PROVA 1 – ESTRUTURAS ALGÉBRICAS II

Questão 1 (a): Sejam $H = \langle a \rangle$ ($|H| = 11$), $K = \langle b \rangle$ ($|K| = 5$). Então:

(i) $H \trianglelefteq G$, em conseqüência do teorema de Sylow, ou, mais diretamente, porque

$$(cx+d) \circ (x+1) \circ (cx+d)^{-1} = (cx+d) \circ (c^{-1}x - c^{-1}d + 1) = x + c.$$

(Note que $c^{-1} \in \{1, -2, 3, 4, 5\}$ se c pertence a esse mesmo conjunto.)

(ii) $H \cap K = \mathrm{id}$, pois $a^i(0) = i$, enquanto $b^j(0) = 0$.

(iii) $HK = G$, pois a função $(h, k) \mapsto h \circ k$ é injetora (em conseqüência de (ii)) e $|G| = 55 = |H|\,|K|$.

De (ii) e (iii) concluímos que todo $f \in G$ pode ser escrito, de forma única, como $f = a^i b^j$, para $i \in \{0, 1, 2, \ldots, 10\}$ e $j \in \{0, 1, 2, 3, 4\}$.

Além disto, $bab^{-1} = a^3 b$, por isto $ba = a^3 b$ e

$$b^\nu a^\mu = a^{\mu 3^\nu} b^\nu \qquad (0 \le \mu \le 10,\ 0 \le \nu \le 4).$$

Esta fórmula nos permite encontrar a forma geral de um conjugado de um elemento $a^u b^v$ de G:

$$(a^i b^j)(a^u b^v)(a^i b^j)^{-1} = a^{i(1-3^v) + u3^j} b^v,$$

o que, por sua vez, nos permite encontrar as classes de conjugação de G. São elas 7 em número:

$$c(1) = \{1\}\,, \quad c(a) = \left\{a, a^3, a^4, a^5, a^9\right\}, \quad c(a^2) = c(a^{-1}) = \left\{a^2, a^6, a^7, a^8, a^{10}\right\},$$
$$c(b) = \{a^u b\}\,, \quad c(b^2) = \left\{a^u b^2\right\}, \quad c(b^3) = \left\{a^u b^3\right\}, \quad c(b^4) = \left\{a^u b^4\right\}, \qquad 0 \le u \le 10.$$

Questão 1 (b): Dada uma representação $\tilde{\rho}\colon K \to \mathbf{GL}(V)$ de K com carácter $\tilde{\chi}$, podemos obter uma representação $\rho\colon G \to \mathbf{GL}(V)$ pondo $\rho(hk) = \tilde{\rho}(k)$. Como

$$\rho\big((hk)(h'k')\big) = \rho\big(h(kh'k^{-1})kk'\big) = \tilde{\rho}(kk') = \tilde{\rho}(k)\tilde{\rho}(k') = \rho(hk)\rho(h'k')$$

ρ é de fato um homomorfismo. (Note que $kh'k^{-1} \in H$ porque $H \trianglelefteq G$.) Se χ é o carácter de ρ, vale $\chi(hk) = \mathrm{tr}(\rho_{hk}) = \mathrm{tr}(\tilde{\rho}_k) = \tilde{\chi}(k)$. Mas $K = \langle b \rangle$ é cíclico de ordem 5, por isso suas representações irredutíves $\tilde{\rho}_i$ são todas de grau 1, dadas por

$$\tilde{\rho}_i(b^j) = \zeta^{ij},$$

onde ζ é raiz quinta primitiva da unidade (i.e., $\zeta^5 = 1$ e $\zeta \ne 1$). Obtemos assim cinco representações de G, todas irredutíveis porque têm grau 1; como G possui sete classes de conjugação, a relação:

$$55 = |G| = \sum_{i=1}^{7} n_i^2,$$

onde n_i é o grau da i-ésima representação irredutível de G, nos permite deduzir que os dois graus restantes, n_6 e n_7, são ambos iguais a 5.

Notando que $|c(g)| = 11$ se $g = b$, b^2, b^3 ou b^4, e usando a relação

$$\sum_{i=1}^{7} |\chi(g)|^2 = |G| \,/\, |c(g)| \qquad\qquad (g \in G),$$

(veja Serre, p. 20), obtemos que χ_6 e χ_7 são ambos nulos nas classes dos elementos citados. Assim, já podemos completar grande parte da tabela de caracteres de G:

	$c(1)$	$c(a)$	$c(a^2)$	$c(b)$	$c(b^2)$	$c(b^3)$	$c(b^4)$
χ_1	1	1	1	1	1	1	1
χ_2	1	1	1	ζ	ζ^2	ζ^3	ζ^4
χ_3	1	1	1	ζ^2	ζ^4	ζ	ζ^3
χ_4	1	1	1	ζ^3	ζ	ζ^4	ζ^2
χ_5	1	1	1	ζ^4	ζ^3	ζ^2	ζ
χ_6	5	α	β	0	0	0	0
χ_7	5	γ	δ	0	0	0	0

