Leçon 122 : Anneaux principaux. Exemples et applications.

Tous anneaux et corps seront, sauf mention contraire, supposés commutatifs. [Ulm18]

I Arithmétique dans un anneau principal

Soit A un anneau commutatif. $A^\times$ l'ensemble de ses inverses.

I.1 Divisibilité

Déf 1. Un idéal $I \subseteq A$ est dit principal s'il existe un élément a dans A tel que $I = (a)$.

Déf 2. Soient $a, b \in A$. On dit que a divise b, noté $a \mid b$, s'il existe $a \in A^\times$ tel que $b = ac$.

Prop 3. Pour tout $a, b \in A$, $a \mid b \iff (b) \subseteq (a)$.

Déf 4. Soient $a_1, \dots, a_m \in A \backslash \{0_A\}$:

1. L'élément $d \in A$ est appelé plus petit commun multiple de $a_1, \dots, a_m$ si pour tout $i \in \{1, \dots, m\}$, $a_i \mid d$, et si pour tout $d' \in A$, $(\forall i \in \{1, \dots, m\},\ a_i \mid d') \Rightarrow d \mid d'$.
2. L'élément $d \in A$ est appelé plus grand commun diviseur de $a_1, \dots, a_m$ si pour tout $i \in \{1, \dots, m\}$, $d \mid a_i$, et si pour tout $d' \in A$, $(\forall i \in \{1, \dots, m\},\ d' \mid a_i) \Rightarrow d' \mid d$.

C-ex 5. On n'a pas toujours existence des ppcm et pgcd. Par exemple, pour l'anneau $A = \{ \sum_{0 \leq i,j} a_{i,j} T^{2i+3j} : a_{i,j} \in \mathbb{Q} \} \subseteq \mathbb{Q}[T]$, T^2 et T^3 n'admettent pas de ppcm car $T^5 \nmid T^6$ dans l'anneau.

Prop 6. Soient $a, b \in A \backslash \{0_A\}$. Un élément $c \in A$ est un ppcm de a et b, si et seulement si, $(a) \cap (b) = (c)$.

Prop 7. Soient $a, b \in A \backslash \{0_A\}$. Pour $d \in A$, sont équivalents :

1. $d \mid a$, $d \mid b$, et il existe $s, t \in A$ tels que $d = as + bt$.
2. d est un pgcd de a et b, et il existe $s, t \in A$ tels que $d = as + bt$.
3. $(a, b) = (d)$.

Déf 8. Un élément $a \in A$ est dit :

1. irréductible, s'il est non nul, non inversible, et que pour tout $b, c \in A$, si $a = bc$, alors b est inversible ou c est inversible.
2. premier, s'il est non nul, non inversible et pour tout $b, c \in A$, $a \mid bc$ implique que $a \mid b$ ou $a \mid c$.

Prop 9. $a \in A$ est premier, si et seulement si, (a) est un idéal premier. C'est à dire que $bc \in (a)$ implique $b \in (a)$ ou $c \in (a)$.

Prop 10. Si A est intégre, alors tout élément premier est irréductible.

I.2 Anneaux principaux

Déf 11. Un anneau A est appelé principal si A est intègre, et si tout idéal de A est principal.

Ex 12. — $\mathbb{Z}$ est un anneau principal.

— $\mathbb{Z}[X]$ n'est pas un anneau principal.

Thm 13 (Décomposition de Bézout)**.** Dans un anneau principal A, le pgcd et le ppcm d'éléments non nuls $a_1, \dots, a_m$ existent. Un pgcd d de $a_1, \dots, a_m$ est tel que $(d) = (a_1, \dots, a_m)$. Un ppcm b de $(a_1, \dots, a_m)$ est tel que $(b) = (a_1) \cap \dots \cap (a_m)$.

Cor 14 (Egalité de Bézout)**.** Soient $a, b \in A$ non nuls. Si A est principal, d est un pgcd de a, b, si et seulement si, il existe $s, t \in A$ tels que $d = sa + tb$.

Cor 15. Dans un anneau principal, tout idéal premier non nul est maximal.

Lemme 16. Soit A un anneau principal. Soient $c \in A$, $a, b \in A$ premiers entre eux. Alors :

1. (Lemme de Gauss) $a \mid bc \Rightarrow a \mid c$.
2. $a \mid b$ et $b \mid c \Rightarrow ab \mid c$.

Prop 17. Si A est principal, un élément de A est premier, si et seulement si, il est irréductible.

Thm 18. Si A est principal, un idéal non nul $(a) \subseteq A$ est maximal, si et seulement si, a est irréductible dans A.

