Departamento de Matemática da Universidade de Coimbra **Álgebra Comutativa**

SOLUÇÕES **Exame (Época Normal)** 18/1/2012

---

1. (a) $\mathbb{Z}[i]$ é um domínio euclidiano com função euclidiana $\delta(a+ib) = |a+ib|^2 = a^2+b^2$ que satisfaz a propriedade $\delta(xy) = \delta(x)\delta(y)$. As unidades de $\mathbb{Z}[i]$ são ± 1 e $\pm i$, pois $\delta(a+ib) = 1$ se e só se $a+ib \in \{\pm 1, \pm i\}$.

   Se $1 \pm i = (a+ib)(c+id)$ então $\delta(1 \pm i) = \delta(a+ib)\delta(c+id)$, isto é, $2 = \delta(a+ib)\delta(c+id)$. Como 2 é primo em $\mathbb{Z}$, então $\delta(a+ib) = 1$ (ou seja, $a+ib$ é uma unidade) ou $\delta(c+id) = 1$ (ou seja, $c+id$ é uma unidade).

   (b) Claro que 2 é irredutível em $\mathbb{Z}$ porque é primo. Mas em $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$, logo é redutível em $\mathbb{Z}[i]$.

   (c) Pelas alíneas anteriores, $2 = (1+i)(1-i)$ é a factorização (única) de 2 em irredutíveis (primos). Como $3+i = (1+i)(2-i)$ é a factorização de $3+i$ em primos (de facto, $2-i$ também é irredutível pois $\delta(2+i) = 5$ é um inteiro primo), então $1+i \in \operatorname{mdc}(2, 3+i)$. Logo,

$$\operatorname{mdc}(2, 3+i) = \{1+i, -1-i, -1+i, 1-i\}.$$

2. Seja $p_1 p_2 \cdots p_n$ a factorização de a em primos. Para cada $i = 1, 2, \ldots, n$, $p_i \mid bc$ logo $p_i \mid b$ ou $p_i \mid c$. Mas como a e b são primos entre si e $p_i \mid a$ (para qualquer i), se p_i dividisse b para algum i teríamos $p_i \mid 1$, isto é, $p_i \in D^*$, um absurdo. Logo nenhum p_i divide b pelo que $p_i \mid c$ para $i = 1, 2, \ldots, n$ e portanto $a \mid c$.

3. Um domínio de integridade D diz-se um *domínio euclidiano* se for possível definir em D uma função $\delta \colon D \setminus \{0\} \to \mathbb{N}$ tal que, para quaisquer $a, b \in D$ $(b \neq 0)$, existem $q, r \in D$ tais que $a = qb + r$ onde ou $r = 0$ ou $\delta(r) < \delta(b)$.

   Seja I um ideal arbitrário de um domínio euclidiano D. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Podemos pois admitir que $I \neq \{0\}$. Nesse caso seja

$$N = \{\delta(a) \mid a \in I,\, a \neq 0\} \subseteq \mathbb{N}.$$

   É claro que N é não vazio (pois $I \neq \{0\}$), pelo que tem um mínimo. Seja b um elemento de $I \setminus \{0\}$ onde esse mínimo é atingido. Provemos que $I = \langle b \rangle$. Como $b \in I$, é óbvio que $\langle b \rangle \subseteq I$. Por outro lado, se $a \in I$, usando a definição de domínio euclidiano, existem $q, r \in D$ tais que $a = qb + r$ com $r = 0$ ou $\delta(r) < \delta(b)$. Dado que I é um ideal, podemos concluir que $r = a - qb \in I$. Mas então $r = 0$ (se r fosse não nulo, teríamos $r \in I \setminus \{0\}$ com $\delta(r) < \delta(b)$, um absurdo). Assim, a é um múltiplo de b pelo que pertence ao ideal $\langle b \rangle$.

4. (a) T é claramente um conjunto não vazio. Sejam $a_1v + n_1v, a_2v + n_2v \in T$. Então

$$(a_1v + n_1v) - (a_2v + n_2v) = (a_1 - a_2)v + (n_1 - n_2)v \in T.$$

Além disso, para quaisquer $b \in A$ e $av + nv \in T$,

$$b(av + nv) = (ba + nb)v \in T$$

(pois $ba + nb$ é um elemento do anel A), o que mostra que T é de facto um submódulo de M.

