142 - PGCD et PPCM, algorithmes de calcul. Applications.

Cadre: Tous les corps sont considérés comme commutatifs.
K désigne un corps, A désigne un anneau intègre, unitaire et commutatif.
On notera $A^\times$ l'ensemble des inversibles de A, $A^* = A \setminus \{0\}$ et (a) l'idéal engendré par $a \in A$.

I. Divisibilité dans un anneau intègre

1) Premières définitions

[Pa] 46 **Déf./Prop. (1):** Soient $a, b \in A$. On dit que a divise b, noté $a|b$, s'il existe $c \in A$ tel que $b = ac$. On a alors : $a|b \iff (b) \subset (a)$

46 **Déf./Prop. (2):** La relation $aRb \overset{\text{déf.}}{\iff} a|b$ et $b|a \iff (a) = (b)$ est une relation d'équivalence sur A, appelée relation d'association.
On a de plus : $aRb \iff \exists\, c \in A^\times / a = bc$.

43 **Déf. (3):** $p \in A$ est dit premier si (p) est un idéal premier, i.e. si $ab \in (p)$, alors $a \in (p)$ ou $b \in (p)$

Déf. (4): $p \in A$ est dit irréductible si $p \notin A^\times$ et si $p = ab \Rightarrow a \in A^\times$ ou $b \in A^\times$.

46 On notera $\mathcal{P}$ un système de représentants des classes d'équivalence des irréductibles pour la relation d'association.

Ex (5): . $A = \mathbb{Z}$: $\mathcal{P} = \{$nombres premiers$\}$

47 . $A = K[X]$: $\mathcal{P} = \{P \in K[X], P$ unitaire et irréductible (sur K...)$\}$.

Déf. (6): $a, b \in A$ sont dits premiers entre eux si :
$\forall\, d \in A,\ d|a$ et $d|b \Rightarrow d \in A^\times$

2) PGCD et PPCM

[Ba] 517 **Déf. (7):** Soient $a, b \in A$.
On dit que $d \in A$ est un pgcd de a et b si : $\forall x \in A,\ x|a$ et $x|b \Rightarrow x|d$.
——— $c \in A$ ——— ppcm ——— : $\forall x \in A,\ a|x$ et $b|x \Rightarrow c|x$.

♡ **Rq (8):** Le pgcd et le ppcm de deux éléments n'existent pas toujours. Par exemple dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2+i\sqrt{5}$ n'ont pas de pgcd, et 9 et $3(2+i\sqrt{5})$ n'ont pas de ppcm.

517 **Rq (9):** Deux pgcd (resp. ppcm) sont associés. Si $a, b \in A$ admettent un pgcd (resp. ppcm), on se permettra d'appeler "le" pgcd (resp. ppcm) de a et b un représentant de la classe d'équivalence modulo R, et on le notera $\text{pgcd}(a,b)$ ou $a \wedge b$ (resp. $\text{ppcm}(a,b)$ ou $a \vee b$).

II. Anneaux factoriels

1) pgcd, ppcm dans un anneau factoriel

[Pa] 47 **Déf (10):** Un anneau intègre A est dit factoriel si :
(E) : tout $a \in A$ peut s'écrire sous la forme $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u \in A^\times$ et les $v_p(a)$ sont des entiers naturels presque tous nuls
(U) : cette écriture est unique (à permutation des éléments de $\mathcal{P}$ près)

48 **Ex. (11):** . $\mathbb{Z}$ est factoriel
. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel : $9 = 3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$

Prop (12): Soient $a, b \in A$, A factoriel. Alors leur pgcd et leur ppcm existent :
1) Si $a = 0$, alors $\text{pgcd}(a,b) = b$. Si $a = 0$ ou $b = 0$, $\text{ppcm}(a,b) = 0$.
49 2) Si $a, b \in A^*$, alors $\text{pgcd}(a,b) = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ et $\text{ppcm}(a,b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$

♡ **Coro (13):** Si A est factoriel et $a, b \in A$, alors $a \wedge b \cdot a \vee b = ab \bmod A^\times$

49 **Rq (14):** On peut également définir le pgcd (resp. ppcm) d'une famille d'éléments de A (pas nécessairement factoriel).

49 **Rq (15):** Soit A factoriel et $a, b \in A$. Alors $(a) \cap (b) = (a \vee b)$. En revanche, on n'a pas nécessairement $(a) + (b) = (a \wedge b)$ (prendre $2, X \in \mathbb{Z}[X]$).

