142 PGCD et PPCM, algorithmes de calcul. Applications.

I - Notion de PGCM/PPCM dans un anneau

Soit A un anneau commutatif unitaire.

Définition 1. Soient $a, b \in A$. [ULM18] p. 39

— On dit que a **divise** b (ou que b est un multiple de a), noté $a \mid b$ s'il existe $c \in A$ tel que $b = ac$.

— On dit que a et b sont **associés**, noté $a \sim b$ si $a \mid b$ et si $b \mid a$.

Remarque 2. Soient $a, b \in A$.

— $a \mid b \iff (b) \subseteq (a)$.

— $a \sim b \iff (b) = (a)$. Ainsi, $\sim$ est une relation d'équivalence sur A.

Proposition 3. Soient $a, b \in A$. Alors,

$$a \sim b \iff \exists u \in A^\times \text{ tel que } b = ua$$

Définition 4. Soient $a_1, \dots, a_n \in A^*$.

— $d \in A$ est un **plus grand commun diviseur** "PGCD" de $a_1, \dots, a_m$ si d satisfait les deux propriétés suivantes :

(i) $d \mid a_i, \forall i \in [\![1, n]\!]$.

(ii) Si $\exists d' \in A$ tel que $d' \mid a_i, \forall i \in [\![1, n]\!]$, alors $d' \mid d$.

— $m \in A$ est un **plus petit commun multiple** "PPCM" de $a_1, \dots, a_n$ si m satisfait les deux propriétés suivantes :

(i) $a_i \mid m, \forall i \in [\![1, n]\!]$.

(ii) Si $\exists m' \in A$ tel que $a_i \mid m', \forall i \in [\![1, n]\!]$, alors $m \mid m'$.

Remarque 5. Un PGCD (resp. un PPCM), lorsqu'il existe, n'est pas toujours unique. Dans un anneau intègre, deux PGCD (resp. PPCM) sont toujours associés puisqu'ils se divisent l'un l'autre. Dans un anneau intègre, on peut donc noter $d \sim \text{pgcd}(a, b)$ (resp. $m \sim \text{pgcd}(a, b)$) lorsque d est un pgcd (resp. m est un ppcm) de a et de b.

Exemple 6. Soient $\mathbb{K}$ un corps commutatif. On pose $P_n = X^n - 1 \in \mathbb{K}[X]$ pour $n \in \mathbb{N}^*$. Alors, pour $a, b \in \mathbb{N}^*$, le PGCD unitaire de P_a et P_b est égal à $P_{\text{pgcd}(a,b)}$. [GOU21] p. 60

Proposition 7. Soient $a, b \in A^*$. Un élément $c \in A$ est un PPCM de a et b si et seulement si $(a) \cap (b) = (c)$. En particulier, a et b admettent un PPCM si et seulement si $(a) \cap (b)$ est un idéal principal. [ULM18] p. 40

Proposition 8. Soient $a, b \in A^*$. Soit $d \in A$. Les assertions suivantes sont équivalentes.

(i) $d \mid a$, $d \mid b$ et il existe $u, v \in A$ tels que $d = au + bv$.

(ii) $d \sim \text{pgcd}(a, b)$ et il existe $u, v \in A$ tels que $d = au + bv$.

(iii) $(d) = (a, b)$.

Définition 9. Deux éléments a et b de A sont dits **premiers entre eux** s'ils admettent un PGCD et $\text{pgcd}(a, b) \sim 1$.

Exemple 10. 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$.

II - Dans un anneau principal

Dans cette section, A désigne toujours un anneau commutatif unitaire. On le suppose de plus principal.

1. Existence

Théorème 11 (Décomposition de Bézout)**.** Soient $a_1, \dots, a_n \in A^*$. Alors :

(i) Il existe d un pgcd de $a_1, \dots, a_n$. d est tel que $(d) = (a_1, \dots, a_n)$. En particulier, d est de la forme $d = b_1 a_1 + \cdots + b_n a_n$ avec $\forall i \in [\![1, n]\!]$, $b_i \in A$.

(ii) Il existe m un ppcm de $a_1, \dots, a_n$. m est tel que $(m) = (a_1) \cap \cdots \cap (a_n)$.

Exemple 12. Dans $\mathbb{F}_2[X]$: p. 52

$$-X(X^3 + X^2 + 1) + (1 + X^2)(X^2 + X + 1) = 1$$

Application 13. $\overline{X}^2 + 1$ est inversible dans $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ d'inverse $\overline{X}^2 + X + 1$.

Lemme 14 (Gauss)**.** Soient $a, b, c \in A$ avec a et b premiers entre eux. Alors, p. 42

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

et

$$a \mid c \text{ et } b \mid c \implies ab \mid c$$

2. Dans les anneaux euclidiens

a. Principalité des anneaux euclidiens

Proposition 15. Un anneau euclidien est principal.

On a donc existence de PGCD et de PPCM dans un tel anneau, mais la structure euclidienne permet de plus de fournir des algorithmes de calculs.

