**Leçon 142 - PGCD et PPCM, algorithmes de calcul. Applications.**

**Références :** Calais (Th. des anneaux), Cohen, Perrin, Demazure, Beck-Malick-Peyré, Combes, Szpirglas, Duverney.

**Développements :** algorithme de Berlekamp, théorème de Sophie Germain.

Cadre : Soit $A$ un anneau intègre, $\mathbb{K}$ un corps. Tous les anneaux sont supposés commutatifs et unitaires.

## 1. Cadre théorique : anneaux factoriels et principaux. —

*1.1. Définition et premières propriétés, cadre des anneaux principaux.* — (Calais (Th. des anneaux)) Définition du pgcd, du ppcm, unicité à un inversible près, exemples, relation entre pgcd et ppcm, caractérisations du pgcd et ppcm en termes d'idéaux, c-ex de $(X)+(Y)=(X,Y)\neq(1)$ dans $\mathbb{K}[X,Y]$, anneaux à pgcd, éléments premiers entre eux, théorème de Gauss. Existence et caractérisation dans un anneau principal, théorème de Bézout, exemples.

*1.2. Existence dans les anneaux factoriels.* — (Calais (Th. des anneaux)) Principal $\Rightarrow$ factoriel, existence et forme du pgcd et du ppcm dans un anneau factoriel. (ou Perrin) Définition du contenu de $f\in A[X]$, multiplicativité du contenu, théorème de Gauss et description des irréductibles.

## 2. Anneaux euclidiens : algorithmes de calcul. —

*2.1. Conséquences de la division euclidienne.* — (Calais (Th. des anneaux)) Euclidien $\Rightarrow$ principal, exemple de $\mathbb{Z},\mathbb{Z}[i]$ et $A[X]$ euclidien ssi $A$ est un corps. Algorithme d'Euclide, exemple de $\text{pgcd}(4+7i,8-i)=1-2i$. (Cohen) Complexité de l'algorithme d'Euclide, algorithme binaire, algorithme d'Euclide étendu, remarque sur le binaire étendu, remarque sur l'inversion modulo $n$, dans un corps fini. Théorème Chinois, algorithme effectif.

*2.2. Anneaux de polynôme.* — (Cohen) Algorithme d'Euclide sur $A[X]$, $A$ euclidien. (Beck-Malick-Peyré) Réduction sans carré sur $\mathbb{F}_p[X]$, **dev** algorithme de Berlekamp.

## 3. Applications du PGCD. —

*3.1. Résultant.* — (Szpirglas) Définition du résultant de deux polynômes sur un anneau factoriel, le résultant est nul ssi ils ont un facteur commun. Application à l'élimination. (Cohen) Algorithme de calcul.

*3.2. Matrices sur un anneau.* — (Cohen) Forme normale de Hermite, algorithme de calcul, application à la détermination d'une base de l'image d'une matrice, du noyau, algorithme. (Beck-Malick-Peyré) Forme normale de smith, algorithme de calcul, application au théorème de la base adaptée, invariants de similitudes, réduction de Frobenius.

*3.3. Équations diophantiennes.* — (Combes) $ax+by=c$ admet une solution ssi $d=a\wedge b\mid c$ et les solutions sont les $(x_0+bk/d,y_0-ak/d)$ pour $k\in\mathbb{Z}$ où $(x_0,y_0)$ est une solution particulière, et on peut trouver une solution particulière par l'algorithme d'Euclide. Exemples de $15x+9y=6$ de solutions $(4+3k,-2-5k)$ et $15x+9y=5$ n'admet pas de solutions. Application de la forme normale de Hermite à la résolution d'un système d'équation diophantiennes. **dev** Théorème de Sophie Germain. (Duverney) Équation de Fermat pour $n=3$.

**4. Annexe.** — Algorithme d'Euclide, binaire, d'Euclide étendu, théorème chinois effectif, d'Euclide sur $A[X]$, de calcul du résultant, forme normale de Hermite, du calcul du noyau d'une matrice, forme normale de Smith.