Anneaux principaux. Applications.

122

Cadre : Par la suite, $A$ désignera un anneau commutatif.

# I) Anneaux principaux

## A] Idéaux d'un anneau

[2]

**Def 1 :** Un idéal de $A$ est un sous-groupe $(I,+)$ de $(A,+)$ tel que : $\forall x \in I, \forall a \in A, ax \in I$. Si $\exists a \in I, I = \{ax \mid x \in A\}$, on note $I = (a)$ et on dit que $I$ est engendré par $a$.

**Ex 2 :** $\forall n \in \mathbb{N}^*$, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

**Prop 3 :** Une intersection d'idéaux est un idéal. Une somme finie d'idéaux est un idéal.

**Prop-def 4 :** Soit $I$ un idéal de $A$. Alors on peut munir $A/I$ d'une structure d'anneau.

**Def 5 :** Un idéal $I$ de $A$ est dit premier si $\forall a, b \in A$, $ab \in I \Leftrightarrow a \in I$ ou $b \in I$.

**Ex 6 :** $\forall n \in \mathbb{N}^*$, $n\mathbb{Z}$ est premier si et seulement si $n$ est premier.

**Prop 7 :** $I$ premier $\Leftrightarrow A/I$ intègre

**Def 8 :** Un idéal $I$ de $A$ est dit maximal si $I \neq A$ et si $J$ est un idéal tel que $I \subsetneq J$, alors $J = A$.

[1]

**Prop 9 :** $I$ est maximal si et seulement si $A/I$ est un corps. En particulier, si $I$ est maximal, $I$ est premier.

## B] Idéaux et anneaux principaux

**Def 10 :** Un idéal $I$ de $A$ est principal si il est engendré par un élément. $A$ est dit principal si tous les idéaux de $A$ sont principaux et est intègre.

**Ex 11 :** $(\mathbb{Z}, +, \times)$ est un anneau principal.

Par la suite, $A$ sera supposé intègre.

**Thm 12 :** $A[X]$ est principal si et seulement si $A$ est un corps.

**Ex 13 :** $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont principaux. En revanche $\mathbb{Z}[X]$ et $\mathbb{R}[X,Y]$ ne le sont pas.

**App 14 :** Si $\alpha \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$, l'idéal des polynômes annulateurs est engendré par un unique $\pi_\alpha \in \mathbb{Q}[X]$ unitaire et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg \pi_\alpha$.

**Def 15 :** Soit $p \in A$.

- $p$ est dit inversible si $\exists q \in A, p.q = q.p = 1$. On note $A^\times$ l'ensemble des inversibles.
- $p$ est irréductible si $p \notin A^\times$ et : $\forall a, b \in A, p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$

**Prop 16 :** Soit $p \notin A^\times$. Si $A$ est principal, alors, $p$ irréductible $\Leftrightarrow (p)$ premier $\Leftrightarrow (p)$ maximal

App : Berlekamp (PEV)

## C] Cas particulier : les anneaux euclidiens

**Def 17 :** $A$ est dit euclidien s'il existe $\delta : A \setminus \{0\} \to \mathbb{N}$ appelé stathme euclidien tel que $\forall a, b \in A \setminus \{0\}, \exists q, r \in A$, $a = qb + r$ et $(r = 0$ ou $\delta(r) < \delta(q))$

**Ex 18 :** $\mathbb{Z}$ muni de $|.|$ est euclidien.

**Thm 19 :** Tout anneau euclidien est principal.

**Prop 20 :** Soit $P \in A[X]$, $P \neq 0$, de coefficient dominant inversible. Alors $\forall F \in A[X], \exists Q, R \in A[X]$ tels que $F = PQ + R$ et $\deg R < \deg P$ ou $R = 0$.

**Cor 21 :** Si $k$ est un corps, $k[X]$ est euclidien, avec le degré comme stathme.

## II] Arithmétique

### A] Divisibilité

**Def 22 :** Soient $a, b \in A$. On dit que $a$ divise $b$, noté $a|b$, si $\exists c \in A \,/\, b = ac$.

**Prop 23 :** $a|b \Leftrightarrow (b) \subset (a)$

[1] **Def 24 :** Soient $a, b \in A$. $a$ et $b$ sont dits associés si $\exists u \in A^\times$, $a = bu$.

**Prop 25 :** Si $A$ est intègre, $a$ et $b$ sont associés si et seulement si ils se divisent mutuellement.

**Def 26 :** $a, b \in A$ sont dits premiers entre eux si :
$\forall d \in A$, $d|a \wedge d|b \Rightarrow d \in A^\times$.

### B] Anneaux factoriels

**Def 27 :** $A$ est dit factoriel s'il est intègre et que $\forall a \in A$, $\exists u \in A^\times$, $\exists p_1, \dots, p_r \in A$ irréductibles tels que $a = u\, p_1 \dots p_r$ et que cette décomposition est unique à un inversible près.