Th. (16): Soit A un anneau intègre vérifiant (E). Sont équivalents
48 1) A est factoriel
2) $\forall p \in A$, p irréductible : $p|ab \Rightarrow p|a$ ou $p|b$ (lemme d'Euclide)
3) p irréductible $\iff p$ premier et $p \neq 0$
4) $a|bc$ et $a \wedge b = 1 \Rightarrow a|c$ (lemme de Gauss)

[Ba] 151 **Appli (17):** Soit G un groupe et $x \in G$ d'ordre fini $o(x)$. Soit $d \in \mathbb{Z}$.
Alors $o(x^d) = \dfrac{o(x)}{\text{pgcd}(d, o(x))}$.
360 (Utilisé dans la partie unicité du théorème de structure des groupes abéliens finis)

2) Application à $A[X]$, A factoriel

A est un anneau factoriel.

Déf. (18) : Soit $P = a_n X^n + \dots + a_0 \in A[X]$ ($P \neq 0$). Le contenu de P, noté $c(P)$ est $c(P) = \text{pgcd}(a_0, \dots, a_n) \in A^*$. P est dit primitif si $c(P) = 1$.

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

Prop. (20) : Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont :
1) les polynômes constants $p \in A$, p irréductible dans A
2) les polynômes de degré ≥ 1, primitifs et irréductibles dans $K[X]$ où $K = Fr(A)$

Th. (21) : Si A est factoriel, alors $A[X]$ est factoriel

Th. (22) : (*critère d'Eisenstein*)
Soit A un anneau factoriel, $K = Fr(A)$ et $P = a_n X^n + \dots + a_0 \in A[X]$, $n \geq 2$.
On suppose qu'il existe $p \in A$, p irréductible tel que :
1) $p \nmid a_n$
2) $\forall\, 0 \leq i \leq n-1$, $p \mid a_i$
3) $p^2 \nmid a_0$
Alors P est irréductible dans $K[X]$ (donc dans $A[X]$ si $c(P) = 1$)

Ex. (23) : Si $p \in \mathbb{N}$ est premier, $\Phi_p = X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}[X]$.

III. Anneaux principaux

1) pgcd, ppcm dans un anneau principal

Déf. (24) : Un anneau A est dit principal s'il est intègre et si tout idéal I de A est engendré par un élément, i.e. il existe $a \in A$ tel que $I = (a)$

Ex. (25) : $\mathbb{Z}$ est principal.

Prop. (26) : Un anneau principal est factoriel.

Rq (27) : La réciproque est fausse (prendre $\mathbb{Z}[X]$ par exemple)

Prop. (28) : $A[X]$ est principal ssi A est un corps.

Th. (29) : (*Bézout*)
Soit A un anneau principal, $a, b \in A^*$ et $d = \text{pgcd}(a, b)$.
Alors $(a) + (b) = (d)$.
En particulier il existe $u, v \in A$ tels que $ua + vb = d$.

Coro. (30) : Soient $a, b \in A$ où A est principal.
Alors : $a \wedge b = 1 \iff \exists\, u, v \in A$ / $ua + vb = 1$

Rq (31) : Le théorème de Bézout est faux dans un anneau factoriel (Rq (15)).

2) Applications de la relation de Bézout

A est un anneau principal.

Rq (32) : On connait exactement les quotients A/I intègres, ce sont les cas $I = \{0\}$ ($A/I \simeq A$) et $I = (p)$ où p est irréductible (A/I est un corps).

Th. (33) : (*théorème des restes chinois*)
Soit A un anneau principal, $a, b \in A$ tels que $a \wedge b = 1$.
Alors $\varphi : A/(ab) \longrightarrow A/(a) \times A/(b)$ est un isomorphisme d'anneaux.
$x \bmod ab \longmapsto (x \bmod a, x \bmod b)$

Coro (34) : Soit $a \in A^*$ de décomposition $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$
Alors $A/(a) \simeq \prod_{i=1}^{n} A/(p_i^{\alpha_i})$.

Appli. (35) : Si on dispose d'un moyen effectif de calculer une relation de Bézout, on peut alors résoudre un système de congruences (voir IV).

Th (36) : (*lemme des noyaux*)
Soit E un K-ev et $P = QR \in K[X]$ où $Q \wedge R = 1$. Soit $u \in \mathcal{L}(E)$.
On pose $F = \text{Ker}(P(u))$, $F_1 = \text{Ker}(Q(u))$ et $F_2 = \text{Ker}(R(u))$ qui sont des sev de E.
Alors : $F = F_1 \oplus F_2$.
De plus le projecteur de F sur F_1 (resp. F_2) parallèlement à F_2 (resp. F_1) est un polynôme en u.

