142 PGCD, PPCM, algorithmes de calcul. Applications

On considère A un anneau intègre, commutatif, unitaire on note (a) l'idéal engendré par a. On suppose connu. A euclidien $\Rightarrow$ A principal $\Rightarrow$ A factoriel.

I. Notion de divisibilité

[P] p46

Def ①: Soient $a, b \in A$, on dit que $a | b$ s'il existe $c \in A$ tel que $b = ac$.

prop ②: $a|b \Leftrightarrow (b) \subset (a)$. En particulier $(0) \subset (a) \subset (u) = A$ $\forall u \in A^\times$ inversible.

Def ③: $a R b \Leftrightarrow a|b$ et $b|a \Leftrightarrow (a) = (b)$ est une relation d'équivalence, et si aRb, on dit que a et b sont associés $\Leftrightarrow \exists u \in A^\times, a = bu$.

Def ④: soient $a, b \in A$. d est un pgcd de a, b (noté $d = \text{pgcd}(a,b)$) si $d|a$, $d|b$ et si $\forall c \in A$ tq $c|a$ et $c|b$ on a $c|d$.
m est un ppcm de a,b (noté : $m = \text{ppcm}(a,b)$) si $a|m$ et $b|m$ et $\forall c \in A$ tq $a|c$ et $b|c$, $m|c$.

Rq ⑤: • ces notions sont définies à un inversible près
• on peut généraliser la définition pour une famille d'élément

p61

C-Ex ⑥: On considère $A = \mathbb{Z}[i\sqrt{5}]$, 3 et $2+i\sqrt{5}$ n'ont pas de ppcm, 9 et $3(2+i\sqrt{5})$ n'ont pas de pgcd.

II. Anneaux factoriels.

p46

Def ⑦: $p \in A$ est irréductible si $\begin{cases} (i) & p \notin A^\times \\ (ii) & p = ab \Rightarrow a \in A^\times \text{ ou } b \in A^\times \end{cases}$

Def ⑧: On dit que A est intègre s'il vérifie :
• A intègre
• (E) $\forall a \in A, a \neq 0$, a s'écrit sous la forme $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u \in A^\times$, $v_p(a) \in \mathbb{N}$, $v_p(a)$ nuls sauf un nombre fini. $\mathcal{P}$ système de représentant des irréductibles
• (U) cette écriture est unique.
$\Leftrightarrow$ (E) : $a \in A \setminus \{0\}$ s'écrit $a = u p_1 \dots p_r$, $u \in A^\times$ et $p_1 \dots p_r$ irréductibles.
(U) : si $a = u p_1 \dots p_r = v q_1 \dots q_s$, on a $r = s$ et $\exists \sigma \in \mathfrak{S}_r$ tq p_i et $q_{\sigma(i)}$ sont associés.

Rq ⑨: si $a, b \neq 0$, $a|b \Rightarrow \forall p \in \mathcal{P}$ $v_p(a) \leq v_p(b)$

p49

Def ⑩: si A est factoriel et $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ $b = v \prod_{p \in \mathcal{P}} p^{v_p(b)}$
on définit $\begin{cases} \text{pgcd}(a,b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))} \\ \text{ppcm}(a,b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))} \end{cases}$

p47

Ex ⑪: dans $\mathbb{Z}$, $\mathcal{P}$ = les nombres premiers $p > 0$
dans $K[X]$ (K corps) : $\mathcal{P} = \{$pol unitaires irréductibles$\}$

p48

Thm ⑫: Soit A intègre vérifiant (E), les conditions suivantes sont équivalentes :
(i) A vérifie (U)
(ii) lemme d'Euclide : si p irréductible et $p|ab$, alors $p|a$ ou $p|b$
(iii) p irréductible $\Leftrightarrow$ (p) premier
(iv) Gauss : si $a|bc$ et si $\text{pgcd}(a,b) \in A^\times$, alors $a|c$

III. Anneaux principaux.

Def ⑬: A est principal si A intègre et si tout idéal de A est de la forme $I = (a)$.

Thm 14 : soit A principal, $a,b \in A\setminus\{0\}$. On note $d = \mathrm{pgcd}(a,b)$ et $c = \mathrm{ppcm}(a,b)$, on a alors :

(i) $(a)\cap(b) = (c)$.

(ii) $(a)+(b) = (d)$.

Cor 15 : (Bézout) soit A principal et $a,b \in A\setminus\{0\}$ et soit $d = \mathrm{pgcd}(a,b)$ alors $\exists \lambda, \mu \in A$ tels que $d = \lambda a + \mu b$.

application 16 : soit A anneau principal et $U \in \mathcal{M}_{n,m}(A)$ $(n,m \geq 1)$ alors il existe $d_1 \dots d_r \neq 0$ tq $d_i \mid d_{i+1}$ $i = 1 \dots r-1$ tels que U soit équivalente à $D = \begin{pmatrix} d_1 & & & & \\ & \ddots & & 0 & \\ & & d_r & & \\ & 0 & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$ [S] p67

(on a unicité de la suite $(d_1 \dots d_r)$ aux inversibles près)

application 17 (Lemme des noyaux) soit $f \in \mathcal{L}(E)$ où E ev de dim n. $P = P_1 \dots P_k \in \mathbb{K}[X]$, P_i premiers entre eux, alors $\ker(P(f)) = \ker(P_1(f)) \oplus \dots \oplus \ker(P_k(f))$. GOU p173

IV Anneaux euclidiens

A = anneau euclidien

Def 18 : Un anneau A est dit euclidien si :

(i) A est intègre

(ii) A est muni d'une division euclienne : il existe une fonction (stathme) $v : A\setminus\{0\} \to \mathbb{N}$ telle que si $a,b \in A\setminus\{0\}$, il existe $q,r \in A$ avec $a = bq + r$ $(r = 0$ ou $v(r) < v(b))$.