**Ex 28 :** $\mathbb{Z}$ est factoriel.

[1] **Thm 29 :** Soit $A$ un anneau intègre vérifiant l'existence de cette décomposition. On a équivalence entre :
- $A$ vérifie l'unicité
- $A$ vérifie le lemme d'Euclide : si $p \in A$ est irréductible, $\forall a, b \in A$, $p|ab \Rightarrow p|a$ ou $p|b$
- $\forall p \in A$, $p$ est irréductible si et seulement si $(p)$ est premier.
- $A$ vérifie le lemme de Gauss : si $a|bc$ et que $a$ et $b$ sont premiers entre eux, alors $a|c$.

**Cor 30 :** Si $A$ est principal, il est factoriel.

Euclidien $\Rightarrow$ Principal $\Rightarrow$ Factoriel

**Ex 31 :** Si $k$ est un corps, $k[X]$ est factoriel.

### C] Conséquences de la factorialité

**Def 32 :** Soient $a$ et $b$ dans $A$ supposé factoriel.
- Si $p$ est irréductible, on appelle valuation $p$-adique de $a$ l'ordre de $p$ dans sa décomposition en irréductibles, notée $v_p(a)$
- On pose $PGCD(a,b) = \prod p^{\min(v_p(a), v_p(b))}$, $PPCM(a,b) = \prod p^{\max(v_p(a), v_p(b))}$, définis à un inversible près.

**Prop 33 :** Si $A$ est principal, $\forall a, b \in A$, si $d = PGCD(a,b)$ alors $(a) + (b) = (d)$. En particulier, si $a$ et $b$ sont premiers entre eux, $(a) + (b) = A$. (Lemme de Bezout)
Remarque : $(X) + (Y) \neq k[X,Y]$

**Lem 34 :** (Chinois) Si $p, q \in A$ sont premiers entre eux, alors $\frac{A}{(pq)} \simeq \frac{A}{(p)} \times \frac{A}{(q)}$. En particulier, si $a \in A$ et $A$ est factoriel, on a une décomposition de $\frac{A}{(a)}$

**Lem 35 :** (de Gauss) Soient $P, Q \in A[X]$. On suppose $A$ principal et on définit $c(P)$ le contenu de $P$, c'est-à-dire le PGCD de ses coefficients. Alors $c(PQ) = c(P)c(Q)$.

**Thm 36 :** (critère d'Eisenstein) Si $A$ est factoriel, soient $k = \mathrm{Frac}(A)$ et $P(X) = a_0 + a_1 X + \dots + a_n X^n \in A[X]$. On suppose qu'il existe $p \in A$ irréductible tel que :
- $\forall i \in [\![0; n-1]\!]$, $p | a_i$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Alors $P$ est irréductible dans $k[X]$ (dans $A[X]$ si $c(P) = 1$)

Ceci donne un critère pour trouver des irréductibles de $A[X]$.

## III) Exemples remarquables

### A] Entiers de Gauss

[1]

**Def 37 :** On définit l'anneau des entiers de Gauss par : $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$.

C'est un sous-anneau intègre de $\mathbb{C}$.

**Thm 38 :** $\mathbb{Z}[i]$ est euclidien et $\mathbb{Z}[i]^\times = \{\pm 1 ; \pm i\}$

**App 39 :** (Théorème des deux carrés) Soit $\Sigma = \{a^2+b^2 \mid a, b \in \mathbb{N}\}$ et soit $p \in \mathbb{N}$ premier. Alors $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1 [4]$

DEV 2

### B] Anneau de polynômes et diagonalisation

[2]

Soient $k$ un corps et $E$ un $k$-espace vectoriel de dimension finie. Soit $f \in \mathcal{L}(E)$.

**Thm 40 :** L'ensemble des polynômes annulateurs de $f$ est un idéal non vide de $k[X]$. On note $\Pi_f$ son unique générateur unitaire, appelé polynôme minimal de $f$.

**Prop 41 :** $\forall \lambda \in k, \lambda \in Sp(f) \Leftrightarrow \Pi_f(\lambda) = 0$

**Thm 42 :** (de décomposition des noyaux) Soient $P$ et $Q$ dans $k[X]$ premiers entre eux. Alors

$$\operatorname{Ker} PQ(f) = \operatorname{Ker} P(f) \oplus \operatorname{Ker} Q(f)$$

De plus, les projections respectives sont des polynômes en $f$.

[2]

**Thm 43 :** $f$ est diagonalisable si et seulement si $\Pi_f$ est scindé à racines simples dans $k[X]$.

**Thm 44 :** $f$ est trigonalisable si et seulement si $\Pi_f$ est scindé dans $k[X]$.

**Thm 45 :** (décomposition de Dunford) Si $\Pi_f$ est scindé, alors $\exists! (d, n) \in \mathcal{L}(E)^2$ avec $d$ diagonalisable, $n$ nilpotente, tels que :

$$\begin{cases} f = d+n \\ dn = nd \end{cases}$$


Références :

- Cours d'algèbre, Perrin [1]
- Algèbre, Gourdon [2]