122. Anneaux principaux. Applications et exemples.

Soit A un anneau unitaire commutatif intègre et K un corps commutatif.

I Notion de principalité

A Les idéaux principaux Rom Per

On considère un idéal I de notre anneau A.

Définition 1 : Pour tout $a \in A$, l'ensemble $(a) = a.A = \{qa \mid q \in A\}$ des multiples de a dans A est un idéal. Un tel idéal est dit principal.

Exemple 2 : Tous les idéaux de $\mathbb{Z}$ sont principaux.

Remarque 3 : Tous les idéaux d'un anneau ne sont pas principaux.

Exemple 4 : L'idéal $I = (2, X) = 2\mathbb{Z} + X\mathbb{Z}$ de l'anneau $\mathbb{Z}[X]$ n'est pas principal.

Définition 5 : Un idéal I de A est dit premier s'il est distinct de A et si $ab \in I$ si et seulement si $a \in I$ ou $b \in I$.

Exemple 6 : L'idéal $\{0\}$ est premier si et seulement si A est intègre.

Définition 7 : Un idéal I de A est dit maximal s'il est distinct de A et si I et A sont les seuls idéaux de A qui contiennent I.

Théorème 8 : On a :
i) Un idéal I de A est maximal $\Leftrightarrow$ l'anneau quotient A/I est un corps.
ii) Un idéal I de A est premier $\Leftrightarrow$ l'anneau quotient A/I est intègre.
iii) Un élément p de A intègre est premier $\Leftrightarrow$ l'idéal (p) est premier.
iv) Un idéal maximal est premier.
v) Si un élément p de A intègre est tel que (p) soit maximal alors p est irréductible.

Exemple 9 : $\{0\} \times \mathbb{Z}$ est un idéal premier non maximal de $\mathbb{Z} \times \mathbb{Z}$ (ex 3.24 Hauchecorne).

B Anneaux principaux. Rom

Définition 10 : On dit que l'anneau A est principal, s'il est intègre et si tout idéal

Exemple 11 : $\mathbb{Z}$ est principal, $K[X]$ pour K un corps est principal.

Proposition 12 : Soit A un anneau principal et $p \in A^* \setminus A^\times$. Alors :
i) p est irréductible si et seulement si il est premier
ii) ((p) premier) $\Leftrightarrow$ (p premier) $\Leftrightarrow$ (p irréductible) $\Leftrightarrow$ ((p) maximal).

Remarque 13 : Cette proposition est utile pour montrer qu'un anneau n'est pas principal.

Exemple 14 : Les anneaux $\mathbb{Z}[i\sqrt{m}]$ ne sont pas principaux pour $m \geq 3$ puisque 2 y est irréductible non premier.

C Cas particulier des anneaux euclidiens Per

Définition 15 : Un anneau A est dit euclidien si :
i) A est intègre
ii) A est muni d'une division euclidienne ie il existe une fonction (appelée position stathme) $\nu : A\setminus\{0\} \to \mathbb{N}$ telle que si $a, b \in A\setminus\{0\}$, il existe $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$)

Exemple 16 : $\mathbb{Z}$ est euclidien (muni de l'application $\nu(m) = |m|$)

Théorème 17 : Un anneau euclidien est principal. Précisément, pour tout idéal I de A non réduit à $\{0_A\}$, il existe $a_0 \in I\setminus\{0_A\}$ tel que $\nu(a_0) = \min_{a \in I\setminus\{0\}} \nu(a)$ et $I = a_0 A$.

Lemme 17 : Soit A un anneau et soit $P \in A[X]$, $P \neq 0$ de coefficient dominant inversible. Soit $F \in A[X]$, il existe $Q, R \in A[X]$ tels que l'on ait :
i) $F = PQ + R$
ii) $d^\circ R < d^\circ P$ ou $R = 0$.

Corollaire 18 : Si k est un corps, l'anneau $k[X]$ est euclidien (avec $\nu(P) = d^\circ P$).

Exemple 19 : L'anneau $\mathbb{Z}\left[\frac{-1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

Application 20 : Algorithme d'Euclide.

II Arithmétique dans un anneau principal

A Existence d'un plus grand diviseur commun Rom

Définition 21 : Soient $n \in \mathbb{N}\setminus\{0,1\}$ et $a_1, \dots, a_n \in A^*$. On dit que ces éléments admettent un

$\begin{cases} \forall k \in [\![1,n]\!],\ S \text{ divise } a_k \\ \text{tout diviseur commun à } a_1,\dots,a_n \text{ divise } S \end{cases}$

Théorème 22 : Soit $(a_1,\dots,a_n) \in (A\setminus\{0\})^n$ avec A principal, $n \geq 2$. Les $a_1,\dots,a_n$ admettent un pgcd $d \in A\setminus\{0\}$ et il existe $(u_1,\dots,u_n) \in A^n$ tel que $\sum u_k a_k = d$.