Ex 19 : $K[X]$ avec K corps.

$\mathbb{Z}[i] = \{a+ib,\ a,b \in \mathbb{Z}\}$ est euclidien pour $N(z) = z\bar{z}$

Thm 20 : (Euclide) Soient a et b deux éléments non nuls d'un anneau euclidien. On note $(r_i)_i$ la suite de A définie par $r_0 = a$, $r_1 = b$ et $\forall i \geq 2$, $r_i = \mathrm{rem}(r_{i-2}, r_{i-1})$ où $\mathrm{rem}(a,b)$ est le reste dans la division euclidienne de a par b [S] p45

Alors cette suite est finie : $\exists n \in \mathbb{N}$ tq $r_{n+1} = 0$ et on a $a \wedge b = r_n$.

application 21 : $\mathrm{pgcd}(X^n - 1, X^m - 1) = X^{\mathrm{pgcd}(m,n)} - 1$ GOU p56

Thm 22 (Euclide Étendu) : On veut pouvoir calculer $\mathrm{pgcd}(a,b)$ et trouver une relation de Bézout. On se place dans A^3 et on pose $W_0 = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$, $W_1 = \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix}$ et $W_i = \begin{pmatrix} r_i \\ u_i \\ v_i \end{pmatrix}$

où pour $i \geq 2$ $r_i = \mathrm{rem}(r_{i-2}, r_{i-1})$ et $\begin{cases} u_i = u_{i-2} - q_i u_{i-1} \\ v_i = v_{i-2} - q_i v_{i-1} \end{cases}$ [S] p46

d'où $W_i = \begin{pmatrix} r_i \\ u_{i-2} - q_i u_{i-1} \\ v_{i-2} - q_i v_{i-1} \end{pmatrix} = W_{i-2} - q_i W_{i-1}$. preuve [S] p49

on a alors $\forall i \in [\![0, n]\!]$ $r_i = a u_i + b v_i$.

En particulier, si n est tq $r_{n+1} = 0$, on a $\mathrm{pgcd}(a,b) = r_n = a u_n + b v_n$.

Lemme (Lamé) 23 soit $(F_n)_n$ la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $\forall n > 1$, $F_n = F_{n-1} + F_{n-2}$ soient a,b tq $a > b > 0$ tq n-itérations sont nécessaires dans Euclide pour obtenir $\mathrm{pgcd}(a,b)$. Alors $a \geq F_{n+2}$ et $b \geq F_{n+1}$. p59

Cor 24 : Le nombre de divisions à réaliser pour calculer $\mathrm{pgcd}(a,b)$ est $O(\log(b))$

prop 25 : pour $a,b \in \mathbb{Z}$, $a > b > 0$, la complexité de l'algorithme d'Euclide est au pire $O(\log(a)\log(b))$ opérations binaire. p52

dans $K[X]$ $A,B \in K[X]$ alors la complexité est de $O(\deg(A)\deg(B))$ opérations p54

[P] p53

Thm 26 (lemme chinois) : si a et b sont tels que $(a)+(b)=A$ alors $A/(ab) \simeq A/(a) \times A/(b)$

cor 27 : si p et q sont premiers entre eux, on a :

$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

[R] p27 p11

application 28 : $\begin{cases} x \equiv 2\ [4] \\ x \equiv 3\ [5] \\ x \equiv 1\ [9] \end{cases}$ admet des solutions dans $\mathbb{Z}$.

V Lien avec la théorie des groupes. G : GAF

[Col] p22

Lemme 29 : Soit H un sous-groupe de G. Tout caractère $\varphi : H \to \mathbb{C}^*$ peut se prolonger en un caractère de G

application 30 : il existe une suite d'entiers $(n_k)_{k=1}^{r}$ telle que $n_1 \geq 2$ et $n_1 | n_2 | \dots | n_r$ et $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$

lemme 31 : Soient $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ deux telles suites, alors elles sont égales SSI :

$\forall m \in \mathbb{N}^* \prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$

Thm 32 : Il existe une unique suites d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 | \dots | n_r$, $n_1 \geq 2$ et

$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$.

Combes p68

Ex 33 : $(\mathbb{Z}/60\mathbb{Z}) \times (\mathbb{Z}/72\mathbb{Z}) \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$

application 34 : ~~le grou~~ tout sous-groupe fini du groupe multiplicatif d'un corps K est cyclique :

Références : GOU : Gourdon (Algèbre)
[P] : Perrin (cours d'Algèbre)
[S] : Saux Picart (Algo...)
[R] : Rombaldi (maths agreg)