Leçon 122 : Anneaux principaux : exemples et applications

I - Principalité

a - Idéaux

$(A,+,\times)$ un anneau commutatif

Def. 1 : Soit $I \subset A$. On dit que I est un idéal de A si :
- $(I,+)$ sous grp de $(A,+)$
- $\forall a \in A, \forall x \in I$ alors $ax \in I$

Exc. 2 : $\{0\}$, A, Si φ morphisme : $\ker(\varphi)$

Prop. 3 : Si I, S sont 2 idéaux de A, $I \cap S$ est un idéal de A

Def. 4 : On appelle idéal de A engendré par $P \subset A$ l'idéal $(P) := \bigcap_{\substack{I \text{ idéal} \\ P \subset I}} I$

[GRAS p.148 - 152]

Rmq 5 : Soit $a \in A$, $(a) = \{ax \mid x \in A\}$

Def. 6 : On dit que I est idéal principal si il est engendré par un élément de A.

Exc. 7 : $\forall n \in \mathbb{N}$ les $n\mathbb{Z}$ sont des idéaux principaux de $\mathbb{Z}$

Def. 8 : On dit que I est un idéal premier de A si :
- $I \neq A$
- $\forall x, y \in A$ tq $xy \in I$ alors $x \in I$ ou $y \in I$

Def. 9 : On dit que I est un idéal maximal de A si
- $I \neq A$
- Si J idéal de A tq $I \subset J \subset A$ alors $J = A$ ou $J = I$

Exc. 10 : Les $p\mathbb{Z}$ (p premiers) sont des idéaux maximaux et premier de $\mathbb{Z}$.

Exc. 11 : $I = \{0\} \times \mathbb{Z}$ idéal premier de $\mathbb{Z} \times \mathbb{Z}$ mais pas maximal car $I \subset 2\mathbb{Z} \times \mathbb{Z} \subset \mathbb{Z}$

[CHAU p.45]

Thm. 12 : I idéal de A on a :
- I premier ssi A/I intègre
- I max. ssi A/I corps

[GRAS p.158 - 159]

Cor. 13 : I maximal alors I premier.

b - Anneaux principaux

Def. 14 : On dit que A est principal si A intègre et tous ses idéaux sont principaux

[ULM p.42]

Prop. 15 : Si A est principale alors les idéaux maximaux sont premiers.

Exc. 16 : $\mathbb{Z}$ est principal, $\mathbb{R}[X]$ est principal, $\mathbb{Z}[i]$ est principal

II - Divisibilité dans les anneaux

a - Divisibilité

Def. 17 : $a, b \in A$ on dit que a divise b (noté $a|b$) si $(a) \subset (b)$

Def. 18 : $a, b \in A$ on dit que a et b sont associées si $(a) = (b)$

Rmq. 19 : Si A est intègre, dire que a et b sont associée c'est dire que $\exists u \in A^\times$ tq $a = ub$.

Def. 20 : $a, b \in A$ on dit que a, b sont premiers entre eux si $\forall d \in A$ tq $d|a$ et $d|b$ alors $d \in A^\times$.

Def. 21 : $a, b \in A$ on dit que d est le pgcd de a et b si :
- $d|a$ et $d|b$
- $\forall c \in A$, $c|a$ et $c|b$ on a $c|d$

On dit que m est le ppcm de a et b si
- $a|m$ et $b|m$
- $\forall c \in A$, $a|c$ et $b|c$ on a $m|c$

[BERS p.513 - 523]

Rmq. 22 : Dans le cas de plus général d'un anneau rien n'assure l'existence d'un pgcd ou d'un ppcm

Rmq 23 : lorsque le pgcd ou le ppcm existe ils sont unique à association près.

Rmq 24 : a et b premiers entre eux ssi $\text{pgcd}(a,b) = 1$

Def. 25 : $\pi \in A$ est dit irréductible si $\pi \neq 0$, $\pi \notin A^\times$ et $\forall a, b \in A$ si $\pi = ab$ alors $a \in A^\times$ ou $b \in A^\times$

Rmq. 26 : Si a, b sont associés si a irr. alors b aussi.

Def. 27 : $\pi \in A$ est dit premier si $\pi \neq 0$, $\pi \notin A^\times$ et $\forall a, b \in A$ $\pi | ab \Rightarrow \pi | a$ ou $\pi | b$

Rmq. 28 : a, b associés a est premier ssi b est premier ($(a) = (b)$)

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

b - Anneaux factoriels

Def. 30 : On appelle système complet de représentant irr. (scri) $P \subset A$ tq tout éléments de P est irr. et tout élément irr. de A est associé à un elt de P.

