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

Cadre : A est un anneau intègre commutatif.

Notation 1. On note $A^\times$ le groupe multiplicatif des inverses.

I Généralités et anneaux à PGCD

1 Généralités

Définition 2. [Per96, p. 46] Soient $a, b \in A$. On dit que a divise b et on écrit $a \mid b$ s'il existe $c \in A$ tel que $b = ac$.

Définition 3. [Per96, p. 46] Un élément $p \in A$ est dit irréductible si $p \neq 0$, n'est pas inversible et

$$p = ab \implies (a \text{ ou } b \text{ est inversible}).$$

Exemple 4.
1. Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et de degré 2 ayant un discriminant strictement négatif.
2. Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Définition 5. [Per96, p. 46] Soient $a, b \in A^*$. On dit que a et b sont associés s'il existe $u \in A^\times$ tel que $b = ua$.

Proposition 6. $a, b \in A^*$ sont associés si, et seulement si $(a) = (b)$.

Définition 7 (PGCD)**.** [Rom21, p. 242] Soient $a_1, \dots, a_r \in A^*$. On dit que ces éléments admettent un plus grand diviseur commun des a_i s'il existe $\delta \in A^*$ tel que

$$\begin{cases} \forall k \in [\![1, r]\!],\ \delta \mid a_k, \\ \text{tout diviseur commun à } a_1, \dots, a_r \text{ divise } \delta. \end{cases}$$

On le note $\mathrm{PGCD}(a_1, \dots, a_r)$.

Définition 8 (PPCM)**.** [Rom21, p. 246] Soient $a_1, \dots a_r \in A^*$. On dit que ces élément admettent un plus petit multiple commun s'il existe $\mu \in A^*$ tel que

$$\begin{cases} \forall k \in [\![1, r]\!], \mu \text{ est multiple de } a_k \\ \text{tout multiple commun à } a_1, \dots, a_r \text{ est multiple de } \mu. \end{cases}$$

On le note $\mathrm{PPCM}(a_1, \dots, a_r)$.

Remarque 9. L'existence d'un PGCD et d'un PPCM n'est pas garantie à priori. S'ils existent, il est unique à un inversible près.

2 Anneau à PGCD

Définition 10. On dit que A est un anneau à PGCD si deux éléments quelconques $a, b \in A^*$ admettent un PGCD.

Théorème 11. L'anneau A est à PGCD si, et seulement si deux éléments quelconques $a, b \in A^*$ admettent un PPCM. Dans ce cas, $ab = \mathrm{PGCD}(a, b)\,\mathrm{PPCM}(a, b)$ à une unité près.

A est désormais un anneau à PGCD.

Définition 12. [Rom21, p.245] Soient $a_1, \dots, a_r \in A$. On dit que $a_1, \dots, a_r$ sont premiers entre eux dans leur ensemble si $\mathrm{PGCD}(a_1, \dots, a_r) \in A^\times$. Si $r = 2$, on dira que a_1 et a_2 sont premiers entre eux.

Proposition 13. Soient $a_1, \dots, a_r \in A^*$. Soit d un diviseur commun aux a_i. En notant pour tout $i \in [\![1, n]\!]$, $a_i = d\alpha_i$,

$$\mathrm{PGCD}(a_1, \dots, a_r) = d\,\mathrm{PGCD}(\alpha_1, \dots, \alpha_r).$$

Théorème 14 (Gauss)**.** Soient $a, b \in A^*$. a et b sont premiers entre eux si, et seulement si pour tout $c \in A^*$

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

II Anneau factoriel, anneau principal

1 Anneau factoriel

Définition 15. On dit que A est factoriel si tout élément non nul de $a \in A$ s'écrit de façon unique, à permutation des facteurs près $a = up_1^{v_{p_1}(a)} \cdots p_r^{v_{p_r}(a)}$ avec $u \in A^\times$ et $p_1, \ldots, p_r$ des irréductibles.
L'entier $v_{p_i}(a)$ est appelé valuation p_i-adique de a.

Remarque 16. Soient $a, b \in A^*$. Si $a \mid b$ alors pour tous irréductible p de A, $v_p(a) \leqslant v_p(b)$.

Exemple 17.
1. Un anneau principal est factoriel.
2. $\mathbb{Z}$ est un anneau factoriel ;
3. $\mathbb{Z}[i]$ est un anneau factoriel ;
4. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $3 \times 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

Proposition 18. Un anneau factoriel est un anneau à PGCD. Soient $a, b \in A^* \setminus A^\times$, $a = up_1^{m_1} \cdots p_r^{m_r}$ et $b = vp_1^{n_1} \cdots p_r^{n_r}$ leur décomposition en facteurs irréductibles avec certains m_k ou n_k pouvant être éventuellement nuls. Alors $\prod_{i=1}^r p_i^{\min(m_i, n_i)}$ est un PGCD.

Théorème 19 (Bézout)**.** Soient $a_1, \ldots, a_r \in A^*$. Ces éléments sont premiers entre eux dans leur ensemble si, et seulement s'il existe $a_1, \ldots, a_r \in A$ tels que $\sum_{k=1}^r u_k a_k = 1$.

Théorème 20 (Critère d'Eisenstein)**.**

2 Anneau principal

Définition 21. A est dit principal si tous ses idéaux sont principaux.

