Instituto Superior Técnico
Departamento de Matemática
Secção de Álgebra e Análise

Fundamentos de Álgebra

LMAC e MMA

Teste 1 – 18 de Novembro de 2013 – Resolução

1. (a) (i) Provamos que $ba^i = a^{-i}b$ por indução em i:
$i = 0$: não há nada a provar.
$i \Rightarrow i+1$: $ba^{i+1} = ba^i a = a^{-i}ba = a^{-i}a^{-1}b = a^{-(i+1)}b$ e podemos concluir a igualdade pedida para $i \geq 0$.
$i \Rightarrow i-1$: $ba^{i-1} = ba^i a^{-1} = a^{-i}ba^{-1} = a^{-i}a^1 b = a^{-(i-1)}b$ e podemos concluir a igualdade pedida para $i \leq 0$.

(ii) Da parte (i) concluimos que qualquer elemento de D_{10} é da forma $a^i b^j$ com $0 \leq i \leq 9$ e $0 \leq j \leq 1$, logo $|D_{10}| \leq 20$. Para termos $D_{10} = 20$ é preciso mostar que para escolhas diferentes de (i, j) obtemos elementos distintos. Seja então $a^{i_1}b^{j_1} = a^{i_2}b^{j_2}$ com $0 \leq i_1, i_2 \leq 9$ e $0 \leq j_1, j_2 \leq 1$. Então

$$\begin{aligned} a^{i_1}b^{j_1} = a^{i_2}b^{j_2} \Leftrightarrow a^{i_1-i_2} = b^{j_2-j_1} \Rightarrow a^{i_1-i_2} = b^{j_2-j_1} = 1 \\ \Rightarrow 10 \mid i_1 - i_2 \quad e \quad 2 \mid j_2 - j_1 \Rightarrow i_1 = i_2 \quad e \quad j_2 = j_1 \ , \end{aligned}$$

onde no último passo se usou $-9 \leq i_1 - i_2 \leq 9$, $-1 \leq j_2 - j_1 \leq 1$.

(b) Sejam n o número de subgrupos-2 de Sylow e m o número de subgrupos-5 de Sylow. Então, pelos Teoremas de Sylow:

$$\begin{aligned} m \equiv 1 \bmod 5 \text{ e } m \mid 2^2 \Rightarrow m = 1; \qquad (*) \\ n \equiv 1 \bmod 2 \text{ e } n \mid 5 \Rightarrow n = 1 \text{ ou } n = 5. \end{aligned}$$

Como $|a| = 10$, então $|a^2| = 5$ e $P = \langle a^2 \rangle \cong \mathbb{Z}_5$ é o subgrupo-5 de Sylow.
Como qualquer reflexão tem ordem 2, então tem de estar contida num subgrupo-2 de Sylow. Logo $n \neq 1$, pois D_{10} contém dez reflexões. Para determinar os 5 subgrupos, basta ver que a^5 tem ordem dois e comuta com b (na realidade $C(D_{10}) = \langle a^5 \rangle$) e, portanto, $Q = \langle a^5, b \rangle = \{1, a^5, b, a^5 b\}$ tem ordem 4, logo é um subgrupo-2 de Sylow. Os restantes podem-se obter por conjugação a partir de Q e a lista completa é

$$\langle a^5, b \rangle, \quad \langle a^5, ab \rangle, \quad \langle a^5, a^2 b \rangle, \quad \langle a^5, a^3 b \rangle \quad \text{e} \quad \langle a^5, a^4 b \rangle \ .$$

(c) Como se viu em $(*)$ da alínea anterior, um grupo G de ordem 20 só tem um subgrupo-5 de Sylow P, com ordem $|P| = 5$. Logo $P \lhd G$ (porque, caso contrário, um seu conjugado seria outro subgrupo-5 de Sylow), $P \neq \{1\}$ e $P \neq G$, logo G não é um grupo simples.

2. (a) Seja $\pi : G \to G/N$ a projecção canónica.

