Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Resolução do 2º Teste de Álgebra

20 de Dezembro de 2004
LMAC e MMA

1. (a) Dado $x \in G$, temos $G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x)$.

(b) Seja $G = S_4$. De acordo com a alínea anterior, o número de elementos de G que comutam com γ é

$$|G_\gamma| = \frac{|G|}{|\mathcal{O}_\gamma|} = \frac{24}{|\{(12)(34), (13)(24), (14)(23)\}|} = 8.$$

2. (a) Notando que

$$\mathrm{SL}_2(\mathbb{F}_p) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \mid a \in \mathbb{F}_p^\times,\, b, c \in \mathbb{F}_p, d = \tfrac{1+bc}{a} \right\} \amalg \left\{ \left(\begin{smallmatrix} 0 & b \\ c & d \end{smallmatrix} \right) \mid b, c \in \mathbb{F}_p^\times,\, c = -\tfrac{1}{b}, d \in \mathbb{F}_p \right\},$$

vem $|\,\mathrm{SL}_2(\mathbb{F}_p)| = (p-1)p^2 + p(p-1)^2 = p(p-1)(p+1)$.

(b) Pela alínea anterior, $|\,\mathrm{SL}_2(\mathbb{F}_3)| = 24$. Seja n o número de 3-subgrupos de Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$. Dos teoremas de Sylow, segue $n \mid 8$ e $n \equiv 1 \mod 3$; ou seja $n = 1$ ou $n = 4$. Como $\{\left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix} \right) \mid c \in \mathbb{F}_3\}$ e $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix} \right) \mid b \in \mathbb{F}_3\}$ são subgrupos distintos de $\mathrm{SL}_2(\mathbb{F}_3)$, com ordem 3, concluímos que $n = 4$.

3. (a) Recorde-se que a *série central inferior* de G, $\{C^k(G)\}_{k\geq 0}$, é definida recursivamente por: $C^0(G) := G$, $C^{k+1}(G) := (G, C^k(G))$. Um grupo G diz-se *nilpotente* se existe $n \in \mathbb{N}$ tal que $C^n(G) = \{1\}$.

(b) Seja $n \in \mathbb{N}$ tal que $C^n(H) = \{1\}$. Como $H < C(G)$, temos $H \lhd G$ e portanto G/H é um grupo. Seja $\pi\colon G \to G/H$ a projecção. Pelas propriedades dos comutadores, $\pi(C^n(G)) = C^n(H) = \{1\}$, o que implica $\pi(C^n(G)) < \ker \pi = H < C(G)$. Donde $C^{n+1}(G) = (G, C^n(G)) < (G, C(G)) = \{1\}$ e portanto G é nilpotente.

4. Note-se que $x = 0$ não é solução para nenhuma das equações, portanto basta contar as soluções $x \in \mathbb{F}_{81}^\times := (\mathbb{F}_{81} - \{0\}, \cdot)$. Recorde-se que $\mathbb{F}_{81}^\times \cong \mathbb{Z}_{80}$. Seja $\tau \in \mathbb{F}_{81}^\times$ um gerador.

(a) Como $|\mathbb{F}_{81}^\times| = 80$, temos $x^{80} = 1$, $\forall x \in \mathbb{F}_{81}^\times$. Concluímos que $x^{80} - 1 = 0$ tem 80 soluções distintas.

(b) Como $\mathrm{char}(\mathbb{F}_{81}) = 3$, temos $x^{81} - 1 = (x-1)^{81}$. Logo $x^{81} - 1 = 0$ tem uma única solução.

(c) Como $\mathbb{F}_{81}^\times \cong \mathbb{Z}_{80}$, temos $x^{85} - 1 = 0 \Leftrightarrow x^5 - 1 = 0 \Leftrightarrow x \in \langle 16\tau \rangle \cong \mathbb{Z}_5$. Portanto, $x^{85} - 1 = 0$ tem 5 soluções distintas.

OP1. Sejam $\omega = e^{\frac{2\pi i}{5}}$ e $G = \mathrm{Gal}(E/\mathbb{Q})$.

