Leçon 122. Anneaux principaux. Applications.

Référéences : ROMBALDI - Algèbre et géométrie // ULMER - Anneaux, corps, résultant // DEMAZURE - Cours d'algèbre // BECK-MALICK-PEYRE - Objectif agreg (abrégé en OA) // BOSTAN and cie Algorithmes efficaces en calcul formel (abrégé en AECF) // CALDERO-PERONNIER - Voyage en Algébrie // FRANCINOU-GIANELLA-NICOLAS - Oraux X-ENS Algèbre 1

1. Anneaux factoriel, principal, euclidien

1.1. Anneau principal

Rombaldi

1. Définition. Idéal principal
2. Contre-exemple. $(2,X)$
3. Définition. Anneau principal
4. Exemple. Rombaldi
5. Proposition. Stabilité par isomorphisme
6. Proposition. lien premier / irréductible
7. Contre-exemple. Exemples d'anneaux non principaux
8. Proposition. Histoire d'intégrité
9. Théorème. $A[X]$ principal ssi A corps
10. Exemple. $\mathbf{Z}[X]$ pas principal, $K[X,Y]$

1.2. Anneau euclidien

Rombaldi

11. Définition. Anneau euclidien
12. Exemple. Nombre décimaux, entiers de Gauss et Eisenstein
13. Proposition. Un anneau euclidien est principal
14. Contre-exemple. Un anneau principal n'est pas nécessairement euclidien (Perrin)

2. Arithmétique

2.1. Divisibilité

Ulmer

15. Théorème. Lemme d'Euclide
16. Théorème. Théorème de Gauss
17. Remarque. Gauss implique Euclide, et si existence de la décomosition, alors l'unicité est équivalente (Perrin)
18. Théorème. pgcd et ppcm
19. Application. Les inversibles de $\mathbb{D}$ décimaux
20. Théorème. Caractérisation ppcm
21. Théorème. Décomposition de Bézout
22. Corollaire. premiers entre eux ssi étrangers entre eux
23. Contre-exemple. Perrin, $(2,X)$
24. Théorème. Chinois (OA)
25. Application. OA

2.2. Algorithme des anneaux euclidiens

Demazure

26. Lemme. $\gcd(u-v,v) = \gcd(u,v)$
27. Application. Algorithme d'Euclide Binaire
28. Remarque. Complexité en $O(\log(\max(u,v))^2)$
29. Théorème. Algorithme d'Euclide étendu Ulmer
30. Exemple. Ulmer
31. Théorème. Fibonacci et Lamé

3. Applications

3.1. Equations dans Z

32. Exemple. Résolution de systèmes de congruence (Rombaldi)
33. Théorème. Equation diophantienne
34. Remarque. On utilise l'algorithme d'Euclide pour trouver des solutions
35. Exemple. Résolution d'une équation de Mordell (Voyage en algébrie)
36. Application. Cryptosystème RSA (OA)
37. Théorème. DEVELOPPEMENT Théorème de Sophie Germain (X-ENS Alg 1)

3.2. Arithmétique dans les polynômes

OA

38. Lemme. Linéarité de l'élévation à la puissance Q
39. Théorème. DEVELOPPEMENT Berlekamp (OA)

AECF

40. Définition. Résultant
41. Proposition. Sur un corps, lien avec le pgcd dans la forme échelonnée
42. Théorème. Existence de U et V tq $PU + VQ = \mathrm{Res}(P,Q)$.
43. Corollaire. A et B premier entre eux ssi $\mathrm{Res}(A,B) = 0$.
44. Application. Trouver des points d'intersection
45. Exemple. Calcul du résultant via algorithme d'Euclide

3.3. Algèbre linéaire

OA

46. Définition. Polynôme minimal
47. Proposition. Réduction avec théorème chinois
48. Théorème. Lemme des noyaux
49. Corollaire. Dunford