142 PGCD, PPCM, algorithmes de calculs, Applications.

Cadre : A désigne un anneau commutatif, unitaire et intègre.

I - Cadre théorique ; anneaux factoriels et principaux

A - Définitions et premières propriétés

Def° ① : Soit $(a_1, \dots, a_n) \in A^n$. On dit que $d \in A$ est un pgcd de $a_1, \dots, a_n$ ssi :
- $\forall i \in [\![1, n]\!]$, $d \mid a_i$.
- si $d' \in A$, $\forall i \in [\![1, n]\!]$, $d' \mid a_i$, alors $d' \mid d$.

Def° ② : Soit $(a_1, \dots, a_n) \in A^n$. On dit que $m \in A$ est un ppcm de $a_1, \dots, a_n$ ssi :
- $\forall i \in [\![1, n]\!]$, $a_i \mid m$
- si $m' \in A$, $\forall i \in [\![1, n]\!]$, $a_i \mid m'$, alors, $m \mid m'$.

Ex ③ : $ppcm_{\mathbb{R}[X]}(X-1, X+2) = (X-1)(X+2)$

Prop° ④ : Soit d un pgcd de $a_1, \dots, a_n \in A$. $d' \in A$ est un pgcd de $a_1, \dots, a_n$ ssi $d' \sim d$.
Soit m un ppcm de $a_1, \dots, a_n \in A$. $m' \in A$ est un ppcm de $a_1, \dots, a_n$ ssi $m' \sim m$.

Ex : $PGCD_{\mathbb{Z}[i]}(2i, -1+3i) = \{-1 \pm i, -1 \pm i\}$.

Rq ⑥ : Dans la suite, on adoptera les notations suivantes : $pgcd(a,b) = a \wedge b$
$ppcm(a,b) = a \vee b$.

Prop° ⑦ : Soient $a_1, a_2, a_3 \in A$. Quand les pgcd et les ppcm existent, on 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) $a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge (a_2 \wedge a_3)$
3) $a_1 \vee a_2 \vee a_3 = (a_1 \vee a_2) \vee a_3 = a_1 \vee (a_2 \vee a_3)$
4) $a_1 \vee a_2 \vee a_3 = (a_1 \vee a_2) \vee (a_2 \vee a_3)$

Coro ⑧ : Soient $a_1, \dots, a_n \in A$. Alors le n-uplet $(a_1, \dots, a_n)$ possède un pgcd (resp. ppcm) si tout couple $(a_i, a_j)_{i,j \in [\![1,n]\!]}$ possède un pgcd (resp. ppcm).

Ex ⑨ : Dans $\mathbb{Z}$, tout n-uplet possède un ppcm.

Prop° ⑩ : Soit $(a_1, \dots, a_n) \in A^n$. Alors, $d \in A$ est un pgcd de $a_1, \dots, a_n$ ssi (d) est le plus petit idéal principal contenant $\sum_{i=1}^{n} (a_i)$.
Soit $(a_1, \dots, a_n) \in A^n$. Alors, $m \in A$ est un ppcm de $a_1, \dots, a_n$ ssi $(m) = (a_1) \cap \dots \cap (a_n)$.

C-E ⑪ : Dans $\mathbb{Z}$, $(12) + (30) \supset (12)$ mais $12 \neq 12 \wedge 30$.

Def° ⑫ : Soit $(a_1, \dots, a_n) \in A^n$. On dit que $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble ssi leurs seuls diviseurs communs sont les éléments inversibles de A.

C-E ⑬ : $28 \wedge 35 \wedge 20 = 1$ mais $28 \wedge 20 = 4$.

Théo ⑭ : (De Gauss) : Soit A un anneau dans lequel tout couple d'éléments admet un pgcd. Alors,
$\forall (a,b) \in A^2$, $a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$.

Prop° ⑮ : Soit $(a,b) \in A^2$. Si a et b admettent un ppcm, alors ils admettent un pgcd et
$(a \vee b)(a \wedge b) = ab$.

C-E ⑯ : Dans $\mathbb{Z}[i\sqrt{5}]$, $2 \wedge (1+i\sqrt{5}) = 1$ mais ce couple n'admet pas de ppcm.

