Leçon 122. Anneaux principaux. Applications.

1. Hypothèse. Au cours de cette leçon, tous les anneaux seront supposés commutatif et unitaire et leurs neutres seront respectivement notés par les chiffres 0 et 1.

1. Arithmétique dans un anneau principal

1.1. Notion d'idéal et de principalité

2. Définition. Un *idéal* d'un anneau A est un sous-groupe additif $I \subset A$ tel que, pour tous éléments $a \in A$ et $x \in I$, on ait $ax \in I$. Un idéal $I \subset A$ est *principal* s'il existe un élément $a \in A$ tel que $I = \langle a \rangle := aA$.
3. Exemple. Les parties A et $\{0\}$ sont toujours des idéaux principaux. Les parties $n\mathbf{Z}$ avec $n \in \mathbf{Z}$ sont des idéaux de l'anneau $\mathbf{Z}$.
4. Définition. Un anneau est principal si tous ses idéaux sont principaux.
5. Exemple. Un corps est un anneau principal. L'anneau $\mathbf{Z}$ est principal.
6. Théorème. Un anneau principal est factoriel.
7. Corollaire *(lemme d'Euclide).* Soit A un anneau principal. Alors un élément est irréductible si et seulement s'il est premier.
8. Théorème. Soient A un anneau principal et $p \in A \setminus (A^\times \cup \{0\})$ un élément. Alors les points suivants sont équivalents :
   – l'élément p est premier ;
   – l'idéal $\langle p \rangle$ est premier ;
   – l'idéal $\langle p \rangle$ est maximal.
9. Exemple. Pour un entier $n \geqslant 3$, l'anneau $\mathbf{Z}[i\sqrt{n}]$ n'est pas principal puisque l'élément 2 est irréductible et non premier.

1.2. PGCD et PPCM

10. Définition. Soit A un anneau. Le PGCD de deux éléments $a, b \in A \setminus \{0\}$ est un élément $d \in A$ vérifiant les points suivants :
   – $d \mid a$ et $d \mid b$;
   – pour tout élément $c \in A$, si $c \mid a$ et $c \mid b$, alors $c \mid d$.

L'anneau A est *à PGCD* si tout couple $(a, b) \in (A \setminus \{0\})^2$ admet un PGCD.
11. Exemple. Deux PGCD des entiers 4 et 6 sont les entiers ± 2.
12. Proposition. Un anneau principal est à PGCD.
13. Théorème *(Bézout).* Soient A un anneau principal et $a, b \in A \setminus \{0\}$ deux éléments non nuls. Soit $d \in A \setminus \{0\}$. Alors les points suivants sont équivalents :
   – l'élément d est un PGCD des éléments a et b ;
   – on a $(d) = (a) + (b)$.

Dans ce cas, il existe deux éléments $u, v \in A$ tels que $d = au + bv$.
14. Contre-exemple. L'hypothèse de principalité est nécessaire : dans l'anneau $K[X, Y]$, les monômes X et Y sont premiers entre eux et pourtant
$$\langle X \rangle + \langle Y \rangle = \langle X, Y \rangle = K[X, Y].$$
15. Théorème *(Gauss).* Soient A un anneau principal et $a, b, c \in A$ trois éléments. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$

1.3. Les anneaux euclidiens

16. Définition. Un anneau A est *euclidien* s'il existe une application $\nu \colon A \setminus \{0\} \longrightarrow \mathbf{N}$ vérifiant la propriété suivante :

pour tous éléments $a, b \in A$ avec $b \neq 0$, il existe deux éléments $q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$.