II Calcul effectif dans un anneau euclidien

II.1 Anneau euclidien

Déf 19. Un anneau A est dit euclidien s'il est intègre et s'il existe une fonction $\nu : A\backslash\{0_A\} \to \mathbb{N}$ avec la propriété que pour tout $a \in A$ et pour tout $b \in A\backslash\{0_A\}$, il existe $q, r \in A$ tels que $a = bq+r$, avec soit $r = 0$, soir $\nu(r) < \nu(b)$.

L'élément q est élément quotient et l'élément r est appelé reste de la division. La fonction ν est appelée stathme pour A.

Ex 20. 1. L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme $\nu(a+ib) = |a+ib|^2 = a^2+b^2$.

Prop 21. Tout anneau euclidien est principal.

C-ex 22. La réciproque est fausse, $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal, mais n'est pas euclidien.

Rq 23. Cette propriété nous donne que tout pgcd vérifie l'égalité de Bézout. La propriété d'anneau euclidien permet d'introduire un algorithme pour le calculer explicitement.

Algorithme 24 (Algorithme d'Euclide étendu généralisé)**.** On souhaite calculer un pgcd de a et b non nuls dans A, et déterminer ses coefficients de Bézout u, v. On pose $d_0 = a$, $d_1 = b$, $u_0 = 1$ et $u_1 = 0$.

- Tant que $d_1 \neq 0$, Faire :
  - Ecrire $d_0 = d_1 q + r$, avec $\nu(r) < \nu(d_1)$. $d_0 \leftarrow d_1$ et $d_1 \leftarrow r$.
  - $x \leftarrow u_1$, $u_1 \leftarrow u_0 - q \times u_1$, $u_0 \leftarrow x$.
- Fin Tant que.
- $r \leftarrow d_1$, $u \leftarrow u_0$ et $v \leftarrow$ "quotient de la division euclidienne de $(r - u \times a)$ par b". Renvoyer (r, u, v)

L'algorithme se termine et renvoie r = le pgcd de a et b, et (u, v) les coefficients de Bézout tels que $r = au + bv$.

Rq 25. L'algorithme dans $\mathbb{Z}$ a pour complexité $O((\ln N)^2)$

Ex 26. 1743 et 763 ont pour pgcd 43. Sa décomposition de Bézout est : $43 = 5 \times 1763 - 12 \times 731$.

Ex 27. Soient $f = X^3 + X^2 + 1$ et $g = X^2 + X + 1$ dans $\mathbb{F}_2[X]$. L'algorithme d'Euclide étendu nous donne que l'inverse de g dans $\mathbb{F}_2[X]/(f)$ est $\overline{X}^2 + \overline{1}$.

Déf 28. On considère $SL_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = 1\}$

Prop 29. Pour tout $M \in SL_2(\mathbb{Z})$, pour tout $a, b \in \mathbb{Z}$ non nuls, $\text{pgcd}(a, b) = \text{pgcd}(M \cdot \begin{pmatrix} a \\ b \end{pmatrix})$

Thm 30 (DEV 1.a)**.** Soient $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Alors S et T engendrent $SL_2(\mathbb{Z})$.

II.2 Anneau $\mathbb{K}[X]$

Thm 31. Si $\mathbb{K}$ est un corps, alors $\deg : \mathbb{K}[X]\backslash\{0\} \to \mathbb{N}$, $P \mapsto \deg(P)$ est un stathme pour l'anneau $\mathbb{K}[X]$. Dans l'anneau euclidien $\mathbb{K}[X]$, le quotient et le reste de la division sont uniques.

Thm 32. Soit A un anneau commutatif unitaire. Les propositions suivantes sont équivalentes :

i) A est un corps.

ii) $A[X]$ est euclidien.

iii) $A[X]$ est principal.

Cor 33. Soit $\mathbb{K}$ un corps et $f \in \mathbb{K}[X]$ non nul. L'anneau $\mathbb{K}[X]/(f)$ est un corps, si et seulement si, f est irréductible dans $\mathbb{K}[X]$.

Ex 34. $\mathbb{F}_5[X]/(X^3 + X + 1)$ est un corps.

II.3 Théorème chinois

Thm 35. Soit A un anneau commutatif unitaire, $n \geq 1$ un entier et $I_1, \ldots, I_n$ des idéaux de A tels que pour tout $i \neq j$, $I_i + I_j = A$. Alors l'application

$$\varphi : \begin{cases} A & \longrightarrow & A/I_1 \times \cdots \times A/I_n \\ a & \longmapsto & (a + I_1, \ldots, a + I_n) \end{cases}$$

est un morphisme d'anneau surjectif, de noyau $I := I_1 I_2 \cdots I_n \bigcap_{i=1}^{n} I_i$. En particulier, $A/I \simeq \prod_{i=1}^{n} A/I_i$.

