122 - Anneaux principaux. Applications.

Références	[Perrin], [UlmA], [GOU_AGP], [Obj_pas_chômage], [ROM_AG]
Section	Algèbre
Date	@28 janvier 2025
Statut leçon	Plan détaillé ok
Enseignant	Lionel Fourquaux
Développements choisis	Entiers de Gauss et Théorèmes des deux carrés., Smith Version Principal
Nb choisis	2
Développements	Algorithme de Berlekamp, Entiers de Gauss et Théorèmes des deux carrés.

Rapport de Jury

Introduction

→ anneaux factoriels: étendre des notions qu'on connait sur les entiers : thm de décomp des facteurs premiers, faire de l'arithmétique

→ anneaux principaux: Bézout

→ anneaux Euclidien: Euclide

Plans

▼ ***Plan***

I. Notion de principalité

1. Anneaux principaux
2. Anneaux euclidiens

II. Arithmétique dans un anneau principal

1. Caractère factoriel d'un anneau principal
2. Théorème de Bézout
3. Résolution d'équation diophantienne du premier ordre
4. Entiers de Gauss

III. Réduction de matrices dans les anneaux principaux

1. Résolution d'un système d'équations diophantiennes
2. Forme normale de Smith

▼ ***Plan détaillé***

▼ I.1. Anneaux principaux

- Def idéaux principaux + A principal + exemple d'un corps
- Ex Z/nZ non principal car non intègre pour n premier

▼ I. 2. Anneaux euclidiens

- Def Anneaux euclidien
- ex : (Z,|.|), (K[X], deg), (Z[i], N(z)=a^2+b^2), (K[[X]], val)
- Thm: euclidien ⇒ principal
- Prop : A[X] principal ssi A est un corps + ex Z[X] non principal car <2,X> non principal
- Application : Polynôme minimal pour un élément algébrique
- Application polynome minimal µ_u en dimension fini et µ_{u,x}
- Z[1+i\sqrt(19))/2] principal non euclidien

▼ II. 1. Caractère factoriel d'un anneau principal

- prop : A principal, p \in A non inversible, p ≠ 0 alors p irréductible ssi (p)
  premier ssi (p) maximal
- ex : A pas un corps mais intègre alors {0} pas maximal mais premier
- Rq on a toujours (p) premier ⇒ p irréductible
- App Def de C comme le coprs de rupture de R[X]/<X²+1>
- Def A factoriel
- Prop : A intègre et verifie l'existence dans factorialité
  alors unicité ssi lemme d'euclide ssi TH de gauss ssi p irréductible ssi p
  premier
- th : A principal alors A factoriel
- Z[i\sqrt(5)] n'est pas facoriel, pas (U)

▼ II. 2. Théorème de Bézout

- Bézout + cas des 1er entre eux
- prop : si A euclidien, algo d'euclide étendu
- th chinois + iso réciproque
- app : inversible de Z/nZ
- app : lemme des noyaux
- app : il existe $x \in E$ tq $\mu_u = \mu_{u,x}$ + G groupe abélien d'exposant fini, alors il existe x $\in$ G d'ordre exp(G)=ppcm(o(x),x) $\in$ G

▼ II. 3. Résolution d'équation diophantienne du premier ordre

- idée de l'algorithme de
  résolution du th chinois
- Résolution de ax+by=d [ULMA] + lien avec résolution d'un système de congruence
- Rq matrice [a,b] [[u, -b'],[v,a']] = [d,0] avec la matrice dans GL2(Z) et au+bv=d , a=da',b=db'
- Résolution d'un système de congruence (saux picards?)

▼ II. 4. Entiers de Gauss

- Prop : Z[i] euclidien
- prop : p nb premier, p somme de 2 carrés ssi p n'est pas irréductible dans Z[i]
- Thm des deux carrés DEV1
- Exemple : $41=5^2++4^2$

▼ III. 1. Résolution d'un système d'équations diophantiennes

- th : forme de Hermite dans le cas euclidien + ex
- rq : th reste vrai dans anneau principal

▼ III.2. Forme normale de Smith

- th : forme normale de Smith dans le cadre d'un anneau principal DEV2
- rq : quand anneau en plus euclidien, on a un algo
- app : invariant de similitude

(garder en tête théo de la base adaptée)