2^a PROVA ÁLGEBRA 2 - 24/05/2016

Gabarito (Martino Garonzi)

Exercício 1.

(a) Sejam $x, y \in f^{-1}(J) = I$, $a \in A$: precisamos mostrar que $x+y \in I$ e $ax \in I$.

- $f(x+y) = f(x) + f(y) \in J$ (pois $J \trianglelefteq B$) $\Rightarrow x+y \in I$
- $f(ax) = f(a)f(x) \in J$ (pois $J \trianglelefteq B$) $\Rightarrow ax \in I$

(b) Sejam $x+I, y+I \in A/I$ com $(x+I)(y+I) = 0+I$. Precisamos mostrar que um entre $x+I$ e $y+I$ é zero.

$(x+I)(y+I) = 0+I \Rightarrow xy \in I \Rightarrow f(xy) \in J \Rightarrow$

$f(x)f(y) = f(xy) \in J \Rightarrow (f(x)+J)(f(y)+J) = 0+J \Rightarrow$

como B/J é domínio de integridade, um entre $f(x)+J$ e $f(y)+J$ é zero $\Rightarrow$ por exemplo $f(x)+J = 0+J$ (o outro caso é analogo) $\Rightarrow f(x) \in J \Rightarrow x \in f^{-1}(J) = I \Rightarrow x+I = 0+I$.

(também o argumento $A/I \lesssim B/J$ está certo)

Exercício 2.

(a) É claro que $f(1)=1$. Sejam $a+ib, c+id \in \mathbb{Z}[i]$.

$f((a+ib)+(c+id)) = f((a+c)+i(b+d)) = a+c+2(b+d)+5\mathbb{Z}$

$f(a+ib)+f(c+id) = a+2b+c+2d+5\mathbb{Z}$ $\|$ $\Rightarrow$ são iguais.

$f((a+ib)(c+id)) = f(ac-bd+i(bc+ad)) = \boxed{ac-bd+2(bc+ad)+5\mathbb{Z}}$

$f(a+ib)f(c+id) = (a+2b+5\mathbb{Z})(c+2d+5\mathbb{Z}) = \boxed{(a+2b)(c+2d)+5\mathbb{Z}}$ $\|$ são iguais:

$[ac-bd+2(bc+ad)] - [(a+2b)(c+2d)] = -5bd \in 5\mathbb{Z}$ #

(b) Para mostrar $\ker(f) = J$ mostramos as 2 inclusões.

($\subseteq$) Se $a+ib \in \ker(f)$, $a+2b+5\mathbb{Z} = 0+5\mathbb{Z} \Rightarrow a+2b = 5t$ com $t \in \mathbb{Z}$.

Quero encontrar $x, y \in \mathbb{Z}$ tais que

$$\begin{cases} a = x-2y \\ b = 2x+y \end{cases} \quad \underline{\text{ou seja}}: \begin{cases} a+2b = 5x \\ b-2a = 5y \end{cases} \quad \text{ou seja } (a = 5t-2b): \begin{cases} t = x \\ b-2t = y \end{cases}$$

$\Rightarrow$ Basta escolher $x = t$ e $y = b-2t$.

($\supseteq$) $f((x-2y)+i(2x+y)) = x-2y+2(2x+y)+5\mathbb{Z} = 5x+5\mathbb{Z} = 0+5\mathbb{Z}$.

Isso mostra que $(x-2y)+i(2x+y) \in \ker(f)$ $\blacksquare$.

(c) f é sobrejetiva pois se $m+5\mathbb{Z} \in \mathbb{Z}/5\mathbb{Z}$, $f(m) = m+5\mathbb{Z}$.
Logo pelo teorema de isomorfismo $\mathbb{Z}[i]/\ker(f) \cong \mathbb{Z}/5\mathbb{Z} \Rightarrow$
$\mathbb{Z}[i]/J \cong \mathbb{Z}/5\mathbb{Z}$ é um <u>corpo</u> $\Rightarrow$ J é maximal.

