

Leçon 122 : Anneaux principaux. Exemples et applications.

Matei Lefebvre

2025/2026

1 Notion de principalité.

A est un anneau commutatif intègre unitaire.

1.1 Idéaux et principalité.

[Ber20], XIV.4, XV.1-2

~ 15 items.

définition idéal | exemples | comportement avec les morphismes | anneau quotient | théorème de factorisation | intersection et somme d'idéaux | idéal engendré | définition idéal principal | exemple, contre-exemple | définition anneau principal | exemple : $\mathbb{Z}$ | définition idéal premier, maximal | caractérisation par le quotient | cas des anneaux principaux, exemple | lemme Krull

1.2 Un critère pratique : les anneaux euclidiens.

[Ber20], XVII.3

~ 5 items.

définition anneau euclidien | exemples | euclidien $\Rightarrow$ principal | corollaires | DEV 1

D1

Théorème. $\mathbb{Z} \left[\frac{1 + i\sqrt{19}}{2} \right]$ est un anneau principal non euclidien.

[Per96], II.5

2 Arithmétique dans les anneaux principaux .

2.1 Anneaux factoriels, résultats théoriques.

[Ber20], XVII.2 et XVII.5

~ 6 items.

définition anneau factoriel | principal $\Rightarrow$ factoriel | exemples | irréductible $\Rightarrow$ premier (Euclide) | théorème de Gauss | existence pgcd, ppcm

2.2 Résultats pratiques.

[Ber20], XVII.2-3 et XV.3 et [Rom21], X.3-4

~ 9 items.

relations de Bézout | caractérisation éléments premiers entre eux | exemple | $A/(a)$ corps $\Leftrightarrow A/(a)$ intègre $\Leftrightarrow a$ irréductible | exemple | théorème chinois | exemple | algorithme d'Euclide | exemple

2.3 Entiers de Gauss, théorème des deux carrés.

[Per96], II.6

~ 7 items.

définition Σ | exemples | définition $\mathbb{Z}[i]$, norme | Σ stable par multiplication | inversibles de $\mathbb{Z}[i]$ | DEV 1 : théorème des deux carrés

D1

Théorème. 1. Soit $p \in \mathcal{P}$. Alors, p est somme de deux carrés $\Leftrightarrow p$ n'est pas irréductible dans $\mathbb{Z}[i]$ $\Leftrightarrow p = 2$ ou $p \equiv 1[4]$.

2. Soit $n = \prod_{p \in \mathcal{P}} p^{vp(n)} \geq 2$. Alors, n est somme de deux carrés si et seulement si $\forall p \equiv 3[4], vp(n) \in 2\mathbb{N}$.

3. Les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près, les $p \in \mathcal{P}$ avec $p \equiv 3[4]$ et les $z \in \mathbb{Z}[i]$ avec $N(z) \in \mathcal{P}$.

[Per96], II.6

3 Applications.

3.1 Algèbre linéaire.

[MM22], I et IV

~ 7 items

idéal des polynômes annulateurs d'un endomorphisme | polynôme minimal | exemple | polynôme minimal local | exemple | lemme des noyaux | remarque sur les projecteur

3.2 Extensions de corps, éléments algébriques.

[Per96], III.1

~ 5 items

structure des extensions monogènes | définition élément algébrique, polynôme minimal | exemple | a algébrique $\Leftrightarrow \mathbb{K}(a) = \mathbb{K}[a]$

Références

- [Per96] D. PERRIN. *Cours d'algèbre (Agrégation)*. ELLIPSES, 1996. ISBN : 9782729855529.
- [Ber20] G. BERHUY. *Algèbre : le grand combat*. CALVAGE&MOUNET, 2020. ISBN : 9782916352831.
- [Rom21] J.E. ROMBALDI. *Mathématiques pour l'agrégation - Algèbre et géométrie*. DEBOECK, 2021. ISBN : 9782807332201.
- [MM22] R. MANSUY et R. MNEIMNÉ. *Algèbre linéaire. Réduction des endomorphismes*. DEBOECK, 2022. ISBN : 9782807336612.