(b) No caso do anel ser unitário, podemos reescrever cada elemento $av + nv$ de T, caso n seja positivo, na forma

$$av + nv = av + \underbrace{v + v + \cdots + v}_{n} = av + \underbrace{1v + 1v + \cdots + 1v}_{n} =$$
$$= (a + \underbrace{1 + 1 + \cdots + 1}_{n})v = (\underbrace{a + n1}_{\in A})v.$$

O caso $n < 0$ é análogo:

$$av + nv = av\underbrace{-v - v - \cdots - v}_{-n} = av\underbrace{-1v - 1v - \cdots - 1v}_{-n} =$$
$$= (a\underbrace{-1 - 1 - \cdots - 1}_{-n})v = (\underbrace{a + n1}_{\in A})v.$$

5. Como p_1, p_2, p_3, p_4 são primos entre si, temos

$$\frac{D}{\langle p_1\, p_2^2\, p_3\rangle} \oplus \frac{D}{\langle p_1\, p_2^3\, p_3^2\, p_4\rangle} \oplus \frac{D}{\langle p_1^3\, p_2^2\, p_4^5\rangle}$$
$$\simeq \frac{D}{\langle p_1\rangle} \oplus \frac{D}{\langle p_2^2\rangle} \oplus \frac{D}{\langle p_3\rangle} \oplus \frac{D}{\langle p_1\rangle} \oplus \frac{D}{\langle p_2^3\rangle} \oplus \frac{D}{\langle p_3^2\rangle} \oplus \frac{D}{\langle p_4\rangle} \oplus \frac{D}{\langle p_1^3\rangle} \oplus \frac{D}{\langle p_2^2\rangle} \oplus \frac{D}{\langle p_4^5\rangle}.$$

Esta última é a decomposição em factores cíclicos primários. Os respectivos divisores elementares são então as potências primas $p_1, p_2^2, p_3, p_1, p_2^3, p_3^2, p_4, p_1^3, p_2^2, p_4^5$. Consequentemente, os factores invariantes são

$$\begin{array}{ccccccc} p_1 & \times & p_2^2 & \times & p_3^0 & \times & p_4^0 \\ p_1 & \times & p_2^2 & \times & p_3 & \times & p_4 \\ p_1^3 & \times & p_2^3 & \times & p_3^2 & \times & p_4^5 \end{array}$$

e a decomposição em factores cíclicos invariantes é

$$\frac{D}{\langle p_1\, p_2^2\rangle} \oplus \frac{D}{\langle p_1\, p_2^2\, p_3\, p_4\rangle} \oplus \frac{D}{\langle p_1^3\, p_2^3\, p_3^2\, p_4^5\rangle}.$$

6. Bastará mostrar que (a) $N(f) \cap Im(f) = \{0\}$ e (b) $M = N(f) + Im(f)$.

(a): Se $v \in N(f) \cap Im(f)$ então $v = f(u)$ e $0 = f(v) = ff(u) = f(u) = v$.

(b): Seja $v \in M$. Como $v = v - f(v) + f(v)$ e $f(v - f(v)) = f(v) - f(v) = 0$, está provado.

7. (a) Um A-módulo M é noetheriano se toda a cadeia ascendente de submódulos de M,

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots ,$$

estabiliza (isto é, existe $k_0 \in \mathbb{N}$ tal que $N_{K_0} = N_{k_0+1} = \cdots$).

(b) Seja M um A-módulo cujos submódulos são de tipo finito e consideremos uma cadeia ascendente de submódulos de M,

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots .$$

Como

$$\bigcup_{k=1}^{\infty} N_k$$

é um submódulo de M, é de tipo finito. Seja $S = \{v_1, \ldots, v_r\}$ um seu conjunto gerador. Então para cada $i = 1, 2, \ldots, r$ existe $k_i \in \mathbb{N}$ tal que $v_i \in N_{k_i}$. Seja $k_0 = \max\{k_1, \ldots, k_r\}$. É evidente que $S \subseteq \bigcup_{k=1}^{k_0} N_k = N_{k_0}$, pelo que

$$N_{K_0} = N_{k_0+1} = \cdots$$

e M é noetheriano.

(c) Pela alínea anterior, basta provar que todos os submódulos de N e M/N são de tipo finito:

- Seja S um submódulo de N. Então é um submódulo de M, logo é de tipo finito.
- Por outro lado, todo o submódulo de M/N é da forma S/N onde S é um submódulo de M e $N \subseteq S \subseteq M$. Pela hipótese (e alínea anterior) S possui um conjunto gerador finito $\{v_1, \ldots, v_r\}$. É evidente que então $\{v_1 + N, \ldots, v_r + N\}$ é um conjunto gerador de S/N.
