122 Anneaux principaux. Exemples et applications.

Soit A un anneau unitaire.

I - Structures algébriques

1. Idéaux

Définition 1. Un sous ensemble $I \subseteq A$ est un **idéal** de A si : [ULM18] p. 5

(i) $(I,+)$ est un sous groupe de $(A,+)$.

(ii) Les produits ai et ia appartiennent à I pour tout a dans A et $i \in I$ (propriété d'absorption). p. 11

Si I est un idéal de A. Alors,

$$A/I = \{\overline{a} = a + I \mid a \in A\}$$

est un anneau, muni des lois $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a}\overline{b} = \overline{ab}$, et est appelé **anneau quotient** de A par I.

Remarque 2. — Un anneau non nul possède toujours les deux idéaux 0 et lui-même. p. 5

— Un idéal contenant 1 est égal à l'anneau entier (à cause de la propriété d'absorption). Par conséquent, un idéal différent de l'anneau ambiant n'est jamais un sous-anneau de celui-ci.

Exemple 3. Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ pour $n \in \mathbb{Z}$.

Proposition 4. Soient $\varphi : A \to B$ un morphisme d'anneaux et $I \subseteq A$, $J \subseteq B$ deux idéaux.

(i) L'ensemble $\varphi^{-1}(J)$ est un idéal de A. En particulier, $\mathrm{Ker}(\varphi)$ est un idéal de A.

(ii) Si φ est surjectif, alors $\varphi(I)$ est un idéal de B.

Définition 5. Soit $S \subseteq A$.

— $\bigcap\{I \text{ idéal de } A \mid S \subseteq I\}$ est un idéal de A noté (S) est appelé **idéal engendré** par S.

— On a $(S) = \{\sum_{i=1}^{n} a_i s_i b_i \mid a_i, b_i \in A, s_i \in S, n \in \mathbb{N}\}$. Si A est commutatif, $(S) = \{\sum_{i=1}^{n} a_i s_i \mid a_i \in A, s_i \in S, n \in \mathbb{N}\}$.

Définition 6. Soit I un idéal de A. p. 31

— I est dit **maximal** si $I \subsetneq A$ et si A et I sont les seuls idéaux de A qui le contiennent.

— On suppose A commutatif. I est dit **premier** si $I \subsetneq A$ et

$$\forall a, b \in A,\ ab \in I \implies a \in I \text{ ou } b \in I$$

Proposition 7. On suppose A commutatif. Soit I un idéal de A.

(i) I est maximal si et seulement si A/I est un corps.

(ii) I est premier si et seulement si A/I est un anneau intègre.

Corollaire 8. Dans un anneau commutatif, un idéal maximal est premier.

Contre-exemple 9. $\{0\}$ est un idéal premier de $\mathbb{Z}$ mais non maximal.

2. Anneaux principaux

Définition 10. — Un idéal est dit **principal** s'il est engendré par un seul élément.

— Un anneau est dit **principal** s'il est intègre (donc commutatif) et si tous ses idéaux sont principaux.

p. 39

Exemple 11. Comme dit dans l'Exemple 3, $\mathbb{Z}$ est un anneau principal.

Définition 12. On suppose A commutatif. Un élément a de A est dit **irréductible** si

$$a \notin A^\times, a \neq 0 \text{ et } a = bc \implies b \in A^\times \text{ ou } b \in A^\times$$

où $A^\times$ désigne le groupe des inversibles de A.

p. 45

Théorème 13. On suppose A principal. Soit $a \in A$.

(i) (a) est premier si et seulement si a est irréductible.

(ii) En supposant $a \neq 0$, (a) est premier si et seulement si (a) est maximal.

3. Anneaux euclidiens

Définition 14. — A est dit **euclidien** s'il est intègre et s'il existe une fonction $\nu : A^* \to \mathbb{N}$ telle que

$$\forall a, b \in A^*, \exists q, r \in A \text{ tels que } a = bq + r \text{ avec } (r = 0 \text{ ou } \nu(r) < \nu(b))$$

— L'élément q est le **quotient** et l'élément r est le **reste** de la division.

— La fonction ν est appelée **stathme euclidien** pour A.

p. 43

Exemple 15. $\mathbb{Z}$ est un anneau euclidien pour le stathme $\nu : n \mapsto |n|$.

