142 : PGCD et PPCM, algorithmes de calcul. Applications.

Contexte : Dans cette leçon, A désigne un anneau unitaire commutatif intègre et $\mathbf{K}$ un corps.

1. PGCD et PPCM dans un anneau intègre

Définition 1. Soient $a, b \in A$. On dit que a **divise** b s'il existe $c \in A$ tel que $b = ac$. On note alors $a|b$.

Définition 2. Soient $a, b \in A^*$ et $d, m \in A$. On dit que :

- ⋆ d est un **PGCD** de a et b si $m|a$, $m|b$ et $\forall c \in A$, $(c|a$ et $c|b) \Rightarrow c|m$.
- ⋆ m est un **PPCM** de a et b si $a|m$, $b|m$ et $\forall c \in A$, $(a|c$ et $b|c) \Rightarrow m|c$.

Remarque 3. Pour $a \in A$, a est un PGCD de 0 et a et 0 est un PPCM de 0 et a.

Exemple 4. 4 et -4 sont des PGCD de 16 et 12 dans $\mathbf{Z}$. $X^3 + 3X^2 + 2X$ est un PPCM de $X^2 + X$ et $X^2 + 3X + 2$ dans $\mathbf{K}[X]$.

Remarque 5. Les notions de PGCD et de PPCM s'étendent de manière analogue à un nombre fini d'éléments de A.

Exemple 6. 2 est un PGCD de $(4, 6, 12, 20)$ dans $\mathbf{Z}$.

Remarque 7. Les PGCD (resp. PPCM) de a et b sont tous égaux à multiplication par un élément inversible près. Ainsi, on note $a \wedge b$ (resp. $a \vee b$) un PGCD (resp. un PPCM) de a et b.

Proposition 8. Soient $a, b, c \in A$. On a $a \wedge b = b \wedge a$ et $a \wedge (b \wedge c) = (a \wedge b) \wedge c$. De même, $a \vee b = b \vee a$ et $a \vee (b \vee c) = (a \vee b) \vee c$

Proposition 9. Soient $a, b, k \in A$. Supposons que a et b ont un PGCD. Alors a et $b + ka$ ont un PGCD et $a \wedge (b + ka) = a \wedge b$. De plus, si ka et kb ont un PGCD, $ka \wedge kb = k(a \wedge b)$.

Proposition 10. Soient $a, b \in A$. Si a et b ont un PPCM, alors ils ont un PGCD et $(a \wedge b)(a \vee b) = ab$.

Exemple 11. 3 et $2 + i\sqrt{5}$ ont un PGCD mais pas de PPCM dans $\mathbf{Z}[i\sqrt{5}]$. 6 et $2 + 2i\sqrt{5}$ n'ont pas de PGCD dans $\mathbf{Z}[i\sqrt{5}]$.

Définition 12. On dit que $a_1, \ldots, a_r \in A$ sont **premiers entre eux** (dans leur ensemble) si $a_1 \wedge \ldots \wedge a_r = 1$. On dit que $a_1, \ldots, a_r$ sont **premiers entre eux deux à deux** si $\forall 1 \leq i < j \leq r$, $a_i \wedge a_j = 1$.

Exemple 13. 2, 4 et 5 sont premiers entre eux, mais pas deux à deux.

Remarque 14. Ces notions se confondent si $r = 2$.

Théorème 15 : Gauss. Soient $a, b, c \in A$. Si $a|bc$, $a \wedge b = 1$ et que $ac \wedge bc$ existe, alors $a|c$.

2. Cas des anneaux factoriels et principaux

2.1. Anneaux factoriels

On suppose désormais A factoriel.

Théorème 16. Soient $a, b \in A$. Alors ils possèdent un PGCD et un PPCM.

Proposition 17. Soit $\mathcal{P}$ un système complet de représentants irréductibles de A. Alors $\prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ est un PGCD et $\prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$ est PPCM de $a \in A$ et $b \in A$.

2.2. Anneaux principaux

On suppose désormais A principal. En particulier, A est factoriel.

Proposition 18. Soient $a, b, d, m \in A$. d est un PGCD (resp. m est un PPCM) de a et b ssi $aA + bA = dA$ (resp. $aA \cap bA = mA$).

Théorème 19 : Bézout. Soient $a, b \in A$. Ils sont premiers entre eux si et seulement s'il existe $u, v \in A$ tels que $au + bv = 1$.

Corollaire 20. Si $a \wedge b = d$, alors il existe $u, v \in A$ tels que $au + bv = d$.

Remarque 21. Les deux points précédents se généralisent au PGCD de $a_1, \ldots, a_r \in A$.

Application 22. Résolution de $ax + by = c$ dans A, où $a, b, c \in A$.

Application 23. Inversibilité de $\overline{m} \in \mathbf{Z}/n\mathbf{Z}$.

