142

PGCD et PPCM. Algorithmes de calcul. Exemples.

I] PGCD et PPCM dans un anneau factoriel

1] À partir de la divisibilité

Soit A un anneau intègre unitaire.

Définition 1 : Soit $a_1;\dots;a_n \in A^*$. On appelle PGCD des $(a_i)_{i=1}^n$ tout élément $d \in A^*$ tel que :
(1) $\forall i \in [\![1;n]\!], d \mid a_i$
(2) $\forall c \in A^*, (\forall i \in [\![1;n]\!], c \mid a_i) \Rightarrow c \mid d$

Proposition 2 : Soit $a_1;\dots;a_n \in A^*$ et d un PGCD des $(a_i)_{i=1}^n$.
Alors : $d' \in A^*$ est un autre PGCD de $(a_i)_{i=1}^n$ ssi d et d' sont associés ($\exists c \in A^\times$ tel que $d = cd'$)
ssi $\langle d \rangle = \langle d' \rangle$

Exemple 3 : X et $2X$ sont des PGCD de $X(X-1)$ et $X(X+1)$ dans $\mathbb{R}[X]$.

Remarque 4 : Dans ce cas, on note $a_1 \wedge \dots \wedge a_n$ la classe d'équivalence des PGCD modulo la relation d'association dans A.

Proposition 5 : Soit A tel que pour tout $(a_i)_{i=1}^n$, il existe un PGCD.
Alors : pour tout $a_1, a_2, a_3 \in A^*$, (1) $a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge a_3 = a_1 \wedge (a_2 \wedge a_3)$
(2) $a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge (a_2 \wedge a_3)$

Corollaire 6 : $\forall (a_i)_{i=1}^n \in A^*$ ont un PGCD ssi $\forall a_1, a_2 \in A^\times$, ont un PGCD.

Exemple 7 : Les PGCD existent dans $\mathbb{Z}$

Contrexemple 8 : Dans $\mathbb{Z}[i\sqrt{5}]$, $(2+i\sqrt{5})(2-i\sqrt{5}) = 9$ et $3(2+i\sqrt{5})$ n'admettent pas de PGCD car $3 \not\sim 2 + i\sqrt{5}$ (ne sont pas associés)

Définition 9 : Soit $a_1;\dots;a_n \in A^*$. On appelle PPCM des $(a_i)_{i=1}^n$ tout élément $m \in A^*$ tel que :
(1) $\forall i \in [\![1;n]\!], a_i \mid m$
(2) $\forall \ell \in A^*, (\forall i \in [\![1;n]\!], a_i \mid \ell) \Rightarrow m \mid \ell$

On note $a_1 \vee \dots \vee a_n$ la classe d'équivalence des PPCM modulo la relation d'association dans A.

Les résultats précédents s'adaptent au PPCM.

Remarque 10 : Les résultats

Proposition 11 : (1) Soit A anneau à PGCD et $a, b \in A^*$ tels que $d = a \wedge b$
Alors : il existe un PPCM $m \in A^*$, $m = a \vee b$ tel que $md = ab$
(2) Soit A anneau à PPCM et $a, b \in A^*$ tels que $m = a \vee b$
Alors : il existe un PGCD $d = a \wedge b \in A^*$ tel que $md = ab$

2] Dans un anneau factoriel

Définition 12 : A est factoriel si pour tout $a \in A^* \setminus A^\times$, a s'écrit de manière unique, à permutation près, $a = r_1 \times \dots \times r_n$ avec $(r_i)_{i=1}^n$ irréductibles dans A.

On considère par la suite un anneau factoriel A.

Exemple 13 : $\mathbb{Z}$ est un anneau factoriel

Théorème 14 : Dans tout anneau factoriel, les PGCD et PPCM existent et si $a = u \prod r_i^{n_i(a)}$ et $b = v \prod r_i^{n_i(b)} \in A^*$
Alors : $a \wedge b = \prod r_i^{\inf(n_i(a);n_i(b))}$ et $a \vee b = \prod r_i^{\sup(n_i(a);n_i(b))}$

Exemple 15 : Dans $\mathbb{Z}$, $24 = 2 \times 3 \times 4$ et $60 = 2 \times 5 \times 6$
alors $24 \wedge 60 = 2$ et $24 \vee 60 = 2 \times 3 \times 4 \times 5 \times 6$

Lemme 16 : (d'Euclide) Soit $p \in A$ irréductible et $a, b \in A$ tels que $p \mid ab$
Alors : $p \mid a$ ou $p \mid b$

Théorème 17 : (de Gauss) Soit $a, b, c \in A$ tels que $a \mid bc$ et $a \wedge b = 1$
Alors : $b \mid a$ et $b \mid c$

3] Application à $A[X]$ avec A factoriel

Définition 18 : Soit $P \in A[X] \setminus \{0\}$ tel que $P(X) = \sum_{k=0}^{n} a_k X^k$. Le contenu de P est : $c(P) := a_0 \wedge \dots \wedge a_n$. On dit que P est primitif si $c(P) = 1$.

