Anneaux principaux. Exemples et applications.

122

I - Principalité, factorialité et division euclidienne

1) Anneaux principaux et factoriels

Def 1 : Un anneau A est dit principal s'il est intègre et si tout idéal de A est principal, i.e. engendré par un élément.

Def 2 : Soit A un anneau et $\mathcal{P}$ un système de représentants de ses irréductibles pour la relation d'association. L'anneau A est dit factoriel s'il est intègre et qu'il vérifie

(E) Tout élément $a \in A \setminus \{0\}$ s'écrit sous la forme $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ avec $u \in A^*$, $v_p(a) \in \mathbb{N}$ et les $v_p(a)$ presque tous nuls.

(U) cette écriture est unique.

Ex 3 : L'anneau $\mathbb{Z}[X]$ n'est pas principal ($\langle 2, X \rangle$ n'est pas principal) et $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel ($9 = 3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$).

Prop 4 : Soit A un anneau intègre vérifiant (E). Les conditions suivantes sont équivalentes.

(i) A vérifie (U)

(ii) (Lemme d'Euclide) : si p est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

(iii) (Théorème de Gauss) : si $a \mid bc$ et a est premier avec b, alors $a \mid c$.

Cor 5 : Un anneau principal est factoriel.

Thm 6 : Soit A un anneau factoriel. Deux éléments a et $b \neq 0$ admettent un plus grand commun diviseur noté $\mathrm{pgcd}(a,b)$ et un plus petit commun multiple noté $\mathrm{ppcm}(a,b)$.

Prop 7 : Soit A un anneau principal et $a, b \in A \setminus \{0\}$ et $d = \mathrm{pgcd}(a,b)$. On a $(d) = (a) + (b)$, c.e. il existe $\lambda, \mu \in A$ tq $d = \lambda a + \mu b$.

2) Anneaux euclidiens

Def 8 : Un anneau A est dit euclidien si A est intègre et s'il existe une fonction $\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$ (appelée stathme euclidien) telle que si $a, b \in A \setminus \{0\}$, alors il existe $q, r \in A$ vérifiant

$$a = bq + r \quad \text{et} \quad r = 0 \text{ ou } \nu(r) < \nu(b).$$

Ex 9 : $\mathbb{Z}$ est euclidien, si k est un corps, $k[X]$ est euclidien. avec respectivement $\nu = |\cdot|$ et $\nu = \deg(\cdot)$.

Thm 10 : Un anneau euclidien est principal (et donc factoriel).

Ex 11 : Soit k un corps. L'anneau $k[X,Y]/(Y - X^2)$ est un anneau principal.

Prop 12 : Soit A un anneau euclidien et $a, b \in A \setminus \{0\}$. On note $(r_0, u_0, v_0) := (a, 1, 0)$ et $(r_1, u_1, v_1) := (b, 0, 1)$. et pour tout $i \geq 2$, si $r_{i-2} = q_i r_{i-1} + r_i$ est la division euclidienne de r_{i-2} par r_{i-1}, on note $(r_i, u_i, v_i) := (r_i, u_{i-2} - q_i u_{i-1}, v_{i-2} - q_i v_{i-1})$. Il existe un plus petit indice n tel que $r_{n+1} = 0$ et alors :

$$a u_n + b v_n = r_n = \mathrm{pgcd}(a,b).$$

Appl 13 : Soient $a, b, c \in \mathbb{Z}$ tels que $\mathrm{pgcd}(a,b)$ divise c. Soit (x_0, y_0) une solution particulière de l'équation $ax + by = c$ (*) dans $\mathbb{Z}^2$. Les solutions de (*) sont exactement les éléments de

$$S = \{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\}$$

où $a' = \frac{a}{\mathrm{pgcd}(a,b)}$ et $b' = \frac{b}{\mathrm{pgcd}(a,b)}$.

DVP 1

Prop 14 : Soit A un anneau euclidien. Il existe $u \in A \setminus A^*$ tel que la restriction à $A^* \cup \{0\}$ de la projection canonique $\pi : A \twoheadrightarrow A/(u)$ soit surjective

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

3) Le cas des anneaux de polynômes

Prop 16 : Soit A un anneau. L'anneau $A[X]$ est principal ssi A est un corps.

Prop 17 : Si A est factoriel, alors $A[X]$ est factoriel.

Coro 18 : Si A est factoriel, alors $A[X_1, \dots, X_n]$ est factoriel.

Def 19 : Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit algébrique sur K s'il existe $P \in K[X]$ non-nul tel que $P(\alpha) = 0$.

Ex 20 : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, π ne l'est pas (admis).

Thm 21 : Si $\alpha \in L$ est algébrique sur K, alors il existe unique polynôme unitaire $\mu_\alpha \in K[X]$ tel que $\{P \in K[X] \mid P(\alpha) = 0\} = \langle \mu_\alpha \rangle$, il est appelé polynôme minimal de α.

Ex 22 : Le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2$.

Thm 23 : L'ensemble $\bar{K}$ des éléments de L qui sont algébriques sur K est un sous-corps de L contenant K.

II - Anneaux principaux et équations diophantiennes.

