Leçon 122 : Anneaux principaux. Exemples et applications

Références : Ulmer (Algèbre), Perrin, Rombaldi, Francinou (les oraux agreg) Combes, Berhuy

I - Notion de principalité

1) Idéaux

2) Anneaux euclidiens

II - Arithmétique dans les anneaux principaux

1) Divisibilité

2) PGCD et PPCM

3) Anneaux factoriels

III - Applications

1) Algèbre linéaire

2) Anneau des entiers de Gauss $\mathbb{Z}[i]$

3) Théorème et isomorphisme chinois

DEV 1 : $\mathbb{C}[X,Y]/(XY-1)$ est principal

DEV 2 : Théorème chinois et application à l'éco des pirates.

Leçon 122 : Anneaux principaux. Exemples et applications

Dans toute la leçon, on considère $(A,+,\cdot)$ un anneau commutatif unitaire.

I - Notion de principalité

[ULM] 1) Idéaux, idéaux premiers, idéaux maximaux

DEF 1 : On dit que A est intègre lorsque $A \neq \{0\}$ et 0 est le seul diviseur de 0, c'est-à-dire : $\forall a,b \in A^2$, $ab=0 \Rightarrow a=0$ ou $b=0$.

DEF 2 : Soit $I \subset A$. On dit que I est un idéal de A lorsque
- $(I,+)$ est un sous-groupe de $(A,+)$
- $\forall a \in I, \forall b \in A, ab \in I$

EX 3 : Si $A \neq \{0\}$, A possède toujours deux idéaux : $\{0\}$ et A. Si $\varphi : A \to B$ est un morphisme d'anneaux, $\ker(\varphi)$ est un idéal de A. Les seuls idéaux d'un corps K sont $\{0\}$ et K.

EX 4 : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

PROP 5 : Soit J un idéal de A et $\pi : A \to A/J$ le morphisme canonique. L'application $\Psi : \{\text{Idéaux de } A \text{ contenant } J\} \to \{\text{Idéaux de } A/J\}$, $I \mapsto \pi(I)$ est une bijection.

DEF 6 : Un idéal I de A est dit propre si $I \neq A$, maximal s'il est propre et si pour tout idéal J : $I \subset J \subset A \Rightarrow J = I$ ou $J = A$.

PROP 7 : I est un idéal maximal de $A \Leftrightarrow A/I$ est un corps.

DEF 8 : Un idéal I de A est dit premier lorsqu'il est propre et pour tous $a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.

PROP 9 : I est un idéal premier $\Leftrightarrow A/I$ est intègre

COR 10 : Un idéal maximal est premier

DEF 11 : Un idéal $I \subset A$ est dit principal lorsqu'il existe $a \in I$ tel que $I = aA = \{ax \mid x \in A\}$.

DEF 12 : Un anneau A est dit principal s'il est intègre et si tous ses idéaux sont principaux.

EX 13 : $\mathbb{Z}$ est principal. Si K est un corps, $K[X]$ l'est aussi, car il est dans une classe particulière :

2) Anneaux euclidiens [ULM, PER]

DEF 14 : Un anneau A est dit euclidien, lorsqu'il est intègre et qu'il une fonction $\delta : A \setminus \{0\} \to \mathbb{N}$ telle que :
$\forall (a,b) \in A \times A \setminus \{0\}$, $\exists (q,r) \in A \times A$ tels que $\begin{cases} a = bq + r \\ \delta(r) < \delta(b) \text{ ou } r = 0 \end{cases}$
q est le quotient, r est le reste de la division, δ est appelé stathme euclidien pour A.

REM 15 : On peut alors diviser tout élément par un autre élément non nul sans demander d'hypothèse supplémentaire comme dans $\mathbb{Z}[X]$ par exemple.

EX 16 : • $\mathbb{Z}$ est euclidien pour le stathme $\delta(a) = |a|$.
• $K[X]$ est euclidien pour le stathme $\delta(P) = \deg(P)$.

