10 Leçon 122 : Anneaux principaux. Exemples et applications.

I. Notion de principalité

1. Idéaux [ULM]

Idéal, idéal maximal, idéal premier

2. Anneau principal [ULM]

Idéal principal, anneau principal, exemples, contre-exemple $\mathbb{Z}[X]$

3. Anneau euclidien [ULM]

Anneau euclidien, euclidien $\Rightarrow$ principal, $A[X]$ est principal ssi A est un corps

II. Arithmétique dans les anneaux principaux

1. Divisibilité [ULM]

a divise b, éléments associés, éléments premiers entre eux, élément irréductible, élément premier, cas d'un anneau principal

2. PGCD et PPCM [BER] [PER]

PGCD, PPCM, cas d'un anneau principal, théorème de Bézout, lemme de Gauss, contenu,
DEV 1 : critère d'Eisenstein

III. Applications

1. Théorème chinois [ROM]

DEV 2 : théorème chinois + formule générale de l'indicatrice d'Euler

exemple de système de congruences

2. En algèbre linéaire [MAN] [BER]

Lemme des noyaux, annulateur de u, polynôme minimal, critères de diagonalisabilité

Présentation :

- Dans cette leçon, on souhaite généraliser les propriétés des anneaux classiques, et notamment celles de $\mathbb{Z}$ en ce qui concerne l'arithmétique.
- Dans les anneaux euclidiens, on dispose de l'algorithme d'Euclide qui permet, une fois trouvé le PGCD de deux éléments, de remonter pour trouver une relation de Bézout.
- Dans $A[X]$, même si A n'est pas un corps, on peut tout de même effectuer la division euclidienne par un polynôme à condition que celui-ci ait son coefficient dominant inversible.
- Dans le lemme des noyaux, c'est le fait que $K[X]$ soit principal et donc qu'il existe une relation de Bézout entre les polynômes qui permet de faire fonctionner la preuve.

Développements :

- Théorème chinois + application à l'indicatrice d'Euler

- Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p249-283

- Critère d'Eisenstein
  - Algèbre-Probabilités, Gourdon, p62
  - Cours d'algèbre, Perrin, p51 et 76
  - Théorie de Galois, Gozard, p10

Références :

- [ULM] Anneaux-corps-résultants, Ulmer
- [BER] Algèbre : le grand combat, Berhuy
- [PER] Cours d'algèbre, Perrin
- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [MAN] Algèbre linéaire réduction des endomorphismes, Mansuy-Mneimné

Leçon 122 : Anneaux principaux. Exemples et applications

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

I Notion de principalité

1) Idéaux [ULM]

Déf 1 : Un sous-ensemble $I \subset A$ est un idéal de A si :
1) $(I, +)$ est un sous-groupe de $(A, +)$
2) $\forall a \in A, \forall b \in I, ab \in I$.

Exemple 2 : • Si $A \neq \{0\}$, $\{0\}$ et A sont toujours des idéaux.
• Pour tout morphisme d'anneaux $\ell : A \to B$, $\ker(\ell)$ est un idéal de A.

Exemple 3 : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z} = \{nk ; k \in \mathbb{Z}\}$

Prop 4 : Une intersection quelconque d'idéaux de A est un idéal de A.

Lemme 5 : Les seuls idéaux d'un corps K sont $\{0\}$ et K.
Un anneau ayant exactement 2 idéaux est un corps.

Déf 6 : Un idéal I de A est dit maximal si :
1) $I \neq A$
2) pour tout idéal J de A tel que $I \subset J \subset A$, $J = I$ ou $J = A$

Prop 7 : Un idéal I est maximal ssi A/I est un corps.

Déf 8 : Un idéal I de A est dit premier si :
1) $I \neq A$
2) $\forall a, b \in A$, si $ab \in I$, alors $a \in I$ ou $b \in I$.

Prop 9 : Un idéal I est premier ssi A/I est un anneau intègre.

Corollaire 10 : Tout idéal maximal est premier

Contre-ex 11 : dans $A = \mathbb{Z}$, l'idéal $I = \{0\}$ est premier car $\mathbb{Z}$ est intègre, mais n'est pas maximal ($\mathbb{Z}$ n'est pas un corps).

2) Anneaux principaux [ULM] [Ber]

Déf 12 : Un idéal I de A est dit principal s'il existe $a \in A$ tel que $I = (a)$.

Déf 13 : On dit que A est principal si A est intègre et si tout idéal de A est principal.

