(113)

Anneaux principaux - Exemples et application

122

A désigne un anneau commutatif unitaire (les morphismes d'anneaux sont unitaires, ainsi que les sous-anneaux).

I) Anneaux et idéaux

1) Généralités

Def 1 : $I \subset A$ est un idéal ssi $(I,+)$ est un sous-groupe de $(A,+)$ et $\forall a \in A, \forall b \in I, ab \in I$

On note alors $I \lhd A$.

Ex : $A \lhd A$, $\{0\} \lhd A$. Si $1 \in I$, idéal de A, $I = A$.

Les idéaux d'un corps sont $\{0\}$ et A.

Prop 2 : Si $I \lhd A$, le groupe A/I est muni d'une structure d'anneau quotient et la surjection canonique est un morphisme d'anneaux.

Def 3 : $I \lhd A$ est premier si A/I intègre ssi $A \neq I$ et $\forall a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$

Ex : $\{0\} \lhd A$ est premier ssi A intègre

Def 4 : $I \lhd A$ est maximal si A/I est un corps ssi $I \subset J$ avec $J \lhd A$, $J \neq A \Rightarrow I = J$.

Prop 5 : $I \lhd A$ maximal est premier. Tout idéal $I \lhd A$, $I \neq A$ est inclus dans un idéal maximal (Krull)

2) Arithmétique

Def 6 : $A^\times = \{a \in A \mid \exists b \in A \mid ab = ba = 1\}$ est l'ensemble des inversibles de A. C'est un groupe pour la multiplication.

Ex : A corps ssi $A^\times = A \setminus \{0\}$.

Def 7 : $a, b \in A$, $a \mid b \iff \exists c \in A \mid b = ac$.

Def 8 : Si $S \subset A$, l'idéal de A engendré par S est $(S) = \left\{ \sum_{i=1}^{n} a_i s_i,\ n \in \mathbb{N},\ a_1 \dots a_n \in A,\ s_1 \dots s_n \in S \right\}$.

Ex : $a \in A$, $(a) = aA$.

Prop 9 : $a \mid b \iff (b) \subset (a)$

Def 10 : a et b sont associés $\iff a \mid b$ et $b \mid a \iff (a) = (b)$ si A intègre.

Def 11 : $p \in A$ est irréductible si $p \notin A^\times$ et $\forall a, b \in A$, $p = ab \Rightarrow p \in A^\times$ ou $b \in A^\times$

Ex : Les nombres premiers sont les irréductibles de $\mathbb{Z}$ (modulo ± 1)

Def 12 : $p \in A$ premier si $p \neq 0$ et (p) est premier.

Prop 13 : $p \in A$ premier est irréductible.

II) Anneaux principaux - Exemples

1) Généralités

Def 14 : A est principal si il est intègre et si tout idéal de A est de la forme (a) pour $a \in A$.

Ex : $\mathbb{Z}$ est principal, $K[X]$ pour K un corps est principal (cf. II. 3)

Def 15 : $a, b \in A$. $d \in A$ est un PGCD de a et b si $d \mid a$, $d \mid b$ et d est maximal pour cette propriété : $c \mid a$ et $c \mid b \Rightarrow c \mid d$

a et b sont premiers entre eux si $\forall d \in A$, $d \mid a$ et $d \mid b \Rightarrow d \in A^\times$.

Thm 16 (Bézout) : A principal, $a, b \in A$: a et b sont en PGCD d, unique aux associés près et on a $(a) + (b) = (d)$ si : $\exists \lambda, \mu \in A \mid d = \lambda a + \mu b$.

Cor 17 : $a, b \in A$ principal sont premiers entre eux ssi $(a) + (b) = A$.

Ex : 2 et 3 premiers entre eux donc $\mathbb{Z}$ $\quad PGCD(2,3) = 2 \wedge 3 = 2$

2) Propriétés arithmétiques

Def 18 : A est noethérien si tout idéal de A est de la forme (S) où $S \subset A$ est fini.

Ex : Tout anneau principal est noethérien.

Si A noethérien, $A[X]$ aussi.

