Leçon 122 : Anneaux principaux. Exemples et applications.

Dans cette leçon, sauf mention contraire $(A, +, \cdot)$ désigne un anneau commutatif unitaire.

1 Généralités

1.1 Rappels sur les idéaux

Définition 1. — Un idéal de A est un sous groupe I de $(A, +)$ tel que pour tout $(a, b) \in A \times I, ab \in I$.

— Un idéal I de A est dit premier lorsqu'il est distinct de A et si $ab \in I$ alors $a \in I$ ou $b \in I$.

— Un idéal I de A est dit maximal lorsqu'il est distinct de A et que A et lui même sont les seuls idéaux qui le contiennent.

Théorème 2. — *Un idéal I est maximal si et seulement si l'anneau quotient A/I est un corps.*

— *Un idéal I est premier si et seulement si l'anneau quotient A/I est intègre.*

— *Un idéal maximal est premier.*

Exemple 3. L'idéal nul $\{0\}$ de $\mathbb{Z}$ est premier non maximal.

Définition 4. Un idéal engendré par un seul élément est dit principal on notera pour $a \in A$ comme (a).

Exemple 5. Pour $n \in \mathbb{N}$ l'ensemble des $n\mathbb{Z}$ sont des idéaux de $(\mathbb{Z}, +, \times)$.

Définition 6. Un anneau A est dit principal lorsqu'il est intègre et que tout idéal est principal.

Exemple 7. Un corps est principal.

Définition 8. Un élément $a \in A$ est dit irréductible lorsqu'il n'est pas inversible ni nul et si $a = bc$ alors $b \in A^\times$ ou $c \in A^\times$.

1.2 Anneaux euclidiens

Définition 9. Un anneau A est dit euclidien lorsqu'il est intègre et si il existe une fonction $\nu : A\backslash\{0\} \to \mathbb{N}$ vérifiant que pour tout $a \in A$ et tout $b \in A\backslash\{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$. On dit que q est le quotient et r le reste de la division euclidienne, ν est appelée stathme euclidien pour A.

Exemple 10. L'anneau $\mathbb{Z}$ est euclidien pour le stathme $\nu : k \in \mathbb{Z} \mapsto |k| \in \mathbb{N}$.

Proposition 11. *Tout anneau euclidien est principal.*

Remarque 12. La réciproque est fausse, par exemple l'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$.

Théorème 13. *Si $\mathbb{K}$ est un corps alors le degré est un stathme euclidien pour $\mathbb{K}[X]$.*

Théorème 14. *Les propositions suivantes sont équivalentes :*

— *A est un corps,*

— *$A[X]$ est euclidien,*

— *$A[X]$ est principal.*

Exemple 15. $\mathbb{Z}[X]$ n'est pas un anneau principal.

Corollaire 16. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$, alors $\mathbb{K}[X]/(P)$ est un corps si et seulement si P est irréductible dans $\mathbb{K}[X]$.*

2 Arithmétique des anneaux principaux

2.1 Divisibilité, pgcd, ppcm

Définition 17. Soient $a, b \in A$.

1. On dit que a divise b noté $a|b$ lorsqu'il existe $c \in A$ tel que $b = ac$. C'est équivalent à dire $(b) \subset (a)$.

2. On dit que a et b sont associés noté $a \sim b$ lorsque $a|b$ et $b|a$. c'est équivalent à dire $(a) = (b)$.

Proposition 18. *Dans un anneau intègre, $\sim$ est une relation d'équivalence. Pour tout $a, b \in A$ on a $a \sim b$ si et seulement si il existe $u \in A^\times$ tel que $a = bu$.*

Définition 19. Soient $a_1, \ldots, a_m \in A\backslash\{0\}$.

