

[Ulma]
[Rom]
[Goz]
[Per]

122 - Anneaux principaux - Applications

I - Notion de principalité

1) Idéaux et anneaux principaux

[Ulma] 5-6

- def idéal, max, premier + prop 16 31-32 42
- def idéal principal anneau principal [Rom] 237
- ex et cf $\mathbb{Z}[x]$

2) Cas particulier : anneaux euclidiens

[Ulma] 43 47

- def + exemple
- euclidien $\Rightarrow$ principal
- $\mathbb{Z}[1+i\sqrt{5}]$
- $A[x]$ principal $\Leftrightarrow A$ corps

II - Arithmétique dans les anneaux principaux

1) Divisibilité

[Ulma] 39-45

- def alb
- def premiers entre eux
- irréductible
- éléments premier

2) PGCD, PPCM

[Ulma] 40-42

[Goz] 10

- def, Bézout, Gauss
- contenu + Eisenstein
- algo d'Euclide

DEV1

III - Applications

1) Échiers de Gauss

[Per] 56-57

- def
- Th des 2 carrés

DEV2

DEV3

2) Théorème Chinois

- Th et application

122: Anneaux principaux. Applications

Soit $(A, +, \cdot)$ un anneau commutatif unitaire

I - Notion de principalité

1) Idéaux et anneaux principaux

Définition 1: Un sous ensemble $I \subset A$ est un idéal de A si

1) $(I, +)$ est un sous groupe de $(A, +)$

2) $\forall a \in A, \forall b \in I, ab \in I$

Exemples 2: • Si $A \neq \{0\}$, $\{0\}$ et A sont toujours des idéaux

• Pour tout morphisme d'anneau $\varphi: A \rightarrow B$, $\ker \varphi$ est un idéal de A .

• Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$

Lemme 3: les seuls idéaux d'un corps K sont $\{0\}$ et K

un anneau commutatif ayant exactement deux idéaux est un corps.

Définition 4: Un idéal I de A est maximal si:

1) $I \neq A$

2) $\forall J$ idéal de A tel que $I \subset J \subset A$, $J = I$ ou $J = A$

Proposition 5: Un idéal I est maximal ssi A/I est un corps

Définition 6: Un idéal I de A est premier si

1) $I \neq A$

2) $\forall a, b \in A$ si $ab \in I$ alors $a \in I$ ou $b \in I$

Proposition 7: Un idéal I est premier ssi A/I intègre.

Corollaire 8: Tout idéal maximal est premier.

Définition 9: un idéal I de A est principal s'il existe $a \in A$ tel que $I = (a)$

Définition 10: On dit que A est principal si A est intègre et si tout idéal de A est principal

Exemples 11: • $\mathbb{Z}$ est principal

• Un corps est principal

• Pour K un corps, $K[x]$ est principal

• $\mathbb{Z}[x]$ n'est pas principal $K[x, y]$

principal $\Rightarrow$ factoriel?

2) Cas particulier: anneaux euclidiens

Définition 12: On dit que A est euclidien s'il est intègre et s'il existe une fonction $v: A \setminus \{0\} \rightarrow \mathbb{N}$ telle que pour tout $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$.

L'élément q est le quotient et r le reste.

La fonction v est appelée statut euclidien pour A .

Exemple 13: $\mathbb{Z}$ avec $v(a) = |a|$

Proposition 14: Tout anneau euclidien est principal

Exemple 15: $\mathbb{Z}[\frac{1+i\sqrt{5}}{2}]$ est principal mais non euclidien

Proposition 16: Soit K un corps commutatif. Alors $K[x]$ est un anneau euclidien pour le statut $v(P) = \deg P$

Théorème 17: On a équivalence entre

1) A est un corps

2) $A[x]$ est un anneau euclidien

3) $A[x]$ est un anneau principal

II-Arithmétique dans les anneaux principaux.

1) Divisibilité

- 39 Définition 18: Soit $a, b \in A$,
1) On dit que a divise b , noté $a|b$, s'il existe $c \in A$ tel que $b = ac$. Ainsi $a|b$ ssi $(b) \subset (a)$
2) On dit que a et b sont associés, noté $a \sim b$, si $a|b$ et $b|a$. Ainsi $a \sim b$ ssi $(a) = (b)$

- 41 Définition 19: Deux éléments non nuls a et b dans A sont dits premiers entre eux si tout diviseur commun est inversible.

Exemple 20: 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$

- 45 Définition 21: Un élément $a \in A$ est dit:
1) irréductible si a est non nul et non inversible et que si $a = bc$ alors b est inversible ou c est inversible
2) premier si a est non nul et non inversible, et que si $a|bc$ alors $a|b$ ou $a|c$

Proposition 22: Soit $a \in A \setminus \{0\}$. Alors a est premier ssi (a) est un idéal premier.

Lemme 23: Dans un anneau intègre A , tout élément premier est irréductible

Proposition 24: Dans un anneau principal, $a \in A$ est premier ssi a est irréductible.

