Anneaux principaux. Exemples et applications.

122

Dans cette leçon, A désigne un anneau commutatif intègre.

I - Anneaux principaux et non principaux

A - Rappels : idéaux, primalité, irréductibilité

[R] 213 **Def 1** : Un idéal de A est un sous-groupe de $(A,+)$ tel que $\forall x \in I, \forall a \in A, ax \in I$.

[R] 223 **Def 2** : ▸ Un idéal $\mathfrak{p}$ de A est *premier* si $\mathfrak{p} \neq A$ et :
$$\forall (x,y) \in A^2, xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \text{ ou } y \in \mathfrak{p}$$
▸ Un idéal $\mathfrak{m}$ de A est *maximal* si $\mathfrak{m} \neq A$ et si pour tout idéal I de A tel que $\mathfrak{m} \subseteq I \subseteq A$, $I = \mathfrak{m}$ ou $I = A$.

[R] 223 **Def 3** : ▸ Un élément $p \in A$ est *premier* si $\langle p \rangle$ est premier.
▸ Un élément π est *irréductible* si π est non nul, non inversible, et dont les seuls diviseurs sont les inversibles et les associés.

[R] 215 **Prop 4** : Tout élément premier est irréductible.

[R] 223 **Prop 5** : ▸ $\mathfrak{p}$ est premier $\Leftrightarrow$ $A/\mathfrak{p}$ est intègre
▸ $\mathfrak{m}$ est maximimal $\Leftrightarrow$ $A/\mathfrak{m}$ est un corps

[R] 223 **Cor 6** : Tout idéal maximal est premier.

Rq 7 : La réciproque est fausse : considérer $X\mathbb{Z}[X]$.

[R] 225 **Prop 8** : Dans un anneau factoriel, tout irréductible est premier.

B - Des anneaux factoriels aux anneaux principaux

[R] 237 **Def 9** : On dit qu'un idéal I de A est *principal* s'il est engendré par un élément. On dit que A est principal si tous ses idéaux sont principaux.

Ex 10 : $\mathbb{Z}$ est un anneau principal. Ses quotients $\mathbb{Z}/n\mathbb{Z}$ le sont donc également.

Prop 11 : Tout anneau principal est factoriel. [P] 49

Rq 12 : $\mathbb{Z}[X]$ est factoriel, mais pas principal.

Prop 13 : $A[X]$ est principal $\Leftrightarrow$ A est un corps. [R] 242

Ex 14 : $\mathbb{C}[X]$, $\mathbb{Q}(j)[X]$, $\mathbb{F}_q(X)[T]$ sont principaux.

Prop 15 : Soit $p \in A$. Si pA est maximal, alors p est irréductible. [R] 241
Si A est principal, alors la réciproque est aussi vraie.

Rq 16 : La principalité de A est cruciale : considérer $X \in \mathbb{Z}[X]$.

Prop 17 : Dans un anneau principal, tout idéal premier non nul est maximal. [R] 241

C - Des anneaux principaux aux anneaux euclidiens

[R] 261 **Def 18** : Un *stathme euclidien* sur A est une application $\varphi : A^* \longrightarrow \mathbb{N}$ telle que $\forall (a,b) \in (A \setminus \{0\})^2$, $a \mid b \Rightarrow \varphi(a) \leq \varphi(b)$

[R] 261 **Def 19** : On dit que A est *euclidien* s'il admet un stathme euclidien φ définissant une division euclidienne, i.e. tel que $\forall (a,b) \in A \times A^*$, $\exists (q,r) \in A^2$: $a = bq + r$ et $(r = 0$ ou $\varphi(r) < \varphi(b))$.

Ex 20 : $\mathbb{Z}$ est euclidien pour $|\cdot|$, $K[X]$ est euclidien pour deg.
$\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} = \mathrm{eval}_i(\mathbb{Z}[X])$ est euclidien pour $|\cdot|^2$.
L'anneau $\mathbb{D} = \left\{ \frac{n}{10^m} : n \in \mathbb{Z}, m \in \mathbb{N} \right\} = \{ n 2^p 5^q : (p,q,n) \in \mathbb{Z}^3, n \wedge 10 = 1 \}$ est euclidien pour le stathme euclidien $\varphi : n 2^p 5^q \longmapsto |n|$.

[R] 261 **Prop 21** : Tout anneau euclidien est principal.

[P] 53 **Rq 22** : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal, mais il n'est pas euclidien.