Prop° ⑰ : Si les pgcd existent dans A et $a, b \in A$.
Soit $d = a \wedge b$. Alors il existe $m \in A^*$, $m = a \vee b$ et $md = ab$.
Si les ppcm existent dans A, et $a, b \in A$. Soit $m = a \vee b$. Alors $\exists\, d \in A^*$, $d = a \wedge b$ et $ab = md$.

B - Anneaux principaux

Def° ⑱ : On dit qu'un anneau intègre est principal si tous ses idéaux sont principaux.

Prop° ⑲ : Dans un anneau principal, les pgcd et les ppcm existent.

C-E ⑳ : $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

Ex ㉑ : Dans $\mathbb{K}(X)$, les pgcd et les ppcm existent.

Théo ㉒ : (Bezout) Soit A principal et $a, b \in A^*$. On a :
1) $a \wedge b = d \Leftrightarrow (d) = (a) + (b)$
2) $a \wedge b = d \Rightarrow \exists\, u, v \in A$, $au + bv = d$
3) $a \wedge b = 1 \Leftrightarrow \exists\, u, v \in A$, $au + bv = 1$.

Ex ㉓ : Soient a, b distincts dans $\mathbb{R}$. Dans $\mathbb{R}[X]$, on a :
$$\frac{1}{b-a}(X-a) + \frac{1}{a-b}(X-b) = 1.$$

Coro ㉔ : Soit $m \in \mathbb{N}$. On a : $n \in (\mathbb{Z}/_{m}\mathbb{Z})^* \Leftrightarrow m \wedge n = 1$

C - Anneaux factoriels

Def° ㉕ : Un anneau intègre est dit factoriel si tout élément non nul non inversible admet une décomposition en irréductibles unique à un inversible près et à permutation des facteurs près.

Prop° ㉖ : Un anneau principal est factoriel.

Ex ㉗ : $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps est factoriel.

C-E ㉘ : $\mathbb{Z}[X_1, \dots, X_n]$ est factoriel non principal.

Prop° 29 : Dans un anneau factoriel, les pgcd et les ppcm existent. En effet soient $a, b \in A$. $\exists u, v \in A^\times$ et p_i, $i \in [\![1,n]\!]$ irréductibles tels que :
$a = \prod_{i=1}^{n} p_i^{\nu_i(a)}$ et $b = \prod_{i=1}^{n} p_i^{\nu_i(b)}$.
Alors, $a \wedge b = \prod_{i=1}^{n} p_i^{\min(\nu_i(a), \nu_i(b))}$ et $a \vee b = \prod_{i=1}^{n} p_i^{\max(\nu_i(a), \nu_i(b))}$

Ex 30 : $108 = 2^2 \times 3^3$; $456 = 2^2 \times 3 \times 19 \Rightarrow 108 \wedge 456 = 2^2 \times 3$

Déf° 31 : Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. On appelle contenu de P un pgcd des coefficients de P : $c(P)$.

Lemme 32 : (Gauss) : Soient $P, Q \in A[X]$. $c(PQ) = c(P) \times c(Q)$ où A est un anneau factoriel.

Application 33 : Si A est factoriel, alors $A[X]$ est factoriel.

II. PGCD, PPCM : Anneaux euclidiens et calcul effectif

A / Propriétés

Prop° 34 : Un anneau euclidien ~~euclidien~~ est principal.

Ex 35 : $\mathbb{Z}[i]$ et $\mathbb{K}[X]$ sont euclidiens.

Prop° 36 : Dans un anneau euclidien, les pgcd (et les ppcm) existent et on peut les calculer grâce à l'algorithme d'Euclide.

Théo 37 : (Lamé) : Le nombre de divisions euclidiennes dans $\mathbb{Z}$ que l'algorithme d'Euclide nécessite pour calculer $a \wedge b$ $(1 \leq b \leq a)$ est inférieur à 5 fois le nombre de chiffres de b en écriture décimale.

Prop° 38 : Soient $a, b, N \in \mathbb{N}$ tels que $1 \leq a \leq b \leq N$. Le coût de l'algorithme d'Euclide appliqué à (a,b) est $O(\ln^2(N))$.

