---

1. (a) Como 3 é um inteiro livre de quadrados (ver Exercícios I.1.7 e 1.6), $a+b\sqrt{-3}$ é uma unidade de $\mathbb{Z}[i\sqrt{3}]$ se e só se $N(a+b\sqrt{-3})=1$, isto é,

$$1 =\mid a^2+3b^2 \mid = a^2+3b^2.$$

Portanto as únicas unidades de $\mathbb{Z}[i\sqrt{3}]$ são os inteiros $1,-1$.

(b) Temos

$$\begin{aligned}\mathbb{Z}_{20}\oplus\mathbb{Z}_{40}\oplus\mathbb{Z}_{108} &= \frac{\mathbb{Z}}{\langle 2^2\times 5\rangle}\oplus\frac{\mathbb{Z}}{\langle 2^3\times 5\rangle}\oplus\frac{\mathbb{Z}}{\langle 2^2\times 3^3\rangle}\\ &\simeq \frac{\mathbb{Z}}{\langle 2^2\rangle}\oplus\frac{\mathbb{Z}}{\langle 5\rangle}\oplus\frac{\mathbb{Z}}{\langle 2^3\rangle}\oplus\frac{\mathbb{Z}}{\langle 5\rangle}\oplus\frac{\mathbb{Z}}{\langle 2^2\rangle}\oplus\frac{\mathbb{Z}}{\langle 3^3\rangle}\\ &\simeq \mathbb{Z}_4\oplus\mathbb{Z}_5\oplus\mathbb{Z}_8\oplus\mathbb{Z}_5\oplus\mathbb{Z}_4\oplus\mathbb{Z}_{27}.\end{aligned}$$

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

$$\begin{array}{ccccccc} 2^2 & \times & 3^0 & \times & 5^0 & = & 4\\ 2^2 & \times & 3^0 & \times & 5 & = & 20\\ 2^3 & \times & 3^3 & \times & 5 & = & 1080\end{array}$$

e a decomposição em factores cíclicos invariantes é

$$\mathbb{Z}_4\oplus\mathbb{Z}_{20}\oplus\mathbb{Z}_{1080}.$$

(c) Os ideais primários de $\mathbb{Z}$ são os ideais da forma $\langle p^n\rangle$ com p primo e $n\in\mathbb{N}$. De facto:

- Cada $Q=\langle p^n\rangle$ é primário:

$$ab\in Q \Leftrightarrow p^n \mid ab \overset{(p \text{ primo})}{\Longrightarrow} (p^n \mid a \text{ ou } p \mid b) \Rightarrow (p^n \mid a \text{ ou } p^n \mid b^n),$$

isto é, $a\in Q$ ou $b^n\in Q$.

- Seja $Q=\langle a\rangle$ um ideal primário de $\mathbb{Z}$ e $p_1^{n_1}\cdots p_t^{n_t}$ a factorização prima de a. Se $t>1$ teríamos

$$a=(p_1^{n_1})(p_2^{n_2}\cdots p_t^{n_t})\in Q$$

com $p_1^{n_1}\notin Q$ e $(p_2^{n_2}\cdots p_t^{n_t})^n\notin Q$ (para qualquer $n\in\mathbb{N}$), contrariando a definição de ideal primário. Logo $t=1$.

(d) Seja $p_1^{n_1} \cdots p_t^{n_t}$ a factorização prima de a. Por definição,

$$\sqrt{\langle a \rangle} = \{b \in \mathbb{Z} \mid \exists n \in \mathbb{N} \colon b^n \in \langle a \rangle\} = \{b \in \mathbb{Z} \mid \exists n \in \mathbb{N} \colon a \mid b^n\}.$$

Mas

$$a \mid b^n \Leftrightarrow p_1^{n_1} \cdots p_t^{n_t} \mid b^n \Leftrightarrow p_i \mid b \ (\forall i = 1, \ldots, t) \Leftrightarrow p_1 \cdots p_t \mid b.$$

Portanto $\sqrt{\langle a \rangle} = \langle p_1 \cdots p_t \rangle$.

(e) Por um lado $\langle x \rangle \subseteq \sqrt{I}$ pois $x^2 \in I$. Por outro lado, $I \subseteq \langle x \rangle$ e $\langle x \rangle$ é um ideal primo logo, pela fórmula

$$\sqrt{I} = \bigcap \{P \mid P \text{ primo}, P \supseteq I\},$$

$\sqrt{I} = \langle x \rangle$.