[P] 56 **Ex 23** : $\mathbb{Z}[i]$ est donc principal, donc factoriel. Comme $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, $3 = (2+i)(2-i)$ est réductible, donc non premier dans $\mathbb{Z}[i]$, contrairement à $\mathbb{Z}$.

II - Arithmétique dans les anneaux principaux

A - Divisibilité, PGCD, PPCM

[P] 46 **Prop 24** : $\forall (a,b) \in A^2$, $a|b \iff bA \subset aA$

[R] 215 **Rq 25** : Cela permet de réécrire la définition de primalité en terme de division : $p \in A$ est premier si $\forall (a,b) \in A^2$, $p|ab \Rightarrow p|a$ ou $p|b$.
Cette propriété est parfois appelée "Lemme d'Euclide".

[R] 229 **Notations** : On rappelle que A est *factoriel* si tout $a \in A$ se décompose de manière unique sous la forme $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$, appelée *décomposition en facteurs irréductibles* de a, où $\mathcal{P}$ est un système complet de représentants des irréductibles de A, et $(v_p(a))_{p \in \mathcal{P}} \in \mathbb{N}^{(\mathcal{P})}$. L'entier $v_p(a)$ est appelé *valuation p-adique* de a.

Ex 26 : $9 = 3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$ donc $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel (donc pas principal).

Def 27 : Soit $(a_1, \dots, a_r) \in A^r$ tel que $a_1 \cdots a_r \neq 0$. Sous réserve d'existence, un PGCD (resp. un PPCM) de $a_1, \dots, a_r$ est un plus grand minorant (resp. un plus petit majorant) de $\{a_1, \dots, a_r\}$ pour la relation de divisibilité. On le note $a_1 \wedge \cdots \wedge a_r$ (resp. $a_1 \vee \cdots \vee a_r$).
On pose $a \vee 0 = 0 \wedge 0 = 0$.

Rq 28 : Si d est un PGCD (resp. PPCM) de $a_1, \dots, a_r$, alors les autres PGCD (resp. PPCM) sont les associés de d. Ainsi, l'écriture "$d = a_1 \wedge \cdots \wedge a_r$" signifie "$d$ est un PGCD de $a_1, \dots, a_r$".

[P] 49 **Prop 29** : Si A est factoriel, alors $\forall (a,b) \in A^2$,

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))} \quad \text{et} \quad a \vee b = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$$

(en particulier, le PGCD (resp. PPCM) existe toujours dans un anneau factoriel.

[R] 246 **Thm 30** (de Gauss) : Supposons A factoriel.

$$\forall (a,b,c) \in A^3, \quad \begin{cases} a|bc \\ a \wedge b = 1 \end{cases} \Rightarrow a|c$$

B - Relations de Bézout et théorème des restes chinois

Prop 31 : Supposons A principal. Soit $(a,b) \in A^2$.

- $d = a \wedge b \iff dA = aA + bA$
- $m = a \vee b \iff mA = aA \cap bA$.

Def 32 : Soient a et b dans A ayant un PGCD d. Un *couple de Bézout* pour (a,b) est un couple $(u,v) \in A^2$ tel que $d = au + bv$. Cette égalité est appelée *relation de Bézout* pour a et b.

Rq 33 : Dans un anneau euclidien, l'algorithme d'Euclide étendu permet de trouver des couples de Bézout.

Ex 34 : $\forall (n,m) \in \mathbb{N}^2$, $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$

$$M_n \wedge M_m = M_{n \wedge m} \quad \text{où } M_n = 2^n - 1.$$

Prop 35 : Si A est factoriel et est tel que $\forall (a,b) \in A^2$, $\langle a,b \rangle$ est principal, alors A est principal. C'est une sorte de réciproque de Prop 31.

Rq 36 : D'après Prop 31, si A est principal, alors pour tout $(a,b) \in A^2$, il existe $(u,v) \in A^2$ tel que $a \wedge b = au + bv$, mais la réciproque est fausse en général.
Contre-exemple : $2 = 3 \times (2) + 2 \times (-2)$ mais $3 \wedge 2 = 1 \neq 2$.

Thm 37 (de Bézout) : $\forall (a,b) \in A^2$, $a \wedge b = 1 \iff (\exists (u,v) \in A^2 : au + bv = 1)$.

