122

Anneaux principaux. Exemples et applications

Dans toute la leçon, A est un anneau intègre commutatif.

I Introduction à la notion de principalité

1) Idéaux

Déf 1: • Un idéal I de A est dit principal si $\exists a \in A \,/\, I = aA$ (noté (a)).
• A est dit principal si tous ses idéaux sont principaux.

Ex 2: • $\mathbb{Z}$ est principal car ses idéaux sont de la forme $n\mathbb{Z}$.
• $k[X]$ est principal, avec k corps.

Ex 3: $\mathbb{C}[X,Y]/(XY-1)$ est principal [DVPT 1]

Déf 4: Un idéal I de A est dit
• premier si A/I est intègre
• maximal si $I \neq A$ et si on a J idéal de A tel que $I \subset J \subset A$, alors $J = I$ ou $J = A$.

ex 5: Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ pour p premier.

Prop 6: (i) I premier $\Leftrightarrow I \neq A$ et $\forall a,b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$
(ii) I maximal $\Leftrightarrow A/I$ corps.
(iii) I maximal $\Rightarrow I$ premier.

Contre-ex 7: La réciproque du (iii) est fausse, car pour k corps, l'idéal principal (X) de $k[X,Y]$ est premier mais non maximal.

Déf 8: Soit $p \in A$. p est dit irréductible si $p \notin A^*$ et si $p = ab$, alors $a \in A^*$ ou $b \in A^*$.

Ex 9: Les irréductibles de $\mathbb{Z}$ sont les nombres premiers.

Prop 10: Soit A principal et $p \in A \setminus \{0\}$. Les conditions suivantes sont équivalentes: (i) p est irréductible
(ii) (p) est un idéal maximal de A.
(iii) (p) est un idéal premier de A.
(iv) $A/(p)$ est un corps.

App 11: Construction de $\mathbb{C}$ qui est défini comme $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ avec X^2+1 irréductible dans $\mathbb{R}[X]$.

2) Anneaux euclidiens

Déf 12: A est dit anneau euclidien si $\exists \varphi : A \longrightarrow E$ avec E ensemble ordonné (en général $\mathbb{N}$) tel que $\forall (a,b) \in A \times (A \setminus \{0\})$, $\exists q, r \in A$ tels que $a = bq + r$ avec $\varphi(r) < \varphi(b)$ ou $r = 0$. φ est appelé stathme euclidien.

Prop 13: Un anneau euclidien est principal.

Ex 14: • $\mathbb{Z}$ euclidien pour $\varphi : \begin{array}{l} \mathbb{Z} \longrightarrow \mathbb{N} \\ n \longmapsto |n| \end{array}$
• $k[X]$, avec k corps, est euclidien pour $\varphi : \begin{array}{l} k[X] \longrightarrow \mathbb{N} \cup \{-\infty\} \\ P \longmapsto \deg P \end{array}$ avec $\varphi(0) = -\infty$

Contre-ex 15: $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

Rem 16: $k[X]$ principal $\Leftrightarrow k$ corps.

App 17: Soit A algèbre sur k, $\alpha \in A$.
Pour tout $P = \sum_{k=0}^{n} a_k X^k \in k[X]$, on pose $P(\alpha) = \sum_{k=1}^{n} a_k \alpha^k + a_0 1_A \in A$
Soit α une racine d'un polynôme de $k[X]$. Alors il existe un unique polynôme unitaire de degré minimal, noté Π_α, tel que $\Pi_\alpha(\alpha) = 0$, et $\{P \in k[X] \,/\, P(\alpha) = 0\} = (\Pi_\alpha)$, i.e. $\forall P \in k[X] \,/\, P(\alpha) = 0$, $\Pi_\alpha \,|\, P$.
Π_α est appelé polynôme minimal de α.

II Divisibilité dans les anneaux principaux

1) PGCD, PPCM (A est ici supposé principal)

Déf-Prop 18: Soient $a, b \in A \setminus \{0\}$. (a,b) et $(a) \cap (b)$ sont des idéaux, donc sont principaux.
$\exists (d,m) \in A^2 \,/\, (a,b) = (d)$ et $(a) \cap (b) = (m)$.
d est appelé un PGCD de a et b, et m un PPCM de a et b.

