Anneaux principaux - Applications

Dans toute la suite A est un anneau commutatif unitaire.

I. Anneaux factoriels

Définition : $a \in A \setminus \{0\}$ est dit
- **premier** s'il vérifie l'une des deux propositions suivantes :
  - $a \notin A^\times$ et si pour $b, c \in A$, $a \mid bc \Rightarrow a \mid b$ ou $a \mid c$
  - (a) est un idéal premier (ie $xy \in (a) \Rightarrow x \in (a)$ ou $y \in (a)$)
- **irréductible** s'il vérifie l'une des deux propositions suivantes :
  - $a \notin A^\times$ et si pour $b, c \in A$, $a = bc \Rightarrow b \in A^\times$ ou $c \in A^\times$
  - (a) est maximal parmis les idéaux principaux de A.

  (rappel : un idéal est dit principal s'il est engendré par un seul élément).

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

Proposition : Si A est intègre, alors premier $\Rightarrow$ irréductible

Définition : A est dit factoriel si
(*) A est intègre
(E) $\forall a \in A$, $a \neq 0$, a peut s'écrire sous la forme $a = \varepsilon_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$ avec $\varepsilon_a \in A^\times$, $v_p(a) \in \mathbb{N}$, les $v_p(a)$ nuls sauf un nombre fini et avec $\mathcal{P}$ un système de représentants des irréductibles de A (ie les irréductibles modulo un inversible de A).
(U) l'écriture ci-dessus est unique.

Exemples :
- $\mathbb{Z}$ est factoriel en prenant pour $\mathcal{P}$ l'ensemble des nombres premiers > 0.
- $\mathbb{K}[X]$, avec $\mathbb{K}$ corps commutatifs, avec $\mathcal{P}$ l'ensemble des polynômes unitaires irréductibles
- $\mathbb{Z}[X]$, $\mathbb{K}[X, Y]$ sont factoriels

Théorème : A factoriel $\Rightarrow A[X]$ factoriel

Définition : A est dit noethérien si tout idéal de A est de type fini.

Proposition : A noethérien et intègre $\Rightarrow$ A vérifie (E).

Proposition : A intègre vérifiant (E). Les conditions suivantes sont équivalentes :
(1) A vérifie (U)
(2) le lemme d'Euclide : p irréductible et $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$
(3) p irréductible $\Leftrightarrow$ (p) premier ($\Leftarrow$ p premier)
(4) le théorème de Gauss $a \mid bc$ et a premier avec $b \Rightarrow a \mid c$

II Anneaux principaux - PGCD - PPCM

Définition : A est dit principal s'il est intègre et si tout idéal de A est principal.

Exemples : $\mathbb{Z}$, $\mathbb{K}[X]$ avec $\mathbb{K}$ corps commutatif sont principaux

Proposition : A principal $\Rightarrow$ A factoriel

Proposition : $A[X]$ principal $\Leftrightarrow$ A est un corps

II.1) PGCD dans les anneaux principaux

Définition : A principal, $x_1, \dots, x_n \in A$, $d \in A$ est un pgcd de $x_1, \dots, x_n$ si $\forall i \in [\![1, n]\!]$, $d \mid x_i$ et si pour tout diviseur δ de $x_1, \dots, x_n$ on a $\delta \mid d$
Si d est un pgcd de $x_1, \dots, x_n$ alors les pgcd sont exactement les $d\varepsilon$, $\varepsilon \in A^\times$.

Proposition : A anneau principal, $x_1, \dots, x_n \in A$. Alors les pgcd de $x_1, \dots, x_n$ sont exactement les générateurs de l'idéal $(x_1) + \dots + (x_n)$. On note $\operatorname{pgcd}(x_1, \dots, x_n)$ l'un de ces pgcd.

Théorème de Bezout : $x_1, \dots, x_n \in A$, A anneau principal
$\text{pgcd}(x_1, \dots, x_n) = 1 \iff \exists\, u_1, \dots, u_n \in A,\ u_1 x_1 + \dots + u_n x_n = 1$

Remarque : dans le cas $\text{pgcd}(x_1, \dots, x_n) = d \neq 1$ on a seulement
$\text{pgcd}(x_1, \dots, x_n) = d \Rightarrow \exists\, u_1, \dots, u_n \in A,\ u_1 x_1 + \dots + u_n x_n = d$

Définition : A principal, $x_1, \dots, x_n \in A$. On dit que $x_1, \dots, x_n$ sont premiers entre-eux dans leur ensemble si 1 est un pgcd de $x_1, \dots, x_n$.

Proposition : A principal, p élément premier de A, $a \in A$.
Alors ou bien $p \mid a$ ou bien $\text{pgcd}(p, a) = 1$

II.2) PPCM dans les anneaux principaux

Définition : A anneau principal, $x_1, \dots, x_n \in A$. $m \in A$ est un ppcm de $x_1, \dots, x_n$ si $\forall i \in [\![1, n]\!]$, $x_i \mid m$ et $\forall x \in A$ tq $\forall i \in [\![1, n]\!]$, $x_i \mid x$ alors $m \mid x$
Si m est un ppcm de $x_1, \dots, x_n$ tous les ppcm de $x_1, \dots, x_n$ sont exactement les $m\varepsilon$, $\varepsilon \in A^\times$.

Proposition : A principal, $x_1, \dots, x_n \in A$. Alors les générateurs de l'idéal $(x_1) \cap \dots \cap (x_n)$ sont exactement les ppcm de $x_1, \dots, x_n$. On note $\text{ppcm}(x_1, \dots, x_n)$ l'un de ces ppcm.