Lemme 19 : (de Gauss) Soit $P, Q \in A[X]$
Alors : $c(PQ) = c(P)c(Q)$ modulo A^*.

Proposition 20 : Les polynômes $P \in A[X]$ irréductibles dans $A[X]$:
(1) les constantes $p \in A$ irréductibles dans A
(2) les polynômes P tels que $\deg(P) \geq 1$, $c(P) = 1$ irréductibles dans $\mathrm{Frac}(A)[X]$.

Corollaire 21 : $A[X]$ est factoriel

I.3.A [Cal] I.4 I.6.A [Cal] I.6.B I.3 [Per] I.4 [Per]

4) Application de la factorialité à la factorisation de polynômes

Proposition 22 : L'application $S : \mathbb{F}_q[X] \to \mathbb{F}_q[X]$, $Q \mapsto Q^q$ est un $\mathbb{F}_q$-endomorphisme de l'espace vectoriel $\mathbb{F}_q[X]$.

Lemme 23 : Soit $\mathbb{L}/\mathbb{F}_q$ extension et $x \in \mathbb{L}$
Alors : $x^q = x$ ssi $x \in \mathbb{F}_q$

Théorème 24 : Soit $q = p^n$ avec p premier, $n \in \mathbb{N}$, $P \in \mathbb{F}_q[X]$ sans facteurs carrés et $P = \prod P_i$ la décomposition de P en produit d'irréductibles sur $\mathbb{F}_q[X]$.
Alors : (1) Si $r = 1$, alors P est irréductible
(2) Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tels que $PGCD(P; V-a)$ est facteur non-trivial de P.

[Isen]

II) PGCD et PPCM dans un anneau "plus petit"

1) Dans un anneau principal

Définition 25 : Un anneau $\mathbb{A}$ est principal s'il est intègre et si tout idéal de $\mathbb{A}$ est engendré par un seul élément.
On considère par la suite $\mathbb{A}$ un anneau principal.

Exemple 26 : Un corps est un anneau principal, $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

Proposition 27 : Un anneau principal est factoriel

Contrexemple 28 : La réciproque est fausse. $\mathbb{Z}[X]$ est factoriel non-principal car $\langle 2; X \rangle$ n'est pas principal

Proposition 29 : Soit $a, b \in \mathbb{A}^*$ et $d = a \wedge b$.
Alors : $\langle d \rangle = \langle a \rangle + \langle b \rangle$ i.e. il existe $\lambda, \mu \in \mathbb{A}$ tels que $d = \lambda a + \mu b$

Corollaire 30 : (théorème de Bézout) Soit $a, b \in \mathbb{A}$ premiers entre eux
Alors : $\langle 1 \rangle = \langle a \rangle + \langle b \rangle$ i.e. il existe $\lambda, \mu \in \mathbb{A}$ tels que $1 = \lambda a + \mu b$

Contrexemple 31 : L'hypothèse de principalité est vitale.
Dans $\mathbb{K}[X;Y]$ factoriel, X et Y sont premiers entre eux mais
$\langle X \rangle + \langle Y \rangle = \langle X; Y \rangle \neq \langle 1 \rangle$

II.3 [Per]

2) Dans un anneau euclidien

Définition 32 : Un anneau commutatif intègre $\mathbb{A}$ est euclidien s'il existe une application $\varphi : \mathbb{A}^* \to \mathbb{N}$ telle que pour tout $a, b \in \mathbb{A} \times \mathbb{A}^*$ il existe $q, r \in \mathbb{A}^2$ tel que $a = bq + r$ avec $\varphi(r) < \varphi(b)$.

Exemples 33 : $\mathbb{Z}$; $\mathbb{K}[X]$; $\mathbb{Z}[i]$ sont euclidiens de stathmes $|\cdot|$; $\deg$; $N(z) = z\bar{z}$ respectivement.

Théorème 34 : Un anneau euclidien est principal et alors les PGCD existent.

