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

Développements :

Equations de Fermat. Théorème de structure des groupes finis.

Bibliographie :

Demazure, cours d'algèbre, Goblot, Algèbre commutative, Szpiglas Mathématiques Algèbe L3

Notes

Merci à Matthieu Romagny et Jéremy Leborgne pour leurs avis.

Plan

1 Généralités sous réserve d'existence

Soit A un anneau commutatif intègre

Définition 1 (Sz p.472)**.** Divisibilité et inclusion des idéaux

Définition 2 (Sz p.504)**.** PGCD et PPCM avec les relations de divisibilité

Exemple 3. Dans $\mathbb{Z}$ ...

Remarque 4 (Sz p.504). Il n'y a pas unicité du pgcd. Si d est un pgcd de a et b, alors l'ensemble des pgcd de a et b est dA^*. Ex

Remarque 5 (? ?). Pas toujours existence

Proposition 6 (Sz p. 507)**.** $Pcgd * ppcm = ab$

Remarque 7. On étudie que le pgcd.

2 Un premier type d'anneaux où il y a existence : Anneaux principaux

Définition 8. Anneau principal

Exemple 9. $\mathbb{Z}$ est principal

2.1 PGCD et PPCM

Proposition 10 (Gob p.24)**.** *Existence de pgcd et ppcm et rapport avec idéaux*

Corollaire 11 (Gob p.24)**.** *Pgcd, ppcm et combinaisons linéaires*

Exemple 12. Dans $\mathbb{K}[X]$.

Corollaire 13. *Associativité du pgcd -> on se ramène à l'étude du pgcd de seulement 2 éléments.*

2.2 Eléments premiers entre eux

(à voir avec Ulmer ce qui nécessite "principal")

Définition 14 (Gob p.25)**.** Premiers entre eux

Exemple 15.

Voir le rapport avec éléments étrangers : dans un anneau principal deux éléments premiers entre eux sont étrangers [Gob p.92]

Proposition 16 (Sz p. 507)**.** *a/pgcd et b/pgcd sont premiers entre eux.*

Proposition 17 (Gob p.25)**.** *Thm de Bézout*

Exemple 18. Dans $\mathbb{K}[X]$

Application 19. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier.

Application 20. Lemme des noyaux

Proposition 21 (Gob p.25)**.** *Lemme de Gauss*

Application 22. Résolution THEORIQUE d'équations diophantiennes du type $ax + by = c$

Application 23. Equations de Fermat

Théorème 24. *Thm chinois*

Application 25. Résolution THEORIQUE d'un système de congruences.

3 Calculs effectifs de PGCD

3.1 Anneaux euclidiens

Définition 26 (Sz p.474)**.** Anneau euclidien

Exemple 27. $\mathbb{Z}$ est euclidien, $\mathbb{Z}[i]$ est euclidien

Proposition 28 (Sz p.476)**.** *Euclidien implique principal*

Proposition 29 (Sz p.536)**.** *Division euclidienne dans $A[X]$*

Corollaire 30. *K corps implique $K[X]$ euclidien*

3.2 Algorithmes de calculs du pgcd (et du ppcm ?)

[Demazure +p.176 version matricielle]

3.2.1 Algorithme d'Euclide

Proposition 31 (Dem p.21)**.** *Algorithme d'Euclide classique*

Proposition 32 (Dem p.25)**.** *Complexité en lien avec Fibonacci*

3.2.2 Algorithme binaire

Proposition 33 (Dem p.22)**.** *Algorithme d'Euclide binaire*

Proposition 34 (Dem p.24)**.** *Complexité*

3.2.3 Algorithme d'Euclide étendu

Proposition 35 (Dem p.26+179)**.** *ALgorithme d'Euclide étendu symétrique+version matrices*

Remarque 36 (Dem p.27). La version dissymétrique est plus "rapide"

Proposition 37 (Dem p.28)**.** *Complexité*

Proposition 38 (Dem p.29)**.** *évolution des degrés des polynômes*

Application 39. Détermination d'une relation de Bezout

Exemple 40. Résolution PRATIQUE de $ax + by = c$.

Application 41. Détermination d'un inverse dans $\mathbb{Z}/n\mathbb{Z}$, s'il existe.

Application 42. Détermination d'un inverse dans un corps de rupture.

Exemple 43. Résolution PRATIQUE d'un système de congruences dans $\mathbb{Z}$ et $\mathbb{K}[X]$, avec algo de Newton

Remarque 44 (Dem p.159). Parallèle avec interpolation de Lagrange

4 Pour faire de l'arithmétique comme dans $\mathbb{Z}$: Anneaux factoriels

[Sz]

Définition 45 (Gob p.93 ou Sz p.511)**.** Anneaux factoriels

Exemple 46. $\mathbb{Z}$, etc

Proposition 47 (Gob p.89 ou SZ p.513)**.** *Principal implique factoriel*

Proposition 48 (Gob p. 94 ou Sz p.515)**.** *valuation et divisibilité*

Proposition 49 (Gob p.94 ou Sz p.515)**.** *Ecriture du pgcd ppcm avec les valuations*

Application 50. L'exposant d'un groupe G est le ppcm des ordres des éléments de ce groupe. Il existe un élément d'ordre cet exposant dans G

Conséquence : Thm de structure des groupes abéliens finis Conséquence :

Définition 51. Contenu

Théorème 52 (Gob p.96 ou Sz p. 511)**.** *A factoriel implique A[X] factoriel*

Exemple 53. $\mathbb{K}[X_1, \cdots, X_n]$