Cor 36. En gardant les mêmes notations, pour tous $\beta_1, \dots, \beta_n \in A$, le système de congruence $\begin{cases} u \equiv \beta_1 \pmod{I_1} \\ \vdots \quad \vdots \quad \vdots \\ u \equiv \beta_n \pmod{I_n} \end{cases}$ possède une unique solution u modulo $I_1 I_2 \cdots I_n$.

Cor 37. Soit A un anneau principal, $n \geq 1$ et $m_1, \dots, m_n \in A$ premiers entres eux deux à deux. Alors $A/(m_1 \cdots m_n) \simeq A/(m_1) \times \cdots \times A/(m_n)$. En particulier, pour tous $\beta_1, \dots, \beta_n \in A$, le système $\begin{cases} u \equiv \beta_1 \pmod{m_1} \\ \vdots \quad \vdots \quad \vdots \\ u \equiv \beta_n \pmod{m_n} \end{cases}$ admet une unique solution dans $A/(m_1 \cdots m_n)$.

App 38 (DEV 1.b)**.** Soit $N \geq 2$. On pose $\Gamma_N = \{A \in SL_2(\mathbb{Z}) : A \equiv I_2 \pmod{N}\}$. Alors $SL_2(\mathbb{Z})/\Gamma_N \simeq SL_2(\mathbb{Z}/N\mathbb{Z})$ et $[SL_2(\mathbb{Z}) : \Gamma_N] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$, p premier.

App 39. Soit $\varphi : \mathbb{N} \to \mathbb{N}$, telle que $\varphi(0) = 0$ et pour tout $n \geq 1$, $\varphi(n) = |\{k \leq n : k \wedge n = 1\}|$ l'indicatrice d'Euler. Alors φ est multiplicative. De plus, si $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ est la décomposition en facteurs premiers de n, alors $\varphi(n) = p_i^{\alpha_i - 1}(p_i - 1)$.

Algorithme 40 (Algorithme de Garner)**.** Pour un anneau A euclidien, de stathme ν, l'algorithme de Garner construit de manière récursive une solution u de la forme $u = \gamma_1 + \gamma_2 m_1 + \gamma_3(m_1 m_2) + \dots + \gamma_n(m_1 \dots m_{n-1})$, avec $\nu(\gamma_i) < \nu(m_i)$.

1. Afin de vérifier la première équation $u \equiv \beta_1 \pmod{m_1}$, on pose $\gamma_1 = \beta_1$.
2. Supposons avoir déterminés $\gamma_1, \dots, \gamma_{i-1}$ vérifiants les $i-1$ premières équations. On pose γ_i tel que $\gamma_i(m_1 \dots m_{i-1}) \equiv \beta_i - (\gamma_1 + \gamma_2 m_1 + \dots + \gamma_{i-1}(m_1 \dots m_{i-2}) \pmod{m_i}$. Il suffit alors de déterminer l'inverse de $(m_1 \dots m_{i-1})$ dans $A/(m_i)$, avec l'algorithme d'Euclide étendu par exemple.

Ex 41. Les solutions dans $\mathbb{Z}$ du système $\begin{cases} u \equiv 1 \pmod 3 \\ u \equiv 3 \pmod 5 \\ u \equiv 0 \pmod 7 \end{cases}$ sont de la forme $28 + 105k$, avec $k \in \mathbb{Z}$.

Cor 42 (Interpolation de polynômes)**.** Soit $\mathbb{K}$ un corps, $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ distincts, et $\beta_1, \dots, \beta_n \in \mathbb{K}$. Alors il existe un unique polynôme $P \in \mathbb{K}_n[X]$ tel que $P(\alpha_i) = \beta_i$ pour i.

III Applications

III.1 Algèbre linéaire

Soit $\mathbb{K}$ un corps, et E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

Thm 43. Soit $u \in \mathscr{L}(E)$. L'application $\Theta_u : \mathbb{K}[X] \to \mathscr{L}(E)$, $P \mapsto P(u)$ est un morphisme de $\mathbb{K}$-algèbre. De plus, il existe un unique polynôme unitaire, noté μ_u, tel que $(\mu_u) = \operatorname{Ker} \Theta_u$. On l'appelle polynôme minimal de u.

Cor 44. Soit $u \in \mathscr{L}(E)$. Pour tout $P \in \mathbb{K}[X]$ tel que $P(u) = 0$, $\mu_u \mid P$.

