(3) Fatorar $5+7i$ em $\mathbb{Z}[i]$ $\left(\text{onde } \mathbb{Z}[i] = \frac{\mathbb{Z}[x]}{(x^2+1)}\right)$.

Solução: Temos que como:

$$N(5+7i) = 5^2 + 7^2 = 25+49 = 74$$ não é

primo em $\mathbb{Z}$, então $5+7i$ é redutível em $\mathbb{Z}[i]$.

Se $5+7i = z.w$, com $z, w \in \mathbb{Z}[i]$, então

$$N(5+7i) = N(z).N(w)$$

$$\Rightarrow \quad N(z).N(w) = 74 = 2.37$$

Ou seja, começamos olhando para elementos

$z \in \mathbb{Z}[i]$ com $N(z) = 2$ e $w \in \mathbb{Z}[i]$ com

$N(w) = 37$. Os possíveis $z$ irredutíveis são: $\pm 1 \pm i$

e os possíveis $w$ irredutíveis são: $\pm 6 \pm i$

Ao efetuarmos a multiplicação destas possibilidades, vemos que:

$$5+7i = (1+i)(6+i)$$

onde $1+i$ e $6+i$ são irredutíveis pois

$N(1+i) = 2$ é primo e

$N(6+i) = 37$ é primo

---

(4) Encontrar unidades em $\mathbb{Z}_8[x]$.

Solução:

Procuramos por $a+bx$, $c+dx \in \mathbb{Z}_8[x]$ tq:

$$(a+bx)(c+dx) = 1$$

$$\Leftrightarrow \quad ac + (bc+ad)x + bd\,x^2 = 1$$

$$\Leftrightarrow \quad \begin{cases} ac = 1 & (1) \\ bc + ad = 0 & (2) \\ bd = 0 & (3) \end{cases} \quad \text{em } \mathbb{Z}_8$$

De (1), temos a invertível em $\mathbb{Z}_8$, e c também:

$a, c \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

De (2): $bc = -ad$

$\Rightarrow bac = -a^2 d$

$\Rightarrow \boxed{b = -a^2 d}$

De (3): $bd = 0 \iff a^2 d^2 = 0$

$\iff d^2 = 0$, pois a invertível.

$b, d \in \{\bar{0}, \bar{4}\}$

Ou seja, as unidades em $\mathbb{Z}_8[x]$ são $a + bx$ com:

$a = 1, \quad b = 0, 4$

$a = 3, \quad b = 0, 4$

$a = 5, \quad b = 0, 4$

$a = 7, \quad b = 0, 4$

Então as unidades são:

$$(\mathbb{Z}_8[x])^* = \{a + bx ; \ a \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, b \in \{\bar{0}, \bar{4}\}\}$$

(5)

Daremos um contra-exemplo para a afirmação:

"Todo domínio de integridade finito é isomorfo a $(\mathbb{Z}_p, +, \cdot)$ para algum $p$ primo."

De fato, todo domínio de integridade finito é um corpo mas não necessariamente é isomorfo à $\mathbb{Z}_p$. Na verdade, pode ter ordem $p^n$ para $p$ primo.

Exemplo: Considere

$$\mathbb{Z}_3[i] := \frac{\mathbb{Z}[i]}{(3)}$$

Note que $\mathbb{Z}_3[i]$ é um anel comutativo com unidade. Além disso, suponha:

$$(a+bi)(c+di) = 0$$

$$\Leftrightarrow (ac - bd) + (ad + bc)i = 0$$

$$\Leftrightarrow \begin{cases} ac - bd = 0 & (1) \\ ad + bc = 0 & (2) \end{cases}$$

Suponha $c \neq 0$:
então:

$$a = cbd$$

Substituindo em (2):

$$c b d^2 + bc = 0$$

$$\Rightarrow \quad bc(d^2+1) = 0$$

Como $c$ é inversível:

$$b(d^2+1) = 0$$

e como $d^2+1 \in \{\bar{1}, \bar{2}\}$, então é inversível e segue $b = 0$. Logo, $a = cbd = 0$

Similarmente, supondo $d \neq 0$, obtemos que

$$a + ib = 0.$$

Logo, $\mathbb{Z}_3[i]$ não tem divisores de zero. Isto é, $\mathbb{Z}_3[i]$ é domínio de integridade.

(6) $GL(2, \mathbb{Z})$ tem subgrupo de ordem 12.