Théorème 16. Si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est un anneau euclidien de stathme le degré. De plus, le quotient et le reste sont uniques.

p. 47

Corollaire 17. Les assertions suivantes sont équivalentes :

(i) A est un corps commutatif.

(ii) $A[X]$ est un anneau euclidien.

(iii) $A[X]$ est un anneau principal.

b. Algorithmes de calcul

Lemme 18. On suppose A euclidien de stathme ν. Soient $a, b \in A^*$ et r un reste dans la division euclidienne de a par b. À inversible près, on a alors :

— Si $r = 0$: $\text{pgcd}(a,b) = b$.

— Sinon : $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.

[ROM21] p. 264

Théorème 19 (Algorithme d'Euclide)**.** On suppose A euclidien de stathme ν. Soient $a, b \in A^*$ tels que $\nu(a) \geq \nu(b)$. On définit une suite (r_k) décroissante (au sens du stathme) par :

— $r_k = b$;

— r_1 est un reste dans la division euclidienne de a par b, on a donc $r_1 = 0$ ou $0 \leq \nu(r_1) < \nu(r_0)$;

— pour $k \geq 2$, si $r_{k-1} = 0$, alors $r_k = 0$, sinon r_k est un reste dans la division euclidienne de r_{k-2} par r_{k-1} et on a $r_k = 0$ ou $0 \leq \nu(r_k) < \nu(r_{k-1})$.

$\text{pgcd}(a,b)$ est alors le dernier reste non nul dans cette suite de divisions euclidiennes, que l'on note r_{n-1}.

Remarque 20. On peut “remonter” l’algorithme d’Euclide pour obtenir les coefficients de Bézout. On parle alors d’algorithme d’Euclide “étendu”.

Au lieu de faire les calculs en deux temps (descente, puis remontée), on peut tout faire en même temps via l’algorithme suivant. **[ULM18]** p. 44

Proposition 21 (Algorithme d’Euclide généralisé)**.** En reprenant les notations du Théorème 19 :

- Étape 0 : On écrit $r_0 = a = u_0 \times a + v_0 \times b$ avec $(u_0, v_0) = (1, 0)$.
- Étape 1 : On écrit $r_1 = b = u_1 \times a + v_1 \times b$ avec $(u_1, v_1) = (0, 1)$.
- Étape 2 : On écrit $r_0 - q_1 r_1 = r_2 = u_2 \times a + v_2 \times b$ avec $(u_2, v_2) = (1, -q_1)$.
- …
- Étape k : On écrit $r_{k-1} - q_k r_k = r_{k+1} = u_{k+1} \times a + v_{k+1} \times b$.
- …
- Étape $n-1$: On écrit $r_{n-2} - q_{n-1} r_{n-1} = r_n = u_n \times a + v_n \times b$.
- Étape n : On écrit $r_{n-1} - q_n r_n = 0 = u_{n+1} \times a + v_{n+1} \times b$.

À la fin, on obtient $\text{pgcd}(a, b) = r_n = u_n a + v_n b$.

Exemple 22. Calculons le PGCD et les coefficients de Bézout de 1763 et 731 dans $\mathbb{Z}$.

				1763	=	1	×	1763	+	0	×	731
				731	=	0	×	1763	+	1	×	731
Il y va	2	fois	reste	301	=	1	×	1763	+	(-2)	×	731
	2	fois	reste	129	=	(-2)	×	1763	+	5	×	731
	2	fois	reste	43	=	5	×	1763	+	(-12)	×	731
	3	fois	reste	0	=	(-17)	×	1763	+	41	×	731

On a $\text{pgcd}(1763, 731) = 43 = 5 \times 1763 - 12 \times 731$.

[FFN] p. 23

Proposition 23. En reprenant les notations précédentes, on a

$$\forall k \in [\![0, n-1]\!],\ r_k \geq \left(\frac{1+\sqrt{5}}{2}\right)^{n-k}$$

Corollaire 24. En reprenant les notations précédentes, cet algorithme a une complexité en $O(\ln(a) \times \ln(b))$.

3. Dans un anneau factoriel

Proposition 25. Si A vérifie la relation $(*)$ de la Proposition 26, alors les assertions suivantes sont équivalentes : [PER] p. 48

(i) A vérifie le lemme d'Euclide : si $p \in A$ est irréductible, alors $p \mid ab \implies p \mid a$ ou $p \mid b$.

(ii) Pour tout $p \in A$, p est irréductible si et seulement si (p) premier.

(iii) A vérifie le lemme de Gauss : si $p \in A$ est irréductible, alors $a \mid bc \implies a \mid c$ pour tout $a, b, c \in A$ avec a et b premiers entre eux.

Proposition 26. On suppose A factoriel. Tout élément $a \neq 0$ peut s'écrire de manière unique [ULM18] p. 65

$$a = u_a \prod_{p \in \mathcal{S}} p^{v_p(a)} \qquad (*)$$

où $\mathcal{S}$ est un **système de représentants d'éléments premiers** de A (pour la relation $\sim$), u_a est inversible et $v_p(a) \in \mathbb{N}$ tous nuls sauf un nombre fini.

