Instituto Superior Técnico
Departamento de Matemática

Introdução à Álgebra — LMAC

Exame 2 - 14 de Julho de 2021 - 15:00
Duração: 2 horas

Apresente e justifique todos os cálculos.

[2.0] 1. Mostre que S_n é gerado por $n-1$ permutações de ordem 2.

Sugestão: comece por mostrar que $(1\ k)(1\ k-1)\ldots(1\ 3)(1\ 2)$ é um ciclo de ordem k para qualquer $k \in \mathbb{Z}_{\geq 2}$.

R.: Seja $\sigma = (1\ k)(1\ k-1)\ldots(1\ 3)(1\ 2)$. É simples verificar que $\sigma(1) = 2$, $\sigma(2) = 3$, etc., pelo que

$$(1\ k)(1\ k-1)\ldots(1\ 3)(1\ 2) = (1\ 2\ \ldots\ k-1\ k).$$

Da mesma forma, qualquer k-ciclo $(a_1, \ldots, a_k)$ de S_n pode ser obtido como um produto de permutações de ordem 2,

$$(a_1\ a_k)(a_1\ a_{k-1})\ldots(a_1\ a_3)(a_1\ a_2) = (a_1\ a_2\ \ldots\ a_{k-1}\ a_k),$$

e portanto todas as permutações, que são produtos de ciclos, podem ser obtidas como produtos de 2-ciclos.

[2.0] 2. Descreva todos os homomorfismos $h : D_{2n} \to Q_8$, para cada $n \in \mathbb{Z}_{\geq 2}$ (indique apenas os valores atribuídos aos geradores de D_{2n}, distinguindo os casos n par e n ímpar).

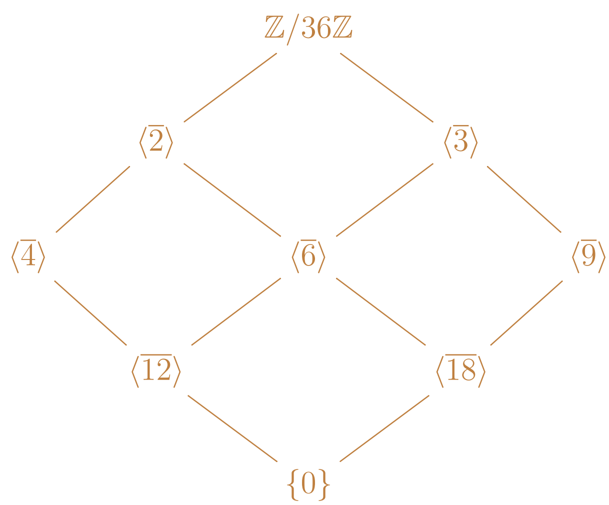
R.: Qualquer homomorfismo $h : D_{2n} \to G$ é unicamente determinado pelos valores $h(r)$ e $h(s)$, e qualquer escolha de tais valores define um homomorfismo se e só se respeita as relações de D_{2n} em G:

$$h(r)^n = 1,\ h(s)^2 = 1,\ h(r)h(s) = h(s)h(r)^{-1}.$$

Todos os elementos de $Q_8 \setminus \{1\}$ têm ordem par e, por isso, se n for ímpar temos de ter $h(r) = 1$. E o único elemento de Q_8 que tem ordem 2 é -1, pelo que tem de ter-se $h(s) = -1$ ou $h(s) = 1$. A relação $h(r)h(s) = h(s)h(r)^{-1}$ é satisfeita em ambos os casos, e portanto para cada n ímpar há exactamente dois homomorfismos, correspondendo às escolhas $h(r) = 1$ e $h(s) = \pm 1$. No caso de n ser par estas escolhas são igualmente válidas, mas podemos também ter $h(r) = -1$ em combinação com $h(s) = -1$ ou $h(s) = 1$. Note-se também que $h(s)$ é central em Q_8, e por isso a relação $h(r)h(s) = h(s)h(r)^{-1}$ impõe $h(r) = h(r)^{-1}$, ou seja, $h(r)^2 = 1$, e portanto, mesmo que $n \geq 4$, não há mais nenhuma opção para o valor de $h(r)$ porque as ordens dos elementos $\pm i$, $\pm j$, e $\pm k$, são iguais a 4. Portanto se n for par há exactamente 4 homomorfismos, correspondentes às 4 atribuições dos valores ± 1 a $h(r)$ and $h(s)$.

