Cadre : On considère $\mathbb{K}$ un corps commutatif et $(A, +, \times)$ un anneau unitaire commutatif intègre.

I Anneau factoriel : pgcd et ppcm

1) Notion de divisibilité

Définition 1. Soient $a, b \in A$. On dit que a divise b, noté $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. C'est équivalent à dire que $(b) \subseteq (a)$.

Définition 2. Soient $a, b \in A$. On dit que a et b sont associés si $a \mid b$ et $b \mid a$. C'est équivalent à dire que $(a) = (b)$.

Remarque 3. *C'est une relation d'équivalence. Deux éléments associés sont indiscernables du point de vue de la divisibilité.*

Proposition 4. *Soient $a, b \in A$. Alors a et b sont associés si, et seulement si, il existe $u \in A^\times$ tel que $b = au$.*

Définition 5. Soit $a \in A$ non inversible et non nul. On dit que a est irréductible si, pour tous $b, c \in A$ tels que $a = bc$, on a $b \in A^\times$ ou $c \in A^\times$.

Exemple 6. *Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.*

Définition 7. $p \in A \setminus \{0\}$ est premier si $p \notin A^\times$ et, pour tous $a, b \in A$, $p \mid ab \Rightarrow (p \mid a$ ou $p \mid b)$.

2) Notions de pgcd et de ppcm

Définition 8. Soient $a, b \in A$. Pour $d \in A$ et $m \in A$, on dit que :

(i) d est pgcd de a et b, noté $d = a \wedge b$, si : $\forall c \in A, (c|a$ et $c|b) \Rightarrow c|d$.

(ii) m est ppcm de a et b, noté $m = a \vee b$, si : $\forall c \in A, (a|c$ et $b|c) \Rightarrow m|c$.

On dit que a et b sont premiers entre eux si $a \wedge b \in A^\times$.

Remarque 9. *L'existence de* pgcd *et* ppcm *n'est pas garantie en général. S'ils existent, ils sont définis à un inversible près. On peut généraliser à une famille quelconque d'éléments.*

Proposition 10. *Deux* pgcd *(ou* ppcm*) sont associés.*

Définition 11. On appelle système de représentants des irréductibles de A un ensemble P d'irréductibles tel que tout irréductible de A admette un unique associé dans P.

Exemple 12. *Les nombres premiers sont un système de représentants des irréductibles de $\mathbb{Z}$.*

Définition 13. Un anneau A est dit factoriel si tout $a \in A\setminus\{0\}$ se décompose sous la forme $a = u\prod_{p\in P} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$ presque tous nuls et P un système de représentants des irréductibles de façon unique à l'ordre des irréductibles près.

Exemple 14. *$\mathbb{Z}$ est factoriel, $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas.*

On suppose maintenant que A est un anneau factoriel.

Proposition 15. *Dans un anneau factoriel, les* pgcd *et* ppcm *existent.*

Proposition 16. *Soient $a, b \in A$, et soient $a = u\prod_{p\in P} p^{v_p(a)}$ et $b = v\prod_{p\in P} p^{v_p(b)}$ leurs décompositions en produits d'irréductibles. Alors :*

(i) $a \wedge b = \prod_{p\in P} p^{\min(v_p(a),v_p(b))}$

(ii) $a \vee b = \prod_{p\in P} p^{\max(v_p(a),v_p(b))}$

Application 17. *Dans un groupe, il existe un élément d'ordre l'exposant du groupe.*

Lemme 18 (Gauss)**.** *Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.*

Lemme 19 (Euclide)**.** *Soit $p \in A$ irréductible, et soit $a, b \in A$, alors $p|ab \Rightarrow p|a$ ou $p|b$.*

Corollaire 20. *Un élément d'un anneau factoriel est premier si, et seulement si, il est irréductible.*

Proposition 21. *Pour $a, b \in A$, $(a\wedge b)(a\vee b) = ab$ et $a\wedge(b\vee a) = a\vee(b\wedge a)$.*

3) Contenu d'un polynôme

Définition 22. Soit $P \in A[X]$ non nul. On appelle contenu de P, noté $c(P)$, le pgcd des coefficients de P. Si $c(P) = 1$, on dit que P est primitif.