Prop 24 : Soit $d \in \mathbb{N}^*$ sans facteurs carrés. L'anneau $\mathbb{Z}[i\sqrt{n}]$ n'est pas euclidien si $d > 2$.

1) L'anneau des entiers de Gauss.

Def-Prop 25 : On note $N : a+ib \in \mathbb{Z}[i] \longmapsto a^2+b^2 \in \mathbb{N}$.
La norme N est multiplicative : $\forall z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$

Coro 26 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Prop 27 : L'anneau $\mathbb{Z}[i]$ est euclidien.

Def-Prop 28 : Soit $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N} \text{ tq } a^2+b^2 = n\}$. L'ensemble Σ est stable par multiplication.

Thm 29 : Soit $p \in \mathbb{N}$ un nombre premier. On a :
$$p \in \Sigma \text{ ssi } p = 2 \text{ ou } p \equiv 1 [4]$$

Ex 30 : $61 = 6^2 + 5^2$

Thm 31 : Soit $n \in \mathbb{N} \setminus \{0, 1\}$ et $n = \prod_{p \in S} p^{v_p(n)}$ sa décomposition en facteurs premiers. On a :
$$n \in \Sigma \text{ ssi } \forall p \in S,\ p \equiv 3 [4] \Rightarrow v_p(n) \in 2\mathbb{N}.$$

Coro 32 : Les irréductibles de $\mathbb{Z}[i]$ sont aux inversibles près les entiers premiers $p \in \mathbb{N}$ avec $p \equiv 3 [4]$ et les $a+ib \in \mathbb{Z}[i]$ tel que a^2+b^2 est un nombre premier.

2) L'anneau $\mathbb{Z}[i\sqrt{2}]$ DVPZ

Def-Prop 33 : On note $N : a+ib\sqrt{2} \longmapsto a^2+2b^2 \in \mathbb{N}$. La norme N est multiplicative : $\forall z, z' \in \mathbb{Z}[i\sqrt{2}]$, $N(zz') = N(z)N(z')$.

Coro 34 : $\mathbb{Z}[i\sqrt{2}]^\times = \{\pm 1\}$.

Prop 35 : Les solutions dans $\mathbb{Z}^2$ de l'équation $x^2+2 = y^3$ sont exactement $(\pm 5, 3)$.

Coro 36 : L'unique entier entre un carré et un cube est $25 < 26 < 27$.

III - Module sur un anneau principal.

1) Premières définitions : (dans la suite, A est un anneau principal)

Def 37 : On dit que $(M, +, \cdot)$ est un A-module si $(M, +)$ est un groupe abélien muni d'une application $\cdot$ de $A \times M$ dans M telle que :
i) $\forall \lambda \in A, \forall u, v \in M,\ \lambda \cdot (u+v) = \lambda \cdot u + \lambda \cdot v$
ii) $\forall \lambda, \mu \in A, \forall u \in M,\ (\lambda+\mu) \cdot u = \lambda \cdot u + \mu \cdot u$ et $(\lambda\mu) \cdot u = \lambda \cdot (\mu \cdot u)$
iii) $\forall u \in M,\ 1_A \cdot u = u$.

Ex 38 : Si k est un corps, alors tout k-espace vectoriel est un k-module.

Ex 39 : Les $\mathbb{Z}$-modules sont les groupes abéliens.

Rmq 40 : Par analogie avec les espaces vectoriels, on définit les notions de famille libre, génératrice, de base, d'application linéaire et de sous-module pour les modules.

Ex 41 : Soit V un k-espace vectoriel et $u \in \mathcal{L}(V)$. On munit V d'une structure de $k[X]$-module par :

$$\forall P \in k[X],\ \forall v \in V,\quad P \cdot v := P(u)(v).$$

Déf 42 : Soit M un A-module. On dit que M est un module libre s'il admet une base et que M est de type fini s'il admet une famille génératrice finie.

Rmq 43 : Soit M un module de type fini engendré par $m_1, \dots, m_n$ et $\Phi_M : \begin{cases} A^n \longrightarrow M \\ (a_1, \dots, a_n) \longmapsto \sum_{i=1}^{n} a_i m_i \end{cases}$. Alors $A^n / \operatorname{Ker} \Phi_M \simeq M$ en tant que A-modules.

2) Forme normale de Smith et structure des A-modules.

Thm 44 : Soit A un anneau principal. Toute matrice $M \in \mathcal{M}_{m,n}(A)$ est équivalente à une matrice $\left(\begin{array}{c|c} f_1 & \\ & f_r \\ \hline & \end{array}\right) \in \mathcal{M}_{m,n}(A)$ où $f_1, \dots, f_r \in A$ tels que $f_1 \mid \dots \mid f_r$.
Ces éléments sont uniques modulo les inversibles et appelés facteurs invariants de M.

Appl 45 : Soit $M \in \mathcal{M}_{m,n}(A)$ et $Y \in A^m$. Si $M = PDQ$ est la forme normale de Smith de M, alors les solutions du système $MX = Y$ dans A^n sont données par les solutions de $DX' = P^{-1}Y$.