Appli. (37) : Décomposition de Dunford

IV. Anneaux euclidiens, algorithmes de calcul

1) Définition, exemples

[Bau] 529

Déf. (38) : Un anneau euclidien est un couple (A, δ) où A est un anneau intègre et $\delta : A^* \to \mathbb{N}$ une application telle que :

$\forall a, b \in A,\ b \neq 0,\ \exists q, r \in A /\ a = qb + r$ où $r = 0$ ou $\delta(r) < \delta(b)$

Ex. (39) : . $(\mathbb{Z}, |\cdot|)$ est euclidien ($|\cdot|$ = valeur absolue)

. $(K[X], \deg)$ est euclidien

. $(\mathbb{Z}[i], |\cdot|^2)$ est euclidien ($|\cdot|$ = module).

530 [Pau] 53

Prop. (40) : Un anneau euclidien est principal

Rq (41) : La réciproque est fausse (c-Ex : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ (admis))

2) Algorithme d'Euclide

Prop. (42) : *(algorithme d'Euclide)*

Soit A un anneau euclidien et $a, b \in A^*$. Alors la suite $(r_i)_{i \in \mathbb{N}}$ définie par $r_0 = a$, $r_1 = b$ et $\forall i \geq 1$, $r_{i+1} = r_{es}(r_{i-1}, r_i)$ (où $r_{es}(r_{i-1}, r_i)$ est le reste de la division euclidienne de r_{i-1} par r_i) compte un nombre fini de termes non nuls. Si l'on note $n \in \mathbb{N}$ le premier entier tel que $r_{n+1} = 0$, alors $r_n = pgcd(a, b)$.

♡

[Bau]

Prop. (43) : *(algorithme d'Euclide étendu)*

Soit A un anneau euclidien et $a, b \in A^*$. On définit les suites $(r_i)_{i \geq -1}$, $(u_i)_{i \geq -1}$, $(v_i)_{i \geq -1}$ et $(q_i)_{i \geq 0}$ par : $\begin{pmatrix} r_{-1} \\ u_{-1} \\ v_{-1} \end{pmatrix} = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} r_0 \\ u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} b \\ 0 \\ -1 \end{pmatrix}$.

$\forall i \geq 0$: $r_{i-1} = q_i r_i + r_{i+1}$ est la division euclidienne de r_{i-1} par r_i

$u_{i+1} = q_i u_i + u_{i-1}$

$v_{i+1} = q_i v_i + v_{i-1}$

$\exists n \in \mathbb{N} /\ r_n \neq 0$ et $r_i = 0\ \forall i \geq n+1$.

On pose $d = r_n$, $u = u_n$ et $v = v_n$.

Alors $d = pgcd(a, b)$ et $ua + vb = d$.

[SP] 51 52

Prop. (44) : 1) $A = \mathbb{Z}$, $a, b \in \mathbb{Z}$ et $|a| > |b|$. L'algorithme d'Euclide est effectué en $O(\log_2 a)$ étapes

2) $A = \mathbb{Z}$, $a, b \in \mathbb{Z}$. L'algorithme d'Euclide étendu est effectué en $O(\log|a| \times \log|b|)$ opérations

3) $A = K[X]$. $P, Q \in K[X]$. L'algorithme d'Euclide est effectué en $O(\deg P \times \deg Q)$ opérations.

3) Applications

Appli. (45) : *(inverse modulaire)*

1) Déterminer l'inverse de 5 dans $\mathbb{F}_3$

2) $(a, b) \in \mathbb{R}^2 \setminus \{0,0\}$. Déterminer l'inverse de $aX + b$ dans $\mathbb{R}[X]/(X^2+1)$

♡

[Bau]

Appli. (46) : *(système de congruences)*

Montrer que l'ensemble de solutions de $\begin{cases} x \equiv 1\ [3] \\ x \equiv 2\ [4] \\ x \equiv -1\ [7] \end{cases}$ est $\{34 + 84t,\ t \in \mathbb{Z}\}$

[BMP] 244

Appli. (47) : *(algorithme de Berlekamp)*

Soit $q = p^\Delta$ / p premier et $\Delta \geq 1$. Soit $P \in \mathbb{F}_q[X]$ de degré ≥ 1 et sans facteur carré. Alors, on peut déterminer $V \in \mathbb{F}_q[X]$ tel que :

1) V est non constant modulo P

2) $P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V - \alpha)$

3) si P n'est pas irréductible, au moins deux des facteurs du produit précédent sont non triviaux.

DVP 2

Références :

- [Pe] Perrin, Cours d'algèbre
- [Bu] Bahuy, Algèbre : le grand combat (2e éd.)
- [BMP] Beck, Objectif agrégation
- [SP] Saux Picart, Cours de calcul formel
- ♡ à savoir par cœur