Leçon 122 : Anneaux principaux. Exemples et applications

Mathieu Alix

Mardi 29 Avril 2025

1 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 $\mathbb{Z}[e^{2i\pi/3}]$) 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. »

2 Questions classiques

1. Donner un exemple d'idéal non principal de $\mathbb{Z}[X]$.

   Solution: On vérifie immédiatement que $(2, X)$ convient.

2. (a) Le produit d'anneaux principaux est-il principal ?
   (b) Un sous-anneau non nul d'un anneau principal est-il principal ?

   Solution:
   (a) En général non, car le produit d'anneaux intègres (et même de corps) n'est pas nécessairement intègre. $((0, 1) \times (1, 0))$.
   (b) Non, $\mathbb{Z}[X]$ n'est pas principal mais $\mathbb{R}[X]$ l'est.

3. Que peut-on dire des idéaux dans un quotient d'un anneau principal ? Quand est-ce que cet anneau est-il principal ?

Solution: On commence par se rappeler que les idéaux d'un quotient sont en bijection avec les idéaux contenant l'idéal qui définit le quotient. Ils sont donc aussi principaux (engendré par l'image de la projection de l'élément engendrant). (on peut les décrire + précisément en terme de divisibilité). Pour la principalité de l'anneau quotient, il suffit de rajouter l'intégrité, et donc que l'idéal soit engendré par un premier.

4. Soit A un anneau commutatif unitaire. Montrer que si A n'est pas un corps, alors $A[X]$ n'est pas principal.

Solution: Supposons A intègre (dans le cas contraire, $A[X]$ ne l'est pas non plus et n'est donc pas principal). Soit $a \in A\backslash(A^\times \cup \{0\})$. Montrons que l'idéal $I = (a) + (X)$ n'est pas principal. En effet, supposons $I = (b)$ avec $b \in A[X]$. Alors, comme on a $\deg(ab) = \deg(a) + \deg(b)$, on a nécessairement $\deg(b) \leq \deg(a) = 0$, c'est-à-dire $b \in A$. De plus, il existe $c \in A[X]$ vérifiant $bc = X$. On a alors $\deg(c) = 1$, et donc il existe $d, e \in A$ tels que $dX + e = c$. Mais on a ainsi $bd = 1$. Cela implique $I = A[X]$, ce qui est absurde puisque son image par la projection $A[X] \twoheadrightarrow A$ est $(a) \neq A$.

5. $\mathbb{Z}/n\mathbb{Z}$ est-il principal ? Déterminer ses idéaux ? lesquels sont premiers ? maximaux ?

Solution: La principalité nécessite d'office l'intégrité, qui n'a lieu ssi $n \in \mathcal{P}$. Dans ce cas, $\mathbb{Z}/n\mathbb{Z}$ est un corps et n'a que deux idéaux qui sont lui même et $\{0\}$. pour les autres n non premiers, $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal, et ses idéaux sont de la forme $d\mathbb{Z}/n\mathbb{Z}$, ils sont donc principaux. pour le caractère premier, on utilise la bijection des ideaux quotients, ce qui nous assure que les $p\mathbb{Z}/n\mathbb{Z}$ pour $p|n$ premiers sont les idéaux premiers. Pour les maximaux, il faut regarder si le quotient formé est un corps ?

6. Donner une factorisation en irréductibles dans l'anneau $\mathbb{Z}[i]$ des éléments suivants :
   (a) 21
   (b) 13
   (c) $2 + 11i$

Solution:

(a) Dans $\mathbb{Z}$, l'entier 21 se factorise comme $21 = 3 \times 7$. Les deux nombres premiers 3 et 7 sont congrus à 3 modulos 4, ce qui implique qu'ils sont irréductibles dans $\mathbb{Z}[i]$. C'est donc la décomposition en irréductibles dans $\mathbb{Z}[i]$.

(b) Dans $\mathbb{Z}$, 13 est premier mais il congru à 1 mod 4, il n'est donc pas irréductible et se factorise dans $\mathbb{Z}[i]$ comme $(a + ib)(a - ib)$ où $13 = a^2 + b^2$. Or $13 = 2^2 + 3^2$. Les deux entiers de Gauss qui apataissent sont non associés et irréductibles (car de norme premier). Ainsi la décomposition en irréductible de 13 dans $\mathbb{Z}[i]$ est $(2 + 3i)(2 - 3i)$.