(a) Uma vez que as raízes de $f(x)$ são $\sqrt[5]{2}\omega^j$, $j = 0, \ldots 4$, temos $E = \mathbb{Q}(\sqrt[5]{2}, \omega)$, o implica

$$[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] \mid [E : \mathbb{Q}] \wedge [\mathbb{Q}(\omega) : \mathbb{Q}] \mid [E : \mathbb{Q}] \wedge [E : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] \quad (1)$$

Aplicando o critério de Eisenstein, concluímos que $f(x)$ e[1] $g(x) := (x^5-1)/(x-1)$ são irredutíveis em $\mathbb{Q}[x]$. Como $f(\sqrt[5]{2}) = g(\omega) = 0$, vem $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$ e $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$. As relações (1) implicam $[E : \mathbb{Q}] = 20$ e portanto $|G| = [E : \mathbb{Q}] = 20$, visto que $E/\mathbb{Q}$ é um extensão decomposição de um polinómio separável.

[1] No caso de $g(x)$ é também necessário usar a mudança de variável $x \mapsto x + 1$

(b) Sejam $H_1 = \mathrm{Gal}(E/\mathbb{Q}(\omega)) < G$, $H_2 = \mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{2})) < G$. Pelo Teorema de Galois, temos $[G : H_1] = [\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ e $[G : H_2] = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$. Portanto, $H_1 \cap H_2 = \{1\}$ e $G = H_1 H_2$. Das igualdades $\deg(f(x)) = [E : \mathbb{Q}(\omega)]$, $\deg(g(x)) = [E : \mathbb{Q}(\sqrt[5]{2})]$ segue que $f(x)$, $g(x)$ são irredutíveis em $\mathbb{Q}(\omega)[x]$ e $\mathbb{Q}(\sqrt[5]{2})[x]$ respectivamente; logo existem $\sigma \in H_1$ e $\gamma \in H_2$ tais que $\sigma(\sqrt[5]{2}) = \sqrt[5]{2}\omega$ e $\gamma(\omega) = \omega^2$. Por iteração, obtemos

$$\begin{array}{ll} \gamma^i(\sqrt[5]{2}) = \sqrt[5]{2}, & \gamma^i(\omega) = \omega^{2^i} \\ \sigma^j(\sqrt[5]{2}) = \sqrt[5]{2}\omega^j, & \sigma^j(\omega) = \omega. \end{array}$$

Em particular, σ, γ são geradores para $H_1 \cong \mathbb{Z}_5$ e $H_2 \cong \mathbb{Z}_4$, respectivamente. Obtemos também $\gamma\sigma = \sigma^2\gamma$, pois $E = \mathbb{Q}(\sqrt[5]{2}, \omega)$ e

$$\begin{array}{rcl} \gamma\sigma(\omega) = & \omega^2 & = \sigma^2\gamma(\omega) \\ \gamma\sigma(\sqrt[5]{2}) = & \sqrt[5]{2}\omega^2 & = \sigma^2\gamma(\sqrt[5]{2}). \end{array}$$

Concluímos que G é gerado por σ e γ com relações:

$$\gamma\sigma = \sigma^2\gamma, \quad \sigma^5 = 1, \quad \gamma^4 = 1.$$

OP2. Sejam $H_1 = \mathrm{Gal}(E/F_1)$ e $H_2 = \mathrm{Gal}(E/F_2)$. As extensões F_1/k e F_2/k são de Galois, logo são normais. Portanto $H_i \lhd G$ e $G/H_i \cong \mathrm{Gal}(F_i/k)$, $i = 1, 2$. Como $\mathrm{Gal}(F_i/k)$ é abeliano, segue das propriedades do grupo derivado que $\mathcal{D}(G) < H_i$, $i = 1, 2$. Assim, $\mathcal{D}(G) < H_1 \cap H_2$. Aplicando a correspondência de Galois à igualdade $E = F_1F_2$, obtemos $H_1 \cap H_2 = \{1\}$. Concluímos que $\mathcal{D}(G) = \{1\}$, ou seja, G é abeliano.