122

# Anneaux principaux. Applications.

Tous les anneaux $A$ considérés sont commutatifs et unitaires. On note $A^*$ le groupe multiplicatif des inversibles de $A$.

## I - Notion de principalité.

**Def 1** : Si $x$ est un élément d'un anneau $A$ on note $(x)$ ou $xA$ l'idéal de $A$ engendré par $x$ :

$$(x) = \{y \in A \,;\, \exists z \in A,\ y = xz\}.$$

Un tel idéal est dit principal

**Def 2** : Un anneau $A$ est dit principal si $A$ est intègre et tout idéal de $A$ est principal.

**Expl 3** : • $\mathbb{Z}$ est principal, ses idéaux sont les $n\mathbb{Z}$, $n \in \mathbb{N}$.

• Un corps est trivialement principal, ses idéaux sont $(0)$ et $(1)$

• Pour $n$ non premier, $\mathbb{Z}/n\mathbb{Z}$ n'est PAS principal, car non intègre. (pourtant tous ses idéaux sont principaux comme image des idéaux de $\mathbb{Z}$ par le morphisme surjectif $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$).

**Def 4** : Un anneau intègre $A$ est dit euclidien s'il existe $v : A\setminus\{0\} \to \mathbb{N}$ tel que $\forall a,b \in A \times A\setminus\{0\}$, $\exists q, r \in A$, $a = bq + r$ et ou bien $r = 0$, ou bien $v(r) < v(b)$.

La fonction $v$ est appelée le stathme de $A$.

**Thm 5** : Tout anneau euclidien est principal.

**Expl 6** : exemples d'anneaux euclidiens avec leurs stathmes :

$\mathbb{Z}$, $v = |.|$, $K[X]$, $v =$ degré

$\mathbb{Z}[i]$, $\mathbb{Z}[j]$, $v = |.|^2$.

$D = \mathbb{Z}[1/10]$, $v(p\, 2^n 5^m) = |p|$

**Contre-expl 7** : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal non euclidien.

**Thm 8** : $A[X]$ principal $\Leftrightarrow$ $A$ est un corps.

**Expl 9** : • $\mathbb{Z}[X]$ non principal, $(2, X)$ est un exemple d'idéal non principal.

• $K[X_1, .., X_n]$ est principal ssi $n = 1$, $I = (X_1, X_2)$ est non principal dès que $n \geq 2$.

## II - Divisibilité

**Def 10** : Soient $a, b \in A$. On dit que $b$ divise $a$ s'il existe $q \in A$ tel que $a = bq$. On note $b \mid a$.

**Prop 11** : $b \mid a$ ssi $(b) \supset (a)$.

**Déf 12** : $a, b \in A$ sont associés s'il existe $c \in A^*$ tel que $a = cb$ (et donc $b = c^{-1}a$)

**Prop 13** : $a$ et $b$ sont associés ssi $(a) = (b)$.

**Déf 14** : • Un élément $p \in A$ est irréductible si $p \notin A^*$ et $p = ab$ implique $a \in A^*$ ou $b \in A^*$.

• $p \in A$ est premier si $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

**Prop 15** : Dans un anneau intègre $A$, $\forall p \neq 0$ dans $A$, $p$ premier $\Rightarrow$ $p$ irréductible.

**Exple 16** : • Dans $\mathbb{Z}[i\sqrt{5}]$, 2 est irréductible mais pas premier, car $(1+i\sqrt{5})(1-i\sqrt{5}) = 2.3$.

• Dans $\mathbb{Z}/6\mathbb{Z}$, 2 est premier mais pas irréductible car $2 = 2.4$.

**Thm 17** : Les irréductibles de $\mathbb{Z}[i]$ sont, aux inversibles près :
• les entiers premiers $p \in \mathbb{N}$ avec $p \equiv 3\ [4]$
• les $a+ib$ avec $a^2+b^2$ premier.

**Déf 18** : Un anneau $A$ est factoriel si $A$ est intègre et : (1) Tout élément $a \neq 0$ de $A$ s'écrit $a = u p_1 \cdots p_r$ avec $u \in A^*$, $p_1, \dots, p_r$ irréductibles
(2) Cette écriture est unique à permutation et inversibles près.

**Prop 19** : Dans un anneau factoriel $p$ irréductible $\Rightarrow$ $p$ premier.

**Thm 20** : Tout anneau principal est factoriel.

**Thm 21** : Si $A$ est factoriel, alors $A[X]$ est factoriel.

**Déf 22** : Dans un anneau $A$ factoriel, si $a = u \prod p^{v_p(a)}$ et $b = v \prod p^{v_p(b)}$, on pose

$PGCD(a,b) = \prod p^{\min(v_p(a), v_p(b))}$

$PPCM(a,b) = \prod p^{\max(v_p(a), v_p(b))}$

Ces éléments sont définis à un inversible près.

