso $g(u) = -u$ (sendo $g(u)$ uma raiz de $X^2 - 5$) e temos duas possibilidades: $g(v) = v$ ou $g(v) = -v$. No segundo caso $g(v) = -v$ (sendo $g(v)$ uma raiz de $X^2 + 1$) e temos duas possibilidades: $g(u) = u$ ou $g(u) = -u$. Isso nos dá quatro possibilidades, e cada uma delas ocorre sendo $|G| = |M : \mathbb{Q}| = 4$. Podemos resumir tudo na tabela seguinte.

Elemento	Imagem de u	Imagem de v	Estrutura
g_1	u	v	Identidade
g_2	u	$-v$	2-cíclo $(v, -v)$
g_3	$-u$	v	2-cíclo $(u, -u)$
g_4	$-u$	$-v$	$(u, -u)(v, -v)$

Observe que $g_1 = 1$ e $g_2 g_3 = g_4$. Escrevendo então $G = \{1, g_2, g_3, g_4\}$ os subgrupos de G são $\{1\}$, G, $H = \langle g_2 \rangle$, $K = \langle g_3 \rangle$, $J = \langle g_4 \rangle$. Como $|H' : \mathbb{Q}| = |G : H| = 2$ e a mesma coisa vale para K' e J', os subcorpos H', K' e J' têm grau 2 sobre $\mathbb{Q}$. Os subcorpos $\mathbb{Q}(u)$, $\mathbb{Q}(v)$, $\mathbb{Q}(uv)$ são distintos e têm grau 2 sobre $\mathbb{Q}$, e da tabela segue $u \in H'$, $v \in K'$, $uv \in J'$. Segue que os reticulados $[M/\mathbb{Q}]$ e $\mathscr{L}(G)$ são os seguintes, onde as setas são inclusões e os

números indicam os graus a esquerda, os índices a direita.

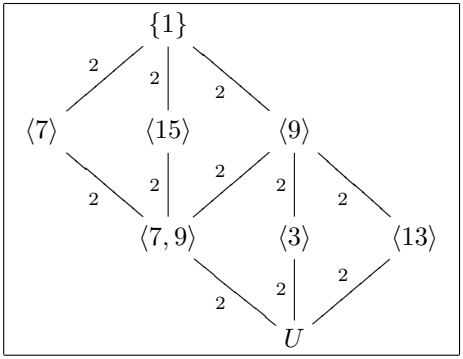


(c) (1 ponto) Calcule $g_1(\alpha) \cdot \ldots \cdot g_m(\alpha)$.

É ugual a

$$(i+\sqrt{5})(-i+\sqrt{5})(i-\sqrt{5})(-i-\sqrt{5}) = 6 \cdot 6 = 36.$$

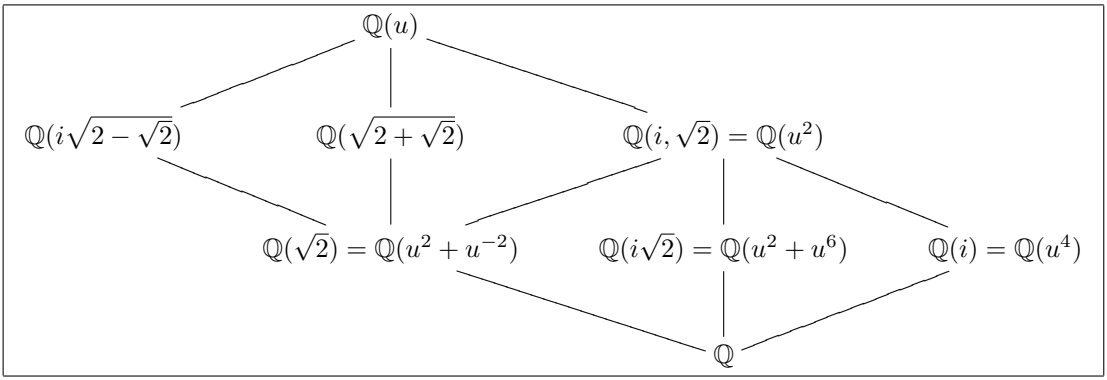
(4) (2 pontos) Seja $u = e^{i2\pi/16} = \cos(2\pi/16) + i\sin(2\pi/16)$, raiz de $\Phi_{16}(X) = X^8 + 1$, irredutível em $\mathbb{Q}[X]$. Seja $G = \mathscr{G}(\mathbb{Q}(u)/\mathbb{Q})$. Para todo $H \leq G$ determine geradores do corpo H' correspondente a H por meio das correspondências de Galois. O reticulado dos subgrupos de $U = U(\mathbb{Z}/16\mathbb{Z}) = \{1,3,5,7,9,11,13,15\}$ é o seguinte:



[Lembre-se que todo elemento de G é do tipo g_h determinado pela igualdade $g_h(u) = u^h$, onde $h \in U$.]

