Álgebra I - Exame de 12 de Julho de 2005

Uma forma de resolução

1. Considere o conjunto $\mathbb{Z}$ munido com a seguinte operação:

$$a \circ b = a + b - 1 \ \ a, b \in \mathbb{Z}.$$

   (a) Mostre que $(\mathbb{Z}, \circ)$ é um grupo.

   (b) Prove que a aplicação $f : (\mathbb{Z}, +) \to (\mathbb{Z}, \circ)$ definida por $f(a) = a + 1$ é um isomorfismo de grupos.

   (c) Conclua que $(\mathbb{Z}, \circ)$ é cíclico e indique todos os seus geradores.

   1.(a) (i) Como $\mathbb{Z}$ é fechado para a adição usual de inteiros, $a \circ b \in \mathbb{Z}$, para $a, b \in \mathbb{Z}$;

   (ii) Se $a, b, c \in G$ então $(a \circ b) \circ c = (a+b-1)+c-1$ e $a \circ (b \circ c) = a+(b+c-1)-1$. Como a adição é uma operação associativa e comutativa em $\mathbb{Z}$, podemos concluir que $(a \circ b) \circ c = a \circ (b \circ c)$;

   (iii) o elemento neutro é 1 uma vez que $a \circ 1 = a = 1 \circ a$, para qualquer $a \in \mathbb{Z}$;

   (iv) se $a \in \mathbb{Z}$, o seu oposto é o inteiro $2 - a$ pois $a \circ (2 - a) = 1 = (2 - a) \circ a$.

   Conclusão: de (i), (ii), (iii) e (iv) podemos concluir que $(\mathbb{Z}, \circ)$ é um grupo.

   1.(b) A aplicação f é bijectiva e, como, para todo o $a, b \in \mathbb{Z}$,

$$f(a) \circ f(b) = (a + 1) \circ (b + 1) = a + b + 1 = f(a + b),$$

   f é um isomorfismo.

   1.(c) Uma vez que os grupos $(\mathbb{Z}, +)$ e $(\mathbb{Z}, \circ)$ são isomorfos e $(\mathbb{Z}, +)$ é cíclico, podemos concluir que $(\mathbb{Z}, \circ)$ é também cíclico.

   Por f ser um isomorfismo de grupos, os geradores de $(\mathbb{Z}, \circ)$ vão ser as imagens por f dos geradores de $(\mathbb{Z}, +)$. Assim, $(\mathbb{Z}, \circ) =< f(1) = 2 >$ e $(\mathbb{Z}, \circ) =< f(-1) = 0 >$.

2. Determine todos os subgrupos próprios de $\mathbb{Z}_{21}$ e os respectivos grupos quocientes.

   Como $\mathbb{Z}_{21}$ é um grupo cíclico de ordem 21 tem um e um só subgrupo de cada ordem que divide 21, logo $\mathbb{Z}_{21}$ tem só dois subgrupo próprios: um de ordem 3 e outro de ordem 7. Então, os subgrupos próprios de $\mathbb{Z}_{21}$ são: $< 3 >= \{0, 3, 6, 9, 12, 15, 18\}$ e $< 7 >= \{0, 7, 14\}$.

   Como $\mathbb{Z}_{21}$ é um grupo cíclico, logo abeliano, todos os seus subgrupos são normais e podemos considerar os respectivos os grupos quocientes: $\mathbb{Z}_{21}/ < 3 >= \{< 3 >, 1+ < 3 >, 2+ < 3 >\}$ e $\mathbb{Z}_{21}/ < 7 >= \{< 7 >, 1+ < 7 >, 2+ < 7 >, 3+ < 7 >, 4+ < 7 >, 5+ < 7 >, 6+ < 7 >\}$, uma vez que $a + H = b + H$ se e só se $a - b \in H$.

3. (a) Prove que O_n e SO_n são subgrupos do grupo linear $GL_n(\mathbb{R})$.

   (b) Mostre que SO_n é um subgrupo normal de O_n.