Rem 19: m et d sont uniques à un facteur inversible près.

Prop 20: • d PGCD de a et $b \Leftrightarrow \exists (a',b',u,v) \in A^4 \,/\, \begin{cases} a = da' \\ b = db' \\ d = au + bv \end{cases}$
• Avec les mêmes notations,
m PPCM de a et $b \Leftrightarrow m = a'b'd$ et $md = ab$.

App 21: Dans le cas où A est euclidien, pour déterminer un PGCD, on utilise l'algorithme d'Euclide étendu.

2) Primalité et théorème chinois

A est supposé à nouveau principal.

Déf. 22: Soit $(a,b)\in A^2$.
- On dit que a divise b (noté $a|b$) si $\exists c\in A \,/\, b=ac$.
- a et b sont dits premiers entre eux si 1 est un PGCD de a et b.

Prop. 23 : (Bezout). Soit $(a,b)\in A^2$:
a et b sont premiers entre eux $\Longleftrightarrow \exists (u,v)\in A^2 / au+bv=1$.

Cor. 24 : Soit $(a,b,c)\in (A\setminus\{0\})^3$. Alors si a et b sont premiers entre eux et que $a|bc$, on a $a|c$.

App. 25 : Soit $u\in\mathcal{L}(E)$ (E un k-ev) et $P=P_1\dots P_r\in k[X]$, où les polynômes P_i sont premiers entre eux 2 à 2. Alors
$$\operatorname{Ker} P(u) = \operatorname{Ker} P_1(u)\oplus\dots\oplus \operatorname{Ker} P_r(u).$$

Prop. 26 : Soient $a_1,\dots,a_m\in A$ deux à deux premiers entre eux.
Alors $A/_{(a_1\dots a_m)} \simeq A/_{(a_1)}\times\dots\times A/_{(a_m)}$

Prop. 27 : Soient a et b premiers entre eux. $\exists u,v\in A / au+bv=1$.
Soit $(k,c)\in A^2$, je note $k_{[c]}$ la classe de k dans $A/_{(c)}$.
Alors
$$\begin{array}{rcl} A/_{(ab)} & \longrightarrow & A/_{(a)}\times A/_{(b)} \\ k_{[ab]} & \longmapsto & (k_{[a]}, k_{[b]}) \end{array}$$
est un isomorphisme d'anneaux, d'application réciproque
$$(k_{[a]}, \ell_{[b]}) \longmapsto (x_{[ab]}) \text{ où } x = vbk + ua\ell.$$

App. 28 : Résolution de $\begin{cases} x\equiv 2[4] \\ x\equiv 3[5] \\ x\equiv 1[9] \end{cases}$

3) Anneaux factoriels

Déf. 29 : Sur A, on prend P un système de représentants des irréductibles de A, i.e. $\forall q\in A$ irréductible, $\exists (u,p)\in A^*\times P / q=up$.
A est dit factoriel si :
(i) $\forall a\in A\setminus\{0\}$, a s'écrit sous la forme $a=u\prod_{p\in P} p^{v_p(a)}$ avec $u\in A^*$, $v_p(a)\in\mathbb{N}$ et $\{p\in P \mid v_p(a)\neq 0\}$ est fini.
(ii) Cette décomposition est unique.

Ex. 30 :
- $\mathbb{Z}$ avec $P=\{p>0,\ p \text{ premier}\}$
- $k[X]$ avec $P=\{\text{polynômes irréductibles unitaires}\}$

Rem. 31 : Si A est factoriel, en étendant la notion de divisibilité à A, on a : $a|b \Longleftrightarrow \forall p\in P,\ v_p(a)\leq v_p(b)$.

Prop. 32 : Un anneau principal est factoriel.

