P. Maurer
ENS Rennes

Leçon 122 : Anneaux principaux. Applications.

Devs :

- Théorème des deux carrés
- Critère d'Eisenstein

Références :

1. Perrin, Cours d'algèbre
2. Gourdon, Algèbre
3. Combes, Algèbre et géométrie
4. Saux-Picart, Cours de calcul formel

Dans toute la leçon, A désigne un anneau commutatif unitaire.

1 Principalité

1.1 Idéaux et anneaux principaux

Définition 1. *On appelle idéal de A un sous-groupe I de $(A,+)$ absorbant pour le produit, c'est-à-dire vérifiant :*

$$\forall a \in A \quad \forall b \in I \quad a \times b \in I$$

Définition 2. *On dit qu'un idéal I est principal s'il est engendré par un élément $x \in A$, i.e si on a $I = \{ax \,:\, a \in A\}$.*

Exemple 3. $n\mathbb{Z}$ est un idéal principal de $\mathbb{Z}$, $(X^2+1)\mathbb{R}[X]$ est un idéal principal de $\mathbb{R}[X]$.

Définition 4. *Un anneau A est dit intègre si pour tout $a, b \in A$, $ab = 0$ implique $a = 0$ ou $b = 0$.*

Définition 5. *Un anneau intègre est dit principal si tous ses idéaux sont principaux.*

Exemple 6. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont des anneaux principaux, si $\mathbb{K}$ est un corps commutatif.

Définition 7. *Un anneau intègre A est dit noethérien si tout idéal de A est engendré par un nombre fini d'éléments.*

Exemple 8. Tout anneau principal est noethérien.

Proposition 9. *Un anneau intègre est noethérien si et seulement si toute suite croissante d'idéaux est stationnaire.*

1.2 Anneaux euclidiens

Définition 10. *Un anneau intègre A est dit euclidien si il existe une application $f : A\setminus\{0\} \to \mathbb{N}$ telle que pour tout $(a,b) \in A \times A\setminus\{0\}$, il existe un couple $(q,r) \in A^2$ vérifiant $a = bq + r$ et $(r = 0$ ou $f(r) < f(b))$.*

Proposition 11. *Si A est euclidien, le couple (q,r) obtenu pour tout $(a,b) \in A \times A\setminus\{0\}$ ci-dessus est unique.*

Exemple 12. L'anneau $\mathbb{Z}$ muni de l'application $f(n) = |n|$ est euclidien. L'anneau $k[X]$ muni de l'application $f(P) = \deg(P)$ est euclidien.

Proposition 13. *Tout anneau euclidien est principal.*

Théorème 14. *L'anneau $A[X]$ est principal si et seulement si A est un corps. Si A n'est pas un corps, alors $A[X]$ n'est pas principal.*

Proposition 15. *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.*

1.3 Entiers de Gauss

Définition 16. *On définit l'anneau des entiers de Gauss comme :*

$$\mathbb{Z}[i] = \{a + ib \,:\, a, b \in \mathbb{Z}\}$$

On muni cet anneau de la « norme » $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a+ib) = a^2 + b^2$.

Proposition 17. *On a $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.*

Proposition 18. *L'ensemble Σ des sommes de deux carrés est stable par multiplication.*

Théorème 19. *L'anneau $\mathbb{Z}[i]$ est euclidien relativement à la fonction N, donc principal.*

Développement 1 :

Théorème 20. [DEV 1] *(Théorème des deux carrés)*
Soit $p \in \mathbb{N}$ un nombre premier. On a l'équivalence $p \in \Sigma \iff p = 2$ ou $p \equiv 1 \pmod 4$

2 Arithmétique sur un anneau

2.1 Définitions.

Définition 21. *On note $A^\times$ le groupe des inversibles de A, aussi appelés unités.*

Définition 22. *Soit $a, b \in A$. On dit que a divise b si il existe $r \in A$ tel que $b = ar$.*
Un élément $d \in A$ est appelé diviseur commun de $n_1, \ldots n_m \in A$ si d divise n_i pour tout i.
Un élément $m \in A$ est appelé multiple commun de $n_1, \ldots, n_m \in A$ si n_i divise m pour tout i.