Thm 46 : Soit A un anneau principal et M un A-module libre de type fini de rang n. Si N est un sous-module de M, alors il existe une base $(e_1, \dots, e_n)$ de M et $s \in \{0, \dots, n\}$ et $d_1, \dots, d_s \in A \setminus \{0\}$ tels que $d_1 \mid \dots \mid d_s$ et $(d_1 e_1, \dots, d_s e_s)$ est une base de N.

Cor 47 : Soit M un A-module de type fini. Il existe un unique couple d'entiers (r, s) et une unique suite $d_1 \mid \dots \mid d_s \in A \setminus \{0\}$ tels que $M \simeq A^r \oplus \left(\bigoplus_{i=1}^{s} A/(d_i)\right)$.

Cor 48 : Théorème de structure des groupes abéliens de type fini, Théorème de réduction de Frobenius et forme de Jordan.

3) Application aux réseaux. (V est un $\mathbb{R}$-espace vectoriel de dim $< \infty$)

Déf 49 : Une partie Γ de V est appelée un sous-réseau de V s'il existe une famille libre $\mathcal{B} = (e_1, \dots, e_r)$ de V telle que $\Gamma = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_r$. On dit que $\mathcal{B}$ est une base de Γ. Si $\operatorname{Vect}(\Gamma) = V$, on dit que Γ est un réseau de V.

Prop 50 : Soit Γ un réseau de V et Λ un sous-groupe de Γ.
(i) Λ est un sous-réseau de V tel que $\operatorname{rg}(\Lambda) \leq \operatorname{rg}(\Gamma)$
(ii) Il existe une base $(e_1, \dots, e_r)$ de Γ, $s \in \{0, \dots, r\}$ et $d_1, \dots, d_s \in \mathbb{Z}^*$ tels que $(d_1 e_1, \dots, d_r e_r)$ est une $\mathbb{Z}$-base de Λ et $d_1 \mid \dots \mid d_r$.

Prop 51 : ($(c_i), (\ell_i) \subset \mathbb{R}$) Soit Γ un réseau de $\mathbb{R}^n$ de $\mathbb{Z}$-base $(e_1, \dots, e_n) =: \mathcal{B}$. Le domaine fondamental associé à $\mathcal{B}$ de Γ est $\mathcal{P}_{\mathcal{B},\Gamma} = \{\sum \lambda_i e_i \mid \lambda_i \in [c_i, \ell_i[\}$. Si $\mathcal{C} = (z_1, \dots, z_n)$ est la base canonique de $\mathbb{R}^n$ et $\mathcal{T}_{\mathcal{B},\Gamma} = (\langle e_i, e_j \rangle)_{1 \leq i,j \leq n}$ alors $\mu(\mathcal{P}_{\mathcal{B},\Gamma}) = \sqrt{\det \mathcal{T}_{\mathcal{B},\Gamma}}$ où μ est la mesure de Lebesgue.

Ex 52 : (annexe 1)

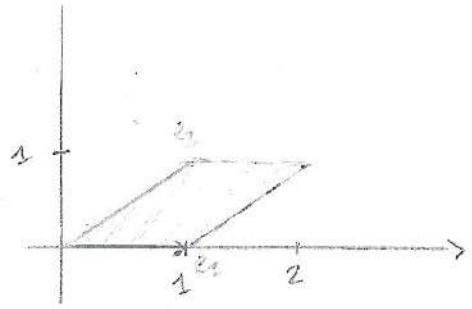
Rmq 53 : $\mu(\mathcal{P}_{\mathcal{B},\Gamma})$ ne dépend pas de $\mathcal{B}$ et est appelée covolume de Γ.

Thm 54 : (Minkowski, admis) Soit Γ un réseau. Une partie $A \subset \mathbb{R}^n$ convexe mesurable et symétrique par rapport à 0 contient un élément de $\Gamma \setminus \{0\}$ dès que : $\mu(A) > 2^n \mu(\mathbb{R}^n/\Gamma)$

Prop 55 : Soit $\Lambda \subset \Gamma$ un sous-réseau. Alors Γ/Λ est fini et le covolume $\operatorname{cov}(\Lambda)$ est $\operatorname{cov}(\Lambda) = |\Gamma/\Lambda| \cdot \operatorname{cov}(\Gamma)$

Appl 56 : On peut démontrer le 2 g via le réseau $\Gamma = \{(a,b) \in \mathbb{Z}^2 \mid a \equiv ub\ [p] \text{ et } c \in \mathbb{Z}\}$ avec $u \in \mathbb{Z}$ tel que $u^2 + 1 \equiv 0\ [p]$.

Appl 57 : Tout entier est somme de quatre carrés via le réseau $\Gamma = \{(a,b,c,d) \in \mathbb{Z}^4 \mid \begin{matrix} ua + vb \equiv c\ [p] \\ ub - va \equiv d\ [p] \end{matrix}\}$ où $u, v \in \mathbb{Z}$ tq $u^2 + v^2 + 1 \equiv 0\ [p]$.



annexe 1 - domaine fondamental du réseau $\Gamma = \mathbb{Z}\cdot(1,0) \oplus \mathbb{Z}(1,2)$