(f) Pelo Teorema dos zeros de Hilbert, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$. Logo, pela alínea anterior, $\mathcal{I}(\mathcal{Z}(I)) = \langle x \rangle$.

2. (a) $\mathrm{Tor}(M) = \{v \in M \mid \exists d \in D \setminus \{0\} \colon dv = 0\}$.

(b) (i) Se $v_1, v_2 \in \mathrm{Tor}(M)$, então existem $a_1, a_2 \in D$ não nulos tais que $a_1 v_1 = 0$ e $a_2 v_2 = 0$. Logo, para quaisquer $d_1, d_2 \in D$,

$$a_1 a_2 (d_1 v_1 + d_2 v_2) = a_2 d_1 a_1 v_1 + a_1 d_2 a_2 v_2 = 0,$$

com $a_1 a_2 \neq 0$ (pois não há divisores de zero em D), o que mostra que $d_1 v_1 + d_2 v_2 \in \mathrm{Tor}(M)$.

(ii) Suponhamos que M é livre, isto é, possui uma base $\{e_i\}_{i \in I}$. Sejam $v \in M \setminus \{0\}$ e $d \in D \setminus \{0\}$. Podemos escrever v na forma

$$v = \sum_{j=1}^{m} a_j \, e_{i_j}$$

para alguns $a_j \in D$ não nulos. Multiplicando por d obtemos

$$dv = \sum_{j=1}^{m} d a_j e_{i_j}.$$

Se $dv = 0$ então, como os e_i são linearmente independentes, $da_j = 0$ para $j = 1, \ldots, m$. Como D é um domínio de integridade e $d \neq 0$ então $a_j = 0$ para $j = 1, \ldots, m$, isto é, $v = 0$ (um absurdo!). Portanto, $dv \neq 0$ para quaisquer $v \in M \setminus \{0\}$ e $d \in D \setminus \{0\}$. Logo $\mathrm{Tor}(M) = \{0\}$.

(iii) Seja $v + \mathrm{Tor}(M)$ um elemento não nulo de $M/\mathrm{Tor}(M)$ (portanto $v \notin \mathrm{Tor}(M)$). Seja $d \in D \setminus \{0\}$. Então $d(v + \mathrm{Tor}(M)) = dv + \mathrm{Tor}(M)$. Mas $v \notin \mathrm{Tor}(M)$ implica obviamente $dv \notin \mathrm{Tor}(M)$ pelo que $d(v + \mathrm{Tor}(M)) \neq 0$, donde $\mathrm{Tor}(M/\mathrm{Tor}(M)) = \{0\}$ como desejávamos provar.

3. (a) f^n é a composição

$$\underbrace{f \circ f \circ \cdots \circ f}_{n}$$

e a composição de homomorfismos é um homomorfismo donde f^n é um homomorfismo. Claro que sendo f sobrejectivo por hipótese, também cada f^n o é (de facto, para cada $y \in M$ existe $x_1 \in M$ tal que $f(x_1) = y$ e, por sua vez, existe $x_2 \in M$ tal que $f(x_2) = x_1$, ou seja, $f^2(x_2) = f(x_1) = y$; continuando este raciocínio obteremos $x_n \in M$ tal que $f^n(x_n) = y$). Finalmente, se $x \in N(f^n)$, isto é, $f^n(x) = 0$ então $f^{n+1}(x) = f(f^n(x)) = f(0) = 0$ e $x \in N(f^{n+1})$ também.

(b) A cadeia

$$N(f) \subseteq N(f^2) \subseteq N(f^3) \subseteq \cdots$$

é uma cadeia ascendente de submódulos de M. Como M é noetheriano, terá que existir um natural k tal que $N(f^k) = N(f^{k+1})$.

(c) Basta provar que f é injectivo, isto é, $N(f) = \{0\}$. Seja então $x \in N(f)$. Como f^k é sobrejectiva, existe um $y \in M$ tal que $f^k(y) = x$. Mas então $0 = f(x) = f^{k+1}(y)$, ou seja, $y \in N(f^{k+1}) = N(f^k)$. Logo $x = f^k(y) = 0$.