Prop 19: Anneau noethérien si toute suite croissante d'idéaux de A est stationnaire.
Si $I \lhd A$, Anneau, A/I aussi.
Ex: $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z}[X]/(X^2+5)$ est noethérien

Def 20: A est factoriel si A intègre et :
(E) $\forall a \in A \setminus \{0\}$, $\exists u \in A^\times$, $p_1 \dots p_n \in A$ irréductibles tq $a = u p_1 \dots p_n$.
(U) Si $a = u p_1 \dots p_n = v q_1 \dots q_n$ avec irréductibles, $n = n$ et $\exists \sigma \in \mathfrak{S}_n \mid \forall i \in [\![1,n]\!]$ p_i et $q_{\sigma(i)}$ sont associés.

Thm 21: Anneau noethérien vérifie (E).

Thm 22: Soit A intègre vérifiant (E). Equivalence entre
(i) A factoriel, (ii) Si p irréductible, $a, b \in A$, $p \mid ab$, $p \mid a$ ou $p \mid b$ (Euclide) (iii) p irréductible $\Leftrightarrow$ p premier
(iv) Si $a \mid bc$ et a et b premiers entre eux, $a \mid b$ (Gauss)

Cor 23: A principal $\Rightarrow$ A factoriel.
Ex: Décomposition en produit de facteurs premiers dans $\mathbb{Z}$, en irréductible dans $K[X]$.
$\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel donc pas principal.

Cor 24: A principal vérifie le lemme de Gauss et le lemme d'Euclide.
On fixe un système de représentants $\mathcal{O}$ des irréductibles de A modulo association : $\forall a \in A$, $\exists! u \in A^\times$, $\exists! (v_p(a))_{p \in \mathcal{O}}$ presque nulle $\mid a = u \prod_{p \in \mathcal{O}} p^{v_p(a)}$: $v_p(a)$ est la valuation p-adique de a.

Cor 25: A principal, $a, b \in A$: (i) $a \mid b \Leftrightarrow \forall p \in \mathcal{O}$, $v_p(a) \leq v_p(b)$
(ii) $\mathrm{PGCD}(a,b) = \prod_{p \in \mathcal{O}} p^{\min(v_p(a), v_p(b))}$ (modulo $A^\times$)

Def 26: A quelconque, $a, b \in A$: a et b ont un PPCM $c \in A$ si $a \mid c$ et $b \mid c$ et c minimal pour cette propriété

Def 27: A principal, $a, b \in A$: $\mathrm{PPCM}(a,b) := a \vee b$ existe, unique modulo $A^\times$ et : (i) $(a) \cap (b) = (c)$
(ii) $c = \prod_{p \in \mathcal{O}} p^{\max(v_p(a), v_p(b))}$ (modulo $A^\times$)
(iii) $ab = (a \vee b)(a \wedge b)$ modulo $A^\times$.
Ex: $60 \wedge 27 = 3$, $60 \vee 27 = 540$
Ex: $\mathbb{Z}[X]$ factoriel (Gauss) mais pas principal car $A[X]$ principal ssi A est un corps.
Rq: On définit par récurrence le PGCD et le PPCM de n éléments de A principal

i3) Anneaux euclidiens

Def 28: A intègre est euclidien si il existe $\nu : A \setminus \{0\} \to \mathbb{N}$ (stathme) tq si $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tq $a = bq + r$ et $r = 0$ ou $\nu(r) < \nu(b)$)
Ex: $\mathbb{Z}$ est factoriel car $\nu(n) = |n|$.
$K[X]$ est factoriel car $\nu(P) = \deg P$
$\mathbb{Z}[\underbrace{\tfrac{1+i\sqrt{3}}{2}}_{j}] = \{a + bj \mid a, b \in \mathbb{Z}\}$ est euclidien par $\nu(x + jy) = |y|^2$

Thm 29: A euclidien est principal.

Rq fondamentale 30: Si A euclidien on dispose de l'algorithme d'Euclide pour calculer le PGCD de deux éléments, et en cas $(\lambda, \mu) \mid$ tq $\lambda a + \mu b = a \wedge b$.
En effet si $a = bq + r$, $\nu(r) < \nu(a)$, $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r)$
et si $b \wedge r = \lambda b + \mu r$, $a \wedge b = b \wedge r = \lambda b + \mu(a - bq)$
$= \mu a + b(\lambda - b\mu)$.
Ex: $42 \wedge 10 = 2 = 42 - 4 \times 10$.
Prop 30: A euclidien : il existe $\alpha \in A \setminus A^\times$ tq la projection DM ||

(3/3)

Corollaire π : A → A/(x) restreinte à A^× ∪ {0} est surjective

Ca 31 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais pas euclidien.