Proposition 16. Un anneau euclidien est principal.

Contre-exemple 17. $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal mais n'est pas euclidien.

[PER] p. 53

Théorème 18. Si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est un anneau euclidien de stathme le degré. De plus, le quotient et le reste sont uniques.

[ULM18] p. 47

Corollaire 19. On suppose A commutatif. Les assertions suivantes sont équivalentes :

(i) A est un corps commutatif.

(ii) $A[X]$ est un anneau euclidien.

(iii) $A[X]$ est un anneau principal.

Corollaire 20. Soient $\mathbb{K}$ un corps commutatif et $f \in \mathbb{K}[X]$. Alors $\mathbb{K}[X]/(f)$ est un corps si et seulement si P est irréductible dans $\mathbb{K}[X]$.

II - Arithmétique dans les anneaux

On suppose A commutatif dans toute cette section.

1. Divisibilité dans un anneau principal

Définition 21. Soient $a, b \in A$. p. 39

- On dit que a **divise** b (ou que b est un multiple de a), noté $a \mid b$ s'il existe $c \in A$ tel que $b = ac$.
- On dit que a et b sont **associés**, noté $a \sim b$ si $a \mid b$ et si $b \mid a$.

Remarque 22. Soient $a, b \in A$.

- $a \mid b \iff (b) \subseteq (a)$.
- $a \sim b \iff (b) = (a)$. Ainsi, $\sim$ est une relation d'équivalence sur A.

Proposition 23. Soient $a, b \in A$. Alors,

$$a \sim b \iff \exists u \in A^\times \text{ tel que } b = ua$$

Définition 24. Soient $a_1, \dots, a_n \in A^*$.

- $d \in A$ est un **plus grand commun diviseur** "PGCD" de $a_1, \dots, a_m$ si d satisfait les deux propriétés suivantes :
  (i) $d \mid a_i, \forall i \in [\![1, n]\!]$.
  (ii) Si $\exists d' \in A$ tel que $d' \mid a_i, \forall i \in [\![1, n]\!]$, alors $d' \mid d$.
- $m \in A$ est un **plus petit commun multiple** "PPCM" de $a_1, \dots, a_n$ si m satisfait les deux propriétés suivantes :
  (i) $a_i \mid m, \forall i \in [\![1, n]\!]$.
  (ii) Si $\exists m' \in A$ tel que $a_i \mid m', \forall i \in [\![1, n]\!]$, alors $m \mid m'$.

Remarque 25. Un PGCD (resp. un PPCM), lorsqu'il existe, n'est pas toujours unique. Dans un anneau intègre, deux PGCD (resp. PPCM) sont toujours associés puisqu'ils se divisent l'un l'autre. Dans un anneau intègre, on peut donc noter $d \sim \text{pgcd}(a, b)$ (resp. $m \sim \text{pgcd}(a, b)$) lorsque d est un pgcd (resp. m est un ppcm) de a et de b.

Exemple 26. Soient $\mathbb{K}$ un corps commutatif. On pose $P_n = X^n - 1 \in \mathbb{K}[X]$ pour $n \in \mathbb{N}^*$. Alors, pour $a, b \in \mathbb{N}^*$, le PGCD unitaire de P_a et P_b est égal à $P_{\text{pgcd}(a,b)}$. **[GOU21]** p. 60

[ULM18] p. 40

Proposition 27. Soient $a, b \in A^*$. Un élément $c \in A$ est un PPCM de a et b si et seulement si $(a) \cap (b) = (c)$. En particulier, a et b admettent un PPCM si et seulement si $(a) \cap (b)$ est un idéal principal.

Proposition 28. Soient $a, b \in A^*$. Soit $d \in A$. Les assertions suivantes sont équivalentes.

(i) $d \mid a$, $d \mid b$ et il existe $u, v \in A$ tels que $d = au + bv$.

(ii) $d \sim \text{pgcd}(a, b)$ et il existe $u, v \in A$ tels que $d = au + bv$.

(iii) $(d) = (a, b)$.

Théorème 29 (Décomposition de Bézout)**.** On suppose A principal. Soient $a_1, \dots, a_n \in A^*$. Alors :

(i) Il existe d un pgcd de $a_1, \dots, a_n$. d est tel que $(d) = (a_1, \dots, a_n)$. En particulier, d est de la forme $d = b_1 a_1 + \cdots + b_n a_n$ avec $\forall i \in [\![1, n]\!]$, $b_i \in A$.