Remarque 23 : Dans le cadre des anneaux euclidiens, l'algorithme d'Euclide permet de déterminer le pgcd de deux éléments et l'algorithme d'Euclide étendu permet de trouver une relation de Bézout.

Définition 24 : Soient $(a_1,\dots,a_n) \in A^n$, on dit que $a_1,\dots,a_n$ sont premiers entre eux dans leur ensemble (ou étrangers) si leurs pgcd est dans $A^\times$.

Corollaire 25 (Bézout) : Soit $(a_1,\dots,a_n) \in A^n$ des éléments tous non nuls. Ces éléments sont premiers entre eux dans leur ensemble si et seulement si il existe $(u_1,\dots,u_n) \in A^n$ tel que $\sum_{k=1}^{n} u_k a_k = 1$.

Application 26 : Lemme des noyaux (voir partie III)

B La factorialité d'un anneau principal

Définition 27 : On dit que A est factoriel s'il vérifie :
i) A est intègre
ii) $\forall a \in A$, $\exists u \in A^\times$, $p_1,\dots,p_r$ irréductibles, $a = u p_1 \dots p_r$.
iii) Cette décomposition est unique à permutation près et à des inversibles près : si $a = u p_1 \dots p_r = v q_1 \dots q_s$ on a $r = s$ et il existe $\sigma \in S_r$ tel que p_i et $q_{\sigma(i)}$ soient associés.

Théorème 28 : L'anneau A est factoriel si et seulement si il est intègre et :
i) toute suite croissante d'idéaux principaux de A est stationnaire.
ii) tout élément irréductible de A est premier.

Corollaire 29 (Euclide) : Dans un anneau factoriel, un élément est irréductible si et seulement si il est premier.

Exemple 30 : Les anneaux $\mathbb{Z}[i\sqrt{m}]$ ne sont pas factoriels pour $m \geq 3$ puisque 2 y est irréductible non premier.

Corollaire 31 : Un anneau principal est factoriel.

Remarque 32 : La réciproque est fausse : $\mathbb{Z}[X]$ est factoriel non principal. cf ex 4

Proposition 33 : On a équivalence entre :
i) $A[X]$ est principal
ii) A est un corps

Théorème 34 (Gauss) : Si $a \mid bc$, $a \wedge b = 1$, alors $a \mid c$ avec $a,b,c \in A^3$ où A est principal.

Lemme 35 (Euclide) : Si p irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$ avec $p,a,b \in A^3$ où A est supposé principal.

C Un isomorphisme entre anneaux quotients. Rem

Lemme 36 : Soit $a_1,\dots,a_n$ éléments deux à deux premiers entre eux dans A principal et pour tout $k \in [\![1,n]\!]$, $b_k = \prod_{\substack{i=1 \\ i\neq k}}^{n} a_i$. Alors les $(b_k)_{k\in[\![1,n]\!]}$ sont premiers entre eux dans leur ensemble.

Théorème 37 (chinois) : Supposons les a_i, pour $1 \leq i \leq n$, deux à deux premiers entre eux, l'application $\varphi : x \in A \mapsto (\pi_i(x))_{1\leq i\leq n} \in \prod_{i=1}^{n} A/(a_i)$ est un morphisme d'anneaux surjectif de noyau $\ker\varphi = \left(\prod_{i=1}^{n} a_i\right)$ et φ induit un isomorphisme d'anneaux

$$\overline{\varphi} : \begin{array}{ccc} A/\left(\prod_{i=1}^{n} a_i\right) & \longrightarrow & \prod_{i=1}^{n} A/(a_i) \\ \pi(x) & \longmapsto & (\pi_i(x))_{1\leq i\leq n} \end{array}$$

dont l'inverse est donné par :

$$\overline{\varphi^{-1}} : \begin{array}{ccc} \prod_{i=1}^{n} A/(a_i) & \longrightarrow & A/\left(\prod_{i=1}^{n} a_i\right) \\ (\pi_i(x))_{1\leq i\leq n} & \longmapsto & \sum_{i=1}^{n} x_i u_i b_i \end{array}$$

où $(u_i)_{1\leq i\leq n}$ est une suite d'éléments de A telle que $\sum_{i=1}^{n} u_i b_i = 1$.