[2.0] 3. Desenhe o reticulado de subgrupos de $\mathbb{Z}/36\mathbb{Z}$.

R.: Uma vez que $36 = 2^2 \times 3^3$, tem-se



[2.0] 4. Calcule o centralizador do conjunto $\{s, r^3\}$ em D_{16}.

R.: s comuta com r^k se e só se $sr^k = r^k s = sr^{-k}$ se e só se $r^{2k} = 1$, o que significa que $k = 0$ ou $k = 4$ são os únicos valores de $k \in \{0, \ldots, 7\}$ para os quais s comuta com r^k. Portanto $C(s) = \langle s, r^4 \rangle$. Por outro lado, sr^k comuta com r^3 se e só se $sr^{k+3} = sr^k r^3 = r^3 sr^k = sr^{k-3}$, se e só se $r^6 = 1$, o que é falso em D_{16}. Logo, $C(r^3) = \langle r \rangle$, e por isso $C(\{s, r^3\}) = C(r^3) \cap C(s) = \langle r^4 \rangle$.

[2.0] 5. (a) Seja $n \in \mathbb{N}$. Mostre que qualquer subgrupo de $\mathbb{Z}/n\mathbb{Z}$ é um subanel.

R.: Seja $A \subset \mathbb{Z}/n\mathbb{Z}$ um subgrupo. Para mostrar que A é subanel temos apenas de verificar que $\overline{a}\overline{b} \in A$ para quaisquer $\overline{a}, \overline{b} \in A$. Sejam $a, b \in \{0, 1, \ldots, n-1\}$. Então, devido à distributividade do anel $\mathbb{Z}/n\mathbb{Z}$,

$$\overline{a}\overline{b} = \overline{a}(\underbrace{\overline{1} + \cdots + \overline{1}}_{b \text{ times}}) = \underbrace{\overline{a}\overline{1} + \cdots + \overline{a}\overline{1}}_{b \text{ times}} = \underbrace{\overline{a} + \cdots + \overline{a}}_{b \text{ times}} \in A.$$

[1.0] (b) Dê um exemplo de um anel R e de um subgrupo de R que não é um subanel.

R.: Tome-se por exemplo $R = \mathbb{Z}[x]$ e $A = \mathbb{Z}x = \{\ldots, -2x, -x, 0, x, 2x, \ldots\}$. Obviamente A não é fechado para o produto de polinómios.

[2.0] 6. Sendo B um anel booleano, mostre que a relação binária $\leq$ definida em B por

$$x \leq y \iff xy = x$$

é uma ordem parcial (i.e., uma relação reflexiva, transitiva e anti-simétrica), e que nessa ordem quaisquer dois elementos $x, y \in B$ têm ínfimo igual a xy.

R.: Vamos verificar que $\leq$ é uma ordem parcial:

Reflexividade: $x \leq x$ porque $xx = x$.

Transitividade: Seja $x \leq y \leq z$, ou seja, $xy = x$ e $yz = y$. Então $xz = (xy)z = x(yz) = xy = x$, e portanto $x \leq z$.

Anti-simetria: Seja $x \leq y$ e $y \leq x$, ou seja, $xy = x$ e $yx = y$. Uma vez que qualquer anel booleano é comutativo, conclui-se $x = y$.

Agora vamos ver que xy é o ínfimo de x e de y. Primeiro, vejamos que é um minorante:

- A condição $xy \leq y$ é equivalente a $(xy)y = xy$, que é verdadeira porque $y^2 = y$.
- A condição $xy \leq x$ é equivalente a $(xy)x = xy$, que é verdadeira porque $x^2 = x$ e qualquer anel booleano é comutativo.

Agora provemos que xy é o maior dos minorantes de $\{x, y\}$. Seja z outro minorante. Então tem-se $zx = z$ e $zy = z$, e portanto $zxy = zy = z$, ou seja, $z \leq xy$.

[0.5] 7. (a) Enumere todos os elementos invertíveis de $\mathbb{Z}[i]$.