1. L'élément $p \in A$ est appelé un Plus Petit Multiple Commun (PPCM) de $a_1, \ldots, a_m$ lorsque pour tout $i \in [\![1, m]\!]$ on a $a_i|p$ et pour tout autre élément $q \in A$ vérifiant cette propriété on a $p|q$.
2. L'élément $d \in A$ est appelé un Plus Grand Diviseur Commun (PGCD) de $a_1, \ldots, a_m$ lorsque pour tout $i \in [\![1, m]\!]$ on a $d|a_i$ et pour tout autre élément $q \in A$ vérifiant cette propriété on a $q|d$.

Remarque 20. Ces éléments n'existent pas obligatoirement dans tous les anneaux.

Proposition 21. *Soient $a, b \in A\backslash\{0\}$, $c \in A$ est un PPCM de a et b si et seulement si $(a) \cap (b) = (c)$.*

Proposition 22. *Dans un anneau principal, tout idéal premier non nul est maximal.*

Définition 23. Deux éléments non nuls $a, b \in A$ sont dits premiers entre eux si et seulement si tout diviseur commun est inversible. C'est équivalent à dire que $\text{pgcd}(a, b) \sim 1$.

Lemme 24. *(Euclide) Soit A principal, $a, b \in A$ premiers entre eux et $c \in A$, si $a|bc$ alors $a|c$.*

Lemme 25. *(Gauss) Soit A principal, $a, b \in A$ premiers entre eux et $c \in A$, si $a|c$ et $b|c$ alors $ab|c$.*

2.2 Anneaux factoriels

Définition 26. Un anneau A est dit factoriel lorsqu'il est intègre et si pour tout élément $a \in A$ non inversible et non nul il existe une décomposition $a = q_1 q_2 \ldots q_r$ avec les q_i irréductibles qui est unique a permutation près et à multiplication par in inversible près.

Théorème 27. *Soit A un anneau intègre, les propositions suivantes sont équivalentes :*

— *A est factoriel,*

— *Tout élément non nul non inversible possède une décomposition en produit d'irréductibles et tout élément irréductible est premier,*

— *Tout élément non nul, non inversible de A est produit d'éléments premiers.*

Proposition 28. *Si A est factoriel alors $A[X]$ est factoriel.*

Définition 29. Dans un anneau factoriel tout élément $a \in A$ possède une unique décomposition $a = u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u_a \in A^\times$, $\mathcal{P}$ un système de représentants des éléments premiers et $v_p(a)$ des entiers presque tous nuls.

Proposition 30. *Soit A factoriel et $a, b \in A$ non nuls alors un PGCD et un PPCM existent et on a :*

— *$a|b \iff v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathcal{P}$.*

— *$\prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et de b.*

— *$\prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et de b.*

Théorème 31. *Tout anneau principal est factoriel.*

2.3 Bézout et Théorème chinois

Proposition 32. *Pour A intègre, $a, b \in A\backslash\{0\}$ et $d \in A$, les propriétés suivantes sont équivalentes :*

— *$d|a$, $d|b$ et il existe $u, v \in A$ tels que $d = au + bv$,*

— *$d \sim pgcd(a, b)$ et il existe $u, v \in A$ tel que $d = au + bv$,*

— *$(a, b) = (a) + (b) = (d)$.*

Théorème 33. *(Bézout) Dans un anneau principal A, le PGCD et le PPCM d'éléments non nuls $a_1, \ldots, a_m$ existent. Un PGCD d de cette famille est générateur de $(a_1, \ldots, a_m)$. Un PPCM b de cette famille est générateur de $(a_1) \cap \cdots \cap (a_m)$. En particulier d peut s'écrire comme combinaison linéaire des a_i c'est à dire $d = a_1 b_1 + \cdots + a_m b_m$ avec $b_i \in A$.*

Remarque 34. Dans un anneau Euclidien, on dispose de l'algorithme d'Euclide pour retrouver les multiplicateurs de Bézout. Il est basé sur le principe que si $a, b \in A$ tels que $\nu(b) \leqslant \nu(a)$ alors avec la division euclidienne $a = bq + r$, on a $\text{pgcd}(a, b) \sim \text{pgcd}(b, r)$.