(d) J é principal pois é um ideal de $\mathbb{Z}[i]$ que é um domínio Euclidiano (em um domínio Euclidiano todo ideal é principal). Um gerador de J é um elemento de J de norma mínima. Se $(x-2y)+i(2x+y) \in J$ então

$$N((x-2y)+i(2x+y)) = (x-2y)^2+(2x+y)^2 = 5(x^2+y^2)$$

logo se $\alpha \in J$ e $\alpha \neq 0$, $N(\alpha) \geq 5 \Rightarrow$ a norma mínima de um elemento não-nulo de J é 5 e escolhendo $x = 1$ e $y = 0$ obtemos $1+2i \in J$ e $N(1+2i) = 5 \Rightarrow J = (1+2i)$.

<u>Exercício 3.</u>

(a) $P(X) = X^3 - 2X^2 + X = X(X^2-2X+1) =$
$= X(X-1)^2$ (X e $X-1$ são irredutíveis: eles tem grau 1)

(b) Aplicamos o algoritmo de Euclide a $P(x)$ e $X+1$. A divisão com resto dá:

$$\begin{array}{r|l} x^3 - 2x^2 + x & x+1 \\ \underline{x^3 + x^2} & x^2 - 3x + 4 \\ -3x^2 + x & \\ \underline{-3x^2 - 3x} & \\ 4x & \\ \underline{4x + 4} & \\ -4 & \end{array}$$

Logo temos:

Quociênte: $x^2 - 3x + 4 = Q(x)$

Resto: $-4 = R(x)$

$$(x^3 - 2x^2 + x) = (x+1)\,Q(x) + R(x) =$$
$$= (x+1)(x^2 - 3x + 4) - 4$$

Logo $(x+1)(x^2-3x+4) - (x^3 - 2x^2 + x) = 4$.

Dividindo por 4, $(x+1)\frac{1}{4}(x^2-3x+4) - \frac{1}{4}(x^3 - 2x^2 + x) = 1$

Reduzindo módulo $x^3 - 2x^2 + x$ $(= P(x))$, $(x+1)\frac{1}{4}(x^2-3x+4) \equiv 1 \bmod (P(x))$

$\Rightarrow$ o inverso de $x+1+I$ é $\frac{1}{4}(x^2-3x+4) + I$. #

(c) Pelo teorema de correspondência, os ideais de A correspondem aos ideais J de $\mathbb{R}[x]$ tais que $I \subseteq J$; como $\mathbb{R}[x]$ é Euclidiano, J é principal, $J = (F(x))$ com $F(x) \in \mathbb{R}[x]$ e $(F(x)) \supseteq (P(x))$ significa que $F(x) \mid P(x)$ $\Rightarrow$

$$\boxed{\begin{array}{c} \mathbb{R}[x] \\ \cup\!\mid \\ J \\ \cup\!\mid \\ I \end{array}}$$

temos que contar os <u>divisores</u> de $P(x) = x(x-1)^2$ (a menos de associados) $\rightsquigarrow$ Os divisores de $P(x)$ são 1, x, $x-1$, $(x-1)^2$, $x(x-1)$ e $x(x-1)^2$ $\to$ <u>6 divisores</u> (a menos de associados) $\Rightarrow$ <u>A tem 6 ideais</u> #

(d) $a = x(x-1) + I$. Temos $a \neq 0$ pois $P(x) = x(x-1)^2$ não divide $x(x-1)$ (observe que $F(x) + I = 0 + I$ sse $F(x) \in I = (P(x))$, i.e. $P(x) \mid F(x)$)

Por outro lado $a^2 = x^2(x-1)^2 + I = 0 + I$ pois $P(x) = x(x-1)^2$ divide $x^2(x-1)^2$.

Obs. em 1(b) pode fazer assim também:

$A \xrightarrow{f} B \xrightarrow{\pi} B/J \rightsquigarrow \pi \circ f : A \to B/J$, $\ker(\pi \circ f) = I$

Pelo teorema de isomorfismo A/I é isomorfo a um subanel de B/J ($A/I \underset{\sim}{\leq} B/J$) e como B/J é domínio, A/I também é (subanel de domínio é domínio)