PROP 17 : Un anneau euclidien est principal

REM 17 : La réciproque est fausse : $\mathbb{Z}\left[\frac{1}{2}(1+i\sqrt{19})\right]$ est principal non euclidien.

PROP 18 : $A[X]$ est principal si et seulement si A est un corps. [ROT]

REM 19 : Si A n'est pas un corps, on peut tout de même effectuer la division euclidienne de $P \in A[X]$ par $Q \in A[X] \setminus \{0\}$ à condition que $\text{dom}(Q) \in A^*$.

PROP 20 : $\mathbb{C}[X,Y]/(XY-1)$ est un anneau principal [TPA]

II - Arithmétique dans les anneaux principaux

1) Divisibilité On suppose A intègre [PER]

DEF 21 : Soient $a,b \in A$. On dit que a divise b et on note $a \mid b$ lorsqu'il existe $c \in A$ tel que $b = ac$

PROP 22 : Soient $a,b \in A$. $b \mid a \Leftrightarrow (a) \subset (b)$.

DEF 23 : Soient $a,b \in A$. On dit que a et b sont associés lorsque $(a) = (b)$ ou de manière équivalente lorsque $\exists u \in A^*$, $a = bu$. On notera $a \sim b$.

REM 24 : La relation d'association est une relation d'équivalence. Les éléments associés jouent des rôles identiques pour la divisibilité.

DEF 25 : Soit $p \in A$, $p \neq 0$, $p \notin A^*$. On dit que :
• p est premier lorsque : $\forall a,b \in A$, $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$
• p est irréductible lorsque : $\forall a,b \in A$, $p = ab \Rightarrow a \in A^*$ ou $b \in A^*$

REM 26 : p premier $\Leftrightarrow (p)$ premier

PROP 27 : Si p est premier, alors p est irréductible.

PROP 28 : On suppose A principal et $p \in A \setminus (A^* \cup \{0\})$ [ROT ou ULM]
p est irréductible $\Leftrightarrow$ p est premier et :
(p) premier $\Leftrightarrow$ p premier $\Leftrightarrow$ p irréductible $\Leftrightarrow$ (p) maximal

EX 29 : Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés. Les irréductibles de $K[X]$ sont les polynômes irréductibles.

DEF 30: Soient $a, b \in A$. On dit que a et b sont premiers entre eux (ou étrangers) lorsque leurs seuls diviseurs communs sont les inversibles : $\forall d \in A,\ d|a$ et $d|b \Rightarrow d \in A^\times$.

PROP 31: (A principal) a et b sont étrangers si et seulement si a) et (b) sont comaximaux i.e $(a)+(b)=A$.

2) PGCD et PPCM [CAM]

PROP 32: On suppose A principal, $a, b \in A$ non nuls
(i) Un générateur m de l'idéal $(a) \cap (b)$ est un plus petit multiple de a et b (au sens de la divisibilité)
(ii) Un générateur d de l'idéal $aA+bA$ est un plus grand diviseur de a et b (au sens de la divisibilité)

REM 33: Les PGCD et PPCM de a et b sont uniques à association près.

REM 34: On peut définir de la même manière $\mathrm{PGCD}(a_1, \dots, a_k)$ $(k \geq 2)$ et $\mathrm{PPCM}(a_1, \dots, a_k)$ à association près.

REM 35: Deux éléments a et b sont premiers entre eux si et seulement si $\mathrm{PGCD}(a,b) \sim 1$.

COR 36: Soient $a_1, \dots, a_k$ des éléments de A principal. Un diviseur commun d de $a_1, \dots, a_k$ est PGCD de $a_1, \dots, a_k$ si et seulement s'il existe $u_1, \dots, u_k \in A$ tels que :
$$d = a_1 u_1 + \dots + a_k u_k \quad \text{(Relation de Bezout)}$$

COR 37: (Théorème de Bezout) : Des éléments $a_1, \dots, a_k$ de A principal sont premiers entre eux dans leur ensemble si et seulement si : $\exists u_1, \dots, u_k \in A$ tels que $1 = a_1 u_1 + \dots + a_k u_k$.

