122. Anneaux principaux. Exemples et applications.

Introduction : Peut-on étendre les propriétés arithmétiques de $\mathbb{Z}$ à d'autres structures ?

1 Anneaux principaux

Soit $(A, +, \times)$ anneau commutatif intègre unitaire.

1.1 Définitions et premières propriétés

Définition 1. Une partie I de A est appelée idéal de A si $(I, +)$ sous-groupe de $(A, +)$ et si $\forall a \in A, x \in I, ax \in I$.

***Exemple* 2.** *Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}, n \in \mathbb{N}$.*

Proposition 3. Si I idéal de A, on a $I = A$ ssi I contient un inversible de A.

Proposition 4. Si I, J idéaux de A, $I + J$ et $IJ := \left\{ \sum_{k=1}^{m} i_k j_k, i_k \in I, j_k \in J \right\}$ sont des idéaux de A.

Définition 5. Un idéal I de A est dit principal s'il existe $a \in A$ tel que $I = aA$. a est alors appelé générateur de I. A est dit principal si tous ses idéaux sont principaux.

***Exemple* 6.** *$\mathbb{Z}$ et $K[X]$ (si K est un corps) sont des anneaux principaux.*
$\mathbb{Z}[X]$ n'est pas un anneau principal ($2\mathbb{Z}[X] + X\mathbb{Z}[X]$ n'est pas principal).

***Application* 7.** *Soient L/K une extension de corps, $a \in L$. L'ensemble $\{P \in K[X], P(a) = 0\}$ est un idéal de $K[X]$. Il existe donc un unique $\pi \in K[X]$ unitaire engendrant cet idéal, on l'appelle le polynôme minimal de a.*

1.2 Anneaux euclidiens

Définition 8. A est dit euclidien s'il existe $\nu : A \to \mathbb{N}$ tel que pour tous $a, b \in A\backslash\{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et $\nu(r) < \nu(b)$. ν est alors appelé stathme euclidien.

***Exemple* 9.** *$\mathbb{Z}$ est un anneau euclidien, ainsi que $K[X]$ muni du stathme $\nu = \deg$.*

Théorème 10. Tout anneau euclidien est principal.

***Contre-exemple* 11.** *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.*

Proposition 12. Soient K le corps des fractions de A, $S \subseteq A$ stable par produit, contenant 1 et pas 0. On note $\frac{A}{S} = \{\frac{a}{s} \in K, a \in A, s \in S\}$. C'est un sous-anneau de K, principal si A l'est, euclidien si A l'est.

***Application* 13.** *$\mathbb{D}$ (anneau des nombres décimaux) est euclidien.*

2 Arithmétique dans les anneaux principaux

Supposons A principal.

2.1 Divisibilité, PGCD et PPCM

Définition 14. Soient $a, b \in A$. On dit que b divise a (ou que a multiple de b), et on note $b|a$, s'il existe $c \in A$ tel que $a = bc$. On dit que a et b sont premiers entre eux si leurs seuls diviseurs communs sont les éléments de $A^\times$. Si $a_1, \cdots, a_k \in A$, on dit qu'ils sont premiers entre eux dans leur ensemble si leurs seuls diviseurs communs sont les éléments de $A^\times$.

Proposition 15. $b|a \Leftrightarrow aA \subset bA$, et la divisibilité définit un préordre.

Proposition 16. Un générateur de l'idéal $aA \cap bA$ est un plus petit multiple commun (noté ppcm) de a et b (au sens du préordre précédent). Un générateur de $aA + bA$ est un plus grand diviseur commun (noté pgcd) de a et b. Le ppcm et le pgcd sont uniques à multiplication par un inversible près. On définit de même les ppcm et pgcd de k éléments.

***Contre-exemple* 17.** *Dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm.*

Corollaire 18 (Bézout)**.** Si $a_1, \cdots, a_k \in A$, un diviseur commun d de $a_1, \cdots, a_k$ est un pgcd ssi il existe $u_1, \cdots, u_k \in A$ tels que $a_1u_1 + \cdots + a_ku_k = d$.

***Application* 19** (Noyaux)**.** *Soient E un K-espace vectoriel de dimension finie, $f \in \mathcal{L}(E)$, $P, Q \in K[X]$ premiers entre eux. On a $\ker(PQ(f)) = \ker(P(f)) \oplus \ker(Q(f))$.*

Corollaire 20 (Gauss)**.** Si $a, b, c \in A$, avec a, b premiers entre eux et $a|bc$, alors $a|c$.

Définition 21. $a \in A$ est dit irréductible si ses seuls diviseurs sont $1, a$ et leurs associés.

***Exemple* 22.** *Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés, les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Théorème 23. Si A principal, tout $a \in A$ non inversible possède une décomposition en produit d'irréductibles, unique à association près.

***Application* 24.** *$\{\ln(p), p$ premier$\}$ est une famille $\mathbb{Q}$-libre dans $\mathbb{R}$, et $[\mathbb{R} : \mathbb{Q}] = \infty$.*

2.2 Lemme chinois

Lemme 25. Si A principal et I, J idéaux de A vérifiant $IJ = I \cap J$, alors $I + J = A$.

***Contre-exemple* 26.** *C'est faux en général : considérer $K[X, Y]$ et les idéaux engendrés par X et Y.*

Théorème 27. Soient $a_1, \cdots, a_k \in A$ deux à deux premiers entre eux.
Alors $\phi \begin{cases} A/(a_1 \cdots a_k)A & \to A/a_1A \times \cdots \times A/a_kA \\ \overline{x} & \mapsto (\overline{x}^{a_1}, \cdots, \overline{x}^{a_k}) \end{cases}$ est un isomorphisme.