Usaremos as várias relações entre os caracteres irredutíveis para calcular $\alpha, \beta, \gamma, \delta$. A equação

$$\sum_{i=1}^{7} \chi_i(g_1)\overline{\chi_i(g_2)} = 0, \qquad (g_1, g_2 \in G \text{ em classes de conjugação distintas})$$

(veja Serre p. 20) nos diz, fazendo $g_1 = a$, $g_2 = a^2$, que

$$\alpha + \gamma \;=\; -1 \;=\; \beta + \delta \;;$$

a ortogonalidade de χ_6 e χ_5, e de χ_7 e χ_5 nos dizem, respectivamente, que:

$$\alpha + \beta \;=\; -1 \;=\; \gamma + \delta \;;$$

logo $\alpha = \delta$ e $\beta = -(1+\alpha) = \gamma$. De posse destas, a comparação das partes imaginárias de $\langle \chi_6 \,|\, \chi_6 \rangle = 1$ nos dá que $\operatorname{Re}\alpha = -1/2$; e a relação $\langle \chi_6 \,|\, \chi_7 \rangle$ nos dá então que $|\alpha|^2 = 3$, ou seja,

$$\alpha = -\frac{1}{2} \pm i\frac{\sqrt{11}}{2}.$$

Como o sinal de $\operatorname{Im}\alpha$ não importa (já que podemos permutar χ_6 e χ_7), a tabela de caracteres é:

	$c(1)$	$c(a)$	$c(a^2)$	$c(b)$	$c(b^2)$	$c(b^3)$	$c(b^4)$
χ_1	1	1	1	1	1	1	1
χ_2	1	1	1	ζ	ζ^2	ζ^3	ζ^4
χ_3	1	1	1	ζ^2	ζ^4	ζ	ζ^3
χ_4	1	1	1	ζ^3	ζ	ζ^4	ζ^2
χ_5	1	1	1	ζ^4	ζ^3	ζ^2	ζ
χ_6	5	α	$\overline{\alpha}$	0	0	0	0
χ_7	5	$\overline{\alpha}$	α	0	0	0	0

onde $\alpha = -\frac{1}{2} + i\frac{\sqrt{11}}{2}$.

Questão 2: Uma questão parecida foi resolvida em aula.

Questão 3: Sejam A um domínio de ideais principais, (e_i) a base canônica de A^n e $N \subseteq A^n$ um submódulo gerado por $\{f_1, \dots, f_n\}$.[†] Considere a matriz B cuja j-ésima coluna é a expressão de f_j na base (e_i). Então existem matrizes invertíveis P e Q tais que PBQ^{-1} é diagonal:

$$PBQ^{-1} = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}.$$

Se $\bar{f}_j = \sum_{\nu=1}^{n} p_{\nu j} f_\nu$ e $\bar{e}_j = \sum_{\nu=1}^{n} q_{\nu j} e_j$, resulta que $\bar{f}_j = d_j \bar{e}_j$. Desta relação concluímos que

$$\frac{A^n}{N} = \frac{A\bar{e}_1 \oplus \cdots \oplus A\bar{e}_n}{A\bar{f}_1 \oplus \cdots \oplus A\bar{f}_n} \simeq A/(d_1) \oplus \cdots \oplus A/(d_n);$$

em particular, A^n/N possui $|A/(d_1)| \cdots |A/(d_n)|$ elementos. No nosso caso $A = \mathbf{Z}/2\mathbf{Z}[x]$, $N = M_1$,

$$B = \begin{pmatrix} x^2+x+1 & x^3+1 & x^4+x^3+x+1 \\ x^3+x^2+x & x^4+1 & x^5+x^4+x+1 \\ x^3+x^2+x & x^4+x^3+x^2+x & x^5+x+1 \end{pmatrix}$$

e 5 operações elementares sobre as linhas de B, a saber,

$$L_3' = L_3 + L_2; \qquad L_2' = L_2 + xL_1; \qquad L_3'' = L_3' + (x^2+1)L_2';$$
$$L_1' = L_1 + (x^2+x+1)L_2'; \quad \text{e} \quad L_2'' = L_2' + (x^2+1)L_3'',$$

[†]Qualquer submódulo de A^n é um módulo livre sobre $m \le n$ geradores. Podemos supor que N é gerado por exatamente n elementos porque podemos tomar $f_{m+1} = \cdots = f_n = 0$ se $m < n$.

nesta ordem,† transformam B na matriz diagonal

$$D = \begin{pmatrix} x^2+x+1 & 0 & 0 \\ 0 & x+1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Da discussão acima resulta que

$$\frac{A^3}{M_1} \simeq \frac{A}{(x^2+x+1)} \oplus \frac{A}{(x+1)}.$$

(Note que suprimimos o termo $A/(1) = (0)$.) Cada um dos dois módulos na decomposição em soma direta acima é irredutível porque os polinômios nos denominadores são ambos irredutíveis. (Um submódulo de $A/(p(x))$ tem a forma $A/(q(x))$, onde $(p(x)) \subseteq (q(x))$, i.e., $q(x) \mid p(x)$.)