REM 38: L'avantage supplémentaire des anneaux euclidiens repose sur l'existence de l'algorithme d'Euclide pour calculer un PGCD et des coefficients de Bezout.

THM 39: (Gauss) Soient a, b, c dans A principal. Si $a|bc$ et a est premier avec b, alors $a|c$.

COR 40: Soient a, b, c dans A principal. Si $\mathrm{PGCD}(a,b) \sim 1$ et $\mathrm{PGCD}(a,c) \sim 1$, alors $\mathrm{PGCD}(a, bc) \sim 1$.

3) Anneaux factoriels [PER] [ULM]

On veut se placer dans un cadre plus général que les anneaux principaux tout en conservant une propriété semblable à $\mathbb{Z}$: la décomposition en produit d'irréductibles.

DEF 41: On dit que A est factoriel lorsque A est intègre et
E) $\forall a \in A,\ a \neq 0,\ \exists u \in A^\times,\ \exists p_1, \dots, p_r$ irréductibles tels que $a = u p_1 \cdots p_r$.
U) Cette décomposition est unique à permutation et association près : si $a = u p_1 \cdots p_r = v q_1 \cdots q_s$, on a $r = s$ et $\exists \sigma \in \mathfrak{S}_r$ tel que $p_i \sim q_{\sigma(i)}$.

REM 42: On peut reformuler cette définition en introduisant un système $\mathcal{P}$ de représentants des irréductibles :
$a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$, $u \in A^\times$, $v_p(a)$ nuls sauf un nombre fini, et cette écriture est unique.

REM 43: Avec ces notations, $a, b \neq 0$: $a|b \Leftrightarrow \forall p \in \mathcal{P},\ v_p(a) \leq v_p(b)$

EX 44: $\mathbb{Z}$ est factoriel, $K[X]$ aussi, $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

PROP 45: Soit A vérifiant (E). LASSE :
(i) A vérifie (U)
(ii) Lemme d'Euclide : Si p est irréductible et $p|ab$, alors $p|a$ ou $p|b$.
(iii) p irréductible $\Leftrightarrow$ (p) premier
(iv) Théorème de Gauss : Si $a|bc$ et a est premier avec b, alors a divise c.

DEF 46: On peut étendre la notion de PGCD et de PPCM à A factoriel, toujours à association près :
$$\mathrm{PGCD}(a,b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))} \qquad \mathrm{PPCM}(a,b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$$

PROP 47: Tout anneau principal est factoriel.

THM 48: (Transfert) Si A est factoriel, alors $A[X]$ l'est également.

EX 49: Ainsi, $\mathbb{Z}[X]$ est factoriel non principal. De même pour $A[X_1, \dots, X_n]$, $n \geq 2$.

III - Applications

1) Algèbre linéaire [ROM]

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.

DEF 50: Soit $u \in \mathcal{L}(E)$. L'application $\Phi : \mathbb{K}[X] \to \mathcal{L}(E)$
$P = \sum_{k=0}^{n} a_k X^k \mapsto P(u) = \sum_{k=0}^{n} a_k u^k$
avec $\forall k \in [\![0,n]\!],\ u^k = u \circ u \circ \cdots \circ u$ (k fois), est un morphisme d'algèbres d'image $\mathbb{K}[u]$. $\mathbb{K}[u]$ est une sous-algèbre commutative de $\mathcal{L}(E)$.

REM 51 : Comme E est de dimension finie, on a ψ non injectif donc $\ker(\psi) \neq \{0\}$.

DEF 52 : Comme $K[X]$ est principal, $\ker(\psi)$ est principal engendré par un polynôme unitaire et irréductible sur K. On le note π_u et on l'appelle polynôme minimal de u.