Exemple 14 : • $\mathbb{Z}$ est principal
• Un corps est principal
• Pour K un corps, $K[X]$ est principal

Contre-ex 15 : L'anneau $\mathbb{Z}[X]$ n'est pas principal car $(2, X)$ n'est pas un idéal principal.

Prop 16 : Dans un anneau principal, tout idéal premier non nul est maximal.

3) Anneau euclidien [ULM]

Déf 17 : On dit que A est euclidien s'il est intègre et s'il existe une fonction $v : A \setminus \{0\} \to \mathbb{N}$ tel que pour tout $a \in A$ et $b \in A \setminus \{0\}$, il existe $q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$.
L'élément q est le quotient et r est le reste
La fonction v est appelée stathme euclidien pour A

Exemple 18 : L'anneau $\mathbb{Z}$ est euclidien pour $v(a) = |a|$

Prop 19 : Tout anneau euclidien est principal.

Contre-ex 20 ADMIS : $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ est un anneau principal mais non euclidien.

Prop 21 : Soit K un corps. Alors $K[X]$ est un anneau euclidien pour le stathme $v(P) = \deg(P)$.

Théorème 22 : 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 [ULM]

ULM 39

Déf 23 : Soit $a, b \in A$

1) On dit que a divise b, noté $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. Ainsi $a \mid b$ ssi $(b) \subset (a)$.

2) On dit que a et b sont associés, noté $a \sim b$, si $a \mid b$ et $b \mid a$. Ainsi $a \sim b$ ssi $(a) = (b)$.

Prop 24 : Si A est intègre, $\sim$ est une relation d'équivalence. Soit A. Ainsi on a $a \sim b$ ssi il existe $u \in A^\times$ tel que $b = u.a$.

ULM 41

Déf 25 : Deux éléments non nuls a et b dans A sont dits premiers entre eux si tout diviseur commun est inversible.

Exemple 26 : 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$.

ULM 45

Déf 27 : 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 $a \mid bc$ alors $a \mid b$ ou $a \mid c$.

Prop 28 : Soit $a \in A \setminus \{0\}$. Alors a est premier ssi (a) est un idéal premier.

Lemme 29 : Si A est intègre, tout élément premier est irréductible.

Prop 30 : Dans un anneau principal, un élément est premier ssi il est irréductible.

Corollaire 31 : Soit A principal. Un idéal non nul $(a) \subset A$ est maximal ssi a est irréductible dans A.

2) PGCD et PPCM [BER] [PER]

BER 519

Déf 32 : Soit $a, b \in A$.

On dit que $d \in A$ est un PGCD de a et b si :

1) $d \mid a$ et $d \mid b$ 2) $\forall c \in A$ tel que $c \mid a$ et $c \mid b$, on a $c \mid d$

On dit que $m \in A$ est un PPCM de a et b si :

1) $a \mid m$ et $b \mid m$ 2) $\forall c \in A$ tel que $a \mid c$ et $b \mid c$, on a $m \mid c$.

Remarque 33 : Si A est intègre, deux PGCD (resp PPCM) sont associés donc sont égaux à un inversible près.

Remarque 34 : a et b sont premiers entre eux ssi 1 est un PGCD de a et b.

BER 526

Prop 35 : Soit A principal. Soit $a, b, d, m \in A$ tel que $(a) + (b) = (d)$ et $(a) \cap (b) = (m)$

Alors d est un PGCD de a et b, et m un PPCM de a et b.

Théorème 36 (de Bézout) : Soit A principal. Deux éléments $a, b \in A$ sont premiers entre eux ssi il existe $u, v \in A$ tel que $au + bv = 1$.

Lemme 37 (de Gauss) : Soit A principal. Soit $a, b \in A$ premiers entre eux. Alors pour $c \in A$: $a \mid bc \Rightarrow a \mid c$.

On suppose que A est principal et on note K son corps des fractions

PER 51

Déf 38 : Soit $P \in A[X] \setminus \{0\}$. On appelle contenu de P, noté $c(P)$, un PGCD de ses coefficients.

Si $c(P) = 1$, on dit que P est primitif.

Lemme 39 : On a : $c(PQ) = c(P)\,c(Q)$.

Prop 40 : Si $P \in A[X]$ est de degré ≥ 1 et irréductible dans $A[X]$, alors il est primitif et irréductible dans $K[X]$.