(c) La norme de $2+11i$ vaut $125 = 5^3$. L'entier 5 est congru à 1 mod 4 donc se décompose en deux éléments irréductibles de norme 5. Or $5 = 1^2 + 2^2$, donc $5 = (1+2i)(1-2i)$. Les associés de ces deux éléments sont les seuls éléments de norme 5 de $\mathbb{Z}[i]$. De plus, en considérant les coefficients de $2+11i$ dans la base $(1, i)$, on observe que 5 ne divise pas $2 + 11i$. Il suit que $2 + 11i$ est associé au cube de l'un des deux irréductibles ci-dessus. Or il reste à savoir lequel des deux irréductibles le divise, on vérifie que

$$\frac{2+11i}{1-2i} = \frac{(2+11i)(1+2i)}{5} = \frac{-20+15i}{5} = -4+3i$$

Ainsi $1-2i$ divise $2+11i$ dans $\mathbb{Z}[i]$. On calcule alors le cube $(1-2i)^3 = -11+2i$. Ainsi, la décomposition en irreductible est la suivant : $2+11i = -i(1-2i)^3$.

7. Montrer que l'ensemble $\mathbb{K}^{(\mathbb{N})}$ des suites à valeurs dans un corps $\mathbb{K}$ nulles à partir d'un certain rang est un idéal non principal de $\mathbb{K}^{\mathbb{N}}$

Solution: Le caractère d'idéal est laissé au lecteur. Supposons que cet idéal soit principal, *i.e.* supposons qu'il existe $\zeta \in \mathbb{K}^{\mathbb{N}}$ tel que $(\zeta) = \mathbb{K}^{(\mathbb{N})}$. Il existe donc un entier $N \geq 1$ tel que $\forall k \geq N, \zeta(k) = 0$. Soit $\xi \in \mathbb{K}^{(\mathbb{N})}$ avec $\xi(N) \neq 0$. Il existe alors par principalité $\theta \in \mathbb{K}^{\mathbb{N}}$ tel que $\xi = \theta\zeta$. Il suit que $\xi(N) = \theta(N)\zeta(N) = 0$ et ceci donne une contradiction.

8. Soit $f \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$. Montrer que $P(f)$ est inversible dans $\mathbb{K}[f]$ si, et seulement si, P est premier avec π_f (pol min.).

Solution: Soit $P \in \mathbb{K}[X]$. L'endomorphisme $P(f)$ est inversible si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $P(f) \circ Q(f) = Id_E$, c'est à dire si $PQ - 1$ est un polynôme annulateur de f, donc un multiple de π_f. D'après le théorème de Bézout, cette dernière condition est équivalent à P et μ_f premiers entre eux.
Remarque : On peut remarque que l'algorithme d'Euclide (étendu) nous fournit donc l'inverse. Cet exercice a comme deuxième intérêt de montrer que $\mathbb{K}[f]$ est un corps ssi μ_f est irréductible sur $\mathbb{K}$

3 Question plus exotique ?

1. L'objectif de cet exercice est de vérifier que tout anneau factoriel vérifiant la propriété de Bezout est principal. (*i.e.* Supposons que A soit un anneau factoriel vérifiant que pour tout $(a, b) \in A$ premiers entre eux, il existe $(u, v) \in A$ tel que $au + bv = 1$)
   (a) Montrer que si $a, b \in A$ ont pour pgcd d, alors il existe $u, v \in A$ tel que $au + bv = d$.
   (b) Montrer que A est principal. *Indication : On pourra raisonner sur le nombre de facteurs irréductibles.*

Solution:

(a) C'est immédiat en remarquant que $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux. (cela a bien un sens d'écrire ces divisions car A est factoriel donc intègre).

(b) Si $I = (0)$, c'est bon. Si $I \neq (0)$, on peut considérer $x \in I$ l'élément dont le nombre de facteurs irréductibles (avec multiplicité) est minimal parmi les éléments non-nuls de I. (possible car forme une partie non vide de $\mathbb{N}$). On a alors que pour tout $a \in I$, $pgcd(a, x)|x$, et donc $pgcd(a, x) \in I$ par la question (a) et a moins de facteurs irréductibles que x. Alors par minimalité, $pgcd(a, x) = ux$ avec $u \in A^\times$, autrement dit $x|a$ et donc $I \subseteq (x)$. L'autre inclusion était immédiate, et donc $I = (x)$.

Remarque : il n'est pas difficile de voir que x est le pgcd de tous les éléments de I.

2. L'objectif de cet exercice est de démontrer le résultat suivant : si $u \in \mathcal{L}(E)$ vérifie π_u irréductible alors u est un endomorphisme semi-simple (*i.e.* tout sev F de E stable par u admet un supplémentaire dans E stable par u). Considérons dès lors F un sev stable de E par u

(a) Traiter le cas $F = E$

(b) Si $F \neq E$, il existe $x_1 \in E\backslash F$, considérons l'ensemble suivant $E_{x_1,u} = \{P(u)(x_1), P \in \mathbb{K}[X]\}$, vérifier qu'il est stable par u ?

i) Notons $I_{x_1} = \{P \in \mathbb{K}[X], P(u)(x_1) = 0\}$, Montrer que I_{x_1} est un idéal principal non-nul. On notera pour la suite π_{x_1} un générateur.

ii) Montrer que $\pi_u = \pi_{x_1}$ et en déduire l'irréductibilité de π_{x_1}.

iii) Montrer que $E_{x_1,u} \cap F = \{0\}$

iv) Conclure en fonction de si $E_{x_1,u}$ est supplémentaire par rapport à F. Sinon en déduire un procédé qui permet de conclure.