THM 53 : L'espace vectoriel $K[u]$ est de dimension $\deg(\pi_u)$. Une base est $(u^k)_{k \in [\![0, \deg(\pi_u)-1]\!]}$.

THM 54 : (Lemme des noyaux) Soit $(P_j)_{j \in [\![1;p]\!]}$ une famille de $p \geq 2$ polynômes deux à deux premiers entre eux dans $K[X]$, $\neq \{0\}$ et $P = \prod_{k=1}^{p} P_k$. On a alors

$$\ker(P(u)) = \bigoplus_{k=1} \ker(P_k(u))$$

THM 55 : Les assertions suivantes sont équivalentes
(i) u est diagonalisable
(ii) Il existe un polynôme annulateur de u qui est scindé à racines simples.
(iii) Le polynôme minimal est scindé à racines simples.

2) Anneau des entiers de Gauss $\mathbb{Z}[i]$ [PER]

On s'intéresse à la détermination des entiers $n \in \mathbb{N}$ qui sont somme de deux carrés : $n = a^2+b^2$, $a, b \in \mathbb{N}$.
On pose $\Sigma = \{ n \in \mathbb{N} / n = a^2+b^2 / a, b \in \mathbb{N} \}$

EX 56 : $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$
$3, 6, 7, 11, 12 \notin \Sigma$.

REM 57 : Si $n \equiv 3 \bmod 4$, alors $n \notin \Sigma$.

DEF 58 : On définit l'anneau $\mathbb{Z}[i]$ des entiers de Gauss : $\mathbb{Z}[i] = \{a+ib \mid (a,b) \in \mathbb{Z}^2\}$.

PROP 59 : $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ donc intègre. On a aussi que l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, $a+ib \mapsto a^2+b^2$ est multiplicative.

COR 60 : Les inversibles de $\mathbb{Z}[i]$ sont $\{-1; 1; -i; i\}$

PROP 61 : Σ est stable par multiplication.

PROP 62 : $\mathbb{Z}[i]$ est euclidien de stathme N. Il est donc principal.

LEMME 63 : $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$

THM 64 : Soit $p \in \mathbb{N}$ un nombre premier.
$p \in \Sigma \iff p = 2$ ou $p \equiv 1 \bmod 4$.

THM 65 : Soit $n \in \mathbb{N}$, $n \geq 1$, $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$
Alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3 \bmod 4$.

THM 66 : Les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près :
a) les entiers $p \in \mathbb{N}$ avec $p \equiv 3 \bmod 4$
b) les $a+ib$ tels que a^2+b^2 soit premier.

3) Théorème d'isomorphisme chinois [ULM]

PROP 67 : Soient $I_1, \dots, I_n$ des idéaux deux à deux comaximaux. Alors $\forall i \in [\![1;n]\!]$, I_i est comaximal avec $\prod_{j \neq i} I_j$.

THM 68 (chinois dans les anneaux principaux) :
Soit A un anneau principal et $m_1, \dots, m_n$ dans A des éléments de A deux à deux étrangers. Alors

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

↳ isomorphisme d'anneaux

[BERHUY]

APPLICATION 69 : Sur un bateau, il y a 17 pirates et un cuisinier. Les pirates ont volé un coffre de pièces d'or, dont ils décident de partager les pièces équitablement. Au terme de ce partage, il reste 3 pièces, qu'ils projettent de donner au cuisinier. Mais le bateau essuie alors une tempête au cours de laquelle six pirates sont noyés. Les pirates survivants recommencent le partage, au terme duquel il doit rester 4 pièces pour le cuisinier. Une effroyable dispute éclate alors entre les pirates et 5 pirates y perdent la vie. Les pirates restants recommencent encore le partage qui doit alors laisser 5 pièces au cuisinier. Lassé d'attendre, celui-ci décide d'empoisonner le reste des pirates et de garder le coffre pour lui. Combien de pièces peut-il espérer au minimum. Réponse : 485