

Problema 1

- Num grupo G , sejam a e b dois elementos diferentes da identidade e tais que $a^3 = b^2 = e$ e $ba = a^2b$.
 - Indique, justificando, se:
 - a é sempre igual a b ;
 - a nunca é igual a b ;
 - a pode ser ou não igual a b , consoante o grupo G .
 - Determine a ordem de G e construa a sua tabela.
- Considere agora o grupo H composto pelas simetrias do plano em relação às rectas que passam pela origem e fazem um ângulo múltiplo de 60° com o eixo dos xx e pelas rotações de ângulo múltiplo de 120° em torno da origem.
Averigüe se G e H são isomorfos.

Resolução

- Se fosse $a = b$ ter-se-ia $a^3 = a^2$. Multiplicando ambos os membros por a^{-2} viria $a = e$ contradizendo o enunciado. Logo a e b são distintos (ii).
 - Devido à relação $ba = a^2b$, qualquer produto de a 's, b 's e dos seus inversos pode ser escrito na forma $a^n b^m$, com $n, m \in \mathbb{Z}$. Como a tem ordem 3 e b tem ordem 2, temos os elementos e, a, a^2, b, ab, a^2b e a tabela de G é dada por

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

- O grupo H contém 3 simetrias: em relação ao eixo dos xx , e das duas rectas que fazem um ângulo de 60° com este eixo. Contém ainda 3 rotações: a identidade, e as rotações de 120° e 240° em torno da origem. Assim H é isomorfo ao grupo D_3 que é gerado por dois elementos r e s tais que $r^3 = e$, $s^2 = e$ e $sr = r^2s$. Ora, como em G se tem $a^3 = e$, $b^2 = e$ e $ba = a^2b$, então existe um isomorfismo $\Phi : G \rightarrow H$ definido por $\Phi(a) = r$ e $\Phi(b) = s$. Este é

$$\begin{array}{rcl}
\Phi : & G & \rightarrow H \\
& e & \mapsto e \\
& a & \mapsto r \\
& a^2 & \mapsto r^2 \\
& b & \mapsto s \\
& ab & \mapsto rs \\
& a^2b & \mapsto r^2s
\end{array}$$

Problema 2

Sejam α e β elementos de $S_n - \{\epsilon\}$ e r um número natural. Determine condições suficientes para que

- (i) $\{\epsilon, \alpha, \beta\}$ seja subgrupo de S_n ;
- (ii) $\alpha \circ \beta = \beta \circ \alpha$;
- (iii) α^r seja um ciclo se α for um ciclo;

e averigúe se são também necessárias.

Resolução

- (i) Para que $\{\epsilon, \alpha, \beta\}$ seja subgrupo de S_n é necessário e suficiente que α (e $\beta = \alpha^{-1}$) seja um elemento de ordem três. Portanto S_n tem um tal subgrupo se e só se $n \geq 3$ e, nesse caso, α é qualquer ciclo $(a \ b \ c)$ de comprimento três.
- (ii) $\alpha \circ \beta = \beta \circ \alpha$ se e só se $\alpha = \beta \circ \alpha \circ \beta^{-1}$ o que quer dizer que β é uma das o permutações que se obtêm (Veja Notas, 14.1.3)
 - decompondo α no produto de ciclos disjuntos, por ordem crescente dos seus comprimentos, sem omitir os ciclos de comprimento um,
 - escrevendo α debaixo de α
 - e fazendo corresponder a cada elemento de α o elemento que está na vertical por baixo.
- (iii) Se α é um ciclo de comprimento n , α^r é um ciclo se e só se $m.d.c.(r, n) = 1$:
Se $\sigma = (1 \ 2 \ \dots \ n)$ então

$$\sigma^r = (1 \ 1+_n r \ 1+_n 2r \ \dots \ 1+_n (k-1)r) \dots,$$

sendo k o menor inteiro tal que $1+_n kr = 1$, o que é equivalente a ter $kr \equiv 0$ módulo n .

Como $kr \equiv 0$ se e só se $n|kr$, isso implica que $n|k$ se $m.d.c.(n, r) = 1$. Nesse caso, e o menor valor de k é n e σ^r é um ciclo de comprimento n .

Reciprocamente, suponhamos que $m.d.c.(n, r) = d > 1$. Então

$$\sigma^r = (1 \ 1 +_n r \ 1 +_n 2r \ \cdots \ 1 +_n (n' - 1)r)(\cdots,$$

sendo $n' = n/d$ o que significa que σ^r não é um ciclo mas um produto de ciclos disjuntos.