PER 76

Théorème 41 (critère d'Eisenstein) : Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$

Soit $p \in A$ un élément irréductible. On suppose que :

1) $p \nmid a_n$

2) $p \mid a_i \quad \forall i \in [\![0, n-1]\!]$

3) $p^2 \nmid a_0$

Alors P est irréductible dans $K[X]$. DEV 1

Application 42 : le p-ième cyclotomique est irréductible sur $\mathbb{Q}$ (p-ième polynôme)

III Applications

1) Théorème chinois [ROM] [BER]

ROM 249 Soit A un anneau principal.

Lemme 43 : Soit $a_1, \dots, a_n \in A$ deux à deux premiers entre eux. Soit $a = \hat{\prod}_{j=1} a_j$ et $b_j = \frac{a}{a_j} = \hat{\prod}_{i \neq j} a_i$ $\forall j \in [\![1;n]\!]$. Alors les b_j sont premiers entre eux dans leur ensemble.

Théorème 44 (chinois) : Soit $a_1, \dots, a_n$ deux à deux premiers entre eux. Alors l'application

$\ell : A \to \hat{\prod}_{j=1} A/(a_j)$ est un morphisme d'anneaux
$x \mapsto (\pi_j(x))_{1 \le j \le n}$ surjectif de noyau $\ker(\ell) = (a)$

Ainsi ℓ induit un isomorphisme d'anneaux

$\bar{\ell} : A/(a) \to \hat{\prod}_{j=1} A/(a_j)$ d'inverse $\bar{\ell}^{-1} : \hat{\prod}_{j=1} A/(a_j) \to A/(a)$
$\pi(x) \mapsto (\pi_j(x))_{1 \le j \le n}$ $(\pi_j(x_j))_j \mapsto \pi\left(\hat{\sum}_{i=1} x_i m_i b_i\right)$

où les m_i sont tel que $\hat{\sum}_{j=1} m_j b_j = 1$

BER 90 **Application 45 :** On définit l'indicatrice d'Euler $\ell(n)$ comme étant le nombre d'entiers de $[\![1;n]\!]$ premiers avec n. Ainsi $|(\mathbb{Z}/n\mathbb{Z})^\times| = \ell(n)$.

Soit $n \geq 2$ et $n = p_1^{m_1} \times \dots \times p_n^{m_n}$ sa décomposition en facteurs premiers. Alors on a :

$$\ell(n) = \hat{\prod}_{i=1} p_i^{m_i - 1}(p_i - 1) = n \hat{\prod}_{i=1} \left(1 - \frac{1}{p_i}\right)$$

DEV 2

ROM 91 **Application 46 :** Le système de congruences

$$\begin{cases} h \equiv 2 \ [4] \\ h \equiv 3 \ [5] \\ h \equiv 1 \ [9] \end{cases}$$

admet pour solutions l'ensemble $S = \{838 + 180q \ ; \ q \in \mathbb{Z}\}$

2) En algèbre linéaire [MAN] [BER]

Soit K un corps et E un K-espace vectoriel de dimension finie $n \geq 1$. Soit $u \in \mathcal{L}(E)$.

MAN 43 **Lemme 47 (des noyaux) :** Soit $P_1, \dots, P_N$ une famille de polynômes deux à deux premiers entre eux. Alors : $\ker(P_1 P_2 \dots P_N)(u) = \bigoplus_{k=1}^{N} \ker(P_k(u))$. De plus, le projecteur de $\ker(P_1 P_2 \dots P_N)(u)$ sur l'un de ces SEV parallèlement à la somme des autres est dans $K[u]$.

BER 946 **Déf 48 :** L'annulateur de u, noté $\mathrm{Ann}(u)$, est l'ensemble $\mathrm{Ann}(u) = \{P \in K[X] \ ; \ P(u) = 0\}$

Prop 49 : $\mathrm{Ann}(u)$ est un idéal de $K[X]$, et est non nul. Ainsi il existe un unique polynôme unitaire $\mu_u \in K[X]$ qui engendre $\mathrm{Ann}(u)$.

Déf 50 : Le polynôme μ_u est appelé le polynôme minimal de u.

MAN 4 **Prop 51 :** $\dim(K[u]) = \deg(\mu_u)$.

MAN 90 **Théorème 52 :** Il y a équivalence entre :

1) u est diagonalisable
2) u admet un polynôme annulateur scindé à racines simples.
3) μ_u est scindé à racines simples.