[CBERS p.528]

Def. 31 : P scri, on dit que A est factoriel si il est intègre et $\forall a \in A$ $\exists ! u \in A^\times$ et $\exists ! (n_\pi)_{\pi \in P}$ tous nuls sauf un nb fini tq $a = u \prod_{\pi \in P} \pi^{n_\pi}$
n_π est appelé valuation π-adique de a noté $v_\pi(a)$.

[CBERS p.542 - 545]

Lemme 32 : (Euclide) A factoriel. pour tout π irr. et $\forall a, b \in A$, si $\pi | ab$ alors $\pi | a$ ou $\pi | b$

Lemme 33 : (Gauss) A factoriel $a, b, c \in A$ tq $a|bc$ et a, b premiers entre eux alors $a|c$

Rmq. 34 : P scri, A factoriel, $a, b \in A$. $a|b$ ssi $\forall p \in P$ $v_p(a) \leq v_p(b)$

Prop. 35 : A fact, $a, b \in A$. $\text{pgcd}(a,b)$ et $\text{ppcm}(a,b)$ existent et $\text{pgcd}(a,b) = \prod_{\pi \in P} \pi^{\min(v_\pi(a), v_\pi(b))}$ et

[BER] p.545 -547

$\text{ppcm}(a,b) = \prod_{\pi \in P} \pi^{\max(v_\pi(a), v_\pi(b))}$

Prop. 36: A intègre. A factoriel ssi $\begin{cases} \forall a \in A\setminus\{0\},\ a = u\pi_1 \cdots \pi_r,\ u \in A^\times, (\pi_i)_i^r \text{ irr.} \\ \text{tout élément irr. est premier} \end{cases}$

c- Arithmétique dans les anneaux principaux

[BER] p.547

Thm 37: Tout anneau principal est factoriel.

Rmq 38: Ainsi toutes les prop. définissant sur un anneau factoriel sont valables. En particulier les lemmes de Gauss et Euclide, l'existence de pgcd et ppcm.

[BER] p.548 -525

Prop. 39: A principal. $a,b,d,m \in A$ tq $(a)+(b)=(d)$ et $(a)\cap(b)=(m)$. d et m sont alors un pgcd de a,b et un ppcm de a,b.

Thm 40: (Bezout) A principal. $a,b \in A$ premiers entre eux ssi $\exists u,v \in A$ tq $ua+vb=1$.

Prop. 41: A principal. Tout élément irréductible engendre un idéal maximal. Et tout élément irréductible est premier.

Prop. 42: A principal. Tout idéal premier non nul est maximal.

[MAU] p.89

Ex. 43: Dans $\mathbb{Z}[X]$, $J = (2, X)$ n'est pas principal

d- Exemple d'anneau principal : anneau Euclidien

[BER] p.529 -530

Def. 44: Un anneau euclidien est un couple (A,δ), A anneau intègre et $\delta : A\setminus\{0\} \to \mathbb{N}$ tq $\forall a \in A, \forall b \in A\setminus\{0\}$ $\exists q,r$ tq :

$a = qb + r$ tq $r = 0$ ou $\delta(r) < \delta(b)$

Ex. 45: $\mathbb{Z}$ est euclidien pour la valeur absolue. $K[X]$ est euclidien pour le degré des polynômes. K est euclidien.

Prop. 46: Tout anneau euclidien est principal.

[BER] p.53

C-ex. 47: $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais pas euclidien.

Ex. 48: $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$

[BER] p.530 -533

Prop. 50: (relation de Bezout) A eucl., $a,b \in A$. Si $d = \text{pgcd}(a,b)$ alors $\exists u,v \in A$ tq $ua + bv = d$.

Rmq 51: L'avantage d'un anneau euclidien est l'existence d'un algorithme pour trouver les coefs de Bezout.

III. Applications

a) Algèbre linéaire

E ev. de dim. fini, $u \in \mathcal{L}(E)$

[BERS] p.667

Prop. 52: A corps ssi $A[X]$ euclidien ssi $A[X]$ principal

Rmq. 53: $K[X]$ est euclidien donc on a les notions de pgcd, ppcm et Bezout.

[CROU] p.533 -536

Prop. 54: $\mathbb{K}[u] = \{P(u) \mid u \in \mathbb{K}[X]\}$ est une algèbre commutative

Def/prop 55: On appelle idéal annulateur de u l'idéal $I_u = \{P \in \mathbb{K}[X] \mid P(u) = 0\}$. On appelle polynôme minimal de u le générateur unitaire de cet idéal. (Noté π_u)

Thm 56: $\dim(\mathbb{K}[u]) = \deg(\pi_u)$. Une base de $\mathbb{K}[u]$ est $(u^k)_{1 \le k \le \deg(\pi_u)}$

Thm 57: $\mathbb{K}[u]$ corps $\iff$ $\mathbb{K}[u]$ intègre $\iff$ π_u irréductible.