Problema 3

Considere o grupo $G = \left\{ \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} : ae - bd \neq 0 \right\}$ munido da operação

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \diamond \begin{bmatrix} g & h & i \\ j & k & l \end{bmatrix} = \begin{bmatrix} ag + bj & ah + bk & c + i \\ dg + ej & dh + ek & f + l \end{bmatrix}.$$

1. Mostre que G tem uma estrutura de grupo produto com 3 factores.
2. Considere agora os subgrupos H e K de G definidos por

$$H = \left\langle \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right\rangle$$

$$K = \left\{ \begin{bmatrix} 1 & 0 & m \\ 0 & 1 & n \end{bmatrix} : m, n \in 2\mathbb{Z} \right\}.$$

Mostre que K é um subgrupo de H e determine $[H : K]$.

Resolução

1. Seja $H = (GL_2(\mathbb{R}), \cdot) \times (\mathbb{R}, +) \times (\mathbb{R}, +)$ e consideremos a aplicação

$$\Phi : \begin{matrix} G & \rightarrow & H \\ \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} & \mapsto & \left(\begin{bmatrix} a & b \\ d & e \end{bmatrix}, c, f \right). \end{matrix}$$

- Φ é homomorfismo, uma vez que $\Phi \left(\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \diamond \begin{bmatrix} g & h & i \\ j & k & l \end{bmatrix} \right) =$
 $= \Phi \left(\begin{bmatrix} ag + bj & ah + bk & c + i \\ dg + ej & dh + ek & f + l \end{bmatrix} \right) = \left(\begin{bmatrix} ag + bj & ah + bk \\ dg + ej & dh + ek \end{bmatrix}, c + i, f + l \right) =$
 $= \left(\begin{bmatrix} a & b \\ d & e \end{bmatrix}, c, f \right) \left(\begin{bmatrix} g & h \\ j & k \end{bmatrix}, i, l \right) = \Phi \left(\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \right) \Phi \left(\begin{bmatrix} g & h & i \\ j & k & l \end{bmatrix} \right),$
para todos os pares de elementos de G .
- É imediata a verificação de que Φ é bijectiva, logo Φ é um isomorfismo.

2. Sejam $a = \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}$ e $b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$.

Como $ab = \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix} = ba$, então

$$H = \langle a, b \rangle = \{a^n b^m : n, m \in \mathbb{Z}\} = \left\{ \begin{bmatrix} 1 & 0 & n \\ 0 & (-1)^n & m \end{bmatrix} : n, m \in \mathbb{Z} \right\} \supset K.$$

Para determinar $[H : K]$ vamos averiguar quando é que duas classes laterais esquerdas de K coincidem. Tem-se

$$\begin{aligned} \begin{bmatrix} 1 & 0 & n \\ 0 & (-1)^n & m \end{bmatrix} K &= \begin{bmatrix} 1 & 0 & p \\ 0 & (-1)^p & q \end{bmatrix} K \Leftrightarrow \\ \Leftrightarrow \begin{bmatrix} 1 & 0 & n \\ 0 & (-1)^n & m \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 & p \\ 0 & (-1)^p & q \end{bmatrix} &\in K \Leftrightarrow \\ \Leftrightarrow \begin{bmatrix} 1 & 0 & p-n \\ 0 & (-1)^{p-n} & q-m \end{bmatrix} &\in K \Leftrightarrow p-n \in 2\mathbb{Z} \wedge q-m \in 2\mathbb{Z}. \end{aligned}$$

Logo há quatro classes laterais correspondentes às paridades das entradas da 3ª coluna dos elementos de H . Explicitamente, as 4 classes laterais são

$$K, \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} K, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} K \text{ e } \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \end{bmatrix} K.$$

Problema 4

Determine

- (i) todos os subgrupos do grupo $\mathbb{Z}_n$;
- (ii) quantos homomorfismos existem de $\mathbb{Z}_n$ em $\mathbb{Z}_m$;
- (iii) condições de existência de um homomorfismo sobrejectivo de $\mathbb{Z}_n$ em $\mathbb{Z}_m$.

Resolução

1. $\mathbb{Z}_n$ tem um e um só subgrupo de ordem m para cada factor m de n :

- Todo o subgrupo H do grupo cíclico $\mathbb{Z}_n$ (de qualquer grupo cíclico) é cíclico:
 - $H = \{0\}$ é cíclico;
 - se $H \neq \{0\}$ e m é o menor inteiro positivo que pertence a H então $H = \langle m \rangle$: se $s \in H$ e $s = mq + r$, com $0 \leq r < m$, como $r = s - mq \in H$, pela minimabilidade de m , $r = 0$.