Como $A/(p(x))$ tem $2^{\deg(p)}$ elementos (isto só é verdade porque $A = \mathbf{Z}/2\mathbf{Z}[x]$!), concluímos que $M = A^3/M_1$ possui $8 = 4 \cdot 2$ elementos. Isto resolve os itens (a) e (b).

Questão 4 (a): Verdadeira. Começamos provando o seguinte: *Seja I um ideal de um anel noetheriano A. Então I é finitamente gerado.* Suponha o contrário. Por indução, existem $x_k \in I$ ($k \in \mathbf{N}$) tais que

$$\cdots \subsetneq I_k = (x_1, \ldots, x_k) \subsetneq I_{k+1} = (x_1, \ldots, x_{k+1}) \subsetneq \cdots ,$$

o que contradiz a hipótese de ser A noetheriano.

Agora seja D um domínio noetheriano, mas não-principal. Seja $I \subseteq D$ um ideal finitamente gerado não-principal; como todo ideal de D, I é um D-módulo. Suponha que I possa ser escrito como soma direta de módulos do tipo $D/(p^e)$ ou D, como no enunciado. Como para quaisquer $x \in I$ e $a \in D$ não-nulos vale $ax \neq 0$ (pois D é domínio), I não possui torção. Portanto, uma tal soma direta não pode envolver qualquer termo do tipo $D/(p^e)$. Assim, $I \simeq D^n$ para algum n. Se $n = 1$ então I seria principal, logo $n \geq 2$. Seja $\varphi\colon D^n \to I$ um isomorfismo (de D-módulos), e sejam $x_1 = \varphi(e_1)$, $x_2 = \varphi(e_2)$ (onde (e_i) é a base canônica de D^n). De $(-x_2)x_1 + (x_1)x_2 = 0$ obtemos que

$$\varphi(-x_2\, e_1 + x_1\, e_2) = 0, \qquad \text{logo} \qquad -x_2\, e_1 + x_1\, e_2 = 0,$$

pois φ é injetivo; por sua vez, a última relação implica que $x_1 = x_2 = 0$, o que é absurdo. Concluímos que I não pode ser escrito como soma direta de D-módulos cíclicos.

Questão 4 (b): Verdadeira. Seja $\rho\colon G \to \mathbf{GL}(V)$ a representação correspondente a χ, $\dim V = n$. Então $(\rho_g)^2 = \rho_{g^2} = I$, portanto qualquer autovalor λ de ρ_g satisfaz $\lambda^2 = 1$, i.e., $\lambda = \pm 1$. Logo $\chi_g = \mathrm{tr}(\rho_g)$ é soma de 1s e $-1s$, sendo n termos ao todo. Assim: $\chi_g \in \mathbf{Z}$, $-n \leq \chi_g \leq n$ e $\chi_g \equiv n \pmod 2$, já que $1 \equiv -1 \pmod 2$.‡

Questão 4 (c): Verdadeira. Seja $\rho\colon G \to \mathbf{GL}(V)$ a representação de G correspondente a χ e defina uma nova representação $\tilde{\rho}\colon G \to \mathbf{GL}(V)$ por $\tilde{\rho} = \rho \circ \alpha$. Se $\tilde{\chi}$ é seu caracter, vale $\tilde{\chi}_g = \chi_{\alpha(g)}$, logo $\tilde{\chi}_{g_0} = z_1$ e $\tilde{\chi}_{g_1} = z_0$. Além disto,

$$\begin{aligned} \langle \tilde{\chi} \,|\, \tilde{\chi} \rangle &= \frac{1}{|G|} \sum_{g \in G} \left|\chi_{\alpha(g)}\right|^2 \\ &= \frac{1}{|G|} \sum_{g \in G} |\chi_g|^2 = \langle \chi \,|\, \chi \rangle = 1 , \end{aligned}$$

pois α é bijetivo. Concluímos portanto que $\tilde{\chi}$ tem norma 1, ou seja, é irredutível.

† Há mais de um caminho para diagonalizar B por meio de operações elementares sobre suas linhas e colunas, mas o resultado final deve ser D, a menos de uma permutação das entradas diagonais.

‡ Note que a hipótese de ser χ irredutível não era necessária.