   3.(a) $GL_n(\mathbb{R})$ é o grupo das matrizes reais quadradas de ordem n invertíveis com a multiplicação usual de matrizes, $O_n = \{A \in GL_n(\mathbb{R}) \mid A^t A = I_n\}$ e $SO_n = \{A \in O_n \mid det(A) = 1\}$

   (i) $O_n \neq \emptyset$ pois a matriz identidade é ortogonal;

   (ii) Se $A, B \in O_n$ então, como $B^{-1} = B^t$,

$$\begin{aligned} (AB^{-1})^t(AB^{-1}) &= (B^{-1})^t A^t AB^{-1} \\ &= (B^t)^t B^{-1} \\ &= BB^{-1} = I_n \end{aligned}$$

e $AB^{-1} \in O_n$. Podemos assim concluir que O_n é subgrupo de $GL_n(\mathbb{R})$.

(iii) SO_n é um subconjunto de $GL_n(\mathbb{R})$ diferente do vazio uma vez que o determinante da matriz identidade é igual a 1;

(iv) Se $A, B \in SO_n$, então, por (ii), $AB^{-1} \in O_n$ e $det(AB^{-1}) = det(A)det(B^{-1}) = det(A)\frac{1}{det(B)} = 1$ e $AB^{-1} \in SO_n$. Assim, SO_n é subgrupo de $GL_n(\mathbb{R})$.

3.(b) Como SO_n é subconjunto de O_n e é grupo para a mesma operação (alínea anterior), é também subgrupo de O_n.

Mostremos que é normal em SO_n. Sejam $A \in SO_n$ e $B \in O_n$: Então $BAB^{-1} \in O_n$ e $det(BAB^{-1}) = det(B)det(A)\frac{1}{det(B)} = det(A) = 1$, logo $BAB^{-1} \in SO_n$.

4. Considere função $f : S_n \to S_{n+2}$ definida por $f(\alpha) = \alpha_*$, onde

$$\alpha_* = \begin{cases} \alpha & \text{se } \alpha \text{ é par} \\ \alpha\,(n+1\;\;n+2) & \text{se } \alpha \text{ é ímpar.} \end{cases}$$

(a) Prove f define um isomorfismo de S_n num subgrupo H de A_{n+2}.

(b) Indentifique H no caso $n = 3$.

(c) Use o teorema de Cayley para provar que qualquer grupo G de ordem n é isomorfo a um subgrupo de A_{n+2}.

4.(a) Provemos que é um homomorfismo de grupos, isto é, $f(\alpha\beta) = f(\alpha)f(\beta)$, $\alpha, \beta \in S_n$:

(i) se α e β são pares então $\alpha\beta$ é uma permutação par e temos $f(\alpha)f(\beta) = \alpha\beta = f(\alpha\beta)$;

(ii) se α e β são ímpares então $\alpha\beta$ é uma permutação par e temos

$$f(\alpha)f(\beta) = \alpha\,(n+1\;\;n+2)\,\beta\,(n+1\;\;n+2) = \alpha\beta = f(\alpha\beta),$$

porque $\beta\,(n+1\;\;n+2) = (n+1\;\;n+2)\,\beta$, pois β e $(n+1\;\;n+2)$ actuam em conjuntos disjuntos;

(iii) se α é par e β é ímpar então $\alpha\beta$ é uma permutação ímpar e temos

$$f(\alpha)f(\beta) = \alpha\beta\,(n+1\;\;n+2) = f(\alpha\beta);$$

(iv) se α é ímpar e β é par então $\alpha\beta$ é uma permutação ímpar e temos

$$f(\alpha)f(\beta) = \alpha\,(n+1\;\;n+2)\beta = \alpha\beta\,(n+1\;\;n+2) = f(\alpha\beta).$$

Como a aplicação f é injectiva, f define um isomorfismo de S_n no subgrupo de S_{n+2}, $f(S_n)$. Denotemos $f(S_n)$ por H.

Temos ainda, que, para todo $\alpha \in S_n$ a permutação α_* de S_{n+2} é par, logo H é um subgrupo de A_{n+2}.