On dira que l'expression $a = bq + r$ est la *division euclidien* de l'élément a par l'élément b et que les éléments q et r en sont respectivement le *quotient* et le *reste*. Une telle application ν est un *stathme* sur l'anneau A.
17. Théorème. L'anneau $\mathbf{Z}$ est euclidien pour le stathme $x \longmapsto |x|$. Pour un corps K, l'anneau $K[X]$ pour le stahme $P \longmapsto \deg P$.
18. Corollaire. Soit A un anneau. Alors l'anneau $A[X]$ est principal si et seulement si l'anneau A est un corps.
19. Exemple. On retrouve que l'anneau $K[X, Y] \simeq K[X][Y]$ n'est pas principal.
20. Corollaire. Soit L/K une extension de corps. Alors le PGCD dans L de deux polynômes à coefficients dans K est le même que dans K.
21. Théorème. Un anneau euclidien est principal.
22. Corollaire. Soient K un corps et $P \in K[X]$ un polynôme. Alors l'anneau quotient $K[X]/\langle P \rangle$ est un corps si et seulement si le polynôme P est irréductible.
23. Définition. On considère l'anneau l'anneau
$$\mathbf{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbf{Z}\} \quad \text{avec} \quad a := \tfrac{1}{2}(1 + i\sqrt{19})$$
On introduit la norme $N \colon \mathbf{Z}[\alpha] \longrightarrow \mathbf{N}$ définie par l'égalité
$$N(z) = z\overline{z} = a^2 + ab + 5b^2, \qquad z = a + b\alpha \in \mathbf{Z}[\alpha].$$
24. Lemme. Soit A un anneau euclidien. Alors il existe un élément $x \in A \setminus A^\times$ tel que la restriction $A^\times \cup \{0\} \longrightarrow A/\langle x \rangle$ de la projection canonique soit surjective.
25. Proposition. L'anneau $\mathbf{Z}[\alpha]$ n'est pas euclidien.
26. Lemme. Soient $a, b \in \mathbf{Z}[\alpha] \setminus \{0\}$ deux éléments non nuls. Alors il existe deux éléments $q, r \in \mathbf{Z}[\alpha]$ vérifiant les points suivants : D1
   – $r = 0$ ou $N(r) < N(b)$;
   – $a = bq + r$ ou $2a = bq + r$.
27. Proposition. L'anneau $\mathbf{Z}[\alpha]$ est principal.

2. Résolution de problèmes arithmétiques

2.1. L'algorithme d'Euclide dans le cas euclidien

28. Théorème *(algorithme d'Euclide étendu).* Soient $a, b \in A \setminus \{0\}$ deux éléments non nuls d'un anneau euclidien A. Considérons les suites $(r_i)_{i \in \mathbf{N}}$, $(u_i)_{i \in \mathbf{N}}$ et $(v_i)_{i \in \mathbf{N}}$ de A définies de la manière suivante :
   – $r_0 = a$ et $r_1 = b$;
   – $u_0 = 1$ et $u_1 = 0$;
   – $v_0 = 0$ et $v_1 = 1$;
   – si $r_i \neq 0$, alors

- $\circ$ l'élément r_{i+1} est le reste d'une division euclidienne de r_{i-1} par r_i, associé au quotient q_i,
- $\circ$ si $i > 1$, alors $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$.

– si $r_i = 0$, alors $r_{i+1} = 0$.

Soit $N \in \mathbf{N}$ le plus petit entier tel que $r_{N+1} = 0$. Alors
$$\operatorname{pgcd}(a,b) \sim r_N \qquad \text{et} \qquad u_N a + v_N a = r_N.$$
29. Exemple. Plaçons-nous dans l'anneau $\mathbf{Z}$. On veut calculer une relation de Bézout associée aux entiers 15 et 36. On trouve successivement
$$\begin{aligned} 36 &= 1 \times 36 + 0 \times 15, \\ 15 &= 0 \times 36 + 1 \times 15, \\ 6 &= 1 \times 36 - 2 \times 15, \\ 3 &= -2 \times 36 + 5 \times 15. \end{aligned}$$
30. Théorème. L'algorithme d'Euclide étendu calcul le PGCD de deux polynômes non nuls $P, Q \in K[X] \setminus \{0\}$ en $\mathrm{O}(\deg P \deg Q)$ opérations sur le corps K.

31. Théorème. L'algorithme d'Euclide étendu calcul le PGCD de deux entiers non nuls $a, b \in \mathbf{Z}^*$ en $\mathrm{O}(\log a \log b)$ opérations binaires.

32. Application. Dans l'anneau $\mathbf{R}[X]/\langle X^2+1\rangle \simeq \mathbf{C}$, l'inverse d'un élément $\overline{a+bX}$ avec $(a,b) \neq (0,0)$ est la classe du polynôme $(a - iX)/(a^2+b^2)$.