Exemple 22.
1. Si A est un corps, $A[X]$ est principal.
2. Tout sous-anneau de $\mathbb{Q}$ est principal.

Proposition 23. Un anneau principal est factoriel.

On suppose désormais que A est principal.

Remarque 24. Les anneaux factoriels ne sont pas nécessairement principaux.

Proposition 25. Un anneau principal est un anneau à PGCD. Pour toute famille $a_1, \dots, a_r \in A^*$, il existe $\delta \in A^*$ tel que $(a_1, \dots, a_r) = (\delta)$. Cet élément s'écrit $\delta = \sum_{k=1}^{r} u_k a_k$ où $u_1, \dots, u_r$ sont des éléments de A et δ est un PGCD de $a_1, \dots, a_r$.

Théorème 26 (Bézout)**.** Soient $a_1, \dots, a_r \in A^*$. Ces éléments sont premiers entre eux si, et seulement s'il existe $(u_1, \dots, u_r) \in A^r$ tel que $\sum_{k=1}^{r} u_k a_k = 1$.

Corollaire 27. Soient $a, b, c \in A^*$ Si c est premier avec a, alors $a \wedge b = a \wedge (bc)$.

Corollaire 28. Soient $a_1, \dots, a_r, c \in A^*$. Si c est premier avec chacun des a_k, alors c est premier avec $\prod_{k=1}^{r} a_k$.

Corollaire 29 (Gauss)**.** Soient $a, b, c \in A^*$. Si a divise bc et a est premier avec b, alors a divise c.

Théorème 30. Soient $a_1, \dots, a_r \in A^*$. Il existe $\mu \in A$ tel que $(a_1) \cap \dots \cap (a_r) = (\mu)$.

Corollaire 31. Soient $a_1, \dots, a_r \in A^*$. Si les a_k sont deux à deux premiers entre eux, alors $\mathrm{PPCM}(a_1, \dots, a_r) = \prod_{k=1}^{r} a_k$.

Théorème 32 (Chinois)**.** Soient $a_1, \dots a_r \in A^*$ deux à deux premiers entre eux. L'application $\varphi : \begin{array}{ccc} A & \longrightarrow & \prod_{j=1}^{r} \frac{A}{(a_j)} \\ x & \longmapsto & (\pi_j(x))_{1 \leqslant j \leqslant r} \end{array}$ est un morphisme d'anneaux surjectifs de noyau $\ker(\varphi) = \left(\prod_{j=1}^{r} a_j\right)$. φ induit un isomorphisme d'anneaux $\overline{\varphi} : \begin{array}{ccc} \frac{A}{\left(\prod_{j=1}^{r} a_j\right)} & \longrightarrow & \prod_{j=1}^{r} \frac{A}{(a_j)} \\ \pi(x) & \longmapsto & (\pi_j(x))_{1 \leqslant j \leqslant r} \end{array}$ d'inverse $\overline{\varphi}^{-1} : \begin{array}{ccc} \prod_{j=1}^{r} \frac{A}{(a_j)} & \longrightarrow & \frac{A}{\prod_{j=1}^{r}(a_j)} \\ (\pi'_j x_j)_{1 \leqslant j \leqslant r} & \longmapsto & \frac{}{\sum_{i=1}^{r} x_i u_i b_i} \end{array}$ où $(u_j)_{1 \leqslant j \leqslant r}$ est une suite de A telle que $\sum_{j=1}^{r} u_j b_j = 1$.

Application 33. Résolution d'une équation diophantienne dans $\mathbb{Z}$.

III Anneau euclidien et algorithmes de calculs

Définition 34. A est dit euclidien s'il existe un stathme, *i.e.* une application $\varphi : A^* \longrightarrow \mathbb{N}$ tel que pour tout couple $(a, b) \in A$ avec $b \neq 0$, il existe $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$.

Proposition 35. Un anneau euclidien est principal.

Méthode 36 (Algorithme d'Euclide)**.** Soient $a, b \in A^*$ tels que $\varphi(a) \geqslant \varphi(b)$.
On note $r_0 = b$. Soit r_1 le reste de la division euclidienne de a par b. $r_1 = 0$ ou bien $r_1 \neq 0$ et $0 \leqslant \varphi(r_1) < \varphi(r_0)$.
Pour $n \geqslant 2$, si $r_{n-1} = 0$, alors $r_n = 0$ sinon r_n est le reste de la division euclidienne de r_{n-2} par r_{n-1}.
Il existe $p \in \mathbb{N}$ tel que $r_p = 0$, $0 \leqslant \varphi(r_{p-1}) < \cdots < \varphi(r_1) < \varphi(r_0)$ et $a \wedge b = r_{p-1}$.

Exemple 37. [Gou21, p. 12] $(26, -11)$ est une solution de $47u + 111v = 1$.

Méthode 38 (Algorithme d'Euclide étendu)**.**

Méthode 39 (Décomposition en éléments simples)**.**

Application 40. [Gou21, p. 204]

Références

[Per96] Daniel Perrin. Cours d'algèbre. Ellipses, 1996.

[Gou21] Xavier Gourdon. Les maths en tête, Algèbre. Ellipses, 2021.

[Rom21] Jean-Étienne Rombaldi. Mathématiques pour l'Agrégation, Algèbre et Géométrie. De Boeck, 2021.