[R] 247

Thm 38 (des restes chinois effectif) : Soit $(a_1, \dots, a_r) \in (A \setminus (A^\times \cup \{0\}))^r$. Si $a_1, \dots, a_r$ sont deux à deux premiers entre eux, alors :

$$\varphi : A/a_1 \cdots a_r A \longrightarrow A/a_1 A \times \cdots \times A/a_r A$$

DEV 1

$$x \bmod a_1 \cdots a_r \longmapsto (x \bmod a_1, \dots, x \bmod a_r)$$

est un isomorphisme d'anneaux. De plus, il existe $(u_1, \dots, u_r) \in A^r$ tel que $\sum_{i=1}^{r} u_i b_i = 1$, où $b_i = \frac{a_1 \cdots a_r}{a_i}$ $(1 \leq i \leq r)$, et la réciproque de φ s'exprime :

$$\varphi^{-1} : (x_1 \bmod a_1, \dots, x_r \bmod a_r) \longmapsto \sum_{i=1}^{r} x_i b_i u_i \bmod a_1 \cdots a_r$$

[R] 250

Appli 39 : Recherche d'un polynôme de degré minimal $P \in (\mathbb{Z}/5\mathbb{Z})[X]$ tel que $P(\bar{0}) = \bar{2}$, $P(\bar{1}) = \bar{0}$ et $P(\bar{2}) = \bar{1}$. DEV 1

III - Autres exemples (d'utilisation) d'anneaux principaux

A - En algèbre linéaire

Soit K un corps, soit L une extension de K

Soient E un K-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$.

[R] 69 Lemme 40 (des noyaux) : $\forall (P,Q) \in K[X]^2$, $P \wedge Q = 1 \Rightarrow \mathrm{Ker}((PQ)(u)) = \mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u))$.

[R] 604 Thm 41 (de structure) : Soit $\varphi_u : K[X] \longrightarrow \mathcal{L}(E)$, $P \longmapsto P(u)$. Le noyau de φ_u, appelé idéal annulateur de u, est non nul, et son unique générateur unitaire, noté μ_u, est appelé *polynôme minimal* de u.

[R] 251 Def 42 : Soit $\alpha \in L$. Soit $\varphi_\alpha : K[X] \longrightarrow L$, $P \longmapsto P(\alpha)$. Si le noyau de φ_α, appelé idéal annulateur de α, est non nul, alors on dit que α est algébrique sur K, et l'unique générateur unitaire $P_{\alpha,K}$ de $\mathrm{Ker}(\varphi_\alpha)$ est appelé polynôme minimal de α sur K. Dans le cas contraire, on dit que α est transcendant.

B - Résolution d'équations diophantiennes

Équations de MORDELL :

- $\{(x,y) \in \mathbb{Z}^2 \mid x^3 = y^2 + 1\} = \{(1,0)\}$

  ↳ étude dans $\mathbb{Z}[i]$ (euclidien) en écrivant $y^2 + 1 = (y+i)(y-i)$

- [C] 193 $\{(x,y) \in \mathbb{Z}^2 \mid x^3 = y^2 + 2\} = \{(3,5),(3,-5)\}$

  ↳ étude dans $\mathbb{Z}[i\sqrt{2}]$ (euclidien) en écrivant $y^2 + 2 = (y+i\sqrt{2})(y-i\sqrt{2})$

Équation de FERMAT pour $n = 3$:

On ramène l'étude à $\mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j = \mathrm{eval}_j(\mathbb{Z}[X]) \simeq \dfrac{\mathbb{Z}[X]}{\langle X^2 + X + 1 \rangle}$

$\left(j = e^{\frac{2i\pi}{3}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$ en écrivant $x^3 + y^3 = (x+y)(x+jy)(x+j^2y)$

Rq 43 : $\mathbb{Z}[j]$ est euclidien pour $|.|^2$.

C - Le théorème des deux carrés de FERMAT

[P] 56 Lemme 44 : -1 est un carré dans $\mathbb{F}_p$ si, et seulement si $p \equiv 1\ [4]$

Thm 45 (des deux carrés de FERMAT) : Soit $E = \{n \in \mathbb{N}^* \mid \exists (a,b) \in \mathbb{N}^2 : n = a^2 + b^2\}$.

$n \in E \iff \forall p \in \mathcal{P},\ p \equiv 3\ [4] \Rightarrow v_p(n)$ pair DEV 2

RÉFÉRENCES

[R] : Mathématiques pour l'agrégation - Algèbre et géométrie (Jean-Étienne Rombaldi) [3e édition]

[P] : Cours d'algèbre (Daniel Perrin)

[C] : Carnets de voyage en Algebrie (Philippe Caldero, Marie Peronnier)