142

PGCD, PPCM, algorithmes et calculs

A un anneau commutatif, intègre, $a, b \in A$

I - Cadre théorique général : anneaux factoriels

1) Dans un anneau quelconque

Def 1 : $d \in A$ est un pgcd de a, b si $d|a$, $d|b$ et si $c \in A$ avec $c|a$ et $c|b$ alors $c|d$.
m est un ppcm de a et b si $a|m$, $b|m$ et si $c \in A$ avec $a|c$ et $b|c$ alors $m|c$

Exemples : Dans $\mathbb{Z}$, 2 est un pgcd de 4 et 6
12 est un ppcm de 4 et 6
Dans $\mathbb{Z}[i\sqrt{5}]$, 6 et $2+i\sqrt{5}$ n'ont pas de pgcd
Dans $\mathbb{C}[X,Y,Z,T]/_{(XY-ZT)}$, $\bar{X}$ et $\bar{Z}$ n'ont pas de ppcm

Prop 3 : "Le" pgcd et "le" ppcm sont définis à associé près. On note $a \wedge b$ le pgcd de a et b et $a \vee b$ le ppcm de a et b lorsqu'ils sont définis.

Prop 4 : Le pgcd et le ppcm sont associatifs (lorsqu'ils sont définis) : $c \in A$ on a : $(a \vee b) \vee c = a \vee (b \vee c)$
$(a \wedge b) \wedge c = a \wedge (b \wedge c)$

Prop 5 : Soit $c \in A$. Si $ca \wedge cb$ existe alors $a \wedge b$ aussi et $ca \wedge cb = c(a \wedge b)$

Prop 6 : Si $a \vee b$ existe alors $a \wedge b$ aussi et $(a \vee b)(a \wedge b) = ab$

Rq 7 : La réciproque est fausse : dans $\mathbb{C}[X,Y,Z,T]/_{(XY-ZT)}$
$\bar{X}$ et $\bar{Z}$ ont un pgcd mais pas de ppcm

2) Dans un anneau factoriel

Def 8 : Un anneau A intègre est factoriel s'il existe un ensemble $\mathcal{B}$ d'irréductibles de A tq tout $a \in A$ peut s'écrire d'une unique manière $a = u \prod_{p \in \mathcal{B}} p^{\alpha_p}$, $\alpha_p \in \mathbb{N}$, $u \in A^\times$ à permutations près

Prop 9 : Si A est factoriel alors $a \vee b$ et $a \wedge b$ existent et on a : $a \wedge b = \prod_{p \in \mathcal{B}} p^{\min(v_p(a); v_p(b))}$

$$a \vee b = \prod_{p \in \mathcal{B}} p^{\max(v_p(a); v_p(b))}$$

Rq : Si $a \wedge b = d$, $a = a'd$ et $b = b'd$ et on a $a' \wedge b' = 1$
On dit que a' et b' sont premiers entre eux

Exemple 11 : Dans $\mathbb{C}[X]$, $(X-1) \wedge (X^2+1) = 1$

Def 12 : Soit $P \in A[X]$. On note $c(P)$ le pgcd de ses coefficients

Lemme 13 : $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$

thm 14 : A factoriel $\Rightarrow$ $A[X]$ factoriel

Appli 15 : A commutatif et $(a_1, \dots, a_m) \in A^m$, alors :

$$\begin{vmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_m \\ \vdots & & \vdots \\ a_1^{m-1} & \cdots & a_m^{m-1} \end{vmatrix} = \prod_{1 \le i < j \le m} (a_j - a_i)$$

II - Cadre effectif : anneaux euclidiens

1) Dans un anneau principal

Def 16 : Un anneau A intègre est principal si tout idéal de A est de la forme (x), $x \in A$.