2.2. Les systèmes de congruence

33. Théorème *(des restes chinois)*. Soient A un anneau unitaire et $I_1, \dots, I_n \subset A$ des idéaux deux à deux étrangers ($I_i + I_j = A$ si $i \neq j$). Alors l'application
$$\left| \begin{aligned} &A \longrightarrow A/I_1 \times \cdots \times A/I_n, \\ &x \longmapsto (x \mod I_1, \dots, x \mod I_n) \end{aligned} \right.$$
est un morphisme d'anneaux surjectif de noyau $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. En particulier, il induit un isomorphisme d'anneaux
$$A/I_1 \cdots I_n \longrightarrow A/I_1 \times \cdots \times A/I_n.$$
34. Corollaire *(des restes chinois dans $\mathbf{Z}$)*. Soient $m_1, \dots, m_n \in \mathbf{N}^*$ des entiers deux à deux premiers entre eux et $v_1, \dots, v_n \in \mathbf{Z}$ d'autres entiers. Alors il existe une unique solution $x \in [\![0, m_1 \cdots m_n - 1]\!]$ du système
$$\forall i \in [\![1, r]\!], \qquad x \equiv v_i \mod m_i. \tag{1}$$
35. Proposition *(interpolation de Lagrange)*. En reprenant les notations précédentes, pour tout indice $i \in [\![1, r]\!]$, il existe un entier $N_i \in [\![0, m_i - 1]\!]$ tel que $N_i M_i \equiv 1 \mod m_i$ avec $M_i = m_1 \cdots m_r / m_i$. Alors l'unique solution du système (1) est l'entier
$$\sum_{i=1}^{n} v_i N_i M_i.$$
36. Remarque. Les inverses N_i des entiers M_i modulo m_i se trouvent grâce à l'algorithme d'Euclide étendu.

37. Exemple. On souhaite résoudre le système
$$\begin{cases} x \equiv 0 & \mod 2, \\ x \equiv 2 & \mod 3, \\ x \equiv -2 & \mod 7. \end{cases}$$
On calcul d'abord $M := 2 \times 3 \times 7 = 42$. Les entiers 2, 3 et 7 étant premiers, ce système admet une unique solution dans l'intervalle $[\![0, 41]\!]$.

- L'élément $M_1 := M/2 = 21 \equiv 1$ est d'inverse $N_1 = 1$ dans $\mathbf{Z}/2\mathbf{Z}$.
- L'élément $M_2 := M/3 = 14 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/3\mathbf{Z}$.
- L'élément $M_3 := M/7 = 6 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/7\mathbf{Z}$.

Finalement, l'unique solution est $0 \times 21 \times 1 + 2 \times 14 \times (-1) - 2 \times 6 \times (-1) = -16$.

2.3. Le théorème des deux carrés

38. Cadre. On souhaite trouver les nombres entiers $n \in \mathbf{N}$ qui peuvent s'écrire sous la forme $n = a^2 + b^2$ avec $a, b \in \mathbf{N}$. On note $\Sigma \subset \mathbf{N}$ leur ensemble.

39. Remarque. Pour un *entier de Gauss* $z = a + ib \in \mathbf{Z}[i]$, on introduit sa *norme* comme étant la quantité réelle $N(z) := z\overline{z} = a^2 + b^2$. Alors un entier appartient à l'ensemble Σ si et seulement s'il est la norme d'un entier de Gauss.

40. Théorème. La norme $N \colon \mathbf{Z}[i] \longrightarrow \mathbf{N}$ est une application multiplicative. De plus, les éléments inversibles de l'anneau $\mathbf{Z}[i]$ sont les nombres ± 1 et $\pm i$.

41. Proposition. L'ensemble Σ est stable par multiplication.

42. Proposition. L'anneau $\mathbf{Z}[i]$ est euclidien pour le stathme N.

43. Lemme. Un élément $p \in \mathbf{Z}[i]$ appartient à l'ensemble Σ si et seulement s'il est irréductible dans l'anneau $\mathbf{Z}[i]$.

44. Théorème. Soit p un nombre premier. Alors
$$p \in \Sigma \iff p \equiv 1, 2 \mod 4.$$
45. Exemple. Le nombre 41 est premier et s'écrit $41 = 4^2 + 5^2$.

