Leçon N° 122 : Anneaux principaux. Exemples et applications

Dans toute cette leçon A désigne un anneau commutatif, unitaire.

I) Notion de principalité.

1) Idéaux et anneaux principaux

Définition 1 : Soit I un idéal de A. On dit que I est principal lorsqu'il existe $a \in A$ tel que $I = (a)$.

Définition 2 : On dit que A est principal lorsque A est intègre et lorsque tout idéal de A est principal.

Exemples 3 : 1) Tout corps est un anneau principal.

2) $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps commutatif sont principaux.

Théorème 4 : $A[X]$ est principal ssi A est un corps.

Exemple 5 : $\mathbb{K}$ corps commutatif. $\mathbb{K}[X,Y]$ est pas principal.

2) PGCD et PPCM.

Définition 6 : On dit que A est factoriel lorsqu'il vérifie

1) A est intègre

2) tout $a \in A \setminus \{0\}$ s'écrit $a = u p_1 \dots p_n$ avec $u \in A^*$ et $p_1, \dots, p_n$ irréductibles

3) Cette décomposition est unique à inversible et permutation près.

Définition 7 : Soit $P \subset A$. On dit que P est un système de représentants des irréductibles lorsque $\forall p$ irréductible $\in A$, $\exists ! q \in P$, $\exists ! u \in A^*$ tq $p = uq$.

Proposition 8 : A factoriel ssi A vérifie :

1) A est intègre

2) $\forall a \in A \setminus \{0\}$, $a = u \prod_{p \in P} p^{v_p(a)}$ avec $u \in A^*$, $v_p(a) \in \mathbb{N}$ presque tous nuls

3) Cette écriture est unique.

Proposition 9 : Un anneau principal est factoriel.

Définition 10 : Soient $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_r \in A^*$. On dit que ces éléments admettent un plus grand commun diviseur lorsqu'il $\exists\, \delta \in A^*$ tel que $\begin{cases} \forall i \in [\![1,r]\!],\ \delta \mid a_i \\ \text{tout diviseur commun à } a_1, \dots, a_r \text{ divise } \delta \end{cases}$.

Théorème 11 : Si A est factoriel (c'est le cas si A est principal), pour $a = u \prod_{i=1}^{r} p_i^{m_i}$ et $b = v \prod_{i=1}^{r} p_i^{n_i}$, a et b admettent un pgcd et $\operatorname{pgcd}(a,b) = \prod_{i=1}^{r} p_i^{\min(m_i,n_i)}$

Remarque 12 : On définit de manière analogue le plus petit commun multiple.

Lemme 13 : (Gauss) Si A est factoriel. Soit $(a,b) \in A^2 \setminus \{0\}$ $\operatorname{pgcd}(a,b) = 1$ ssi $\forall c \in A^*, (a \mid bc \Rightarrow a \mid c)$.

Théorème 14 : (Bézout) Si A est principal : Soit $r \in \mathbb{N} \setminus \{0,1\}$ et $a_1, \dots, a_r$ des éléments tous non nuls dans A. Ces éléments sont premiers entre eux dans leur ensemble ssi $\exists (u_1, \dots, u_r) \in A^r$ tel que $\sum_{i=1}^{r} u_i a_i = 1$.

Corollaire 15 : Si A est principal. Soient $(a_1, \dots, a_r)$ et c non nuls. Si c est premier avec chacun des a_i, $\forall i \in [\![1,r]\!]$, il est premier avec leur produit.

Application 16 : Si $(G, \cdot)$ est un groupe commutatif, $r \geq 2$ entier et $g_1, \dots, g_r$ des éléments deux à deux distincts de G d'ordre respectifs $m_1, \dots, m_r$. $\exists\, g \in G$ d'ordre égal au ppcm de ces ordres.

Théorème 17 : Tout sous groupe fini du groupe multiplicatif $\mathbb{K}^*$, $\mathbb{K}$ étant un corps commutatif est cyclique.

Corollaire 18 : $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K},\ \lambda^n = 1\}$ est un sous groupe cyclique de $\mathbb{K}^*$.

3) Théorème chinois

Théorème 19 : Si A est principal. Soit $(a_j)_{1\le j\le r}$ $r \ge 2$ des éléments non nuls et non inversibles.
$\forall j \in [\![1, r]\!]$, π_j désigne la surjection canonique de A sur $A/(a_j)$
Si les (a_j) sont premiers entre eux 2-à-2.

$$\Psi : A \longrightarrow \prod_{j=1}^{r} A/(a_j) \qquad x \longmapsto (\pi_j(x))_{1\le j\le r}$$

est un morphisme d'anneaux surjectif

de noyau $\ker(\Psi) = \left(\prod_{j=1}^{r} a_j\right)$

et Ψ induit un isomorphisme d'anneaux $\bar{\Psi} : A/\left(\prod_{j=1}^{r} a_j\right) \longrightarrow \prod_{j=1}^{r} A/(a_j)$

$\pi(x) \longmapsto (\pi_j(x))_{1\le j\le r}$

d'inverse $\bar{\Psi}^{-1} : (\pi_j(x_j))_{1\le j\le r} \mapsto \sum_{i=1}^{r} x_i u_i b_i$ où $\sum_{j=1}^{r} u_j b_j = 1$ et $b_j = \prod_{\substack{i=1 \\ i\neq j}} a_i$

Remarque 20 : Le théorème chinois peut être utilisé pour étudier un système d'équation diophantienne : $q \equiv a_j (n_j)$.
Dans le cas où $n_1, \dots, n_r$ sont premier entre eux 2-à-2, cela revient à trouver l'antécédent dans $\prod_{n\mathbb{Z}} \mathbb{Z}/n_j\mathbb{Z}$ de $(\pi_1(a_1), \dots, \pi_r(a_r))$ par l'isomorphisme $\Psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z}$.

