TD N° 6 - **Arithmétique dans les anneaux**

Exo 1. Dans $\mathbb{Z}/7\mathbb{Z}[X]$, effectuer la division euclidienne de P par Q dans les cas suivants :

1) $P = \overline{2}X^2 + \overline{3}, Q = \overline{3}X + \overline{1}$.

2) $P = \overline{2}X^3 + \overline{2}X^2 + \overline{3}, Q = X^2 + \overline{2}X + \overline{1}$.

Exo 2. Le polynôme $P = X^3 + 1401X + 503 \in \mathbb{Z}[X]$ est-il irréductible dans $\mathbb{Z}[X]$ (réduire modulo 2) ? et le polynôme $2P$?

Exo 3. Dans $\mathbb{R}[X]$, déterminer un pgcd et un ppcm, ainsi qu'un couple de Bézout dans les cas suivants :

1) $X^3 + X + 4$ et $X^2 + X + 2$

2) $X^4 + 2X^2 - X + 5$ et $X^4 + 3X^2 + X + 1$.

Exo 4. Trouver l'isomorphisme inverse de l'isomorphisme canonique

$$\mathbb{Z}/30\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},$$

ainsi que l'isomorphisme inverse de

$$\mathbb{R}[X]/(X^4 + X^2) \xrightarrow{\sim} \mathbb{R}[X]/(X^2) \times \mathbb{R}[X]/(X^2 + 1).$$

Exo 5. Les anneaux $\mathbb{R}[X]/(X^3+X+4)$ et $\mathbb{R}[X]/(X^2+X+2)$ sont-ils des corps ? Si oui, les identifier à des corps connus.

Exo 6. Considérons l'anneau des entiers de Gauss $A = \mathbb{Z}[i]$. Soit

$$N\colon \begin{array}{rcl} A & \longrightarrow & \mathbb{N} \\ z = a + ib & \longmapsto & |z|^2 = a^2 + b^2. \end{array}$$

On rappelle que $N(zz') = N(z)N(z')$ pour tous $z, z' \in A$, et que l'on a, pour $z \in A$,

$$N(z) = 1 \iff z \in A^\times \iff z \in \{\pm 1, \pm i\}.$$

1) Soient $z, z' \in A$. Montrer que si $z \mid z'$ dans A, alors $N(z) \mid N(z')$. La réciproque est-elle vraie ?

2) Les éléments 2 et 3 sont-il irréductibles dans A ?

3) Montrer que si $N(z)$ est un nombre premier, alors z est irréductible dans A. La réciproque est-elle vraie ?

4) Montrer que tout élément non nul $z \in A$ s'écrit comme produit d'un inversible et d'éléments irréductibles de A, en raisonnant par récurrence sur $N(z)$. (On verra plus bas que A est en fait euclidien.)

5) Lister tous les éléments $z \in A$ irréductibles tels que $N(z) \leq 10$.

6) Décomposer les éléments suivants en produit d'éléments irréductibles dans A : $10, 1+5i, 6+8i, 22+19i$.

7) Nous allons à présent montrer que, pour tous $z, z' \in A$ avec $z' \neq 0$, il existe $q, r \in A$ tels que $z = qz' + r$, et $N(r) < N(z')$. On dit que (A, N) est un anneau euclidien ; cf. exercice 7.

7.a) Montrer que pour tout $z \in \mathbb{C}$, il existe $q \in A$ tel que $|z-q|^2 < 1$ (faire un dessin).

7.b) Conclure.

Exo 7. Un anneau euclidien est un couple (A, N) où A est un anneau intègre et $N : A \setminus \{0\} \longrightarrow \mathbb{N}$ une application tels que, pour tous $a, b \in A, b \neq 0$, il existe $q, r \in A$ vérifiant :

- $a = bq + r$
- $N(r) < N(b)$.

1) Montrer que $\mathbb{Z}, K[X], K$ (K corps) et $\mathbb{Z}[i]$ sont des anneaux euclidiens pour une fonction N que l'on précisera.

2) Montrer qu'un anneau euclidien est principal.

3) Etendre l'algorithme d'Euclide pour le calcul des pgcd aux anneaux euclidiens.

4) Calculer un pgcd d de a et b, et un couple de Bézout associé dans les cas suivants :

4.a) $A = \mathbb{Z}[i], a = 1+5i, b = 6+8i$

4.b) $A = \mathbb{Z}[i], a = 5-i, b = 4+7i$

Exo 8. Soit $A = \{P \in \mathbb{Q}[X] \mid P'(0) = 0\}$.

1) Montrer que A est un sous-anneau de $\mathbb{Q}[X]$.

2) Quels sont les éléments inversibles de A ?

3) Montrer que X^2 et X^3 sont irréductibles dans A.

4) Donner deux décomposition distinctes, même à permutation et produit par des inversibles près, de X^6 en produit d'irréductibles.

5) Pourquoi peut-on en déduire que A n'est pas principal ?

6) On peut donner un exemple explicite d'idéal non principal de A. Montrer que $I = (X^2, X^3)$ n'est pas un idéal principal.