---

1. **(a1)** Como 1 é um inteiro livre de quadrados (ver Exercícios I.1.7 e 1.6), se $1 \pm i = (a+ib)(c+id)$ então $N(1 \pm i) = N(a+ib)N(c+id)$, isto é, $2 = N(a+ib)N(c+id)$. Como 2 é primo em $\mathbb{Z}$, então $N(a+ib) = 1$ (ou seja, $a+ib$ é uma unidade) ou $N(c+id) = 1$ (ou seja, $c+id$ é uma unidade).

(a2) 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 $\mathbb{Z}[i]$.

(b1) Do Exercício 1 sabemos já que $2 = (1+i)(1-i)$ 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 $N(2+i) = 5$ é um inteiro primo), então $1+i \in \mathrm{mdc}(2, 3+i)$. Logo, $\mathrm{mdc}(2, 3+i) = \{1+i, -1-i, -1+i, 1-i\}$.

(b2) Como em qualquer DIP $\langle a \rangle + \langle b \rangle = \langle \mathrm{mdc}(a,b) \rangle$, então $\langle 2 \rangle + \langle 3+i \rangle = \langle \mathrm{mdc}(2, 3+i) \rangle = \langle 1+i \rangle = \{(a+ib)(1+i) \mid a, b \in \mathbb{Z}\} = \{(a-b)+i(a+b) \mid a, b \in \mathbb{Z}\}$.

(b3) Como em qualquer DIP $\langle a \rangle \cap \langle b \rangle = \langle \mathrm{mmc}(a,b) \rangle$, então $\langle 2 \rangle \cap \langle 3+i \rangle = \langle \mathrm{mmc}(2, 3+i) \rangle = \langle (1+i)(1-i)(2-i) \rangle = \langle 4-2i \rangle = \{(4a+2b)+i(-2a+4b) \mid a, b \in \mathbb{Z}\}$.

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. **(a)** $p(x)$ é um *polinómio primitivo* se $\mathrm{gr}(p(x)) \geq 1$ e os únicos divisores de $p(x)$ de grau zero forem unidades.

(b1) Seja $d \in D$ um divisor de $q(x)$ de grau zero. Como $d \mid p(x)$ então d é uma unidade.

(b2) Seja $p(x)$ um polinómio primitivo de $D[x]$. Faremos a demonstração por indução sobre o grau $n \geq 1$ de $p(x)$:

Se $n = 1$ então $p(x)$ não admite factorizações próprias e, sendo primitivo, é irredutível e está provado.

Tomemos $p(x)$ de grau n e suponhamos, como hipótese de indução, que o resultado é válido para todos os polinómios de grau $< n$. Se $p(x)$ admitir uma factorização própria então $p(x) = q(x)r(x)$ com $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < n$ e, pela hipótese de indução, ambos são factorizáveis em polinómios irredutíveis, o que nos dá uma factorização de $p(x)$ em irredutíveis. No caso em que $p(x)$ não admite factorizações próprias, como é primitivo, então é irredutível e está provado.