Remarque : Ce résultat est essentielle pour pouvoir montrer le résultat suivant sur les endomorphismes semi-simples (voir Gourdon, Algèbre et probabilités pour une démonstration) : « u est semi-simple si et seulement si $\pi_u = M_1 \dots M_r$ où les M_i sont unitaires, irréductibles et distincts »

Solution: ▷ Soit F un sev stable par u. Montrons l'existence d'un supplémentaire S stable par u.

(a) Si $F = E$, c'est terminé en prenant $S = \{0\}$ qui est bien stable par u.

(b) Sinon, considérons $x_1 \in E\backslash F$ et posons l'ensemble suivant qui est stable par u

$$E_{x_1,u} = \{P(u)(x_1), P \in \mathbb{K}[X]\}$$

Montrons que cet ensemble pourrait être un potentiel candidat de supplémentaire en commençant par montrer le caractère direct. Montrons que $E_{x_1,u} \cap F = \{0\}$. Pour se faire, on s'intéresse à l'ensemble

$$I_{x_1} = \{P \in \mathbb{K}[X], P(u)(x_1) = 0\}$$

i) Il est laissé au lecteur de vérifier que I_{x_1} est un idéal de $\mathbb{K}[X]$. Or $\mathbb{K}[X]$ est principal car $\mathbb{K}$ est un corps, I_{x_1} est donc principal, celui-ci est non réduit à $\{0\}$ car $\pi_u \in I_{x_1}$. Il est donc engendré par un élément $\pi_{x_1} \in \mathbb{K}[X]$.

ii) Or comme dit précedement, on a $\pi_u \in I_{x_1} = (\pi_{x_1})$ donc $\pi_{x_1} \mid \pi_u$ et comme π_u est irréductible (et que $\pi_{x_1} \neq 1$ car $x_1 \neq 0$ étant dans $E \backslash F$) alors $\pi_u = \pi_{x_1}$ et donc π_{x_1} est irréductible.

iii) Considérons $y \in E_{x_1,u} \cap F$, alors, il existe $P \in \mathbb{K}[X], y = P(u)(x_1)$. Maintenant supposons que $y \neq 0$. alors $P \notin I_{x_1} = (\pi_{x_1})$ donc π_{x_1} ne divise pas P et comme π_{x_1} est irréductible, alors π_{x_1} et P sont premiers entre eux. Comme $\mathbb{K}[X]$ est principal, par le théorème de Bezout :
Il existe $U, V \in \mathbb{K}[X], UP + V\pi_{x_1} = 1$ donc :

$$x_1 = U(u) \circ P(u)(x_1) + V(u) \circ \pi_{x_1}(u)(x_1) = U(u)(y)$$

Or $y \in F$ et comme F est stable par u alors par l'égalité au dessus, on devrait avoir $x_1 \in F$, ce qui est impossible. d'où le caractère direct.

iv) Si $F \oplus E_{x_1} = E$, c'est terminé en choisissant $S = E_{x_1}$. Sinon, on choisit $x_2 \in E \backslash (E_{x_1} \oplus F)$ et on recommence. On itère ainsi ce procédé qui se termine en un nombre fini d'itération car E est de dimension fini (et que $\dim(E_{x_i}) \geq 1$). Il existe donc $x_1, \dots x_r$ tel que

$$E = F \oplus E_{x_1} \oplus \cdots \oplus E_{x_r}$$

et comme pour tout $i \in \{1, \cdots, r\}, E_{x_i}$ est stabe par u alors $S = E_{x_1} \oplus \cdots \oplus E_{x_r}$ est stable par u et $F \oplus S = E$.

3. (a) Donner la définition d'anneaux noethérien. (proposer des caractérisations équivalentes ?)
   (b) Lien avec les autres types d'anneaux ?
   (c) Donner une classe faible d'anneau qui garantit l'existence de factorisation en irréductible.

Solution:

(a) Un anneau commutatif A est noetherien si tout idéal I de A est engendré par un nombre fini d'éléments (aka. de t.f).
LASSE :

i) A est un anneau noetherien

ii) Toute suite croissante d'idéaux de A est stationnaire.

iii) Tout ensemble non-vide d'idéaux de A admet un élément maximal.

(b) Principal implique noetherien mais la réciproque est fausse ($\mathbb{Z}[X]$), de même noetherien n'implique pas factoriel ($\mathbb{Z}[i\sqrt{5}]$) ni la réciproque.

(c) noetherien + intègre (voir [ROM] la démo de principal implique noetherien)