Leçon 122 : Anneaux principaux. Exemples et applications.

Pauline BESSERVE

Références : Perrin, Combes, Calais

Dans ce qui suit, A désigne un anneau commutatif unitaire et intègre.

I. Définitions et propriétés

1. Arithmétique dans un anneau

• Déf.1 : Soit $a,b \in A$. On dit que a divise b et on note $a|b$ ssi $\exists c \in A \,/\, b = ac$.

• Déf.2 : Soit $a \in A$, on dit que a est inversible s'il existe $b \in A \,/\, ab = 1$. On notera $A^\times = \{a \in A$ inversibles$\}$

• Déf.3 : Soit $a,b \in A$. On dit que d est un pgcd de a et b si $d|a$, $d|b$ et $\forall c \in A \,/\, c|a$ et $c|b$, on a $c|d$. On dit que m est un ppcm de a et b si $a|m$, $b|m$ et $\forall c \in A \,/$ $a|c$ et $b|c$, on a $m|c$.

• Déf.4 : On dit que $a,b \in A$ sont premiers entre eux si 1 est un pgcd de a et b.

• Déf.5 : Soit $a \in A^\times$, on dit que a est premier si $\forall b \in A$, $c \in A \,/\, a|bc$, on a $a|b$ ou $a|c$. On dit que a est irréductible si $a = bc \Rightarrow b \in A^\times$ ou $c \in A^\times$.

• Prop.6 : Si $a \in A^\times$ est premier, alors a est irréductible.

• Prop.7 : $a \in A^\times$ est premier ssi $A/(a)$ est intègre.

2. Anneaux principaux

• Déf.8 : Un idéal I de A est dit principal s'il est engendré par un seul élément $a \in A$. On note $I = (a)$.

• Déf.9 : A est principal si tous ses idéaux sont principaux.

Ex.10 : $\mathbb{Z}$, $\mathbb{K}[X]$ ($\mathbb{K}$ corps) sont principaux.

• Prop.11 : Si A est principal, alors tout élément a de $A \setminus \{0\}$ se décompose de manière unique à permutation près des facteurs et à multiplication par des inversibles près sous la forme $a = u p_1 \cdots p_s$ avec $u \in A^\times$ et $p_1, \dots, p_s$ irréductibles.
Cela traduit qu'un anneau principal est factoriel.

Ex.12 : Dans $\mathbb{N}$ cela correspond au théorème fondamental de l'arithmétique.

Rq 13 Un anneau factoriel n'est pas nécessairement principal.
Contre-ex 14 $\mathbb{Z}[X]$ est factoriel mais pas principal ($(2,X)$ est un idéal non principal).

• Prop.15 : (Théorème de Bezout) Soit A principal et $a,b \in A$. Alors il existe $d \in A \,/\, (a,b) = (d)$ et d est un pgcd de a, b. De plus il existe $u, v \in A \,/\, au + bv = d$.

Ex.16 Dans $\mathbb{Z}$, $a = 6$ et $b = 9$: $3 = 2 \times 6 - 1 \times 9$.

• Prop.16 : (Théorème chinois) Soit $a_1, \dots, a_m \in A$ principal, premiers entre eux deux à deux. Alors :
$A/(a_1 \cdots a_m) \cong A/(a_1) \times \cdots \times A/(a_m)$.

• Prop.17 : Soit $p \in A$ principal. Alors p est irréductible ssi $A/(p)$ est un corps, ssi $A/(p)$ est intègre.

3. Anneaux euclidiens

• Déf.18 : A est euclidien s'il existe une application $N : A \setminus \{0\} \to \mathbb{N}$ ~~telle que~~ $\forall a,b \in A$ avec $b \neq 0$, $\exists q, r \in A \,/$ $a = qb + r$ et $N(r) < N(b)$ ou $r = 0$.
N est appelé stathme euclidien.

Ex.19 : $\mathbb{Z}$ est euclidien pour la valeur absolue.
$\mathbb{K}[X]$ est euclidien pour le degré.

