Série 7 ①

Exercice 1

a) $x \in \sqrt{30\mathbb{Z}} \Rightarrow \exists\, n \in \mathbb{N}$ tq $x^n \in 30\mathbb{Z}$

$\Rightarrow \exists\, m \in \mathbb{N}$ tq $x^n = 2 \cdot 3 \cdot 5 \cdot m$.

Soient $p_1, \dots, p_k \in \mathbb{P}$, $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ tq

$x = \prod p_i^{\alpha_i}$ (décomposition de x en facteurs premiers).

$\Rightarrow$ On peut supposer $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, grâce à l'unicité de la décomposition.

$\Rightarrow \dots$

b) Point délicat : $x, y \in \sqrt{I} \Rightarrow x + y \in \sqrt{I}$

$\exists\, n, m \in \mathbb{N}$ tq $x^n, y^m \in I$, par hypothèse.

On calcule :

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k\, y^{n+m-k}$$

Si $k < n \Rightarrow n+m-k > m$

Donc, $\forall k$, soit x^k soit $y^{n+m-k} \in I$

$\Rightarrow x^k y^{n+m-k} \in I \quad \forall k$

$\Rightarrow (x+y)^{n+m} \in I$

$\Rightarrow x + y \in \sqrt{I}$

Exercice 3

(a) Si R est un anneau, pour montrer que $R' \subseteq R$ est un sous-anneau, n'oubliez pas de montrer que $1_R \in R'$

(b) Montrez d'abord que deg est multiplicative, c.-à-d. :

$$\deg(x \cdot y) = \deg(x) \cdot \deg(y) \quad \forall x, y \in \mathbb{Z}[i].$$

d) On trouve :

1) $\text{pgcd}(5+2i, 2-5i)$

2) $\text{pgcd}(11+3i, 15-2i)$.

Pour le 2), soit appliquer l'algorithme, soit calculer :

$$\deg(11+3i) = 130 = 2 \cdot 5 \cdot 13$$

$$\deg(15-2i) = 229 \in \mathbb{P}$$

$$\text{pgcd}(130, 229) = 1$$

$$\Rightarrow \deg(\text{pgcd}(11+3i, 15-2i)) = 1$$

$$\Rightarrow \text{pgcd}(11+3i, 15-2i) = 1$$

Exercice 4

(a) On pose :

$$\varphi : \mathbb{Z}[t] \longrightarrow \mathbb{Z}[i]$$
$$p \longmapsto p(i)$$

- A vérifier :
  - bien défini
  - φ homomorphisme
  - φ surjectif.
- $I \subseteq \ker \varphi$: clair
- $\ker \varphi \subseteq I$

Soit p tq $\varphi(p) = p(i) = 0 \Rightarrow i$ racine de $p \Rightarrow -i$ racine de $p \Rightarrow t^2+1$ divise $p(t)$ dans $\mathbb{Q}[t]$! C-à-d : $\exists\, q(t) \in \mathbb{Q}[t]$ tq $(t^2+1)\,q(t) = p(t)$. Comme t^2+1 est unitaire, on a en fait $q(t) \in \mathbb{Z}[t] \Rightarrow p \in I$, comme voulu.

$$\Rightarrow \mathbb{Z}[t]/_I \cong \mathbb{Z}[i]$$

(b) & (c) $\mathbb{Z}[i] \subseteq \mathbb{C}$ qui est un corps $\Rightarrow \mathbb{Z}[i]$ intègre $\Rightarrow I$ premier

$\mathbb{Z}[i]$ pas un corps $\Rightarrow I$ pas maximal