Prop 17 : A principal $\Rightarrow$ A factoriel

Prop 18 : En plus de la caractérisation du pgcd et du ppcm dûe à la factorialité, on a :
$d = a \wedge b \Leftrightarrow (a) + (b) = (d)$
$m = a \vee b \Leftrightarrow (a) \cap (b) = (m)$

Donc en particulier, on a le résultat :

Thm 19 : de Bachet-Bezout
Si $d = a \wedge b$ il existe $u, v \in A$; $au + bv = d$
Si $d = 1$ c'est une équivalence.
Appli 20 : théorème chinois
Si $a \wedge b = 1$ alors $A/_{(ab)} \simeq A/_{(a)} \times A/_{(b)}$

2) Anneaux euclidiens et algorithmes

Def 21 : Un anneau intègre A est euclidien si on a une appli $\varphi : A \setminus \{0\} \to \mathbb{N}$ tq pour tout a et $b \in A$ avec $\varphi(b) > \varphi(a)$ on a $b = aq + r$, $q, r \in A$ avec $\varphi(r) < \varphi(a)$.
Exemples 22 : $\mathbb{Z}$; $\mathbb{Z}[i]$; $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps
Quand on a un algorithme pour la division, on en a aussi un pour calculer le pgcd :
Algo 23 : d'Euclide
Soient $a, b \in A \setminus \{0\}$ avec $\varphi(b) > \varphi(a)$. On note $(r_i)_{i \in \mathbb{N}}$ la suite définie par : $r_0 = b$, $r_1 = a$, $r_{i+2} = res(r_i ; r_{i+1})$ où $res(x, y)$ le reste de la division de x par y lorsque c'est possible, 0 sinon.
Il existe un rang n_0 tq $r_{n_0} = 0$ et $r_{n_0 - 1} \neq 0$. On a : $r_{n_0 - 1} = a \wedge b$.
Exemple 24 : Dans $\mathbb{Z}$: $21 = 2 \times 9 + 3$, $9 = 3 \times 3 + 0$
Donc $21 \wedge 9 = 3$
Def 25 : On définit la suite de Fibonacci $(F_n)_{n \in \mathbb{N}}$ par :
$F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$
Thm 26 : de Lamé
Soient $a, b \in \mathbb{N}^*$ avec $b > a$
Si $a \leq F_{k+1}$ l'algo d'Euclide finit en moins de k étapes
Prop 27 : L'algo d'Euclide est de complexité au pire $\mathcal{O}(\log(a)\log(b))$ opérations binaires dans $\mathbb{N}$.
Algo : Euclide étendu.
On pose $W_0 = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$, $W_1 = \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix}$, $W_i = \begin{pmatrix} r_i \\ u_i \\ v_i \end{pmatrix}$; $i \geq 2$
Où r_i est tq $r_{i-2} = q_i r_{i-1} + r_i$ avec $\varphi(r_i) < \varphi(r_{i-1})$
Et $u_i = u_{i-2} - q_i u_{i-1}$; $v_i = v_{i-2} - q_i v_{i-1}$
Il existe un plus grand rang tq $r_i \neq 0$, on l'appelle n_0 et on a alors : $a u_{n_0} + b v_{n_0} = a \wedge b$
Exemple 29 : Dans $\mathbb{Z}$ avec 9 et 21 :
$W_0 = \begin{pmatrix} 21 \\ 1 \\ 0 \end{pmatrix}$, $W_1 = \begin{pmatrix} 9 \\ 0 \\ 1 \end{pmatrix}$, $W_2 = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix}$, $W_3 = \begin{pmatrix} 0 \\ \cdot \\ \cdot \end{pmatrix}$

Donc $3 = 21 - 2 \times 9$.