R.: $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

[1.5] (b) Sejam $a, b \in \mathbb{Z}$, e seja N a norma habitual de $\mathbb{Z}[i]$. Mostre que se $N(a+bi)$ for um número primo então $a+bi$ é irredutível em $\mathbb{Z}[i]$.

R.: Se $a+bi$ não fosse irredutível haveria dois elementos não invertíveis $c+di$ e $e+fi$ tais que $(c+di)(e+fi) = a+bi$, e portanto, uma vez que a norma é multiplicativa, ter-se-ia $N(a+bi) = N(c+di)N(e+fi)$. Isto é uma contradição porque $N(a+bi)$ é primo mas nem $N(c+di)$ nem $N(e+fi)$ são invertíveis em $\mathbb{Z}$.

[2.0] (c) Mostre que $\mathbb{Z}[i]/(1+6i)$ é um corpo.

R.: Da alínea anterior resulta que $1+6i$ é irredutível, pois $N(1+6i) = 37$ é primo. Se houvesse um ideal próprio I de $\mathbb{Z}[i]$ tal que $(1+6i) \subset I$ e $(1+6i) \neq I$ então, uma vez que $\mathbb{Z}[i]$ é um domínio de ideais principais (até é domínio euclidiano), teríamos $I = (a)$ para algum $a \in \mathbb{Z}[i]$, e a não pode ser invertível porque caso contrário ter-se-ia $I = \mathbb{Z}[i]$, contradizendo a hipótese de I ser um ideal próprio. Mas então $1+6i$ teria um divisor não invertível a, contradizendo o facto de ser irredutível. Portanto $(1+6i)$ é um ideal maximal, e por isso $\mathbb{Z}[i]/(1+6i)$ é um corpo.

[3.0] 8. Mostre que se um grupo G tiver ordem 14 então tem um e um só subgrupo de ordem 7.

Sugestão: comece por mostrar que existe pelo menos um subgrupo de ordem 7, analisando separadamente o caso em que G é não-abeliano e o caso em que G é abeliano, e recordando que um grupo cujos elementos têm todos ordem menor ou igual a 2 é necessariamente abeliano. Depois demonstre a unicidade do subgrupo de ordem 7.

R.: Em primeiro lugar observamos que, uma vez que 7 é primo, um grupo de ordem 7 é necessariamente cíclico. Logo, existe um subgrupo de G com ordem 7 se e só se existir um elemento de G com ordem 7.

A seguir vamos mostrar que tem de existir algum elemento de G com ordem 7.

Caso 1: assume-se que G não é abeliano. Se todos os elementos $x \in G$ satisfizessem $x^2 = 1$ então G seria abeliano, portanto existe pelo menos um elemento de ordem diferente de 2. Por outro lado, se existisse um elemento de ordem 14 então $G \cong Z_{14}$ e portanto mais uma vez G seria abeliano. Logo, G tem de ter elementos que não são de ordem 2 nem de ordem 14, pelo que existe um elemento de ordem 7 (uma vez que a ordem de cada elemento tem de ser um divisor de 14).

Caso 2: assume-se que G é abeliano. Seja $x \in G$, $x \neq 1$. Então $|x|$ é 2, 7, ou 14. Se $|x| = 7$ então já encontrámos um elemento de ordem 7 em G, como pretendido. Se $|x| = 14$ então $|x^2| = 7$. Se $|x| = 2$ então $H := \{1, x\}$ é subgrupo de G, necessariamente normal porque G é abeliano. Então $|G/H| = 7$, e assim G/H é um grupo cíclico, havendo portanto $z \in G$ tal que zH tem ordem 7 em G/H, e portanto z tem ordem 7 ou 14 em G. Logo, temos $|z| = 7$ ou $|z^2| = 7$, e portanto, mais uma vez, existe necessariamente um elemento de G com ordem 7.

Agora que já provámos que existe necessariamente $H \leq G$ com $|H| = 7$, vamos ver que H é o único subgrupo de ordem 7. Com efeito, suponha-se que $K \leq G$ e $|K| = 7$, e recordemos a fórmula

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Como $H \cap K$ é um subgrupo de H, a sua ordem é 1 ou 7. Então, se $H \neq K$, $H \cap K$ é um subgrupo próprio de H e por isso $|H \cap K| = 1$. Logo, concluímos que $|HK| = 49 > |G|$, o que é absurdo. Por isso tem de ter-se $H = K$.