4.(b) Para $n = 3$ temos

$$\begin{array}{rrl} f: & S_3 \to & H < A_5 \\ & \varepsilon \mapsto & \varepsilon \\ & (12) \mapsto & (12)(45) \\ & (13) \mapsto & (13)(45) \\ & (23) \mapsto & (23)(45) \\ & (123) \mapsto & (123) \\ & (132) \mapsto & (132) \end{array},$$

logo $H = \{\varepsilon, (12)(45), (13)(45), (23)(45), (123), (132)\}$.

4.(c) Seja G um grupo de ordem n. Pelo teorema de Cayley, G é isomorfo a um subgrupo K de S_n, mas, pela alínea anterior, K é isomorfo a um subgrupo $f(K)$ de A_{n+2}, logo G é isomorfo a $f(K)$.

5. Diga, *justificando*, se são verdadeiras ou falsas as afirmações:

   (a) Dois grupos de ordem 17 são isomorfos.

   (b) As permutações de S_9 $\alpha = (456)(1245)$ e $\beta = (153)(1235)(89)$ são conjugadas.

   (c) O conjunto $\{1, 2, \cdots, n-1\}$, para $n \geq 3$, é um grupo para a multiplicação módulo n.

   (d) Um grupo G de ordem 10 não pode ter dois subgrupos distintos de ordem 5.

   5.(a) Verdadeira: Todo o grupo de ordem prima p é cíclico, logo isomorfo a $\mathbb{Z}_p$.

   5.(b) Falsa: Decompondo as permutações em ciclos disjuntos obtemos, $\alpha = (125)(46)$ e $\beta = (12)(89)$, que não têm o mesmo número de ciclos de igual comprimento, logo não são conjugadas.

   5.(c) Falsa: só é verdadeira se n for primo, porque pode não ser fechado para a operação. Por exemplo, se n é composto, $n = ab$ então $a \times_n b = 0 \notin \{1, 2, \cdots, n-1\}$.

   5.(d) Verdadeira: Como $10 = 2 \times 5$, pelos teoremas de Sylow o número de subgrupos de G de ordem 5 é $t \equiv 1 (mod\, 5)$ tal que $t|2$. Logo $t = 1$ e G tem um único subgrupo de ordem 5.

6. Determine os coeficientes de torsão de um grupo abeliano de ordem 180 que não tenha elementos de ordem 9 nem de ordem 12.

   Como $180 = 2^2 \times 3^2 \times 5$, para não ter elementos de ordem 9 nem de ordem 12, G terá de ser isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, logo os seus coeficientes de torsão são 6 e 30.

7. Seja G um grupo que contém um subgrupo normal H isomorfo a $\mathbb{Z}_2$. Se G/H é um grupo cíclico infinito, prove que:

   (a) G contém um subgrupo K isomorfo a $\mathbb{Z}$;

   (b) $G = KH$;

   (c) $G \cong \mathbb{Z} \times \mathbb{Z}_2$.

   7.(a) Como G/H é um grupo cíclico infinito, $G/H =< gH >$, para algum $g \in G$. Seja $K =< g >$. Como gH tem ordem infinita, também g tem ordem infinita, logo K é um subgrupo cíclico infinito de G e $K \cong \mathbb{Z}$.

   7.(b) Como $H \cong \mathbb{Z}_2$, $H = \{e, a\}$. É imediato que $KH \subseteq G$. Provemos a outra inclusão. Seja $x \in G$. Então $x \in g^n H$, para algum $n \in \mathbb{Z}$ e $x = g^n h \in KH$.

   7.(c) (i) $H \cap K = \{e\}$: se $x \in H \cap K$ então $x \in H$ e $x = e$ ou $x = a$.

   $a \notin K$ porque em K o único elemento de ordem finita é o elemento neutro.

   (ii) $hk = kh$ para todo o $h \in H$ e $k \in K$: se $h \in H$ então $h = e$ ou $h = a$. Se $h = e$ a igualdade é imediata.

   Suponhamos que $h = a$. Então $ka \in kH = Hk$, visto H ser normal em G, e $ka = h'k$, para $h' \in H$. Mas $h' \neq e$, porque $a \neq e$, logo $h' = a$ e temos $ka = ak$.

   Conclusão: de (b), (i) e (iii) podemos concluir que $G \cong K \times H \cong \mathbb{Z} \times \mathbb{Z}_2$.