(ii) Il existe m un ppcm de $a_1, \dots, a_n$. m est tel que $(m) = (a_1) \cap \cdots \cap (a_n)$.

Remarque 30. Une façon d'obtenir ces coefficients si A est euclidien est d'utiliser l'algorithme d'Euclide généralisé.

Exemple 31. Dans $\mathbb{F}_2[X]$: p. 52

$$-X(X^3 + X^2 + 1) + (1 + X^2)(X^2 + X + 1) = 1$$

Application 32. $\overline{X}^2 + 1$ est inversible dans $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ d'inverse $\overline{X}^2 + X + 1$.

Définition 33. Deux éléments a et b de A sont dits **premiers entre eux** s'ils admettent un PGCD et $\text{pgcd}(a, b) \sim 1$. p. 41

Exemple 34. 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$.

Lemme 35 (Gauss)**.** On suppose A principal. Soient $a, b, c \in A$ avec a et b premiers entre eux. Alors,

$$a \mid bc \implies a \mid c$$

et

$$a \mid c \text{ et } b \mid c \implies ab \mid c$$

2. Anneaux factoriels

Définition 36. A est dit **factoriel** s'il est intègre et si, pour tout élément $a \in A^*$ non inversible, les conditions suivantes sont satisfaites : p. 63

(i) $a = q_1 q_2 \dots q_s$ avec $\forall i \in [\![1, s]\!]$, q_i irréductible (existence d'une décomposition en produit d'irréductibles).

(ii) Si $a = q_1 q_2 \dots q_s = \widetilde{q_1}\widetilde{q_2} \dots \widetilde{q_m}$ avec $\forall i \in [\![1, s]\!]$, q_i irréductible et $\forall i \in [\![1, s]\!]$, q_i irréductible, alors $s = m$ et pour toute permutation π d'indice, $q_i \widetilde{q_{\pi(i)}}$, $\forall i \in [\![1, s]\!]$ ("unicité" de la décomposition).

Proposition 37. Si A vérifie le Point (i), alors les assertions suivantes sont équivalentes : **[PER]** p. 48

(i) A vérifie le Point (ii).

(ii) A vérifie le lemme d'Euclide : si $p \in A$ est irréductible, alors $p \mid ab \implies p \mid a$ ou $p \mid b$.

(iii) Pour tout $p \in A$, p est irréductible si et seulement si (p) premier.

(iv) A vérifie le lemme de Gauss : si $p \in A$ est irréductible, alors $a \mid bc \implies a \mid c$ pour tout $a, b, c \in A$ avec a et b premiers entre eux.

Proposition 38. On suppose A factoriel. Tout élément $a \neq 0$ peut s'écrire de manière unique **[ULM18]** p. 65

$$a = u_a \prod_{p \in \mathcal{S}} p^{v_p(a)}$$

où $\mathcal{S}$ est un **système de représentants d'éléments premiers** de A (pour le relation $\sim$), u_a est inversible et $v_p(a) \in \mathbb{N}$ tous nuls sauf un nombre fini.

Exemple 39. Dans l'anneau principal (donc factoriel, voir Théorème 41) $\mathbb{Z}$, un choix standard pour $\mathcal{S}$ est l'ensemble des nombres premiers positifs.

Proposition 40. On suppose A factoriel. Soient $a, b \in A^*$. Alors, en reprenant les notations précédentes :

(i) $a \mid b \iff v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{S}$.

(ii) $\prod_{p \in \mathcal{S}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et de b.

(iii) $\prod_{p \in \mathcal{S}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et de b.

Théorème 41. Tout anneau principal est factoriel.

Contre-exemple 42. $\mathbb{Z}[i\sqrt{5}]$ est principal mais n'est pas factoriel.

Lemme 43 (Gauss)**.** On suppose A factoriel. Alors :

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est associé à 1).