Exemple 27. Dans l'anneau principal (donc factoriel, voir Théorème 29) $\mathbb{Z}$, un choix standard pour $\mathcal{S}$ est l'ensemble des nombres premiers positifs.

Proposition 28. On suppose A factoriel. Soient $a, b \in A^*$. Alors, en reprenant les notations précédentes :

(i) $a \mid b \iff v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{S}$.

(ii) $\prod_{p \in \mathcal{S}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et de b.

(iii) $\prod_{p \in \mathcal{S}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et de b.

Théorème 29. Tout anneau principal est factoriel.

Contre-exemple 30. $\mathbb{Z}[i\sqrt{5}]$ est principal mais n'est pas factoriel.

Lemme 31 (Gauss)**.** On suppose A factoriel. Alors :

(i) Le produit de deux polynômes primitifs est primitif (ie. dont le PGCD des coefficients est associé à 1).

(ii) $\forall P, Q \in A[X] \setminus \{0\}$, $\gamma(PQ) = \gamma(P)\gamma(Q)$ (où $\gamma(P)$ est le contenu du polynôme P).

[GOZ] p. 10

[DEV]

Théorème 32 (Critère d'Eisenstein)**.** Soient $\mathbb{K}$ le corps des fractions de A et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$. On suppose que A est factoriel et qu'il existe $p \in A$ irréductible tel que :

(i) $p \mid a_i$, $\forall i \in [\![0, n-1]\!]$.

(ii) $p \nmid a_n$.

(iii) $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{K}[X]$.

Application 33. Soit $n \in \mathbb{N}^*$. Il existe des polynômes irréductibles de degré n sur $\mathbb{Z}$.

[PER] p. 67

III - Applications

1. En algèbre linéaire

Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{K}$. Soit $f : E \to E$ un endomorphisme de E.

Proposition 34. Il existe un unique polynôme de $\mathbb{K}[X]$ unitaire qui engendre l'idéal $\{P \in \mathbb{K}[X] \mid P(f) = 0\}$: c'est le **polynôme minimal** de f, noté π_f. Il s'agit du polynôme unitaire de plus bas degré annulant f. Il divise tous les autres polynômes annulateurs de f.

[GOU21] p. 186

Théorème 35 (Lemme des noyaux)**.** Soit $P = P_1 \dots P_k \in \mathbb{K}[X]$ où les polynômes $P_1, \dots, P_k$ sont premiers entre eux deux à deux. Alors,

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

Application 36. f est diagonalisable si et seulement si π_f est scindé à racines simples.

2. Systèmes de congruences

Proposition 37. Soit a un entier non nul. L'équation

$$ax \equiv 1 \mod n$$

admet des solutions si et seulement si $\text{pgcd}(a,n) = 1$.

[ROM21] p. 289

Corollaire 38. Soient a un entier non nul et b un entier relatif. L'équation

$$ax \equiv b \mod n$$

a des solutions si et seulement si $d = \text{pgcd}(a,n) \mid b$. Dans ce cas, l'ensemble des solutions est

$$\left\{ \frac{b}{d}x_0 + k\frac{n}{d} \mid k \in \mathbb{Z} \right\}$$

où x_0 est une solution de l'équation $\frac{a}{n}x \equiv 1 \mod n$.

[DEV]

Théorème 39 (Chinois)**.** Soient $n_1, \dots, n_r \geq 2$ des entiers. On note $n = \prod_{i=1}^r n_i$ et $\pi_k = \pi_{n_k\mathbb{Z}}$ la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/k\mathbb{Z}$ pour tout $k \in [\![1,r]\!]$.

Les entiers $n_1, \dots, n_r$ sont premiers entre eux si et seulement si les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ sont isomorphes. Dans ce cas, l'isomorphisme est explicité par l'application

$$\psi : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \\ \pi_n k & \mapsto & (\pi_i(k))_{i \in [\![1,r]\!]} \end{array}$$

p. 285

Exemple 40.

$$\begin{cases} k \equiv 2 \mod 4 \\ k \equiv 3 \mod 5 \\ k \equiv 1 \mod 9 \end{cases}$$

admet pour ensemble de solutions $\{838 + 180q \mid q \in \mathbb{Z}\}$.

p. 291

Bibliographie

Les maths en tête **[GOU21]**

Xavier GOURDON. *Les maths en tête. Algèbre et probabilités*. 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

Théorie de Galois **[GOZ]**

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2e éd. Ellipses, 1er avr. 2009.
https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html.

Algèbre et calcul formel **[FFN]**

Loïc Foissy ODILE FLEURY et Alain NINET. *Algèbre et calcul formel. Agrégation de Mathématiques Option C*. 2e éd. Ellipses, 9 mai 2023.
https://www.editions-ellipses.fr/accueil/14799-algebre-et-calcul-formel-agregation-de-mathematiques-option-c-2e-edition-9782340078567.html.

Cours d'algèbre **[PER]**

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

Mathématiques pour l'agrégation **[ROM21]**

Jean-Étienne ROMBALDI. *Mathématiques pour l'agrégation. Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 20 avr. 2021.
https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie.

Anneaux, corps, résultants **[ULM18]**

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.
https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html.