• Prop 20 : Un anneau euclidien est principal.

Rq 21 : En pratique, souvent pour montrer A principal on montre A eucl.

contre-ex 22 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.

II. Exemples et applications

1. Anneau des entiers de Gauss et théorème des 2 carrés

• Déf. 23 : L'anneau $\mathbb{Z}[i] = \{a+ib,\ a,b \in \mathbb{Z}\}$ est appelé anneau des entiers de Gauss.

• Prop. 24 : $\mathbb{Z}[i]$ est euclidien pour le stathme $N : z = a+ib \mapsto z\bar{z} = a^2+b^2$.

• Prop. 25 : $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$.

• Déf. 26 : On note $\Sigma = \{m = a^2+b^2,\ a,b \in \mathbb{N}\}$.

DVP

• Lemme 27 : Σ est stable par multiplication.

• Lemme 28 : Soit $p \in \mathbb{N}$ premier. Alors on a : $p \in \Sigma$ ssi $p = 2$ ou $p \equiv 1\ [4]$.

• Th. 29 : (Théorème des 2 carrés) Soit $m \in \mathbb{N}$. m se décompose sous la forme $m = \prod_{i=1} p_i^{\alpha_i}$ où les p_i sont premiers et deux à deux distincts. Alors $m \in \Sigma$ ssi α_i pair $\forall i \,/\, p_i \equiv 3\ [4]$.

2. Application de la principalité de $\mathbb{K}[X]$ à l'algèbre linéaire

• Prop 30 : $\mathbb{K}[X]$ muni du stathme $N(P) = \deg P$ est euclidien.

Ex. 31 : Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et de degré 2 sans racine réelle.

• Prop. 32 : $\mathbb{K}[X]^\times = \{a \in \mathbb{K}\setminus\{0\}\}$.

• Prop 33 (polynôme minimal) : Soit E un ev de dimension finie sur le corps $\mathbb{K}$. Soit $u \in \mathcal{L}(E)$. On définit φ_u :

$$\begin{aligned} \mathbb{K}[X] &\rightarrow \mathcal{L}(E) \\ P &\overset{\varphi_u}{\mapsto} P(u) \end{aligned}$$

$\mathrm{Ker}(\varphi_u)$ est un idéal de l'anneau principal $\mathbb{K}[X]$ donc $\exists \Pi_u \in \mathbb{K}[X] \,/\, \mathrm{Ker}\,\varphi_u = \Pi_u$. Π_u est appelé polynôme minimal de u. Il divise tout annulateur de u.

• Prop 34 : $u \in \mathcal{L}(E)$ est diagonalisable ssi Π_u est scindé à racines simples sur $\mathbb{K}$.

• Lemme 35 : (Lemme des noyaux) Soit $P = P_1 \cdots P_r$ avec $\forall i \neq j$, P_i et P_j premiers entre eux. Alors :

$$\mathrm{Ker}\, P(u) = \bigoplus_{i=1}^{k} \mathrm{Ker}\, P_i(u).$$

En particulier si $P(u) = 0$ on a

$$E = \bigoplus_{i=1}^{k} \mathrm{Ker}(P_i(u)).$$

3. Résolution d'équations diophantiennes

(E) $ax+by = c \qquad a,b,c \in \mathbb{Z}$

Rappel 36 : (Bezout) Soit $a,b \in A$ et d un pgcd de a et b. $\exists u,v \in A \,/\, d = au+bv$.

Prop. 37 : On note $d = \mathrm{pgcd}(a,b)$ et $u_0,v_0 \in A \,/\, d = au_0+bv_0$. On a alors :

• si $d \nmid c$, (E) n'a pas de solution

• si $c = \lambda d$, (E) admet des solutions de la forme :

$\left(\lambda u_0 + k\frac{b}{d},\ \lambda v_0 - k\frac{a}{d}\right),\ k \in \mathbb{Z}$.