Leçon n° 122 : Anneaux principaux. Applications.

Soit A un anneau commutatif intègre.

I/ Arithmétique dans les anneaux principaux.

A/ Vocabulaire général. [ROM]

Définition 1 : Idéal et idéal principal.

Définition 2 : Divisibilité.

Définition 3 : Éléments associés.

Définition 4 : Éléments premiers et irréductibles.

Proposition 5 : Si a est premier alors a est irréductible.

Exemple 6 : Dans $\mathbb{Z}$, les nombres premiers sont premiers.

Définition 7 : PGCD et PPCM.

Remarque 8 : N'existent pas toujours.

B/ Le cas des anneaux principaux. [ROM]

Définition 9 : Anneau principal.

Exemple 10 : $\mathbb{Z}$ et $\mathbb{K}[X]$.

Lemme 11 : Irréductible $\Rightarrow$ premier et les idéaux.

Proposition 12 : $A[X]$ est principal $\Leftrightarrow$ A est un corps.

Exemple 13 : $\mathbb{Z}[X]$ n'est pas principal car l'idéal $(2, X)$ n'est pas principal et $\mathbb{Q}(\sqrt{j})[X]$ est principal.

Théorème 14 : Existence du PGCD et du PPCM dans les anneaux principaux.

Corollaire 15 : Lemme de Gauss.

Théorème 16 : Théorème chinois.

Remarque 17 : Dans le cas de $\mathbb{Z}$, avec le théorème de structure des groupes abéliens finis, on peut obtenir tous les groupes abéliens finis à isomorphisme près.

Application 18 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n! H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

C/ Anneaux factoriels. [ROM]

Définition 19 : Anneau factoriel.

Théorème 20 : A factoriel $\Leftrightarrow$ toute suite d'idéaux croissante stationne et tout élément premier est irréductible.

Corollaire 21 : Les anneaux principaux sont factoriels.

Application 22 : Décomposition en nombres premiers.

Application 23 : Calcul du PGCD et du PPCM avec la décomposition.

Exemple 24 : $\mathbb{K}[X]$ est factoriel : décomposition dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Proposition 25 : A factoriel $\Longrightarrow$ $A[X]$ factoriel.

II/ Applications aux anneaux euclidiens.

A/ Généralités. [ROM] [PER]

Définition 26 : Anneau euclidien.

Proposition 27 : Euclidien $\Longrightarrow$ principal.

Exemple 28 : $\mathbb{Z}$ et $\mathbb{K}[X]$.

Algorithme 29 : Algorithme d'Euclide et complexité dans $\mathbb{Z}$ et $\mathbb{K}[X]$.

Contre-exemple 30 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ n'est pas euclidien.

B/ L'anneau des entiers de Gauss $\mathbb{Z}[i]$. [PER]

Définition 31 : Entiers de Gauss $\mathbb{Z}[i]$.

Proposition 32 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Développement 1

Proposition 33 : $\mathbb{Z}[i]$ euclidien.

Théorème 34 : Théorème des deux carrés.

Corollaire 35 : Irréductibles de $\mathbb{Z}[i]$.

C/ Théorème des facteurs invariants dans $M_n(A)$. [OBJ]

Développement 2

Théorème 36 : Forme normale de Smith : existence et unicité.

Application 37 : Théorème de la base adaptée sur $\mathbb{Z}$.

Application 38 : Théorème de structure des groupes abéliens finis.

III/ Autres applications.

A/ Équations diophantiennes. [ROM]

Proposition 39 : Résolution de $ax + by = c$: solution ssi $a \wedge b \mid c$.

Application 40 : Résolution de systèmes de congruence dans $\mathbb{Z}$ grâce au théorème chinois.

Exemple 41 : Exemple de résolution.

B/ En algèbre linéaire. [ROM]

Définition 42 : Polynôme minimal d'une matrice.

Proposition 43 : $\dim_{\mathbb{K}}(\mathbb{K}[M]) = \deg(\pi_M)$.

Lemme 44 : Lemme des noyaux.

Théorème 45 : Décomposition de Dunford.

Références :

- [PER] Perrin p. 45-59
- [ROM] Rombaldi Algèbre 2nd éd. p. 213, p. 237 et p. 261
- [OBJ] Beck, Malick Peyré Objectif Agrégation p. 285