Application 24 : lemme des Noyaux. Soient V un $\mathbf{K}$-espace vectoriel de dimension finie et $P, Q \in \mathbf{K}[X]$ tels que $P \wedge Q = 1$. Alors pour tout $f \in \mathcal{L}(V)$, $\mathrm{Ker}(PQ(f)) = \mathrm{Ker}(P(f)) \oplus \mathrm{Ker}(Q(f))$.

Théorème 25 : restes chinois. Soient $a_1, \dots, a_r \in A$ non nuls, non inversibles et deux à deux premiers entre eux. Alors l'application

$$\varphi : \begin{array}{ccc} A/(a_1 \cdots a_r) & \to & A/(a_1) \times \cdots A/(a_r) \\ x \bmod a_1 \cdots a_r & \mapsto & (x \bmod a_1, \dots, x \bmod a_r) \end{array}$$

est un isomorphisme.

Application 26. L'ensemble des solutions de $\begin{cases} x \equiv 1[3] \\ x \equiv 8[5] \\ x \equiv 0[7] \end{cases}$ est $\{28 + 105k \ : \ k \in \mathbf{Z}\}$.

Application 27 : Interpolation de Lagrange.
Soient $x_1, \dots, x_n \in \mathbf{K}$ deux à deux distincts et $y_1, \dots, y_n \in \mathbf{K}$.
Un **polynôme interpolateur** des x_i en y_i est une solution du système $\{\forall 1 \leq i \leq n,\ P \equiv y_i[X - x_i]$.
Le théorème chinois assure l'existence d'un tel polynôme.

Exemple 28. $\overline{4}X^2 + \overline{4}X + \overline{2}$ est la solution de degré minimal dans $\mathbf{Z}/5\mathbf{Z}[X]$ de : $\left\{P(\overline{0}) = \overline{2}, P(\overline{1}) = \overline{0}, P(\overline{2}) = \overline{1}\right.$.

Proposition 29. Pour tous $n, m \geq 2$,

$$\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}/(n \wedge m)\mathbf{Z} \times \mathbf{Z}/(n \vee m)\mathbf{Z}.$$

Théorème 30. [DEV 1] Soient $n, m \in \mathbf{Z}$. Notons $\mu := n \vee m$ et $\delta := n \wedge m$. On dispose alors de deux morphismes φ, ψ :

$$\mathbf{Z}/\mu\mathbf{Z} \overset{\varphi}{\hookrightarrow} \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \overset{\psi}{\twoheadrightarrow} \mathbf{Z}/\delta\mathbf{Z}$$

tels que φ soit injectif, ψ surjectif et $\mathrm{Im}\varphi = \mathrm{Ker}\,\psi$.

Corollaire 31. [DEV 1] Le système $\begin{cases} x \equiv a[n] \\ x \equiv b[m] \end{cases}$ a des solutions si et seulement si $a \equiv b[\delta]$.

Application 32. [DEV 1] Le système $\begin{cases} x \equiv 2[21] \\ x \equiv 11[35] \end{cases}$ n'a pas de solutions.

En revanche, le système $\begin{cases} x \equiv 3[21] \\ x \equiv 10[35] \end{cases}$ est résoluble dans $\mathbf{Z}$.

3. Algorithmes de calcul dans les anneaux euclidiens

On suppose désormais A euclidien. En particulier, A est principal.

3.1. Un premier algorithme pour les entiers

Algorithme 33 : PGCD binaire.

Entrée : $a \geq b \geq 0$ des entiers.
SI $a = 0$: Renvoyer b.
SI $2|a$ et $2|b$: Renvoyer $2\times$ PGCD_binaire$(a/2, b/2)$.
SI $2|a$ et $2 \nmid b$: Renvoyer PGCD_binaire$(a/2, b)$.
SI $2 \nmid a$ et $2|b$: Renvoyer PGCD_binaire$(a, b/2)$.
SINON : Renvoyer PGCD_binaire$(\frac{a-b}{2}, b)$
Sortie : $a \wedge b$.

Proposition 34. L'algorithme du PGCD binaire se termine en au plus $\lceil \log_2(a) \rceil$ appels récursifs et renvoie $a \wedge b$.

3.2. Les algorithmes d'Euclide

Lemme 35. Soient $a, b, q, r \in A$. Si $a = bq + r$, alors $a \wedge b = b \wedge r$.

Algorithme 36 : Euclide.

Entrée : $(a, b) \in A^2$.
SI $b = 0$:
  Renvoyer a.

SINON :
  Renvoyer Euclide$(b, a \mod b)$
Sortie : $r \in A$ tel que $r = a \wedge b$.

Proposition 37. Cel algorithme termine et renvoie $a \wedge b$.

Exemple 38. $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$, où $n, m \in \mathbf{N}$.

Théorème 39 : Lamé. Soient $a > b \geq 1$ tels que $b < F_{k+1}$, où F_k est le k-ième terme de la suite de Fibonacci (définie par $F_0 = 0, F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour tout $n \in \mathbf{N}$). Alors l'algorithme d'Euclide pour (a, b) se termine en moins de k étapes et cette majoration est optimale.