   ($\Rightarrow$) Seja $K = \pi^{-1}(H)$. Então $\pi(K) = H$ e $K > N = \pi^{-1}(1_H)$, ou seja $H = K/N$. Como $H \lhd G/N$ e

   $$\pi(gkg^{-1}) = \pi(g)\pi(k)\pi(g^{-1}) \in H \Leftrightarrow gkg^{-1} \in K \qquad (**)$$

   para quaisquer $g \in G$ e $k \in K$, temos que $K \lhd G$.

   ($\Leftarrow$) A equivalência $(**)$, assumindo agora que $K \lhd G$, dá-nos que $K/N \lhd G/N$.

   (b) Um grupo é resolúvel sse tem uma série resolúvel (i.e. com factores abelianos). Logo existem

   $$1 \lhd N_n \lhd \cdots \lhd N_1 \lhd N_0 := N \ ,$$
   $$1 \lhd H_m \lhd \cdots \lhd H_1 \lhd H_0 := G/N$$

   com N_i/N_{i+1} e H_i/H_{i+1} grupos abelianos. Pela alínea (a), $H_i = K_i/N$ com $K_{i+1} \lhd K_i$ e $N \lhd K_i$. Portanto

   $$1 \lhd N_n \lhd \cdots \lhd N_1 \lhd N \lhd K_m \lhd \cdots \lhd K_0 = G$$

   é uma série resolúvel para G porque

   - $K_m/N = H_m = H_m/1$ é abeliano,
   - $\dfrac{K_i}{K_{i+i}} \cong \dfrac{K_i/N}{K_{i+1}/N} = \dfrac{H_i}{H_{i+i}}$ é abeliano (onde se usou o 3º Teorema de Isomorfismos de Grupos)

   e os restantes factores são também abelianos pois são factores da série resolúvel para N. Logo G é resolúvel.

   (c) Seja $G = S_3$ e $N = A_3$. Como $A_3 \cong \mathbb{Z}_3$ então A_3 é nilpotente (porque é abeliano, ou porque é um grupo-3). Como $[S_3 : A_3] = 2$, então $A_3 \lhd S_3$ e $S_3/A_3 \cong \mathbb{Z}_2$ é nilpotente. Se S_3 fosse nilpotente, então $S_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$ (produto de um Sylow-3 por um Sylow-2) seria um grupo abeliano – contradição.

3. (a) Sejam $g = \sum_{i=0}^{\infty} b_i x^i, h = \sum_{i=0}^{\infty} c_i x^i \in D[[x]]$ tais que $f = gh$. Então

   $$f = gh \underset{\text{(termo } i=0)}{\Rightarrow} a_0 = b_0 c_0 \underset{(a_0 \text{ irredutível})}{\Rightarrow} b_0 \in D^\times \quad \text{ou} \quad c_0 \in D^\times$$
   $$\Leftrightarrow g \in D[[x]]^\times \quad \text{ou} \quad h \in D[[x]]^\times \ ,$$

   donde concluimos que f é irredutível.

   (b) Casos triviais: $I = \{0\} = (0)$ e $I = \mathbb{R}[[x]] = (1)$ são ideais principais.
   Seja $I \subset \mathbb{R}[[x]]$ um ideal próprio não nulo. Então $I \subset (x)$ pois $\mathbb{R}[[x]]$ é um anel local com ideal maximal $\mathbb{R}[[x]] \setminus \mathbb{R}[[x]]^\times = \{\sum_{i=0}^{\infty} a_i x^i \,|\, a_0 = 0\} = (x)$. Portanto $x \mid f$ para qualquer $f \in I \setminus \{0\}$ e $k_f := \max\{i \in \mathbb{N} \,|\, x^i \text{ divide } f\} \in \mathbb{N}$ está bem definido[1] e

   $$\forall\, f \in I \setminus \{0\} \quad \exists\, f' \in \mathbb{R}[[x]]^\times \quad \text{t.q.} \quad f = x^{k_f} f' \ .$$

   Seja $k = \min\{k_f \,|\, f \in I \setminus \{0\}\}$. Então $I = (x^k)$ (logo I é principal) porque:

[1] alternativamente, podemos considerar $k_f := \min\{i \,|\, a_i \neq 0\}$ e não precisamos de usar o facto de $\mathbb{R}[[x]]$ ser um anel local

- Por definição de mínimo existe $f \in I$ t.q. $f = x^k f'$ com $f' \in \mathbb{R}[[x]]^\times$, portanto $x^k = x^k f'(f')^{-1} = f(f')^{-1} \in I$, portanto $I \supset (x^k)$;
- Por definição de k, $x^k \mid f$ para todo o $f \in I \setminus \{0\}$, logo $I \subset (x^k)$.