Corollaire : A principal, $a, b \in A$. $(ab) = (\text{ppcm}(a,b)\ \text{pgcd}(a,b))$

Corollaire : A principal, $x_1, \dots, x_n \in A \setminus \{0\}$. Alors on a l'équivalence
i) $x_1 x_2 \dots x_n = \text{ppcm}(x_1, \dots, x_n)$
ii) $1 = \text{pgcd}(x_i, x_j)$ pour $i \neq j$

Théorème : A anneau principal, $a, b \in A \setminus \{0\}$
$a = \varepsilon_a \prod_{p \in S} p^{\alpha_a(p)}$, $b = \varepsilon_b \prod_{p \in S} p^{\alpha_b(p)}$ leurs factorisation en produit d'irréductibles.
Alors $\text{pgcd}(a,b) = \prod_{p \in S} p^{\inf(\alpha_a(p), \alpha_b(p))}$
$\text{ppcm}(a,b) = \prod_{p \in S} p^{\sup(\alpha_a(p), \alpha_b(p))}$

III Anneaux euclidiens

III.1) Généralités

Définition : A est dit euclidien s'il est intègre et s'il existe une application, appelée stathme euclidien sur A :
$\varphi : A^* = A \setminus \{0\} \longrightarrow \mathbb{N}$ vérifiant
i) $\forall (a,b) \in (A^*)^2$, $\exists (q, r) \in A^2$, $a = bq + r$, avec $r = 0$ ou $\varphi(r) < \varphi(b)$
ii) $\forall a, b \in A^*$, $a \mid b \Rightarrow \varphi(a) \leq \varphi(b)$

Proposition : A euclidien $\Rightarrow$ A principal

Exemples : $\mathbb{Z}$ avec $\varphi(\cdot) = |\cdot|$ est euclidien
$\mathbb{K}[X]$ pour $\mathbb{K}$ corps commutatif en prenant pour φ le degré
$\mathbb{Z}[i] = \{a + ib,\ (a,b) \in \mathbb{Z}^2\}$ en prenant pour φ le module

Proposition : A anneau euclidien. $\forall x \in A$, $x \notin A^\times$ tq la restriction à $A^\times \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.

Proposition : $\mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right]$ est principal mais non euclidien (DÉV)

III. 2) Algorithme de calcul dans les anneaux euclidiens

Théorème : Algorithme d'Euclide : A euclidien, φ un stathme sur A.
$(a,b) \in (A^*)^2$, on pose $u_0 = a$ et $u_1 = b$
Supposons u_p construit, $p \geq 1$ on construit alors u_{p+1} :
- si $u_p = 0$ alors l'algorithme s'arrête
- sinon on effectue la division euclidienne de u_{p-1} par u_p : $u_{p-1} = q_p u_p + u_{p+1}$ avec $u_{p+1} = 0$ ou $\varphi(u_{p+1}) < \varphi(u_p)$

Alors l'algorithme s'arrête pour un indice p_0 et $\text{pgcd}(a,b) = u_{p_0-1}$.
L'algorithme permet de déterminer un couple $(u,v) \in A^2$ tel que $au + bv = \text{pgcd}(a,b)$.

Exemple : $(a,b) \in \mathbb{N}^{*2}$. Dans $\mathbb{R}[X]$ on a :
$\text{PGCD}(X^a - 1, X^b - 1) = X^{\text{pgcd}(a,b)} - 1$

IV. Applications

IV.1. En arithmétique :

Théorème chinois : A anneau principal, $(a,b) \in A^2$, $\text{pgcd}(a,b) = 1$
Alors $A/(ab) \simeq A/(a) \times A/(b)$

Equation diophantienne du premier degré :
A anneau principal, $(a,b,c) \in A^3$. L'équation $ax + by = c$ possède des solutions ssi $\text{pgcd}(a,b) \mid c$.

Théorème des deux carrés : $n \in \mathbb{N}^*$, $n \neq 1$, $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$
Alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3 \pmod 4$ avec $\Sigma = \{x^2 + y^2 ; x,y \in \mathbb{Z}\}$

DÉV

IV.2. En algèbre :

Théorème de décomposition des noyaux :
$f \in \mathcal{L}(E)$, $P = P_1 \dots P_k \in \mathbb{K}[X]$, les P_i étant premiers deux à deux. Alors $\ker P(f) = \ker P_1(f) \oplus \dots \oplus \ker P_k(f)$

Facteurs invariants d'une matrice à coeff dans A
A anneau euclidien, $U \in \mathcal{M}_{m,n}(A)$
Alors il existe une famille $(d_1, \dots, d_s)$ d'éléments non nuls de A vérifiant
- $d_s \mid \dots \mid d_1$
- et telle que U soit équivalente à la matrice

$$D = \begin{pmatrix} d_s & & & 0 \\ & \ddots & & \\ & & d_1 & \\ 0 & & & 0 \end{pmatrix}$$

ie $\exists (P,Q) \in GL_m(A) \times GL_n(A)$, $U = PDQ$

Références :

- Groupes et anneaux D. Guin
- Contre exemples : Hauchecorne
- Les maths en tête - Algèbre - Xavier Gourdon
- Cours d'Algèbre - Daniel Perrin
- Anneaux - Jean Fresnel
- Objectif Agrégation - Beck, Malick, Peyré