

Leçon 122 : Anneaux principaux. Applications.

[Ber] : *Algèbre, le grand combat*, Grégory Berhuy

[Cal-Per] : *Carnet de voyage en Algèbre*, Phillipe Caldero, Marie Peronnier

[Goz] : *Théorie de galois*, Ivan Gozard

[Per] : *Cous d'algèbre*, Daniel Perrin

[Rom] : *Mathématiques pour l'agrégation*, Jean-Étienne Rombaldi

[131] : *131 développements pour l'oral*, Didier Lesesvre, Pierre Montagnon

I Partie A - Généralités [Ber] [Rom]

I.1 Anneaux principaux [Ber] [Rom]

■ **Déf 1 (Idéal principal) :**

■ **Déf 2 (Anneau principal) :**

■ **Ex 3 :** $\mathbb{Z}$, K

■ **Ex 4 :** $\mathbb{Z} \left[\frac{1+i\sqrt{19}}{2} \right]$ est principal.

■ **Contre-Ex 5 :** $\mathbb{Z}/6\mathbb{Z}$ n'est pas principal, bien que tous ses idéaux soient principaux, $\mathbb{Z}[X]$ n'est pas principal.

I.2 Anneaux euclidiens [Ber] [Goz] [Rom]

■ **Déf 6 (Anneau euclidien) :**

■ **Ex 7 :** $\mathbb{Z}$, $K[X]$, $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$.

■ **Thm 8 :** Un anneau euclidien est principal.

■ **Contre-Ex 9 :** $\mathbb{Z}[X]$ n'est pas euclidien.

■ **Contre-Ex 10 :** $\mathbb{Z} \left[\frac{1+i\sqrt{19}}{2} \right]$ n'est pas euclidien.

App 11 (Polynôme minimal d'endomorphismes) :

App 12 (Polynôme minimal d'un nombre algébrique) :

II Partie B - Arithmétique

II.1 Rappels de divisibilité [Ber][Rom]

■ **Déf 13 (Divisibilité) :**

Rem 14 : $a|b$ ssi $\langle b \rangle \subset \langle a \rangle$

■ **Déf 15 (Premier entre eux) :**

■ **Ex 16 :** Exemples dans [Ber].

■ **Déf 17 (pgcd, ppcm) :**

■ **Contre-Ex 18 :** $\mathbb{Z}[i\sqrt{5}]$ avec 3 et $2+i\sqrt{5}$.

■ **Déf 19 (Irréductible, premier) :**

■ **Prop 20 :** Un élément premier est irréductible.

■ **Ex 21 :** Exemples dans [Ber].

■ **Ex 22 :** Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

■ **Contre-Ex 23 :** $\mathbb{Z}[i\sqrt{3}]$ avec 2.

II.2 Arithmétique dans un anneau principal [Ber]

■ **Prop 24 (pgcd et ppcm dans un anneau principal) :**

■ **Thm 25 (Bézout) :**

Rem 26 : Dans le cas euclidien, pour trouver une relation de Bézout, ou un pgcd, on possède l'algorithme d'Euclide.

■ **Ex 27 :** Exemple de calcul de pgcd

■ **Prop 28 (Lemme de Gauss) :**

■ **Prop 29 (Lemme d'Euclide) :**

■ **Prop 30 :** Un élément est irréductible ssi il est premier.

App 31 : $A/\langle \pi \rangle$ est un corps ssi π est irréductible.

App 32 : $\mathbb{C} = \mathbb{R}[X]/\langle X^2 + 1 \rangle$ est un corps

■ **Thm 33 (Décomposition en produit d'irréductibles) :**

II.3 Théorème des restes chinois [Ber] [Rom]

Thm 34 (Restes chinois) :

App 35 (Inversibles de $\mathbb{Z}/n\mathbb{Z}$) :

App 36 (Interpolation de Lagrange) :

Prop 37 (Équation diophantienne) :

App 38 (Système d'équations diophantiennes) :

Ex 39 : Voir dans [Rom]

III Partie C - Systèmes linéaires

 **Dév 40 (Forme de Smith) :**

App 41 (Résolution matricielle) :

App 42 : Invariants de similitude]

IV Partie D - Équations diophantiennes

IV.1 L'anneau des entiers de Gauss [Per] [Ber]

Ex 43 : Calcul d'un pgcd dans $\mathbb{Z}[i]$

Prop 44 : Inversibles de $\mathbb{Z}[i]$.

Prop 45 : p est somme de carrés ssi p n'est pas irréductible dans $\mathbb{Z}[i]$.

App 46 : p est somme de carrés ssi $p = 2$ ou $p \equiv 1[4]$.

Ex 47 : $41 = 5^2 + 4^2$

IV.2 L'anneau $\mathbb{Z}[i\sqrt{2}]$ [131] [Cal-Per]

Prop 48 : Inversibles de $\mathbb{Z}[i\sqrt{2}]$.

 **Dév 49 (Équation de Mordell) :**