Dans la fin de cette partie on considère A est principal, $(a_1, \dots, a_r) \in A$ non nuls et non inversible et $a = \prod_{k=1}^{r} a_k$. Pour tout $j \in [\![1, r]\!]$ on pose π_j la surjection canonique de A sur $A/(a_j)$ et π celle sur $A/(a)$. Enfin on pose pour tout $j \in [\![1, r]\!]$ l'élément $b_j = a/a_j$.

Lemme 35. *Si pour tout $j \in [\![1, r]\!]$, les a_j sont deux à deux premiers entre eux alors les b_j sont premiers entre eux dans leur ensemble.*

Théorème 36. *(Chinois) Supposons que pour tout $j \in [\![1, r]\!]$, les a_j sont 2 à 2 premiers entre eux, alors l'application*

$$\varphi : x \in A \mapsto (\pi_j(x))_{1 \leqslant j \leqslant r} \in \prod_{j=1}^{r} A/(a_j)$$

est un morphisme d'anneau surjectif de noyau $\ker(\varphi) = (a)$ *et induit un isomorphisme d'anneau*

$$\overline{\varphi} : \pi(x) \in A/(a) \mapsto (\pi_j(x))_{1 \leqslant j \leqslant r} \in \prod_{j=1}^{r} A/(a_j)$$

dont l'inverse est

$$\overline{\varphi}^{-1} : (\pi_j(x_j))_{1 \leqslant j \leqslant r} \in \prod_{j=1}^{r} A/(a_j) \mapsto \overline{\sum_{i=1}^{r} x_i u_i b_i} \in A/(a)$$

où les $(u_j)_{1 \leqslant j \leqslant r}$ vérifient $\sum_{j=1}^{r} u_j b_j = 1$.

3 Applications

3.1 Équation diophantiennes

Définition 37. On appelle équation diophantienne dans $\mathbb{Z}$ une équation de la forme $ax \equiv b \mod (n)$ avec $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.

Théorème 38. *L'équation diophantienne $ax \equiv b \mod (n)$ admet des solutions entières si et seulement $\delta = pgcd(a, n)$ divise b. Dans ce cas, en notant $a = \delta a'$, $b = \delta b'$ et $n = \delta n'$, l'ensemble des solutions est alors $S = \{b' x'_0 + kn' \mid k \in \mathbb{Z}\}$ où x'_0 est une solution de $a'x \equiv 1 \mod (n')$.*

Corollaire 39. *Pour un système d'équations diophantiennes $k \equiv a_j \mod (n_j)$ pour $1 \leqslant j \leqslant r$.. Lorsque les $n_1, \dots, n_r$ sont deux à deux premiers entre eux, cela revient à trouver l'antécédent dans $\mathbb{Z}/n\mathbb{Z}$ de $(\pi_1(a_1), \dots, \pi_r(a_r))$ par l'isomorphisme ψ défini dans le théorème Chinois. Cet antécédent est $\overline{k_0}$ où $k_0 = \sum_{i=1}^{r} a_i u_i m_i$. Les autres solutions sont donc les $k = k_0 + qn$ avec $q \in \mathbb{Z}$.*

Exemple 40. Les solutions du système $\begin{cases} k \equiv 2 \mod (4) \\ k \equiv 3 \mod (5) \\ k \equiv 1 \mod (9) \end{cases}$ sont les $k = 118 + 180q$ avec $q \in \mathbb{Z}$.

3.2 L'anneau des entiers de Gauss $\mathbb{Z}[i]$

Définition 41. On appelle anneau des entiers de Gauss l'anneau $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$ muni de l'addition et multiplication usuelle.