***Application* 28.** *Les entiers relatifs x vérifiant $x \equiv 2 \mod 4, x \equiv 3 \mod 5, x \equiv 1 \mod 9$ sont les $118 + 180k, k \in \mathbb{Z}$.*

3 Modules sur les anneaux principaux

3.1 Définitions et premières propriétés

Définition 29. Un ensemble M est appelé A-module s'il est muni d'une loi interne $+$ tel que $(M, +)$ soit un groupe abélien et d'une loi externe $\cdot : A \times M \to M$ telle que pour tous $\lambda, \mu \in A, x, y \in M, (\lambda + \mu)x = \lambda x + \mu x, \lambda(x + y) = \lambda x + \lambda y, \lambda(\mu x) = (\lambda\mu)x$ et $1_A x = x$.

***Exemple* 30.** *Un groupe abélien est un $\mathbb{Z}$-module. Si I idéal de A, alors I et A/I sont des A-modules.*

Définition 31. Soient M, N deux A-modules, soit $f : M \to N$. On dit que f est A-linéaire si $\forall \lambda, \mu \in A, x, y \in M, f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$. Si f est bijective, on dit que c'est un isomorphisme.

Définition 32. Soit M un A-module, soit $(m_i)_{i \in I}$ une famille d'éléments de M.

- On dit qu'elle est libre si $\forall (a_i)_i \in A^{(I)}, \sum_{i \in I} a_i m_i = 0 \Rightarrow \forall i, a_i = 0$.
- On dit qu'elle est génératrice si $\forall m \in M, \exists (a_i)_i \in A^{(I)}, m = \sum_{i \in I} a_i m_i$.
- On dit que c'est une base si elle est libre et génératrice.

Définition 33. M est dit de type fini s'il possède une partie génératrice finie. Il est dit libre s'il possède une base.

***Contre-exemple* 34.** *Le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ n'admet aucune famille libre.*

Théorème 35. Si M est libre de type fini, alors toutes ses bases sont finies et de même cardinal.

Définition 36. Ce cardinal est appelé rang de M.

3.2 Modules de type fini sur les anneaux principaux

On suppose A principal.

Théorème 37 (Bases adaptées)**.** Soient M un A-module libre de rang n, N un sous-module de M. Alors il existe une base $(e_1, \cdots, e_n)$ de M et une famille $(d_1, \cdots, d_s) \in A \backslash \{0\}$ tels que $d_s | \cdots | d_1$ et $(d_1 e_1, \cdots, d_s e_s)$ soit une base de N.

Théorème 38 (Facteurs invariants)**.** Si M est un A-module de type fini, il existe un unique $(r, s) \in \mathbb{N}^2$ et une unique suite $d_s | \cdots | d_1$ tels que $M \simeq A^r \times A/d_1A \times \cdots \times A/d_sA$.

Remarque 39. On retrouve ainsi le théorème de structure des groupes abéliens.

***Exemple* 40.** *À isomorphisme près, il y a 6 groupes abéliens d'ordre 600.*

4 Applications

4.1 Réduction des endomorphismes

Proposition 41. Si E est un K-espace vectoriel, $u \in \mathcal{L}(E)$, E a une structure de $K[X]$-module via $P \cdot x = P(u)(x)$.

Proposition 42. $u, v \in \mathcal{L}(E)$ sont semblables ssi ils induisent sur E deux structures de $K[X]$-module isomorphes.

Définition 43. Il existe d'après ce qui précède une unique famille de polynômes unitaires $P_s | \cdots | P_1$ tels que E soit isomorphe à $K[X]/(P_1) \times \cdots \times K[X]/(P_s)$. $P_1, \cdots, P_s$ sont appelés invariants de similitude de u.

Corollaire 44. u, v sont semblables ssi ils ont les mêmes invariants de similitude.

Théorème 45. Il existe alors $F_1, \cdots, F_s$ sev de E stables par u tels que $E = \bigoplus_{i=1}^{s} F_i$ et que pour tout $i, u_{|F_i}$ soit cyclique et de polynôme minimal P_i.

Corollaire 46. En particulier, P_1 est le polynôme minimal de u.

4.2 Théorème des deux carrés

Proposition 47. $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est euclidien, le stathme étant $\nu = |\cdot|$.

Théorème 48. Un nombre premier $p > 3$ est somme de deux carrés ssi $p \equiv 1 \mod 4$, et la décomposition est alors unique.

Corollaire 49. Un entier est somme de deux carrés ssi ses facteurs premiers congrus à $3 \mod 4$ figurent dans n à une puissance paire.

Développements

— Exemple d'anneau principal non euclidien.
— Théorème des deux carrés.

Références

[1] V. Beck, J. Malick, G. Peyré, Objectif Agrégation, H&K.

[2] F. Combes, Algèbre et géométrie, Bréal.

[3] S. Francinou, H. Gianella, Exercices de mathématiques pour l'agrégation - Algèbre 1, Masson.

[4] B. Hauchecorne, Les contre-exemples en mathématiques, Ellipses.

[5] P. Ortiz, Exercices d'algèbre, Ellipses.

[6] A. Szpirglas et al., Algèbre L3, Pearson.