Lemme 23. *Le produit de deux polynômes primitifs est primitif.*

Lemme 24. *Pour $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Théorème 25. *Soit $P \in A[X]$ non constant. Alors P est irréductible dans $A[X]$ si, et seulement si, il est primitif et irréductible dans $\mathbb{K}[X]$.*

Théorème 26 (Eisenstein)**.** *Soit $P(X) = \sum_{k=1}^{n} a_k X^k \in A[X]$ non constant. On suppose qu'il existe $p \in A$ irréductible divisant tous les a_k sauf a_n et tel que p^2 ne divise pas a_0. Alors P est irréductible dans $\mathbb{K}[X]$.*

Application 27. *Si p est premier, $\sum_{k=0}^{p-1} X^k$ est irréductible dans $\mathbb{Z}[X]$.*

II Anneau principal : Théorème de Bézout

Définition 28. Un idéal I de A est dit principal s'il est monogène. Un anneau A est dit principal s'il est intègre et si ses idéaux sont principaux.

Exemple 29. *L'anneau $\mathbb{Z}$ est principal, ainsi que $\mathbb{K}[X]$, mais pas $\mathbb{Z}[X]$. $\mathbb{Z}/n\mathbb{Z}$ est principal si, et seulement si, n est premier.*

On suppose maintenant que A est un anneau principal.

Proposition 30. *Soient A principal et $a, b \in A$. Alors $a \wedge b$ est un générateur de $(a) + (b)$, et $a \vee n$ est un générateur de $(a) \cap (b)$.*

Théorème 31 (Bézout)**.** *Soit A principal. Alors, pour tous $a, b \in A \setminus \{0\}$, il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = a \wedge b$.*

Corollaire 32. *Soient A principal et $a, b \in A$. Alors, a et b sont premiers si, et seulement si, il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = e$.*

Remarque 33. *Ces propriétés se généralisent à une famille quelconque d'éléments.*

Application 34 (Lemme des noyaux)**.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n. Soient $f \in \mathcal{L}(E)$ et $P = P_1 \dots P_k$ dans $\mathbb{K}[X]$ tel que les P_i sont premiers entre eux deux à deux, alors :*

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

Théorème 35. *Tout anneau principal est factoriel.*

III Anneau euclidien : Algorithmes

1) Obtention du pgcd

Définition 36. Un stathme est une application $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$). Un anneau intègre possédant un stathme est dit euclidien.

Exemple 37. *$\mathbb{Z}$ muni de la valeur absolue et $\mathbb{K}[X]$ muni du degré sont euclidien.*

Théorème 38. *Un anneau euclidien est principal.*

Exemple 39. *L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ est principal et non-euclidien.*

Proposition 40. *Soit $P \in A[X] \setminus \{0\}$ de coefficient dominant inversible, et $F \in A[X]$. Alors il existe $Q, R \in A[X]$ tels que $F = PQ + R$ et ($R = 0$ ou $\deg R < \deg P$).*

Corollaire 41. *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est euclidien.*

On suppose maintenant que A est un anneau euclidien.

Lemme 42. *Soient $a, b \in A$. Soient $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $\nu(r) < \nu(b)$). Si $r = 0$, alors $a \wedge b = b$, sinon, $a \wedge b = b \wedge r$.*

Méthode 43 (Algorithme d'Euclide)**.** *Grâce au lemme précédent, on peut réitérer un calcul de* pgcd *pour obtenir des éléments de stathme strictement plus petit. Ainsi, l'algorithme se termine par stricte décroissance du stathme dans $\mathbb{N}$, et on peut calculer le* pgcd *de deux éléments.*

Exemple 44. *On va calculer le* pgcd *de* 315 *et* 307 *dans $\mathbb{Z}$:*

$$\begin{aligned} 315 &= 1 \times 307 + 8 & \qquad 3 &= 2 \times 1 + 1 \\ 307 &= 8 \times 38 + 3 & \qquad 2 &= 2 \times 1 + 0 \\ 8 &= 2 \times 3 + 2 \end{aligned}$$

Ainsi, $315 \wedge 307 = 1$.

Exemple 45. *On va calculer le* pgcd *de $X^4 - 1$ et $X^3 - 1$:*

$$\begin{aligned} (X^4 - 1) &= (X^3 - 1) \times (X) + (X - 1) \\ (X^3 - 1) &= (X - 1) \times (X^2 + X + 1) \end{aligned}$$

Ainsi, $(X^4 - 1) \wedge (X^3 - 1) = X - 1$.