(ii) $\forall P, Q \in A[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[GOZ] p. 10

Théorème 44 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose que A est factoriel et qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Application 45. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER] p. 67

3. Théorème chinois

[DEV]

Théorème 46 (Chinois)**.** Soient $I_1, \dots I_n$ des idéaux de A tels que $\forall i \neq j$, $I_i + I_j = A$. Alors,

$$\varphi : \begin{array}{ccc} A & \to & A/I_1 \times \cdots \times A/I_n \\ a & \mapsto & (a + I_1, \dots, a + I_n) \end{array}$$

est un morphisme surjectif de noyau $I = \bigcap_{i=1}^{n} I_i$. En particulier, A/I est isomorphe à $A/I_1 \times \cdots \times A/I_n$.

[ULM18] p. 56

Corollaire 47. On suppose A principal. Pour tout $\beta_1, \dots, \beta_n \in A$ et $m_1, \dots, m_n \in A$ premiers entre eux deux à deux, le système de congruences

$$\begin{cases} u \equiv \beta_1 \mod m_1 \\ \vdots \\ u \equiv \beta_n \mod m_n \end{cases}$$

admet une unique solution $u + (m_1 m_2 \dots m_n)$ dans $A/(m_1 m_2 \dots m_n)$. Il existe donc dans A une unique solution u unique à multiples de $m_1 m_2 \dots m_n$ près.

Exemple 48. Le système

$$\begin{cases} u \equiv 1 \mod 3 \\ u \equiv 3 \mod 5 \\ u \equiv 0 \mod 7 \end{cases}$$

admet une unique solution dans $\mathbb{Z}/105\mathbb{Z}$: $\overline{28}$. Les solutions dans $\mathbb{Z}$ sont donc de la forme $28 + 105k$ avec $k \in \mathbb{Z}$.

Application 49 (Polynômes d'interpolation de Lagrange)**.** Soit $\mathbb{K}$ un corps commutatif, $\alpha_1, \dots, \alpha_n$ des éléments distincts de $\mathbb{K}$ et $\beta_1, \dots, \beta_n$ des éléments de $\mathbb{K}$. Alors, il existe un unique polynôme $g \in \mathbb{K}[X]$ de degré inférieur ou égal à n tel que $g(\alpha_i) = \beta_i$ pour tout $i \in [\![1, n]\!]$.

III - Applications

1. Équations diophantiennes

Définition 50. L'anneau $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ est **l'anneau des entiers de Gauss**. On définit

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \to & \mathbb{N} \\ x + iy & \mapsto & x^2 + y^2 \end{array}$$

p. 69

Notation 51. On note Σ l'ensemble des entiers qui sont somme de deux carrés.

[I-P] p. 137

Lemme 52. Soit $p \geq 3$ un nombre premier. Alors $x \in \mathbb{F}_p^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.

Lemme 53. (i) N est multiplicative.

(ii) $\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$.

(iii) $\mathbb{Z}[i]$ est euclidien de stathme N.

Lemme 54. Soit p un nombre premier. Si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors $p \in \Sigma$.

[DEV]

Théorème 55 (Deux carrés de Fermat)**.** Soit $n \in \mathbb{N}^*$. Alors $n \in \Sigma$ si et seulement si $v_p(n)$ est pair pour tout p premier tel que $p \equiv 3 \mod 4$ (où $v_p(n)$ désigne la valuation p-adique de n).

2. En algèbre linéaire

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$. Soit $f : E \to E$ un endomorphisme de E.

Application 56. Il existe un unique polynôme de $\mathbb{K}[X]$ unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(f) = 0\}$: c'est le **polynôme minimal** de f, noté π_f. Il s'agit du polynôme unitaire de plus bas degré annulant f. Il divise tous les autres polynômes annulateurs de f.

[GOU21] p. 186

Théorème 57 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ sont premiers entre eux deux à deux. Alors,

$$\operatorname{Ker}(P(f)) = \bigoplus_{i=1}^{k} \operatorname{Ker}(P_i(f))$$

Application 58. f est diagonalisable si et seulement si π_f est scindé à racines simples.

Bibliographie

Les maths en tête **[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Théorie de Galois **[GOZ]**

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2e éd. Ellipses, 1er avr. 2009.
https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html.

L'oral à l'agrégation de mathématiques **[I-P]**

Lucas ISENMANN et Timothée PECATTE. *L'oral à l'agrégation de mathématiques. Une sélection de développements*. 2e éd. Ellipses, 26 mars 2024.
https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html.

Cours d'algèbre **[PER]**

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

Anneaux, corps, résultants **[ULM18]**

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.
https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html.