Exemple 38 : Le système $\begin{cases} k \equiv 2\ [4] \\ k \equiv 3\ [5] \\ k \equiv -1\ [9] \end{cases}$ a pour solutions $S = \{119 + 180k \mid k \in \mathbb{Z}\}$

Exemple 39 : $\mathbb{Z}_4$ n'est pas isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_2$.

III Applications

A Equations diophantiennes Rem

Définition 40 : Une équation diophantienne est une équation polynomiale à

Exemple 42 : Soit $m \geq 2$, a un entier naturel non nul et b un entier relatif.
Alors $ax \equiv b\ [m]$ est une équation diophantienne.

Proposition 43 : $ux \equiv 1\ [m]$ a des solutions $\Leftrightarrow \bar{u} \in \mathbb{Z}/m\mathbb{Z}^\times \Leftrightarrow u \wedge m = 1$.

Corollaire 44 : Soit $a \in \mathbb{Z}$ et $m \in \mathbb{N} \setminus \{0\}$ tels que $a \wedge m = 1$. Alors l'ensemble des solutions de $ax \equiv 1\ [m]$ est $S = \{x_0 + km,\ k \in \mathbb{Z}\}$ où x_0 est une solution particulière de cette équation.

Théorème 45 : On note $\delta = a \wedge m$ et $a = \delta a'$, $m = \delta m'$ avec $a' \wedge m' = 1$. L'équation diophantienne de l'exemple 42 a des solutions entières si et seulement si δ divise b. Dans ce cas l'ensemble des solutions de cette équation est $S = \{b'x_0' + km' \mid k \in \mathbb{Z}\}$ où x_0' est une solution particulière de $a'x \equiv 1\ [m']$.

Développement (Sophie Germain)
Soit p un nombre premier impair tel que $q = 2p+1$ soit premier. Alors il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $p \nmid xyz$ et $x^p + y^p + z^p = 0$.

B Algèbre linéaire. BHP

Soit $M \in \mathcal{M}_n(\mathbb{K})$

Définition 46 : L'application $\varphi_M : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathbb{K}[M] \\ P & \longmapsto & P(M) \end{array}$ est un morphisme d'algèbres.
Son noyau est un idéal de $\mathbb{K}[X]$ principal donc engendré par un unique polynôme unitaire π_M appelé polynôme minimal de M.

Théorème 47 : On a $\dim(\mathbb{K}[M]) = \deg(\pi_M)$.

Proposition 48 : $\mathbb{K}[M]$ est un corps si et seulement si π_M est irréductible dans $\mathbb{K}[X]$.

Lemme 49 (lemme des noyaux)
Soit E un $\mathbb{K}$-ev, $u \in \mathcal{L}(E)$ et $(P_1, \dots, P_r) \in \mathbb{K}[X]^r$ une famille finie de polynômes deux à deux premiers entre eux et $P = P_1 \dots P_r$ leur produit.
On a alors la décomposition en somme directe :

$$\ker P(u) = \bigoplus_{k=1}^{r} \ker P_k(u)$$

Remarque 50 : En pratique, on utilise souvent ce lemme avec P annulateur de u. On obtient alors une décomposition de E en sous espaces stables, car $\ker Q(u)$ est stable par u pour tout polynôme Q.

Proposition 51 : M est trigonalisable (resp. diagonalisable) si et seulement si π_M est scindé (resp. scindé à racines simples).

Théorème 52 : (Décomposition de Dunford).
Supposons que π_M soit scindé. Alors il existe un unique couple $(D,N) \in \mathcal{M}_n(\mathbb{K})^2$ tel que D est diagonalisable, N est nilpotente, $M = D+N$ et $ND = DN$.
De plus, D et N sont des polynômes en M.

Application 53 : Soit $u \in \mathcal{L}(E)$, u diagonalisable $\Leftrightarrow e^u$ est diagonalisable.

Définition 54 : On dit que $u \in \mathcal{L}(E)$ est semi-simple si tout sev de E stable par u admet un supplémentaire stable par u.

Développement : $u \in \mathcal{L}(E)$ est semi-simple si et seulement si π_u est sans facteur carré dans sa décomposition en facteurs irréductibles dans $\mathbb{K}(X)$.

Exemple 55 : Si u est nilpotente, alors u est semi-simple si et seulement si $u = 0$.

C Anneaux des entiers de Gauss

Si il y a la place, écrire deux mots sur les entiers de Gauss, c'est dans le Perrin

Références :

Rombaldi Mathématiques pour l'agrégation

D. Perrin Cours d'Algèbre

Objectif Agrégation BMP

J'intègre MP - MP*.