Thm 45. Soit $u \in \mathscr{L}(E)$ et $x \in E$. L'application $\Theta_{u,x} : \mathbb{K}[X] \to E$, $P \mapsto P(u)(x)$ est une application linéaire. De plus, son noyau un idéal principal de $\mathbb{K}[X]$. Il existe un unique polynôme unitaire, noté $\mu_{u,x}$, tel que $(\mu_{u,x}) = \operatorname{Ker} \Theta_{u,x}$. On l'appelle polynôme minimal local en x de u.

Thm 46. Soit $\mathbb{L}/\mathbb{K}$ une extension de corps et $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$. L'application $\Psi_x : \mathbb{K}[X] \to \mathbb{L}$, $P \mapsto P(x)$ est un morphisme de $\mathbb{K}$-algèbre. De plus, il existe un unique polynôme unitaire, noté m_x, tel que $(m_x) = \operatorname{Ker} \Psi_x$. On l'appelle polynôme minimal en x.

Rq 47. Ces trois théorèmes découlent du fait que tout idéal de $\mathbb{K}[X]$ est principal.

Prop 48. Soient $u \in \mathscr{L}(E)$ et $P, Q \in \mathbb{K}[X]$. Alors $\operatorname{Ker} P(u) \cap \operatorname{Ker} Q(u) = \operatorname{Ker} \operatorname{pgcd}(P,Q)(u)$ et $\operatorname{Ker} P(u) + \operatorname{Ker} Q(u) = \operatorname{ppcm}(P,Q)(u)$.

Thm 49 (Lemme des noyaux)**.** Soient $u \in \mathscr{L}(E)$, $P_1, \dots, P_s \in \mathbb{K}[X]$ deux à deux premiers entre eux et $P = P_1 \cdots P_s$. Alors $\operatorname{Ker} P(u) = \bigoplus_{i=1}^{s} \operatorname{Ker} P_i(u)$.

Rq 50. Le lien entre pgcd et relation de Bézout, fournit par le fait que $\mathbb{K}[X]$ est principal, est nécessaire.

III.2 Factorisation dans un corps fini

[Odi23] Soit $\mathbb{F}_q$ un corps fini à $q = p^n$ éléments, p premier.

Déf 51. Soit A un anneau commutatif unitaire de caractéristique p. On appelle morphisme de Frobenius le morphisme d'anneau $Fr : A \to A$, $x \mapsto x^p$.

Lemme 52. 1. Si $A = \mathbb{F}_q$, $Fr^n = \mathrm{Id}_A$.

2. Si $A = \mathbb{F}_q[X]$, alors Fr est injectif, d'image $\mathbb{F}_q[X^p]$. Entre autre, pour tout $Q \in \mathbb{F}_q[X]$, il existe un unique $P \in \mathbb{F}_q[X]$ tel que $Q(X) = P(X)^p$.
3. Soient $P \notin \mathbb{F}_q[X^p]$ et $Q \in \mathbb{F}_q[X]$ tel que $P = \text{pgcd}(P, P')Q$. Alors Q est à facteurs simples.

Thm 53 (DEV 2)**.** Soit $P \in \mathbb{F}_q[X]$, unitaire de degré $N \geq 1$, à facteurs simples

i) On considère pour tout $0 \leq j \leq N-1$, le reste de la division euclidienne de X^{qj} par P qu'on note $\sum_{i=0}^{N} b_{ij} X^i$. Et on note $B = (b_{ij})_{0 \leq i,j \leq N-1} \in M_N(\mathbb{F}_q)$. Alors soit $H = \sum_{i=0}^{N-1} h_i X^i \in \mathbb{F}_q[X]$. P divise $H^q - H$ si et seulement si $(h_0, \ldots, h_{N-1}) \in \text{Ker}(B - I_N)$

ii) Soit $H \in \mathbb{F}_q[X]$, tel que $P \mid H^q - H$. Alors :

$$P = \prod_{\lambda \in \mathbb{F}_q} \text{pgcd}(P, H - \lambda)$$

iii) Le nombre de facteurs irréductibles de P est $N - \text{rg}(B - I_N)$

Algorithme 54 (Berlekamp)**.** Si $B - I_N$ est de rang $N - 1$, alors P est irréductible. Sinon, on choisit un polynôme H non constant tel que P divise $H^n - H$ grâce au calcul du noyau de $B - I_N$. On obtient une factorisation de P en facteurs non tous triviaux. En réitérant l'algorithme sur les facteurs trouvés, on obtient une décomposition en facteurs irréductibles de P.

Bibliographie

[Odi23] Alain Ninet Odile Fleury Loic Foissy. *Algèbre et calcul formel.* 2eme edition. ellipses, 2023.

[Ulm18] Felix Ulmer. *Anneaux, corps, résultants.* ellipses, 2018.