Proposition 42. *L'anneau $\mathbb{Z}[i]$ est intègre et ses inversibles sont $\mathbb{Z}[i]^* = \{-1, 1, -i, i\}$.*

Proposition 43. *On pose $\Sigma = \{n \in \mathbb{N} | n = a^2 + b^2, a, b \in \mathbb{N}\}$. Cet ensemble est stable par multiplication*

Proposition 44. *L'anneau $\mathbb{Z}[i]$ est euclidien donc principal, pour le stathme $N : a + ib \mapsto a^2 + b^2$.*

Proposition 45. *On a $p \in \Sigma \iff p$ réductible dans $\mathbb{Z}[i] \iff p = 2$ ou $p \equiv 1[4]$.*

Applications 46. Il existe une infinité de nombre premier de la forme $4m + 1$.

Théorème 47. *Les irréductibles de $\mathbb{Z}[i]$ sont, à inversible près :*

1. *Les entiers premiers $p \in \mathbb{N}$ avec $p \equiv 3[4]$,*
2. *Les entiers de Gauss $a + ib$ tels que $a^2 + b^2 \in \mathcal{P}$.*

3.3 Algèbre linéaire

Définition 48. Soit $M \in \mathcal{M}_n(\mathbb{K})$, on appelle idéal annulateur de M l'idéal$I_M = \{P \in \mathbb{K}[X] | P(M) = 0\}$ de $\mathbb{K}[X]$ et $\pi_M \in \mathbb{K}[X]$ le polynôme minimal générateur unitaire de I_M.

Théorème 49. *(Lemme des noyaux) Soient $(P_j)_{1 \leqslant j \leqslant p}$ une famille de polynômes 2 à 2 premiers entre eux dans $\mathbb{K}[X]$ et $P = \prod_{k=1}^{p} P_k$. On a alors $\ker(P(M)) = \bigoplus_{k=1}^{p} \ker(P_k(M))$ et les projecteurs π_k : $\ker(P(M)) \to \ker(P_k(M))$ sont des éléments de $\mathbb{K}[M]$ pour $k \in \{1, \ldots, p\}$.*

Théorème 50. *(Cayley-Hamilton) Le polynôme caractéristique χ_M de M est annulateur de M.*

Théorème 51. *Une matrice $M \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement π_M est scindé à racine simple dans $\mathbb{K}$.*

Dev 1 : Théorème des 2 carrés 45 et 47
Dev 2 : Théorème des restes chinois 35, 36 et 40

Références

[PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

[ULM18] Félix ULMER : Anneaux, corps, résultants - Algèbre pour L3/M1/agrégation. Ellipses, 2018.

RAPPORT DU JURY :
Cette leçon ne doit pas se cantonner aux aspects théoriques. L'arithmétique des anneaux principaux doit être décrite et les démonstrations doivent être maîtrisées (lemme d'Euclide, théorème de Gauss, décomposition en irréductibles, PGCD et PPCM, équations de type ax+by=d, etc.). On doit présenter des exemples d'utilisation effective du lemme chinois. Les anneaux euclidiens représentent une classe importante d'anneaux principaux et l'algorithme d'Euclide a toute sa place dans cette leçon pour effectuer des calculs. Les applications en algèbre linéaire ne manquent pas et doivent être mentionnées (par exemple, le lemme des noyaux ou la notion de polynôme minimal pour un endomorphisme, pour un endomorphisme relativement à un vecteur ou pour un nombre algébrique). Si les anneaux classiques $\mathbb{Z}$ et $\mathbb{K}[X]$ doivent impérativement figurer, il est possible d'en évoquer d'autres (décimaux, entiers de Gauss $\mathbb{Z}[i]$ ou d'Eisenstein $\mathbb{Z}[e^{i\pi/3}]$) accompagnés d'une description de leurs inversibles, de leurs irréductibles, en lien avec la résolution de problèmes arithmétiques (équations diophantiennes).
Les candidates et candidats peuvent aller plus loin en s'intéressant à l'étude des réseaux, à des exemples d'anneaux non principaux, par exemple $\mathbb{Z}[X]$ ou $\mathbb{K}[X, Y]$. À ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. De même, la résolution des systèmes linéaires sur $\mathbb{Z}$ ou le calcul effectif des facteurs invariants de matrices à coefficients dans un anneau principal peuvent être présentés en lien avec ce sujet.