**Thm 23** (Bezout) Dans un anneau principal $A$, si $d = PGCD(a,b)$, on a $(d) = (a,b)$.
Autrement dit $\exists u, v \in A$, $d = au + bv$ ("relation de Bezout").

**Contre-exemple 24** : Dans $K[X,Y]$, $1 \notin (X,Y)$ même si $PGCD(X,Y) = 1$.

**Cor 25** : Soient $a, b \in A$ avec $A$ principal. Alors $a, b$ premiers entre eux ssi $\exists u, v \in A$, $au + bv = 1$.

## III - Applications

DEV 1

### (a) Lemme des noyaux

**Lemme 26** : Soit $E$ un $K$-ev, $u \in \mathcal{L}(E)$ et $P = \prod P_i$ un polynôme annulateur de $u$ avec les $P_i$ 2 à 2 premiers entre eux.
Alors $E = \operatorname{Ker} P(u) = \bigoplus \operatorname{Ker} P_i(u)$
De plus si $\pi_i \in \mathcal{L}(E)$ est la projection sur le facteur $\operatorname{Ker} P_i(u)$, alors $\pi_i$ est un polynôme en $u$.

**Application 27** : Calcul d'exponentielle de matrices, comme $\exp\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} e & e^2 - e \\ 0 & e^2 \end{pmatrix}$.

**Thm 28** (Dunford) : Soit $u \in \mathcal{L}(E)$ de polynôme minimal scindé. Alors on peut écrire $u = d + n$ avec $d$ diagonalisable, $n$ nilpotente, $dn = nd$. De plus $d, n$ sont uniques, et sont des polynômes en $u$.

### (b) Polynôme minimal :

**Def 29** : Soit $u \in \mathcal{L}(E)$ et $I = \{P \in K[X],\ P(u) = 0\}$. Comme $K[X]$ est principal, $I = (P)$ pour un unique polynôme unitaire $P$, appelé polynôme minimal de $u$.

**Def 30** : De façon similaire, si $x \in E$ et $J = \{P \in K[X];\ P(u)(x) = 0\}$, le générateur unitaire de $J$ est appelé polynôme minimal ponctuel de $u$ en $x$.

**Def 31** : Si $L = K(\alpha)$ est une extension algébrique de corps, le générateur unitaire de $I = \{P \in K[X];\ P(\alpha) = 0\}$ est appelé polynôme minimal de $\alpha$ sur $K$.

### (c) Systèmes linéaires sur $\mathbb{Z}$.

**Lemme 32** : Soit $a, b \in \mathbb{Z}$. $\exists M \in SL_2(\mathbb{Z})$ tel que $(a\ b)M = (0\ d)$ avec $d = \mathrm{PGCD}(a,b)$.

**Def 33** : Une matrice $M \in \mathcal{M}_{m,n}(\mathbb{Z})$ est sous forme normale de Hermite s'il existe $r \geq 0$ et $f : [\![r+1, n]\!] \to [\![1, m]\!]$ croissante telle que les $r$ premières colonnes de $M$ soient nulles, $m_{f(j),j} \geq 1\ \forall j$, $m_{i,j} = 0$ pour $i > f(j)$ et $0 \leq m_{f(j),k} < m_{f(j),j}$ pour $k > j$.

**Exple 34** : $\begin{pmatrix} 6 & -8 & -9 \\ \boxed{2} & 1 & 0 \\ 0 & \boxed{4} & 3 \\ 0 & 0 & \boxed{3} \end{pmatrix} \quad \begin{pmatrix} 0 & \boxed{2} & 1 \\ 0 & 0 & -5 \\ 0 & 0 & \boxed{1} \end{pmatrix} \quad \begin{pmatrix} 0 & \boxed{1} \\ 0 & 0 \end{pmatrix}$

DEV 2

**Thm 35** : Soit $A \in \mathcal{M}_{m,n}(\mathbb{Z})$. Alors $\exists!\ B \in \mathcal{M}_{m,n}(\mathbb{Z})$ sous forme normale de Hermite, et $\exists U \in GL_n(\mathbb{Z})$ tel que $AU = B$.

**Application 36** : On cherche à résoudre l'équation sur $\mathbb{Z}$ : $2x + 3y + 5z = 0$. Le théorème appliqué à $A = (2\ 3\ 5)$ donne $\underbrace{(2\ 3\ 5)}_{A} \cdot \underbrace{\begin{pmatrix} -4 & -3 & 1 \\ 1 & 2 & 1 \\ 1 & 0 & 0 \end{pmatrix}}_{U} = \underbrace{(0\ 0\ 1)}_{=B}$, et Sol $= \mathbb{Z}\begin{pmatrix} -4 \\ 1 \\ 1 \end{pmatrix} + \mathbb{Z}\begin{pmatrix} -3 \\ 2 \\ 0 \end{pmatrix}$