$\pi_n(q) \longmapsto (\pi_1(q), \dots, \pi_r(q))$

Cet antécédent est q_0 où $q_0 = \sum_{i=1}^{r} a_i u_i m_i$ en désignant par (u_j) une suite tq $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$.

Les solutions sont sous $S = \{ q = q_0 + qn, q \in \mathbb{Z} \}$ où q_0 = sol particulière

Exemple 21 :
$$\begin{cases} q \equiv 2\,[4] \\ q \equiv 3\,[5] \\ q \equiv 1\,[9] \end{cases}$$

$S = \{ q = 818 + 1804\, q, q \in \mathbb{Z} \}$

II) Anneaux euclidiens

1) Définition et exemples

Définition 22 : A est dit euclidien lorsque :
1) A est intègre
2) $\exists\, v : A \setminus \{0\} \longrightarrow \mathbb{N}$ telle que $\forall (a,b) \in A \setminus \{0\}$,
$\exists q, r \in A$ avec $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$

Exemple 23 : 1) $\mathbb{Z}$ est euclidien avec le stathme $|\cdot|$
2) $\mathbb{K}[X]$ est euclidien pour le stathme degré.

Proposition 24 : Tout anneau euclidien est principal.

Proposition 25 : Si A est euclidien. $\exists x \in A$, $x \notin A^* \cup \{0\}$ tel que la restriction à $A^* \cup \{0\}$ de la projection canonique de A sur $A/(x)$ soit surjective.

2) Exemples et contre-exemples

Contre-exemple 26 : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais non euclidien.

Notations 27 : On introduit $\Sigma = \{ n \in \mathbb{N}, n = a^2 + b^2, (a,b) \in \mathbb{N}^2 \}$.
$\mathbb{Z}[i] = \{ a + ib, (a,b) \in \mathbb{Z}^2 \}$ sous anneau de $\mathbb{C}$ intègre
$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$
$z = (a+ib) \mapsto z\bar{z} = a^2 + b^2$

Lemme 28 : $\mathbb{Z}[i]^* = \{ \pm 1, \pm i \}$

Lemme 29 : Σ est stable par $\times$.

Proposition 30 : $\mathbb{Z}[i]$ est euclidien

Application 31 : Pour $p \in \mathcal{P}$. $p \in \Sigma$ ssi p pas irréductible dans $\mathbb{Z}[i]$
ssi $p = 2$ ou $p \equiv 1\,[4]$.
(Théorème des deux carrés)

III) Applications

1) En algèbre linéaire

Soient $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-ev de dimension $+\infty$ et $u \in \mathcal{L}(E)$.

Proposition 32 : $\exists!\, P_u \in \mathbb{K}[X]$ tel que $\{P \in \mathbb{K}[X] \mid P(u) = 0\} = (P_u)$

Lemme 33 : (des noyaux) Soit $r \geq 1$, $P_1, \dots, P_r \in \mathbb{K}[X]$ 2-à-2 premiers entre eux, $P = P_1 \dots P_r$
Alors $\forall u \in \mathcal{L}(E)$, 1) $\ker P(u) = \bigoplus_{i=1}^{r} \ker(P_i(u))$
2) Les projecteurs $q_j : \ker(P(u)) \longrightarrow (P_j(u))$ sont dans $\mathbb{K}[u]$.

Théorème 34 : (Dunford) Soit χ_u est scindé sur $\mathbb{K}$, alors
$\exists!\, (d, n) \in \mathcal{L}(E)$ tq 1) d est diagonalisable sur $\mathbb{K}$
2) n est nilpotente
3) $d + n = u$
4) d et n commutent.

De plus, $\det n \in \mathbb{K}[u]$.

2) En théorie des corps

Définition 35. Soient $\mathbb{K} \subset \mathbb{L}$ une extension de corps commutatifs, $\alpha \in \mathbb{L}$, $I_\alpha = \{P \in \mathbb{K}[X] \mid P(\alpha) = 0\}$ idéal annulateur de α.
On dit que α est algébrique sur $\mathbb{K}$ si $I_\alpha \neq \{0\}$, transcendant sinon.

Proposition 36 : Si α est algébrique, $\exists!\, P_\alpha \in \mathbb{K}[X]$ tq $I_\alpha = (P_\alpha)$
c'est le polynôme irréductible de $\mathbb{K}[X]$ annulateur de α.

Théorème 37 : $\forall \alpha \in \mathbb{L}$,
(α algébrique sur $\mathbb{K}$) ssi $(\mathbb{K}[\alpha] = \mathbb{K}(\alpha))$ ssi $([\mathbb{K}[\alpha] : \mathbb{K}] < +\infty)$

Théorème 38 : L'ensemble M des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un sous corps de $\mathbb{L}$.