Proposition 40. Soient $P, Q \in \mathbf{K}[X]$ tels que $\deg P \geq \deg Q \geq 1$. L'algorithme d'Euclide appliqué à (P, Q) termine en au plus $\deg P$ étapes.

Algorithme 41 : Euclide étendu.

Entrée : $(a, b) \in A^2$
$(r, u, v, r', u', v') := (a, 1, 0, b, 0, 1)$
$q := 0$
TANT QUE $r' \neq 0$ FAIRE :
  $q := r/r'$
  $(r, u, v, r', u', v') := (r', u', v', r - qr', u - qu', v - qv')$
FIN TANT QUE
Renvoyer (r, u, v)
Sortie : $(r, u, v) \in A^3$ tels que $r = a \wedge b = au + bv$.

Proposition 42. Cet algorithme termine et renvoie $(r, u, v) \in A^3$ tels que $r = a \wedge b = au + bv$.

Application 43. Calcul d'un inverse dans un corps de rupture.
Dans $\mathbf{Q}[X]/(X^2 - X - 1) \simeq \mathbf{Q}(\alpha)$, on a $(2\alpha + 1)^{-1} = 2\alpha - 3$.

Proposition 44. $\mathrm{GL}_2(\mathbf{Z})$ agit sur $\mathbf{Z}^2$ par

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \alpha a + \beta b \\ \gamma a + \delta b \end{pmatrix}.$$

Les orbites de cette action sont les $E_d := \left\{ \binom{a}{b} \in \mathbf{Z}^2 \mid a \wedge b = d \right\}$, pour $d \in \mathbf{N}$.

Application 45. Pour tout $(a, b) \in \mathbf{Z}^2$, l'algorithme d'Euclide étendu permet de déterminer $P \in \mathrm{GL}_2(\mathbf{Z})$ telle que $P\binom{a}{b} = \binom{a \wedge b}{0}$.

Remarque 46. Plus généralement, pour $(a_1, \ldots, a_n) \in \mathbf{Z}^n$, il existe $P \in \mathrm{GL}_n(\mathbf{Z})$ telle que $P(a_1 \cdots a_n)^\top = (d\, 0 \cdots 0)^\top$, où $d = a_1 \wedge \ldots \wedge a_n$.

3.3. Systèmes linéaires

Soient $n, m \in \mathbf{N}^*$. On cherche à résoudre l'équation $MX = B$, où $M \in \mathcal{M}_{m,n}(A)$ et $B \in A^m$.

Exemple 47. Si $m = 1$ et $A = \mathbf{Z}$, l'équation devient $(a_1 \ldots a_n)X = b$, avec $a_1, \ldots, a_n, b \in \mathbf{Z}$.
Notons $d := a_1 \wedge \ldots \wedge a_n$. D'après la Remarque 46, il existe $P \in \mathrm{GL}_n(\mathbf{Z})$ telle que

$$(a_1 \ \ldots \ a_n)P = (d\, 0 \ \ldots \ 0)$$

Posons $\widehat{X} := P^{-1}X$. L'équation équivaut alors à $d\widehat{x_1} = b$.
Ainsi, elle a une solution ssi $d|b$ et l'ensemble des solutions est alors :

$$\left\{ P(q\ x_2\ \ldots\ x_n)^\top \ :\ (x_2, \ldots, x_n) \in \mathbf{Z}^{n-1} \right\},$$

où q est le quotient de la division euclidienne de b par d.

Théorème 48 : Forme normale de Smith. [DEV 2]
Soit $M \in \mathcal{M}_{m,n}(A)$. Il existe $P \in \mathrm{GL}_m(A)$ et $Q \in \mathrm{GL}_n(A)$ telles que

$$PMQ = \begin{pmatrix} F & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{où } F = \mathrm{diag}(f_1, \ldots, f_r),$$

avec $r \in \mathbf{N}^*$ et $f_1, \ldots, f_r \in A^*$ tels que $f_1 | \ldots | f_r$.
De plus, r et les $(f_i)_{1 \leq i \leq r}$ sont uniques (modulo les unités de A).

Application 49. Calcul effectif des solutions de l'équation $MX = B$.

Exemple 50. L'ensemble des solutions dans $\mathbf{Z}^3$ de

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 12 \end{pmatrix}$$

est $\left\{ (-3 + 3k,\ 4 - 3k,\ k)^\top \ :\ k \in \mathbf{Z} \right\}$.

Références :

- ⋆ Pour la plupart du contenu du plan : Jean-Etienne Rombaldi, *Algèbre et géométrie* (2e édition)
- ⋆ Pour la partie sur les algorithmes : Michel Demazure, *Cours d'algèbre*
- ⋆ Pour le développement 1 : Philippe Caldero, Marie Perronier, *Carnet de voyage en Algébrie*
- ⋆ Pour le développement 2 : Didier Lesesvre, Pierre Montagnon, *131 développements pour l'oral*