III) Application

1) Equation diophantiennes et arithmétique

Prop 31 : A principal, a, b, c ∈ A.

(i) L'équation ax + by = c d'inconnue x, y ∈ A a des solution ssi a ∧ b | c

(ii) L'ensemble des solution est $S = \{(x_0 - \frac{kb}{a\wedge b}, y_0 + \frac{ka}{a\wedge b}) / k \in A\}$ où (x_0, y_0) est une solution particulière. Si A euclidien, (x_0, y_0) est donné par l'algorithme d'Euclide.

Ex : $3x + 2y = 1 \iff \exists k \in \mathbb{Z} \mid x = 1 - 2k, y = -1 + 3k$

Lemme 32 : $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$ est euclidien pour $v(y) = |y|^2$. On a de plus $\mathbb{Z}[i]^\times = \{y \in \mathbb{Z}[i] / v(y) = 1\} = \{\pm 1, \pm i\}$

Def 33 : On note $\Sigma = \{a^2 + b^2, a, b \in \mathbb{N}\}$

Prop 34 : Σ est stable par multiplication car $\Sigma = \{v(y), y \in \mathbb{Z}[i]\}$. p premier est dans Σ ⇒ p ≡ 1 [4]

Lemme 35 : p premier : p ∈ Σ (=) p = 2 ou p ≡ 1 [4]

Ca 36 : $n \in \mathbb{N}^*, n \neq 1$: on décompose n en facteur premier $n = \prod_{p \in P} p^{v_p(n)}$. $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3 [4]$ (Thm des deux carrés)

Thm 37 (chinois) : A principal, a, b ∈ A premier entre

Alors $A/(ab) \cong A/(a) \times A/(b)$

Ca 38 : (lemme chinois) : n, m ∈ ℤ*, équivalence entre (i) n ∧ m = 1, (ii) $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (groupes abéliens), (iii) $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (anneaux)

Exo : n ∧ m = 1, φ(nm) = φ(n) φ(m) où φ(n) = #{k ∈ [1, n] / k ∧ n = 1}. Si $n = \prod_{p \in P} p^{v_p(n)}$, $\varphi(n) = n \prod_{\substack{p \in P \\ v_p(n) \neq 0}} (1 - \frac{1}{p})$

Ex : Si $n_1 \dots n_r$ premiers entre eux deux à deux, $a_1 \dots a_r \in \mathbb{Z}$ le système $\begin{cases} k \equiv a_1 [n_1] \\ \dots \\ k \equiv a_r [n_r] \end{cases}$ d'inconnue k ∈ ℤ a des solutions données par $k = k_0 + qn$, k_0 solution particulière et q ∈ ℤ et $n = n_1 \dots n_r$. Ainsi $\begin{cases} k \equiv 2 [4] \\ k \equiv 3 [5] \\ k \equiv 1 [9] \end{cases} \iff k = 118 + 180q$, $q \in \mathbb{Z}$.

2) Algèbre linéaire (K corps, E K-ev de dim n ≥ 1)

Prop 39 : Si $u \in \mathcal{L}(E)$: $\{P \in K[X] / P(u) = 0\} \lhd K[X]$ non nul donc de la forme $\pi_u K[X]$ où π_u unitaire. π_u est le polynôme minimal de u. Pour $x \in E$ on définit de même $\pi_{u,x}$ tq $P(u)x = 0 \iff \pi_{u,x} \mid P$.

Thm 40 (lemme des noyaux) : P, Q ∈ K[X], u ∈ ℒ(E), P ∧ Q = 1 ⇒ $\ker PQ(u) = \ker P(u) \oplus \ker Q(u)$.

Ca 41 : $u \in \mathcal{L}(E)$, il existe $x \in E / \pi_u = \pi_{u,x}$

Thm 42 (Frobenius) : $u \in \mathcal{L}(E)$, il existe une unique suite de polynômes $P_1 \dots P_r$ tq $P_1 | \dots | P_r$ et une base où la matrice de u est $\begin{pmatrix} C_{P_1} & & (0) \\ & \ddots & \\ (0) & & C_{P_r} \end{pmatrix}$ où C_{P_i} est la matrice compagnon de P_i (Frobenius)