Corentin Bergeron ENS Rennes

Leçon 142 : PGCD, PPCM. Algorithmes de calculs. Exemples et applications

[Bec] : *Objectif agrégation*, Vincent Beck, Jerôme Malick, Gabriel Peyré
[Ber] : *Algèbre, le grand combat*, Grégory Berhuy
[Cal-Per] : *Carnet de voyage en Algébrie*, Phillipe Caldero, Marie Peronnier
[Goz] : *Théorie de galois*, Ivan Gozard
[Gra-Gra] : *Algèbre er Arithmétique fondamentales*, Georges Gras, Marie-Nicole Gras
[Per] : *Cous d'algèbre*, Daniel Perrin
[Rom] : *Mathématiques pour l'agrégation*, Jean-Étienne Rombaldi
[Ulm] : *Anneaux, corps, résultant*, Félix Ulmer
[131] : *131 développements pour l'oral*, Didier Lesesvre, Pierre Montagnon

I Partie A - What is this ? [Ber] [Gra-Gra] [Ulm]

I.1 Définitions

Déf 1 (Divisibilité) :

Rem 2 : Reformulation en terme d'idéaux.

Ex 3 : Voir [Ber].

Déf 4 (PGCD, PPCM) :

Rem 5 : Généralisation à n éléments.

Contre-Ex 6 : Dans $\mathbb{Z}[i\sqrt{5}]$, voir [Ber].

Déf 7 (Premiers entre eux) :

Ex 8 : Deux éléments étrangers sont premiers entre eux, la réciproque est fausse.

Contre-Ex 9 : Voir [Ulm].

Rem 10 : Lien entre premiers entre eux et PGCD.

Prop 11 (Unicité PGCD, PPCM) :

Prop 12 (Formule PGCD / PPCM) :

I.2 Dans un anneau factoriel

Déf 13 (Anneau factoriel) :

Ex 14 : $\mathbb{Z}$.

Contre-Ex 15 : L'anneau des fonctions entières n'est pas factoriel.

Déf 16 (scri) :

Ex 17 : Les nombres premiers dans $\mathbb{Z}$.

Déf 18 (Valuation π-adique) :

Prop 19 (Propriétés de la valuation) :

Thm 20 (Forme du PGCD et PPCM) :

Prop 21 (Lemme de Gauss) :

App 22 (Lemme du dév) :

I.3 Dans un anneau principal

Déf 23 (Idéal principal, anneau principal) :

Ex 24 : Exemples usuels.

Thm 25 : Principal $\Longrightarrow$ factoriel.

Thm 26 (Forme du PGCD et PPCM) :

Ex 27 : Exemple dans Z

Thm 28 (Bézout) :

App 29 (Inversibles dans un quotient) :

Ex 30 (Inversibles dans $\mathbb{Z}/n\mathbb{Z}$) :

Ex 31 : Inverser une polynôme dans un quotien (voir [Ulm]).

II Partie B - Algos à gogo [Ber] [Ulm] [Rom][Per]

II.1 Anneaux euclidiens [131[Cal-Per]]

Déf 32 (Anneau euclidien) :

Ex 33 : Z, $K[X]$, $\mathbb{Z}[i]$.

Thm 34 : Une anneau euclidien est principal.

Contre-Ex 35 : $\mathbb{Z}[X]$ n'est pas euclidien.

Contre-Ex 36 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

Dév 37 : $\mathbb{Z}[i\sqrt{2}]$ est euclidien et ses inversibles sont ± 1.

Dév 38 (Équation de Mordell) :

Dév 39 (Unique entier entre un carré et un cube) :

II.2 Euclide [Ber]

Prop 40 : Si $n \in \mathbb{Z}$, alors $\text{pgcd}(a, b) = \text{pgcd}(a, n - na)$.

Thm 41 (Euclide) :

Ex 42 : Voir [Ber].

II.3 Euclide étendu

Thm 43 (Euclide étendu) :

Ex 44 : Exemples dans $\mathbb{Z}$ et $\mathbb{Z}[i]$ et $\mathbb{F}_2[X]$.

III Partie C - Des systèmes, encore des systèmes... [Ulm] [Ber] [Bec]

III.1 Systèmes de congruence

Thm 45 (Restes chinois) :

Ex 46 (Restes chinois effectif) :

App 47 (Système de congruences) :

Ex 48 : Exemple avec une relation de Bézout.

Ex 49 : Exemple avec l'algorithme de Garner.

III.2 Résolution de systèmes linéaires

Déf 50 (Matrice échelonée) :

Dév 51 (Forme normale de Smith) :

Ex 52 : Voir [Ber].

App 53 (Structure des groupes abéliens) :

IV Partie D - Parce qu'il faut rajourter un peu de bonheur [Per] [Ulm] [Ber]

Déf 54 (Contenu, polynôme primitif) :

Prop 55 (Lemme de Gauss) :

App 56 : Un nombre algébrique est entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

Thm 57 (Transfert) :

App 58 (Irréductibilité et primitivité) :