- Todo o divisor próprio de n gera um subgrupo próprio de $\mathbb{Z}_n$: se $n = mk$ então k tem ordem m e, consequentemente, gera um subgrupo de ordem m .
 - Existe um e um só subgrupo de ordem m para cada factor m de n que é o subgrupo gerado por n/m .
2. Existem d homomorfismos de $\mathbb{Z}_n$ em $\mathbb{Z}_m$ sendo d o máximo divisor comum de n e m :

Se

$$f : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$$

e $f(1) = a$ então $0 = f(n \cdot 1) = nf(1) = na$, portanto $na \equiv 0 \pmod{m}$. Assim, se $na = mk$ vem que

$$a = \frac{mk}{n} = \frac{m'dk}{n'd} = \frac{m'k}{n'}$$

sendo $m.d.c.(m', n') = 1$. Como a é um inteiro, $n'|k$. Temos então que $k = sn'$ com $s = 0, 1, \dots, (d-1)$, a que correspondem d homomorfismos distintos.

3. Existe um homomorfismo sobrejectivo de $\mathbb{Z}_n$ em $\mathbb{Z}_m$ se e só se m divide n :

Se $f : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ é homomorfismo sobrejectivo então, pelo primeiro Teorema de Isomorfismo, $\mathbb{Z}_m \cong \mathbb{Z}_n/N$, sendo N o núcleo de f . Logo

$$|\mathbb{Z}_m| = \frac{|\mathbb{Z}_n|}{|N|},$$

portanto m divide n .

Reciprocamente, se $n = mk$ então $N = \langle m \rangle$ é o subgrupo de $\mathbb{Z}_n$ de ordem k e a projecção canónica $p : \mathbb{Z}_n \rightarrow \mathbb{Z}_n/N$ é um homomorfismo sobrejectivo. Como $\mathbb{Z}_n/N$ é cíclico e tem ordem m ele é isomorfo a $\mathbb{Z}_m$.

Problema 5

Determine todos os subgrupos- p de Sylow normais em G , onde

1. $G = \mathbb{Z}_n$
2. $G = D_n$
3. $G = S_n$

Resolução

Lema: Seja S um subgrupo- p de Sylow de um grupo finito G . Então S é normal sse contém todos os elementos cuja ordem é uma potência de p .

Prova.

($\Rightarrow$) Seja $g \in G$ com ordem potência de p . Então a ordem do elemento $gS \in G/S$ também é uma potência de p . Mas G/S é um grupo cuja ordem é prima com p , logo $gS = S$, ou seja, $g \in S$.

($\Leftarrow$) Seja S' um subgrupo- p de Sylow de G . As ordens dos elementos de S' são potências de p , logo $S' \subseteq S$, donde $S' = S$. Portanto S é normal em G .

Para qualquer grupo G , se p não divide $|G|$, tem-se que o único subgrupo- p de Sylow de G é $S = \{e\}$, logo $S \triangleleft G$. Resta assim analisar os casos em que p divide $|G|$.

1. Como $G = \mathbb{Z}_n$ é abeliano, todos os seus subgrupos são normais.

2. Seja $n = 2^m k$, com $m \geq 0$ e k ímpar.

- Seja S um subgrupo-2 de Sylow de D_n . Pelo lema, se S é normal contém todas as reflexões. O produto de duas reflexões distintas é uma rotação, logo S contém mais de metade dos elementos de D_n e portanto $S = D_n$. Conclui-se que S é normal sse n é uma potência de 2.
- Seja p um primo que divide k . Um subgrupo- p de Sylow S de D_n é um subconjunto do subgrupo cíclico das rotações. Assim, S é único e portanto normal.

Portanto um subgrupo- p de Sylow é normal em D_n sse $p \neq 2$ ou n é uma potência de $p = 2$.

- 3.
- Seja S um subgrupo-2 de Sylow de S_n . Pelo lema, se S é normal contém todas as transposições. Logo $S = S_n$. Ora S_n tem ordem potência de 2 sse $n = 2$, logo $S \triangleleft S_n$ sse $n = 2$.
 - Seja S um subgrupo-3 de Sylow de S_n . Pelo lema, se S é normal contém todos os ciclos de ordem 3. Se $n \geq 4$, S contém o produto $(123)(124) = (13)(24)$ que tem ordem 2, absurdo. Para $n = 3$, S tem metade dos elementos de S_n , logo $S \triangleleft S_3$.
 - Seja S um subgrupo- p de Sylow de S_n , com $p \geq 4$. Pelo lema, se S é normal contém todos os ciclos de ordem p . Ora $(p(p-1)(p-2) \cdots 4312)(1234 \cdots (p-1)p) = (1p2) \in S$ tem ordem 3, absurdo.

Portanto um subgrupo- p de Sylow é normal em S_n sse $p = n = 2$ ou $p = n = 3$ ou $p > n$.