142 : PGCD et PPCM, algorithmes de calcul. Applications.

Cadre : $(A, +, \cdot)$ un anneau unitaire commutatif intègre, $\mathbb{K}$ un corps.

I) **Propriétés arithmétiques**

Définitions de la divisibilité, d'éléments associés, d'irréductibles. PGCD et PPCM de deux éléments. Exemples. Cas d'un anneau factoriel.

II) **Cas d'un anneau principal**

Définition d'un anneau principal, exemples et contre-exemple. Théorème de BACHET-BEZOUT. Cas où $d = pgcd(a, b)$. Exemples

III) **Cas d'un anneau euclidien**

Définition d'un anneau euclidien, stathme, exemple de $\mathbb{K}[X]$. Implication successives des différents anneaux usuels. Algorithme d'EUCLIDE. Exemples. Algorithme d'EUCLIDE étendu : obtention d'une relation de BEZOUT, exemples.

IV) **Application en arithmétique**

A) Équations diophantiennes linéaires

Définition, résolution de $ax = b$. Cas de $b = 1$ et $pgcd(a, b) = 1$, puis de b quelconque. Théorème résumant l'ensemble des solutions dans le cas général. Exemple. Généralisation à n variables. Résolution de $AX = B$ lorsque A est diagonale. **DEV** 1 : FORME NORMALE DE SMITH.

B) Système de congruences

Théorème chinois, exemple et contre-exemple. Isomorphisme réciproque. Application. Cas général. **DEV** 2 : SYSTÈME DE CONGRUENCES.

Références :

- PERRIN
- ROMBALDI
- BECK-MALICK-PEYRÉ