46. Corollaire. Soit $n \geqslant 2$ un entier qu'on écrit sous la forme
$$n = \prod_{p \in \mathscr{P}} p^{\nu_p(n)}.$$
Alors il appartient à l'ensemble Σ si et seulement si, pour tout nombre premier p tel que $p \equiv 3 \mod 4$, l'entier $\nu_p(n)$ est pair.

3. La principalité de l'anneau des polynômes sur un corps

3.1. Application à la théorie des corps

47. Définition. Soit L/K une extension. Un élément $x \in L$ est *algébrique* sur le corps K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$.

48. Exemple. Dans l'extension $\mathbf{C}/\mathbf{Q}$, le réel $\sqrt{2}$ est algébrique sur $\mathbf{Q}$ puisqu'il est annulé par le polynôme $X^2 - 2$.

49. Proposition. Soit $x \in L$ un élément algébrique sur K. Alors l'ensemble
$$\{P \in K[X] \mid P(x) = 0\}$$
est un idéal de l'anneau principal $K[X]$, donc il est engendré par un unique polynôme unitaire $\pi_x \in K[X]$.

50. Proposition. Soit $x \in L$ un élément. S'il existe un polynôme irréductible non nul $P \in K[X]$ vérifiant $P(x) = 0$, alors $\pi_x = P$.
51. Exemple. Dans l'extension $\mathbf{C}/\mathbf{Q}$, on a $\pi_{\sqrt{2}} = X^2 - 2$.
52. Proposition. Soit $x \in L$ un élément algébrique sur K. Alors le polynôme π_x est irréductible sur K.
- D2 -
53. Théorème *(de l'élément primitif)*. Soient L/K une extension finie de caractéristique nulle. Alors il existe un élément $z \in L$ vérifiant $L = K(z)$.

3.2. Application à l'algèbre linéaire

54. Proposition. Soient K un corps et E un K-espace vectoriel de dimension finie. Soit $u \in \mathscr{L}(E)$ un endomorphisme. Alors l'ensemble
$$\{P \in K[X] \mid P(u) = 0\}$$
est un idéal de l'anneau principal $K[X]$, donc il est engendré par un unique polynôme unitaire $\pi_u \in K[X]$.
55. Remarque. Attention, le polynôme minimal d'un endomorphisme n'est pas toujours irréductible : un endomorphisme nilpotent d'un espace vectoriel de dimension n est de polynôme minimal X^n.
56. Théorème. Le polynôme caractéristique χ_u divise le polynôme minimal π_u.
57. Théorème *(lemme des noyaux)*. Soient $P_1, \dots, P_k \in K[X]$ des polynômes deux à deux premiers entre eux. Notons $P \coloneqq P_1 \cdots P_k$. Alors
$$\operatorname{Ker} P(u) = \operatorname{Ker} P_1(u) \oplus \cdots \oplus \operatorname{Ker} P_k(u).$$
De plus, les projections sur chacun des sous-espaces $\operatorname{Ker} P_i(u)$ associés à cette décomposition sont des polynômes en l'endomorphisme u.
58. Application. On suppose que le polynôme χ_u est scindé et qu'on peut donc l'écrire sous la forme $\chi_u = \prod_{i=1}^{r} (X - \lambda_i)^{m_i}$. Alors
$$E = \bigoplus_{i=1}^{r} \operatorname{Ker}(u - \lambda_i \operatorname{Id}_E)^{m_i}.$$
59. Théorème. Soit $u \in \mathscr{L}(E)$ un endomorphisme. Alors les points suivants sont équivalents :
- l'endomorphisme u est diagonalisable ;
- l'endomorphisme u admet un polynôme annulateur scindé simple ;
- son polynôme minimal π_u est scindé simple ;
- son polynôme caractéristique χ_u est scindé et, pour toute racine $\lambda \in K$ du polynôme χ_u de multiplicité m, on a $m = \dim \operatorname{Ker}(u - \lambda \operatorname{Id}_E)$.

[1] Alin Bostan et al. *Algorithmes Efficaces en Calcul Formel.* 2017.
[2] Xavier Gourdon. *Algèbre.* 2e édition. Ellipses, 2009.
[3] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.
[4] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie.* 2e édition. De Boeck Supérieur, 2021.