

Leçon 142 : PGCD et PPCM, algorithmes de calcul, applications

Cadre : Soit A un anneau intègre, commutatif, non réduit à $\{0\}$.

I) PGCD et PPCM, généralités [BER]

1) Définitions

- Définition du PGCD et PPCM
- Pas toujours existence
- "Unicité" à un inversible près
- $\text{PPCM} \Rightarrow \text{PGCD}$
- Définition deux éléments premiers entre eux, et lien avec le PGCD
- Formules basiques
- Identité à mourir de rire

2) Cas d'un anneau factoriel

- Définition
- Lemme de Gauss
- Existence de PGCD et PPCM
- Définition du contenu
- A factoriel $\Rightarrow A[x]$ factoriel

2) Cas d'un anneau principal

- Définition
- Principal $\Rightarrow$ factoriel

II) Algorithmes de calcul (dans un anneau euclidien)

1) Algorithme d'Euclide [BER, SAUX]

(a) Principe et complexité sur $\mathbb{Z}$

- Principe de l'algo et relation de Bézout (sur $\mathbb{Z}$ et $\mathbb{K}[X]$)
- Complexité

(b) Suite de Fibonacci [DEMA]

- Définition et relations
- $F_{n+m} = F_{n+1}F_m + F_nF_{m-1}$
- Grâce à l'algo d'Euclide : $\text{pgcd}(F_n, F_m) = F_{\text{pgcd}(n,m)}$

2) Factorisation de polynômes [BECK]

- Algorithme de Berlekamp
- Cas où le polynôme possède un facteur carré

III) Applications

1) Théorème des restes chinois [ROM]

- Énoncé théorème des restes chinois
- Exemple p469 [BER]
- Lien avec Lagrange

2) Résultant [SZPI]

- Matrice de Sylvester et résultant
- A et B premiers entre eux $\iff R(A, B) \neq 0$
- Théorème de Bézout faible

3) Théorie des groupes [BER]

- Définition de l'exposant
- Expression de l'exposant avec le PPCM
- Structure des groupes abéliens finis (admis)