Définition 23. *Un élément $p \in A$ est dit irréductible si p n'est ni nul ni inversible et si $p|ab \Longrightarrow p|a$ ou $p|b$ pour tout $a, b \in A$.*

Définition 24. *On dit que $a, b \in A$ sont associés s'il existe $u \in A^\times$ tel que $a = ub$.*
On montre que a et b sont associés si et seulement si $(a) = (b)$.

Proposition 25. *Si c est irréductible, alors l'idéal (c) est maximal parmi les idéaux principaux de A.*

Corollaire 26. *Les idéaux maximaux d'un anneau principal sont exactement les idéaux de la forme $I = (c)$ avec $c \in A$ irréductible.*

Exemple 27. Soit K un corps et L une extension de K. Soit $\varphi : K[T] \to L$ l'homomorphisme défini par $\varphi_{|K} = \mathrm{id}_K$ et $\varphi(T) = \alpha$.
Si φ est injectif, on dit que α est transcendant sur K. Sinon, on dit que α est algébrique sur K, et l'idéal $I = \mathrm{Ker}\,\varphi$ étant principal, on a $I = (P)$ avec P irréductible (que l'on peut supposer unitaire). Le polynôme P est, par définition, le polynôme minimal de α sur K

Exemple 28. Les nombres $\sqrt{2}$, i, $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$, de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 2$ et $X^3 - 2$.

2.2 Théorèmes principaux. Aspects algorithmiques.

Théorème 29. *(Théorème de Bézout)*
Soit A un anneau principal et $a, b \in A$. On note $\mathrm{pgcd}(a, b)$ leur plus grand diviseur commun.
Alors il existe $u, v \in A$ tels que $au + bv = \mathrm{pgcd}(a, b)$

Exemple 30. (Lemme des noyaux)
Soit E un K-espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$. Soit $P_1, \ldots, P_r \in K[X]$ deux à deux premiers entre eux. Alors $\mathrm{Ker}\,P(f) = \mathrm{Ker}\,P_1(f) \oplus \cdots \oplus \mathrm{Ker}\,P_r(f)$.

Corollaire 31. *Un endomorphisme $f \in \mathcal{L}(E)$ est diagonalisable si et seulement si son polynôme minimal est scindé à racines simples.*

Théorème 32. *(Algorithme d'Euclide)*
Soit a et b deux éléments non nuls d'un anneau euclidien A, soit $(r_i)_i$ la suite d'éléments définie par $r_0 = a$, $r_1 = b$, puis, pour $r \geq 2$, $r_i = \mathrm{rem}(r_{i-2}, r_{i-1})$, où $\mathrm{rem}(x, y)$ désigne la fonction qui a (x, y) associe le reste dans la division de x par y dans A.
Alors la suite $(r_i)_i$ est finie : il existe un entier $n+1$ pour lequel $r_{n+1} = 0$ et $\mathrm{pgcd}(a, b) = r_n$.

Théorème 33. *(Algorithme d'Euclide étendu)*
Si $a, b \in A \setminus \{0\}$, on définit :

$$W_0 = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix},\ W_1 = \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix},\ W_i = \begin{pmatrix} r_i \\ u_i \\ v_i \end{pmatrix}$$

Où pour $i \geq 2$, r_i est le reste de la division euclidienne (q_i, r_i) de r_{i-2} par r_{i-1}, u_i et v_i étant définis par $u_i = u_{i-2} - q_i u_{i-1}$ et $v_i = v_{i-2} - q_i v_{i-1}$.
Alors pour tout i, $r_i = au_i + bv_i$: en particulier, $\mathrm{pgcd}(a, b) = au_n + bv_n$, où n est le plus petit indice pour lequel $r_{n+1} = 0$.