III Anneaux principaux et réduction matricielle

1) Facteurs invariants

Si A est un anneau euclidien

Thm. 33 : Soit $U\in\mathcal{M}_{m,n}(A)$. Il existe alors une famille $(d_1,\dots,d_s)$ d'éléments non nuls de A avec $d_s|\dots|d_1$, il existe $(P,Q)\in GL_m(A)\times GL_n(A)$ tels que $U=PDQ$
où $D=\begin{bmatrix} d_s & & & (0) \\ & \ddots & & \\ & & d_1 & \\ (0) & & & (0)\end{bmatrix}$. La famille $(d_1,\dots,d_s)$ est unique à des facteurs inversibles près. Elle est appelée famille des facteurs invariants de U.

2) Réduction de Frobenius

Déf. 34 : Soit $P=X^p+\sum_{j=0}^{p-1} a_j X^j\in k[X]$. On appelle matrice compagnon de P la matrice
$$\mathcal{C}(P)=\begin{pmatrix} & & (0) & -a_0 \\ 1 & \ddots & & \vdots \\ (0) & & 1 & -a_{p-1}\end{pmatrix}\in\mathcal{M}_p(k)$$

Thm 35 : Soit E un k-ev, et $u\in\mathcal{L}(E)$. Il existe une suite $F_1,\dots,F_r$ de sev de E, tous stables par u, telle que
(i) $E=F_1\oplus\dots\oplus F_r$
(ii) $\forall i\in[\![1,r]\!]$ $u_{|F_i}$ est cyclique (i.e. $\exists x\in F_i$ tel que $(x, u_{|F_i}(x), \dots, u_{|F_i}^{\dim F_i -1}(x))$ soit une base de E).
(iii) Si P_i est le polynôme minimal de $u_{|F_i}$, alors $\forall i\in[\![1,r-1]\!]$, $P_{i+1}|P_i$.
La suite $(P_1,\dots,P_r)$ ne dépend que de u. Elle est appelée suite des invariants de similitude de u.

Thm 36 : Si $(P_1,\dots,P_r)$ est la suite des invariants de similitude de $u\in\mathcal{L}(E)$, alors il existe une base $\mathcal{B}$ de E telle que
$$\operatorname{Mat}(u,\mathcal{B})=\begin{pmatrix}\mathcal{C}(P_1) & & (0) \\ & \ddots & \\ (0) & & \mathcal{C}(P_r)\end{pmatrix}$$

Rem. 37: $P_1 = \Pi_u$ et $P_1 \cdots P_r = (-1)^n \chi_u$ où $n = \dim E$.

Cor. 38: Deux endomorphismes u et v de $\mathcal{L}(E)$ sont semblables si et seulement si ils ont les mêmes invariants de similitude.

3) Réduction de Jordan

Ici, $\mathbb{K}$ est supposé algébriquement clos.

Thm. 39: Soit E un $\mathbb{K}$-ev, $u \in \mathcal{L}(E)$. Alors $\exists (\lambda_1, \dots, \lambda_e) \in \mathbb{K}^e$ où $\forall i \neq j$, $\lambda_i \neq \lambda_j$, $\forall i \in [\![1; e]\!]$, $\exists j_i \in \mathbb{N}^*$ $\exists n_{i,1} \geq n_{i,2} \geq \dots \geq n_{i,j_i} > 0$ tel qu'il existe $\mathcal{B}$ base de E dans laquelle la matrice de u est diagonale par blocs de Jordan :

$$\mathrm{Mat}(u, \mathcal{B}) = \begin{bmatrix} I_{\lambda_1, n_{1,1}} & & & & (0) \\ & \ddots & & & \\ & & I_{\lambda_1, n_{1,j_1}} & & \\ & & & \ddots & \\ (0) & & & I_{\lambda_e, n_{e,1}} \ddots & I_{\lambda_e, n_{e,j_e}} \end{bmatrix}$$

$$I_{\lambda, n} = \begin{bmatrix} \lambda & 1 & (0) \\ & \ddots & 1 \\ (0) & & \lambda \end{bmatrix} \in \mathcal{M}_n(\mathbb{K})$$

Une telle matrice est appelée réduite de Jordan de u.