[Usou-se diversas vezes que $\sum_{i=0}^{\infty} a_i x^i \in D[[x]]^\times$ sse $a_0 \in D^\times$.]

4. (a) Seja $f \in \hom_{\mathcal{C}}((A,S),(B,R))$, queremos definir um homomorfismo de anéis $F(f) : S^{-1}A \to R^{-1}B$ de modo a F ser um functor. Como $f(S) \subset R$, ou seja, $f(s) \in R$ para todo o $s \in S$, temos $\frac{b}{f(s)} \in R^{-1}B$ para todo o $b \in B$. Seja então

$$\begin{aligned} F(f) : S^{-1}A &\to R^{-1}B \\ \frac{a}{s} &\mapsto \frac{f(a)}{f(s)} \ . \end{aligned} \qquad (*^3)$$

(1º) $F(f)$ está bem definido: Sejam $a, a' \in A$ e $s, s' \in S$ tais que $\frac{a}{s} = \frac{a'}{s'}$ em $S^{-1}A$. Então

$$\begin{aligned} \frac{a}{s} = \frac{a'}{s'} &\Leftrightarrow \exists\, x \in S \text{ t.q. } x(as' - a's) = 0 \\ &\Rightarrow \exists\, y := f(x) \in R \text{ t.q. } y\big(f(a)f(s') - f(a')f(s)\big) = 0 \\ &\Leftrightarrow \frac{f(a)}{f(s)} = \frac{f(a')}{f(s')} \ . \end{aligned}$$

(2º) $F(f)$ é um homomorfismo de anéis: segue directamente da definição de soma e produto em $S^{-1}A$ e $R^{-1}B$.

(3º) F preserva a composição: Sejam $f \in \hom_{\mathcal{C}}((A,S),(B,R))$ e $g \in \hom_{\mathcal{C}}((B,R),(C,T))$. Para $a \in A$ e $s \in S$ temos

$$\begin{aligned} (F(g) \circ F(f)) \left(\frac{a}{s}\right) = F(g)\left(F(f)\left(\frac{a}{s}\right)\right) &= F(g)\left(\frac{f(a)}{f(s)}\right) \\ = \frac{g(f(a))}{g(f(s))} = \frac{(g \circ f)(a)}{(g \circ f)(s)} &= F(g \circ f)\left(\frac{a}{s}\right) \ , \end{aligned}$$

donde $F(g \circ f) = F(g) \circ F(f)$.

(4º) F preserva os morfismos identidade: O morfismo identidade em $\hom_{\mathcal{C}}((A,S),(A,S))$ é a identidade $Id_A \in \hom_{CRing}(A,A)$, logo pela definição $(*^3)$, $F(Id_A) = Id_{S^{-1}A}$.

(b) Dado $f \in \hom_{\mathcal{C}}((A,S),(B,R))$ temos que verificar que o seguinte diagrama

$$\begin{array}{ccc} E(A,S) = A & \xrightarrow{\varphi_S} & S^{-1}A = F(A,S) \\ {\scriptstyle E(f)=f}\downarrow & & \downarrow{\scriptstyle F(f)} \\ E(B,R) = B & \xrightarrow[\varphi_R]{} & R^{-1}B = F(B,R) \end{array}$$

é comutativo. E isso acontece pois, para qualquer $a \in A$, temos

$$\big(F(f) \circ \varphi_S\big)(a) = F(f)\left(\frac{a}{1}\right) = \frac{f(a)}{f(1)} = \frac{f(a)}{1} = \varphi_R(f(a)) = (\varphi_R \circ f)(a) \ .$$