Exemple 34. $\mathrm{pgcd}(X^m - 1, X^k - 1) = X^{\mathrm{pgcd}(m,k)} - 1$.

Théorème 35. *(Théorème chinois)*
Soit I et J des idéaux de A tels que $I + J = A$. L'application φ: $\begin{cases} A/I \cap J & \to & (A/I) \times (A/J) \\ \hat{x} & \mapsto & (\bar{x}, \check{x}) \end{cases}$ est un isomorphisme d'anneau.

Corollaire 36. *Soit A un anneau principal, $m \in A$ et $n \in A$ premiers entre eux. Considérons $u \in A$, $v \in A$ tels que $1 = um + vn$. L'application ψ: $\begin{cases} A/mnA & \to & (A/mA) \times (A/nA) \\ \hat{x} & \mapsto & (\bar{x}, \check{x}) \end{cases}$ est un isomorphisme d'anneau.*
L'isomorphisme réciproque associe à $(\bar{a}, \check{b}) \in (A/mA) \times (A/nA)$ la classe $\hat{x} \in A/mnA$ de $x = vna + umb$.

Exemple 37. Le système de congruences dans $\mathbb{Z}$ $\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 9 \end{cases}$ a pour solutions $x = 838 + 180k$ et $x = 118 + 180k'$ pour $k, k' \in \mathbb{Z}$.

3 Factorialité

Définition 38. *Soit A un anneau intègre. On dit que A est factoriel si tout élément $a \in A$ peut s'écrire, de manière unique à permutation de facteurs près, de la forme :*

$$a = u p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$$

Où $u \in A^\times$ et $p_1, \dots, p_\ell \in A$ sont irréductibles et $\alpha_1, \dots, \alpha_\ell \in \mathbb{N}$.

Exemple 39. Un anneau principal est factoriel.

Les anneaux principaux forment une sous-partie « plus simple » des anneaux factoriels (dans le sens où il est souvent plus facile de montrer qu'un anneau est principal).

Exemple 40. $\mathbb{Z}[i]$ est factoriel. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

Définition 41. *Pour $P \in A[X]$ non nul, on appelle contenu de P, noté $c(P)$ le plus grand diviseur commun de ses coefficients. L'élément $c(P)$ est défini modulo $A^\times$ (à un inversible près).*

Un polynôme est dit primitif si $c(P) = 1$.

Lemme 42. *(Gauss)*

On a $c(PQ) = c(P)\,c(Q)$ modulo $A^\times$.

Théorème 43. *Si A est factoriel, $A[X]$ est factoriel.*

Théorème 44. *Soit A un anneau factoriel. Alors pour tout $p \in A$ irréductible, l'idéal (p) est premier.*

Développement 2 :

Théorème 45. [Dev 2] *(Critère d'Eisenstein)*

Soit A un anneau factoriel. On note $K = \mathrm{Frac}(A)$. Les polynômes de $A[X]$ irréductibles sont :

i. Les constantes $p \in A$ irréductibles dans A

ii. Les polynômes de degré plus grand que 1 primitifs et irréductibles dans $K[X]$

Soit $P = \sum_{i=1}^{n} a_i X^i \in A[X]$, et p un élément irréductible de A tel que $p \nmid a_n$, $p^2 \nmid a_0$ et $p \mid a_i$ pour tout $i \in [\![0, n-1]\!]$. Alors P est irréductible dans $K[X]$.

Théorème 46. *$\mathbb{Z}[X]$ est factoriel.*

Exemple 47. Le polynôme cyclotomique $\Phi_{\mathbb{Q},p}(X) = \prod_{\zeta \in \mu_p^*} (X - \zeta) = \sum_{i=1}^{p-1} X^i$ est irréductible sur $\mathbb{Q}$, où p est un nombre premier et μ_p^* désigne l'ensemble des racines primitives $p^{\text{èmes}}$ de l'unité.