IV Entiers quadratiques

1) Principalité de A_d

Déf. 40: Soit K un sous-corps de $\mathbb{C}$. K est dite extension quadratique de $\mathbb{Q}$ si $[K : \mathbb{Q}] = 2$.

Prop. 41: Si K est une extension quadratique, $K = \mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d}, (x,y) \in \mathbb{Q}^2\} = \mathbb{Q} + \mathbb{Q}\sqrt{d}$

Déf. 42: $z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ (avec $(x,y) \in \mathbb{Q}^2$) est dit entier si $2x \in \mathbb{Z}$ et $x^2 - y^2 d \in \mathbb{Z}$. Soit A_d l'ensemble de ces entiers.

Thm. 43: Si $d \equiv 2[4]$ ou $d \equiv 3[4]$, alors $A_d = \mathbb{Z} + \mathbb{Z}\sqrt{d} = \mathbb{Z}[\sqrt{d}]$

Si $d \equiv 1[4]$, $A_d = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Prop. 44: Pour $d < 0$, soit $N : A_d \longrightarrow A_d$, $z \longmapsto z\bar{z}$

N est un stathme euclidien sur A_d $\iff d \in \{-1, -2, -3, -7, -11\}$

Donc si $d \in \{-1, -2, -3, -7, -11\}$, A_d est euclidien.

Prop. 45: Ici, $d < 0$

- Si $d \equiv 2[4]$ ou $d \equiv 3[4]$, A_d n'est pas principal si $d \notin \{-1, -2\}$
- Si $d \equiv 1[8]$, A_d n'est pas principal si $d \neq -7$.

Dans le cas où $d \equiv 5[8]$, il y a des anneaux qui sont principaux.

Prop. 46: $\mathbb{Z}\left[\frac{1+i\sqrt{4n-1}}{2}\right]$ principal $\iff$ n vérifie cette propriété : soit $2r+1$ le plus grand nombre impair tel que $3(2r+1)^2 \leq 4n-1$, alors la suite des ~~..~~ $r+1$ nombres $n, n+1^2+1, n+2^2+2, \dots, n+k^2+k, \dots, n+r^2+r$ est formée de nombres premiers

App. 47:

- $\mathbb{Z}\left[\frac{1+i\sqrt{43}}{2}\right]$ est principal, avec $n = 11$ et $r = 1$
- $\mathbb{Z}\left[\frac{1+i\sqrt{163}}{2}\right]$ est principal, avec $n = 41$, $r = 7$
- $\mathbb{Z}\left[\frac{1+i\sqrt{155}}{2}\right]$ n'est pas principal, car $n = 39$ n'est pas premier.

2) Entiers de Gauß

Déf. 48: On appelle anneau des entiers de Gauß l'ensemble $\mathbb{Z}[i]$ (cas $d = -1$)

Prop. 49:

- $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$
- $\mathbb{Z}[i]$ est euclidien (avec le stathme $N : z \longmapsto z\bar{z}$).

On pose $\Sigma = \{n \in \mathbb{N} / n = a^2 + b^2, a, b \in \mathbb{N}\}$

Thm. 50: Soit $p \in \mathbb{N}$ premier.

Alors $p \in \Sigma \iff p = 2$ ou $p \equiv 1[4]$

Ex. 51: $41 = 5^2 + 4^2$; $53 = 7^2 + 2^2$; $29 = 5^2 + 2^2$

Thm. 52: Soit $n \in \mathbb{N} \setminus \{0; 1\}$, $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$

Alors $n \in \Sigma \iff v_p(n)$ pair pour $p \equiv 3[4]$

[DVPT 2]

Ex. 53: $260 = 8^2 + 14^2$

Références

[COM] Combes, *Algèbre et géométrie*
[PER] Perrin, *Cours d'algèbre*
[GOB] Goblot, *Algèbre commutative*
[GOU] Gourdon, *Algèbre*
[OBJ] *Objectif agrégation*
) pour la partie III