Prop° 39 : Dans A euclidien, on peut calculer les coefficients de Bezout grâce à l'algorithme d'Euclide étendu.

Ex 40 : $35 = 1 \times 35 + 0 \times 28$; $28 = 0 \times 35 + 1 \times 28$; $7 = 1 \times 35 + (-1) \times 28$.

Rq 41 : En général, il n'y a pas unicité du couple de Bezout : soit $k \in \mathbb{Z}$: $(1 + 28k, -1 - 35k)$ ... ho.

Application 42 : Calcul des inverses modulo $n \in \mathbb{N}$
$7 \times 2 + (-1) \times 13 = 1 \Rightarrow 7 \times 2 \equiv 1 \ [13]$.

Théo 43 (Théorème chinois). Soient A anneau commutatif intègre. Soient $I_1, \dots, I_n$ des idéaux étrangers deux à deux. Alors,
$$A/\left(\prod_{i=1}^{n} I_i\right) \simeq \prod_{i=1}^{n} A/I_i$$

Application 44 : (Interpolation de Lagrange) :
$\forall (a_1, \dots, a_n) \in A^n$ et $(b_1, \dots, b_n) \in A^n$ avec $a_i \neq a_j$, $i \neq j$.
Alors, $\exists !\, P \in A[X]_{\leq n-1}$ tel que $P(a_i) = b_i$ $\forall i \in [\![1,n]\!]$

Ex 45 : $P(0) = 1$, $P(1) = 0$, $P(-1) = 2$ et $P(2) = 5$.
Alors, $P(X) = X^3 - 2X + 1$ dans $\mathbb{Z}[X]$.

B - Anneaux de polynômes

Prop° 46 : Dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps, on peut calculer les coefficients de Bezout et le pgcd de P et Q via l'algorithme d'Euclide étendu en $O(\deg(P)\deg(Q))$

Ex 47 : Dans $\mathbb{Q}[X]$: $5 = 1 \times (X^2+1) - (X+2) \times (X+2)$

Prop° 48 : Calcul d'inverse dans un quotient d'un anneau de polynôme
Dans $\mathbb{F}_2[X]/(X^3+X+1)$, on a : $\overline{(X+1)}^{-1} = \overline{X^2+X}$
car $X^3 + X + 1 + (X^2 + X)(X+1) = 1$.

Lemme 49 : Soit p premier, $s \in \mathbb{N}^*$, $q = p^s$ et $R \in \mathbb{F}_q[X]$.
L'application $S_R : \mathbb{F}_q[X]/\langle R \rangle \to \mathbb{F}_q[X]/\langle R \rangle$, $\overline{Q(X)} \mapsto \overline{Q(X^q)}$ est bien définie et coïncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/\langle R \rangle$.

Prop° 50 Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés. On peut factoriser P dans $\mathbb{F}_q[X]$ en produit d'irréductibles grâce à cet algorithme :
① On calcule la matrice de $S_P - Id$.
② # {facteurs irréductibles de P} $= \dim(\ker(S_P - Id)) := n$.

Si $n = 1$, on renvoit P.
③ Sinon, on calcule $V \in \ker(S_P - Id)$, $V \not\equiv$ cte $[P]$.
④ On calcule $\text{pgcd}(P, V - \alpha)$, $\forall \alpha \in \mathbb{F}_q$ et on a :
$$P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V - \alpha)$$
⑤ On retourne à l'étape ① avec chacun des facteurs non triviaux de ce produit.

DEV 1

III. Applications

A - Matrices sur un anneau

Théo 52 : Soit A un anneau principal. Soit $M \in \mathcal{M}_{n,m}(A)$. Alors, il existe deux matrices P et Q avec $P \in GL_n(A)$, $Q \in GL_m(A)$ et $D \in \mathcal{M}_{n\times m}(A)$ quasi-diagonale telles que :
- $M = PDQ$
- $D = \begin{pmatrix} d_1 & & 0 & \\ & \ddots & & \\ 0 & & d_r & 0 \end{pmatrix}$ avec $\forall i \in [\![1, r-1]\!]$, $d_i \mid d_{i+1}$.

