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

I PGCD et PPCM dans un anneau

1 Notion de PGCD/PPCM

- Définition du PGCD à un inversible près
- Définition de 2 éléments premiers entre eux
- $d = \text{pgcd}(a_1, \cdots, a_n) \iff 1 = \text{pgcd}(\frac{a_1}{d}, \cdots, \frac{a_n}{d})$
- Lemme de Gauss
- Définition du PPCM à un inversible près
- $ab = (a \wedge b)(a \vee b)$

2 Dans un anneau principal

- $(a_1, \cdots, a_n) = (\text{pgcd}(a_1, \cdots, a_n))$ dont on déduit l'existence d'une relation de Bézout
- $(a_1) \cap \cdots \cap (a_n) = (\text{ppcm}(a_1, \cdots, a_n))$
- $\text{pgcd}(a_1, \cdots, a_n) = 1 \iff \exists u_1, \cdots, u_n, \sum u_k a_k = 1$
- $a \wedge c = 1 \implies a \wedge b = a \wedge bc$
- $\forall k, c \wedge a_k = 1 \implies c \wedge \prod a_k = 1$
- $\forall i \neq j, a_i \wedge a_j = 1 \implies a_1 \vee \cdots \vee a_n = \prod a_k$

3 Dans un anneau factoriel

- On calcule le PGCD/PPCM à partir de la décomposition en facteurs irréductibles

II Algorithmes dans un anneau euclidien

- Euclidien $\implies$ principal donc le PGCD/PPCM y est bien défini
- $a = bq + r \implies a \wedge b = b \wedge r$
- $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$
- Algorithme d'Euclide pour calculer le PGCD
- Algorithme d'Euclide étendu pour le calcul de la relation de Bézout

III Applications

1 Théorème chinois

- Calcul d'inverse dans $\mathbb{Z}/n\mathbb{Z}$
- Résolution d'équations diophantiennes
- DEV 1 : Théorème chinois + Système de congruence

2 Polynômes

- Contenu d'un polynôme, lemme des contenus
- P irréductible sur $A \implies P$ irréductible sur $Frac(A)$, pour A factoriel

3 Ordre dans un groupe

- $\text{ord}(g^k) = \frac{\text{ord}(g)}{\text{ord}(g) \wedge k}$
- $hg = gh \implies \text{ord}(gh) | \text{ord}(g) \vee \text{ord}(h)$, avec égalité si $< g > \cap < h > = \{e\}$
- $\text{ord}(g) \wedge \text{ord}(h) = 1 \implies \text{ord}(gh) = \text{ord}(g)\text{ord}(h)$
- DEV 2 : $\mathbb{Q}(\mathbb{U}_n, \mathbb{U}_m) = \mathbb{Q}(\mathbb{U}_{n \vee m}) + \mathbb{Q}(\mathbb{U}_n) \cap \mathbb{Q}(\mathbb{U}_m) = \mathbb{Q}(\mathbb{U}_{n \wedge m})$