Théorème : (forme normale de Smith)

IX.1 [Rom] [Les]

3) Algorithmes de calcul

Lemme 35 : Soit $a, b \in \mathbb{A}^*$ et r un reste de la division euclidienne
Alors : (1) Si $r = 0$, alors $a \wedge b = b$
(2) Si $r \neq 0$, alors : $a \wedge b = b \wedge r$

Théorème 36 : (algorithme d'Euclide) Soit $a, b \in \mathbb{A}^*$, et la suite $r_0 = b$; $r_1 = \text{reste}(a; b)$ et pour tout $n \geq 2$, $r_n = \begin{cases} 0 & \text{si } r_{n-1} = 0 \\ \text{reste}(r_{n-2}; r_{n-1}) & \text{sinon} \end{cases}$
Alors : il existe $p \in \mathbb{N}^*$ tel que $r_p = 0$, $0 \leq \varphi(r_{p-1}) < \dots < \varphi(r_0)$
et $a \wedge b = r_0 \wedge r_1 = \dots = r_{p-1} \wedge r_p = r_{p-1}$

Corollaire 37 : (algorithme d'Euclide étendu) Avec les mêmes notations que précédemment,
Alors : il existe deux suites (u_k) et (v_k) dans $\mathbb{A}$ telles que : pour tout $k \in \mathbb{N}$, $r_k = a u_k + b v_k$ et $a \wedge b = r_{p-1} = a u_{p-1} + b v_{p-1}$

IX.2 [Rom]

III) Utilisation des PGCD et PPCM dans l'anneau $\mathbb{Z}$

1) Équations diophantiennes

Définition 38 : Une équation diophantienne est une équation polynomiale à coefficients entiers à inconnues entières.

Exemple 39 : Soit $n \geq 2$, $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$. $ax = b\ [n]$ est une équation diophantienne.

X.4 [Rom]

X.4 [Rom]

Proposition 40 : $ax = 1\ [n]$ a des solutions ssi $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$
ssi $a \wedge n = 1$

Corollaire 41 : Soit $a, n \in \mathbb{Z} \times \mathbb{N}^*$ tels que $a \wedge n = 1$.
Alors : l'ensemble des solutions de $ax = 1\ [n]$ est :
$$S = \{x_0 + kn \mid k \in \mathbb{Z}\}$$ avec x_0 solution particulière

Théorème 42 : $ax = b\ [n]$ a des solutions ssi $a \wedge n \mid b$
Dans ce cas, l'ensemble des solutions est : $S = \left\{ \frac{b}{a\wedge n} x_0 + k \frac{n}{a \wedge n} \mid k \in \mathbb{Z} \right\}$
avec x_0 solution de $\frac{a}{a\wedge n} x = b \left[\frac{n}{a \wedge n}\right]$

2] Systèmes de congruences

VIII.3 [Rom]

Lemme 43 : Soit $\mathbb{A}$ anneau principal, $(a_j)_{j=1}^r \in \mathbb{A}^* \setminus \mathbb{A}^\times$ deux à deux premiers entre eux et $\left(b_j = \prod_{\substack{i=1 \\ i \neq j}}^{r} a_i\right)_{j=1}^r$
Alors : les (b_j) sont premiers entre eux dans leur ensemble.

Théorème 44 : (lemme chinois) Soit les (a_j) comme précédemment
Alors : l'application $\varphi : \begin{array}{l} \mathbb{A} \to \prod \mathbb{A}/\langle a_j \rangle \\ x \mapsto (\pi_j(x))_{j=1}^r \end{array}$ est un morphisme d'anneaux surjectif de noyau $\ker(\varphi) = \langle \prod a_j \rangle$ et φ induit un isomorphisme d'anneaux $\bar{\varphi} : \begin{array}{l} \mathbb{A}/\langle \prod a_j \rangle \to \prod \mathbb{A}/\langle a_j \rangle \\ \pi(x) \mapsto (\pi_j(x))_{j=1}^r \end{array}$
d'inverse $\bar{\varphi}^{-1} : \begin{array}{l} \prod \mathbb{A}/\langle a_j \rangle \to \mathbb{A}/\langle \prod a_j \rangle \\ (\pi_j(x))_{j=1}^r \mapsto \sum_{j=1}^r x_j u_j b_j \end{array}$ où $(u_j)_{j=1}^r$ est une suite d'éléments de $\mathbb{A}$ telle que $\sum_{j=1}^r u_j b_j = 1$.

X.4

Exemple 45 : Le système $\begin{cases} x \equiv 2\ [4] \\ x \equiv 3\ [5] \\ x \equiv 1\ [9] \end{cases}$ a pour solutions
$S = \{118 + 180 q' \mid q' \in \mathbb{Z}\}$.

3] Existence de solutions d'équations polynomiales.

[FGN Al 1]

Théorème 46 : Soit p premier impair tel que $q := 2p+1$ est premier.
Alors : il n'existe pas d'entiers $(x; y; z) \in \mathbb{Z}^3$ tels que $xyz \not\equiv 0\ [p]$
et $x^p + y^p + z^p = 0$.

Références :

[Cal] Éléments de théorie des anneaux - Calais

[Per] Cours d'Algèbre - Perrin

[Isen] L'oral à l'agrégation de mathématiques - Isenmann

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi

[FGN Al 1] Exercices de mathématiques Oraux X-ENS Algèbre 1 - Francinou

[Les] 131 développements pour l'oral - Lesesure