Lemme 58: $p \ge 2$, $P_1, \dots, P_p \in K[X]$, $i \in \{1, \dots, p\}$ passons $Q_k = \prod_{\substack{j=1 \\ j \ne k}}^{p} P_j$. Si les P_k sont premiers entre eux 2 à 2 alors les Q_k sont premiers dans leur ensemble, de plus P_k et Q_k sont premier entre eux.

DEV1

[CROU] p.595 -600

Thm 59: (Lemme des noyaux) $p \ge 2$, $P_1, \dots, P_p \in K(X)$ 1 à 1 entre eux 2 à 2. Posons $P = \prod_{k=1}^{p} P_k$. Alors $\ker(P(u)) = \bigoplus_{k=1}^{p} \ker(P_k(u))$

De plus les projecteurs $\pi_k : \ker(P(u)) \to \ker(P_k(u))$ sont dans $K[u]$

Thm 60: ASSE :

(i) u est diagonalisable

(ii) Il existe un pol annulateur de u scindé à racines simple

(iii) π_u est scindé à racines simples.

b) Anneau des entiers de Gauss

Notons $\Sigma := \{n \in \mathbb{N} \mid n = a^2+b^2, (a,b) \in \mathbb{N}^2\}$

Ex. 61: $0, 1, 2, 4, 5, 8 \in \Sigma$

Def. 62: $\mathbb{Z}[i] := \{a+ib \mid a,b \in \mathbb{Z}\}$ est un anneau intègre.

$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$

$a+ib \longmapsto a^2+b^2 = (a+ib)(a-ib)$

Prop. 63: $\forall z,z' \in \mathbb{Z}[i]$ $N(zz') = N(z)N(z')$

Prop. 64: $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $z \in \mathbb{Z}[i]^\times$ ssi $N(z) = 1$

[PER] p. 36 - 38

Prop. 65: Σ est stable par multiplication

Prop. 66: $(\mathbb{Z}[i], N)$ est euclidien.

Lemme 67: -1 est un carré dans $\mathbb{F}_p$ ssi $p = 2$ ou $p = 1 [4]$

Lemme 68: p premier, $p \in \Sigma$ ssi p n'est pas irréductible dans $\mathbb{Z}[i]$

DEV 2

[PER] p. 57-58

Thm 69: p premier, $p \in \Sigma$ ssi $p = 2$ ou $p = 1 [4]$

Thm 70: $n \in \mathbb{N}^* \setminus \{1\}$ $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$. $n \in \Sigma$ ssi $v_p(n)$ pair pour $p = 3 [4]$.

Thm 71: Les irr. de $\mathbb{Z}[i]$ sont (à l'inversible près) les p premiers tq $p = 3 [4]$ et les $a+ib$ tq a^2+b^2 est premier.

c) Théorème chinois

A anneau commutatif

Def. 72: I_1, I_2 idéaux de A. On dit que I_1 et I_2 sont étrangers ssi $I_1 + I_2 = A$ (ie $\exists (a_1, a_2) \in I_1 \times I_2$ tq $a_1 + a_2 = 1$)

Prop. 73: $I_1, \dots, I_n$ idéaux de A étrangers 2à 2 ($I_i + I_j = A$). Alors $I_1 \cdots I_n = \bigcap_{i=1}^n I_i$

Thm 74: (Théorème chinois) $I_1, \dots, I_n$ idéaux de A étrangers 2à 2.

$$A \longrightarrow A/I_1 \times \cdots \times A/I_n$$
$$a \longmapsto (a+I_1, \dots, a+I_n)$$

est un morphisme surjectif de noyau $I := I_1 \cdots I_n = \cap I_i$.

En particulier, $A/I \simeq A/I_1 \times \cdots \times A/I_n$

[ULM] p. 53 - 58

Rmq 75: Dans A principal les idéaux I_j sont de la forme (m_j). (m_i) et (m_j) étrangers ssi $(m_i) + (m_j) = A$ ssi m_i et m_j premiers entre eux. De plus $\cap(m_i) = \text{ppcm}(m_j)$

Cor. 76: A principal, $n \geq 1$ $m_1, \dots, m_n$ 1^{2} entre eux 2à 2.

$$A/(m_1 \cdots m_n) \simeq A/(m_1) \times \cdots \times A/(m_n)$$

Ex. 77:
$$\begin{cases} u = 1 [3] \\ u = 3 [5] \\ u = 0 [7] \end{cases}$$

Références :

- [GRA] : G. Grau & U-N. Grau : Algèbre et arithmétique fondamentales
- [HAU] : B. Haudecoeur : Les contres exemples en mathématiques.
- [ULM] : F. Ulmer : Anneaux, corps, résultants
- [BER] : G. Berhuy : Algèbre le grand combat.
- [ROM] : J-E. Rombaldi : Mathématiques pour l'agrégation
- [PER] : D. Perrin : Cours d'algèbre