2) Recherche d'une relation de Bézout

Méthode 46 (Algorithme d'Euclide étendu)**.** *En remontant l'algorithme d'Euclide, on est capable de déterminer une relation de Bézout.*

Exemple 47. *Grâce au calcul de* $315 \wedge 307$*, on a :*

$$\begin{aligned} 1 &= 3 - 2 \times 1 \\ &= 3 - (8 - 2 \times 3) \times 1 = 3 \times 3 - 8 \\ &= (307 - 8 \times 38) \times 3 - 8 = 307 \times 3 - 8 \times 115 \\ &= 307 \times 3 - (315 - 307) \times 115 = 307 \times 118 - 315 \times 115 \end{aligned}$$

IV Applications en arithmétique

1) Équations diophantiennes

Définition 48. Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$. On appelle équation diophantienne toute équation de la forme $P(x_1, \dots, x_n) = 0$, dont on cherche les solutions sur $\mathbb{Z}^n$.

Proposition 49. *Soient $a, b \in \mathbb{Z}$ non nuls simultanément. L'équation $ax = b$ possède une unique solution si, et seulement si $a \mid b$. Dans ce cas, cette unique solution est $x = \frac{b}{a} \in \mathbb{Z}$.*

On s'intéresse à l'équation de la forme $ax + by = c$, avec $a, b, c \in \mathbb{Z}$.

Méthode 50. *On effectue l'algorithme d'Euclide pour trouver le* pgcd *de a et b, noté d. En remontant les étapes de l'algorithme, trouver une solution de $au' + bv' = d$ puis de $au + bv = c$. Si (x_0, y_0) est une solution générale, on obtient $a(x - u_0) = b(v - y_0)$ et par le lemme de Gauss, $a \mid v - y_0$ et $b \mid u - x_0$, donc $v = y_0 + ak$ et $u = x_0 - bk$.*

Théorème 51. *Soient $a, b \in \mathbb{Z}$. L'équation $ax + by = c$ admet des solutions si, et seulement si, $d = \text{pgcd}(a, b) \mid c$. Dans ce cas, soit (x_0, y_0) une solution particulière donnée par l'identité de Bézout. L'ensemble des solutions est donné par :*

$$\left\{ \left(x_0 + k \times \frac{b}{d}, y_0 - k \times \frac{a}{d} \right) \middle| k \in \mathbb{Z} \right\}$$

Exemple 52. *(i)* $42x + 66y = 10$ *n'admet pas de solutions.*

(ii) $112x + 70y = 14$ *a pour solutions les* $(2 + 5k, -3 - 8k)$ *pour* $k \in \mathbb{Z}$.

Théorème 53 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

2) Systèmes de congruence

Théorème 54 (Restes chinois)**.** *Soit $n = m_1 m_2$ avec $m_1 \wedge m_2 = 1$. Alors l'application définie par :*

$$\Phi : \left| \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{n}^m & \longmapsto & (\overline{n}^{m_1}, \dots, \overline{n}^{m_k}) \end{array} \right.$$

est un isomorphisme d'anneaux.

Généralisation 55. *Le théorème des restes chinois se généralise à tout produit d'entiers premiers entre eux deux à deux.*

Exemple 56. *Résolution de systèmes de congruences :*

$$\begin{cases} x & \equiv & 1[3] \\ x & \equiv & 2[4] \\ x & \equiv & 0[5] \end{cases} \Leftrightarrow x = 10 + 60k,\ k \in \mathbb{Z}$$

Corollaire 57. *Soient $m, n \in \mathbb{N}$ premiers entre eux. On a alors $(\mathbb{Z}/nm\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, et donc $\varphi(nm) = \varphi(n)\varphi(m)$.*

Corollaire 58. *Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Alors :*

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/(p_1^{\alpha_1})\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/(p_k^{\alpha_k})\mathbb{Z})^\times$$

Développements

— Critère d'Eisenstein (23,24,25,26) [FGN13a]

— Théorème de Sophie Germain (53) [FGN13a]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie.* DeBoeck

[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1.* Cassini