III - Applications en arithmétique et algèbre linéaire

1) Arithmétique dans $\mathbb{Z}$

Prop 30 : L'équation diophantienne $ax + by = c$ d'inconnues x et y admet des solutions ssi $a \wedge b \mid c$
Elles sont alors de la forme : $\{(bk + x_0 ; -ak + y_0) ; k \in \mathbb{Z}\}$ où $(x_0 ; y_0)$ est une solution particulière
Exemple : $21x + 9y = 9$ a pour solutions $\{(9k ; 1 - 21k) ; k \in \mathbb{Z}\}$
Prop 32 : Si $p_1, \dots, p_n \in \mathbb{N}$ deux à deux premiers entre eux et $a_1, \dots, a_n \in \mathbb{N}$ alors le système $(x \equiv a_i \ (p_i))_{1 \leq i \leq n}$ admet des solutions $x \in \mathbb{Z}$ qui sont :
$\{x_0 + p_1 \cdots p_n k \ ; k \in \mathbb{Z}\}$ où x_0 est une solution particulière
Prop 33 : $n, m \in \mathbb{Z}$. m est inversible modulo n ssi $n \wedge m = 1$

Coro 34 : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n premier

2) Arithmétique dans $\mathbb{K}[X]$

Exemple 35 : $(X^n-1)\wedge(X^m-1) = X^{n\wedge m}-1$

De même que dans $\mathbb{Z}$:

Prop 36 : $P, Q \in \mathbb{K}[X]$. P inversible modulo Q ssi $P\wedge Q = 1$. $\mathbb{K}[X]/(P)$ est un corps ssi P premier.

On peut calculer les inverses grâce à Euclide étendu

thm : Si $P \in \mathbb{F}_q[X]$, $q=p^n$, est réductible sans facteurs carrés, alors il existe $Q \in \mathbb{F}_q[X]$ tq Q non constant modulo P et $\prod_{a\in\mathbb{F}_q}(P\wedge Q-a) = P$

Coro : On dispose d'un algorithme (de Berlekamp) pour factoriser tout polynôme de $\mathbb{F}_q[X]$ en produit d'irréductible : • Si P irré, rendre P.

• Si $P'=0$, $P=(R)^q$, $R\in\mathbb{F}_q[X]$, on applique alors l'algo à R

• Si $P\wedge P' \neq 1$, on applique l'algo à $P\wedge P'$ et $\frac{P}{P\wedge P'}$

• Sinon : P est sans facteurs carrés

On applique le thm, on a une factorisation de P en deux polynômes non triviaux.

On applique l'algo à ces polynômes.

Exemple 39 : Dans $\mathbb{F}_2[X]$: $P(X) = X^2+1$

$P'(X) = 0 \Rightarrow P(X) = (X+1)^2$.

3) En algèbre linéaire

Lemme 40 : $P_1, \dots, P_n \in \mathbb{K}[X]$ deux à deux premiers entre eux. E un $\mathbb{K}$-ev, $u \in \mathrm{End}(E)$

Alors $\mathrm{Ker}(P_1 \cdots P_n(u)) \simeq \bigoplus_{i=1}^{n} \mathrm{Ker}\, P_i(u)$

Prop 41 : A principal, $v_1, v_2 \in A^n$ sont dans la même orbite sous l'action de $GL_n(A)$ ssi les pgcd de leurs coefficients sont égaux.

Thm 42 : $M \in M_{n,m}(A)$ est GL-équivalente (et même SL-équivalente) à une matrice $\begin{pmatrix} d_1 & & 0 \\ & \ddots d_r & \\ 0 & & 0 \end{pmatrix}$ où $d_i \in A$, $d_i | d_{i+1}$ $\forall i \in [\![1, r]\!]$

Si A possède un algorithme de division, on peut même mettre M sous cette forme algorithmiquement

Les d_i, $0 \leq i \leq n$ sont uniques à association près

Appli 43 : Soit G un groupe abélien de type fini. Il existe l, $d_1, \dots, d_n \in \mathbb{N}$ tq $G \simeq \mathbb{Z}^l \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$ avec $d_i | d_{i+1}$ les d_i uniques à association près.

Ref : Cours de calcul formel, Saux Picart
Modules, théorie pratique, Berhuy
Algèbre, Serge Lang
Objectif agrégation : Beck, Malick, Peyré.