Si $M = P'D'Q'$ est une autre décomposition, alors $\forall i$, $d_i \sim d_i'$.

Ex 53 : $\begin{pmatrix} 7 & 11 & 3 \\ 3 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$

Application 54 : Théorème de structure des groupes abéliens finis. Soit G un groupe abélien fini. Alors, $\exists\, r \geq 0$, $d_1, \dots, d_r \geq 2$ avec $d_i \mid d_{i+1}$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$. Les d_i sont uniques au signe près.

Ex 55 : $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

DEV 2

Prop 56 : Soit $\varphi : GL_n(\mathbb{Z}) \times \mathbb{Z}^n \to \mathbb{Z}^n$, $(P, X) \mapsto PX$. On note $\omega_X = \{PX,\ P \in GL_n(\mathbb{Z})\}$.
Soit $X = (x_1, \dots, x_n)^t \in \mathbb{Z}^n$. $a_X = |\bigwedge_{i=1}^{n} x_i|$.
Alors, pour $X, X' \in \mathbb{Z}^n$, on a :
$$\omega_X = \omega_{X'} \iff a_X = a_{X'}.$$

Application 57 : Soit $X_1 \in \mathbb{Z}^n$. On peut compléter X_1 en une base de $\mathbb{Z}^n$ ssi $a_{X_1} = 1$.

B - Équations Diophantiennes

Prop 58 : Soit $(a, b) \in \mathbb{Z}^2$ et $c \in \mathbb{Z}$. Alors $ax + by = c$ admet une solution ssi $a \wedge b \mid c$.
Dans ce cas, si (x_0, y_0) est une solution de $ax + by = c$, les autres solutions sont de la forme $(x_0 + kb', y_0 - ka')$ où $k \in \mathbb{Z}$ et $a = da'$, $b = db'$.

Ex 59 : (E) $2x + 4y = 2$, $S = \{(-1+k, 1-2k),\ k \in \mathbb{Z}\}$

Prop 60 : (Grand théorème de Fermat pour $n = 3$). Il n'existe pas de solution x, y, z dans $\mathbb{Z}$ avec $xyz \neq 0$ à l'équation
$$x^3 + y^3 = z^3.$$

C - Résultant

Déf 61 : Soit A anneau. Soit $A(X) = a_m X^m + \dots + a_0$, $B(X) = b_n X^n + \dots + b_0$ avec $A, B \in A[X]$ et $a_m b_n \neq 0$.
On définit
$$S(A,B) = \begin{pmatrix} a_m & \cdots & a_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & a_m & \cdots & a_0 \\ b_n & \cdots & b_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & b_n & \cdots & b_0 \end{pmatrix} \in \mathcal{M}_{n+m}(A)$$

Le résultant de A et B est $\det(S(A,B))$.

Prop 62 : Soit $\mathcal{B} = ((X^{n-1}, 0), \dots, (1, 0), (\quad), \dots, (\quad))$ et $\mathcal{B}' = (X^{m+n-1}, X^{m+n-2}, \dots, 1)$ et $\mathbb{K}$ un corps. Pour $p \in \mathbb{Z}$, $\mathbb{K}_p[X] = \{$polynômes de degrés $< p\}$.
Alors, $(S(A,B))^t = M_{\mathcal{B},\mathcal{B}'}(\varphi)$
où $\varphi : \mathbb{K}_n[X] \times \mathbb{K}_m[X] \to \mathbb{K}_{m+n}[X]$, $(U, V) \mapsto AU + BV$.

Théo 63 : Avec les notations,
$$\deg(A \wedge B) \geq 1 \iff R(A,B) = 0.$$

Cor 64 : Si $\mathbb{K} = \overline{\mathbb{K}}$, les polynômes A et B ont une racine commune ssi $R(A,B) = 0$.

Prop 65 : Le pgcd de A et B se lit sur la dernière ligne non nulle de la forme échelonnée de $S(A,B)$.

Ex 66 : $\begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ et donc $(X^2 - 1) \wedge (X+1) = X + 1$.