Corollaire 25: Soit A principal. Un idéal non nul $(a) \subset A$ est maximal ssi a est irréductible dans A .

2) PGCD et PPCM

Définition 26: Soit a et $b \in A$.

On dit que $d \in A$ est un pgcd de a et b si:
 $d|a$ et $d|b$ et $\forall d' \in A$ tel que $d'|a$ et $d'|b$ alors $d|d'$

On dit que $m \in A$ est un ppcm de a et b si:
 $a|m$ et $b|m$ et $\forall m' \in A$ tel que $a|m'$ et $b|m'$ alors $m|m'$

Remarque 27: a et b sont premiers entre eux ssi 1 est un pgcd de a et b . $\neq x$

Théorème 28 (Bézout): Soit A principal. Deux éléments a et $b \in A$ sont premiers entre eux ssi $\exists u, v \in A$ tels que $au + bv = 1$ 12

Lemme 29 (Euclide et Gauss) Soit A un anneau principal, $C \in A$, $a, b \in A$ premiers entre eux. Alors

$$1) a|bc \Rightarrow a|c$$

$$2) a|c \text{ et } b|c \Rightarrow ab|c$$

Définition 30: Soit $P \in A[X]$ avec $P \neq 0$. On appelle contenu de P , noté $c(P)$, un pgcd de ses coefficients. On dit que P est primitif si $c(P) = 1$ 10

Lemme 31 (Gauss) Soit $P, Q \in A[X]$. On a:

$$c(PQ) = c(P)c(Q)$$

Théorème 32: Soit A un anneau factoriel, $K = \text{frac}(A)$ le corps des fractions de A . Soit P le polynôme de degré supérieur ou égal à 1 à coefficients dans A . P irréductible dans $A[X]$ ssi P irréductible dans $K[X]$ et $c(P) = 1$

Théorème 33: (critère d'Eisenstein) DEV 1

Soit A factoriel, $K = \text{frac}(A)$. Soit $P = \sum_{i=0}^n a_i X^i \in A[X]$
avec $\deg P \geq 1$.

Soit $p \in A$ irréductible de A tel que $p \nmid a_n$, $\forall i \in [1, n-1]$
 $p \nmid a_0$ et $p^2 \nmid a_0$.

Alors P est irréductible dans $K[X]$

III - Applications

1) Entiers de Gauss

[Per] Définition 34: On définit l'anneau des entiers de

56 Gauss: $\mathbb{Z}[i] := \{a+ib \in \mathbb{C}, a, b \in \mathbb{Z}\}$

On lui attribue la norme $N: \mathbb{Z}[i] \rightarrow \mathbb{N}$

$$z = a+ib \mapsto z\bar{z} = a^2 + b^2$$

Définition 35: On note Σ l'ensemble:

$$\Sigma := \{n \in \mathbb{N} \text{ tq } \exists (a, b) \in \mathbb{N}^2 \text{ tel que } n = a^2 + b^2\}$$

57 Théorème 36: Soit p un nombre premier. On a

$$p \in \Sigma \Leftrightarrow p = 2 \text{ ou } p \equiv 1 [4] \quad \boxed{\text{DEV 2}}$$

2) Théorème Chinois

♥ Théorème 37: Soit $a_1, \dots, a_n \in A$ premiers entre eux
 $\mathbb{Z} \hat{=} \mathbb{Z}$. Alors

$$A_{(a_1, \dots, a_n)} \simeq A_{(a_1)} \times \dots \times A_{(a_n)} \quad \boxed{\text{DEV 3}}$$

122: Anneaux principaux Exemples et applications

But: Généraliser
les propriétés des
anneaux classiques
et de $\mathbb{Z}$

Entiers de Gauss $\mathbb{Z}[i]$

→ on connaît ses irréductibles
avec le Th des 2 carrés (DEV 1)

Th Chinois (DEV 2)
lien entre les éléments
premiers entre eux.

Arithmétique dans un anneau
principal

• Divisibilité

* premier entre eux $\leftrightarrow$ Gauss
Euclide

* irréductible

$\updownarrow$
premier

$\uparrow$ Δ vrai anneau

pgcd ppcm
 $\hookrightarrow$ existence

Bezout
+
Gauss

OK anneau
principal

Notion de principalité

→ idéaux : ils sont pas tous principaux
ex $\mathbb{Z}[x] : (x)$

→ anneau : anneau principal dont
tous les idéaux sont principaux

$\hookrightarrow \mathbb{Z}$, corps

(pas simple de mq
un anneau est principal

Cas particulier

→ anneau euclidien $\Rightarrow$ principal
 $\mathbb{Z}[\frac{1+i\sqrt{5}}{2}]$ $\nRightarrow$

→ Algo d'Euclide pour pgcd
+ relation de Bezout

irréductibilité des
Polynômes

Eisenstein