Seja $G = \mathscr{G}(\mathbb{Q}(u)/\mathbb{Q})$. $u^4 = i$ é fixado por g_{13}, sendo $g_{13}(u^4) = u^{52} = u^4$, e u^4 tem grau 2 sobre $\mathbb{Q}$, igual ao índice de $\langle g_{13}\rangle$ em G, logo $\langle g_{13}\rangle' = \mathbb{Q}(u^4)$. Pelo diagrama segue que $\mathbb{Q}(u^4)$ está contido em um único subcorpo de grau 4 sobre $\mathbb{Q}$, ou seja $\langle g_9\rangle'$, por outro lado u^2 tem grau 4 sobre $\mathbb{Q}$ (sendo um elemento de ordem 8 e $\varphi(8) = 4$) logo $\langle g_9\rangle' = \mathbb{Q}(u^2)$. Observe que $u^2 = \frac{\sqrt{2}}{2}(1+i)$ logo $\mathbb{Q}(u^2) = \mathbb{Q}(i,\sqrt{2})$ contem os subcorpos $\mathbb{Q}(i\sqrt{2})$ e $\mathbb{Q}(\sqrt{2})$, e $i = u^4$ logo (substituindo na igualdade $u^2 = \frac{\sqrt{2}}{2}(1+i)$) temos que $\sqrt{2} = u^2 + u^{-2}$ é fixado por g_7 e g_9, e comparando o grau e o índice obtemos $\langle g_7, g_9\rangle' = \mathbb{Q}(u^2 + u^{-2}) = \mathbb{Q}(\sqrt{2})$. Como tem mais um único subcorpo de grau 2 sobre $\mathbb{Q}$, que é $\mathbb{Q}(i\sqrt{2})$, deduzimos que $\langle g_3\rangle' = \mathbb{Q}(i\sqrt{2})$. Observe que $(u-u^{-1})^2 = u^2 + u^{-2} - 2 = \sqrt{2} - 2$ logo $u - u^{-1} = \pm i\sqrt{2-\sqrt{2}}$ tem grau 4

sobre $\mathbb{Q}$, igual ao índice de $\langle g_7\rangle$, e $g_7(u-u^{-1}) = u^7 - u^{-7} = u^7 - u^9 = u - u^{-1}$ (sendo $u^8 = -1$). Segue que $\langle g_7\rangle' = \mathbb{Q}(u-u^{-1})$. Observe que $(u+u^{-1})^2 = u^2 + u^{-2} + 2 = \sqrt{2} + 2$ logo $u + u^{-1} = \pm\sqrt{2+\sqrt{2}}$ tem grau 4 sobre $\mathbb{Q}$, igual ao índice de $\langle g_{15}\rangle$ em G. Como $g_{15}(u+u^{-1}) = u^{15} + u = u + u^{-1}$ deduzimos que $\langle g_{15}\rangle' = \mathbb{Q}(u+u^{-1})$.



(5) (1 ponto) Uma extensão de corpos é dita abeliana se o seu grupo de Galois é abeliano. Seja M/K uma extensão de Galois de grau finito e sejam $L, T \in [M/K]$ corpos intermediários tais que L/K e T/K são extensões de Galois. Suponha L/K e T/K abelianas e suponha $\langle L, T\rangle = M$, ou seja o corpo gerado por L e T é igual a M. Mostre que M/K é abeliana.

Seja $G = \mathscr{G}(M/K)$. $L', T' \trianglelefteq G$ sendo L, T extensões de Galois de K, e $A = \mathscr{G}(L/K) \cong G/L'$, $B = \mathscr{G}(T/K) \cong G/T'$. Além disso $\{1\} = M' = \langle L, T\rangle' = L' \cap T'$. Segue que o homomorfismo $G \to G/L' \times G/T'$ dado pelas projeções é injetivo (o seu núcleo é $L' \cap T' = \{1\}$). Mas sendo G/L' e G/T' abelianos, obtemos que G é abeliano, sendo isomorfo a um subgrupo de um produto direto de grupos abelianos.

Erro comum: "como $\langle L, T\rangle = M$ deduzimos $\langle L', T'\rangle = G$".

A igualdade $\langle L', T'\rangle = G$ é equivalente (aplicando as correspondências de Galois) a $L \cap T = K$, que em geral é falso.