142 PGCD ET PPCM, ALGORITHMES DE CALCUL. APPLICATIONS.

Soit A un anneau unitaire commutatif intègre et $\mathbb{K}$ un corps.

I. Notion de PGCD et de PPCM sur un anneau factoriel

I. A. Généralités

[Per96, §II.3, p45] [Rom17, Ch7, p205]

Définition 1. [Divisibilité]
Pour $a, b \in A$, on dit que a divise b et on note $a \mid b$ si $\exists c \in A \mid b = ac$, ou encore $(b) \subset (a)$.

Définition 2. [Éléments associés]
$a, b \in A$ sont dits associés si $a \mid b$ et $b \mid a$ (ou s'il existe $u \in A^\times$ tel que $a = ub$).

Remarque 3. C'est une relation d'équivalence (notée $\sim$). Deux éléments associés sont indiscernables du point de vue de la divisibilité.

Définition 4. [Irréductible] $a \in A$ non inversible et non nul est dit irréductible si pour tout $b, c \in A$ tels que $a = bc$, alors $b \in A^\times$ ou $c \in A^\times$.

Exemple 5. Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.

Définition 6. [PGCD, PPCM] Soient $a, b \in A$. On dit que
- $d \in A$ est un PGCD de a et b et on note $d = a \wedge b$ si $\forall c \in A, c \mid a$ et $c \mid b \implies c \mid d$,
- $m \in A$ est un PPCM de a et b et on note $m = a \vee b$ si $\forall c \in A, a \mid c$ et $b \mid c \implies m \mid c$.

a et b sont dits premiers entre eux si $a \wedge b = 1$.

Remarque 7. L'existence de PGCD et PPCM n'est pas garantie en général. S'ils existent, ils sont définis à un inversible près. On peut généraliser à une famille quelconque d'éléments.

Proposition 8. *Deux PGCD (resp. PPCM) de $a, b \in A$ sont associés.*

Anneau factoriel, propriété d'existence et d'unicité. Dans la suite A est factoriel.
Écriture en produit d'irréductibles, valuation p-adique

Exemple 9. $\mathbb{Z}$ et $\mathbb{K}[X]$ sont factoriels.

Existence de PGCD, PPCM, expression en fonction des décompositions en produit d'irréductibles, expression en terme d'idéaux $\rightarrow$ ok pour le PPCM mais pas pour le PGCD (l'anneau n'est pas nécessairement principal !)
Application pour le PPCM : dans un groupe, il existe un élément d'ordre l'exposant du groupe
Lemmes de Gauss

Exemples dans $\mathbb{Z}$, dans les anneaux de polynômes.
On a $(a \wedge b)(a \vee b) = ab$ et $a \wedge (b \vee a) = a = a \vee (b \wedge a)$

I. B. Contenu d'un polynôme

[FGN07, §5.16, p188–190] [Per96, p51]

Contenu, lemme de Gauss

Proposition 10. [Critère d'Eisenstein]
Soit A un anneau factoriel. Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Théorème de Gauss : $A[X]$ factoriel si A l'est

II. Vers le théorème de Bézout : PGCD sur un anneau principal

[Rom17, §8.2, p237] [Per96, §II.3.e, p49]

Anneau principal, exemple de $\mathbb{Z}$, de $\mathbb{K}[X]$
$\mathbb{K}[X, Y]$ est factoriel non principal
Si A est principal, on a bien $(a \wedge b) = (a) + (b)$ (théorème de Bézout). En particulier condition pour que a et b soient premiers entre eux ! Exemples
Généralisation à une famille d'éléments
Application : lemme des noyaux

III. Algorithmes de calcul dans les anneaux euclidiens

III. A. Obtention du PGCD

[Rom17, §9.2, p260]

Anneau euclidien, stathme, exemple de $\mathbb{K}[X]$ avec le degré
Euclidien implique principal implique factoriel
Exemple d'anneau principal non euclidien
Algorithme d'Euclide : on utilise la division euclidienne en s'appuyant sur le fait que si $a = bq + r$ avec $r \neq 0$ alors $a \wedge b = b \wedge r$
Exemple d'application de l'algorithme

III. B. Recherche d'une relation de Bézout

Algorithme d'Euclide étendu : en remontant dans l'algorithme, on obtient une relation de Bézout.
Exemple avec le PGCD de polynômes

IV. Applications aux équations en arithmétique

IV. A. Équations diophantiennes

[Rom17, §10.4, p288] [FGN07, §4.39, p167]

Définition d'une équation diophantienne [Com98, §12.7, p273]
Cas de l'équation $ax = b$
Équation $ax + ny = c$, réécrite $ax \equiv c \mod n$: ensemble des solutions, existence si et seulement si $a \wedge n \mid b$, dans ce cas une solution particulière est donnée par l'identité de Bézout, exemples
Soient $n, m \geq 2$.

Théorème 11. *Soit $a \in \mathbb{N}^*, b \in \mathbb{Z}$. On note $\delta = a \wedge n$ et on écrit $a = \delta a'$ et $n = \delta n'$. L'équation $ax \equiv b \mod n$ a des solutions entières si et seulement si $\delta \mid b$ et dans ce cas, si $b = \delta b'$, les solutions sont les $b'x'_0 + kn'$ avec $k \in \mathbb{Z}$ et x'_0 est une solution particulière de $a'x \equiv 1 \mod n'$.*

Généralisation à $\sum a_i x_i = b$: calcul par récurrence d'une solution

Théorème 12. [Théorème de Sophie Germain]
Soit p un nombre premier impair tel que $q = 2p + 1$ est premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $p \nmid xyz$ et $x^p + y^p + q^p = 0$.

IV. B. Systèmes de congruence

[Rom17, §10.3-4, p283–290]

Théorème 13. [Théorème des restes chinois]
Soient $n_1, \dots, n_r \in \mathbb{N}$ des entiers distincts. Ces entiers sont premiers entre eux si et seulement si $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes, où $n = \prod_{j=1}^r n_j$. Plus précisément, l'application $\phi : \overline{k}_n \longmapsto (\overline{k}^{n_i})_{1 \leq i \leq r}$ est un isomorphisme d'anneaux.

Exemple 14. $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Théorème 15. *L'isomorphisme inverse est donné par $(\overline{k_i}^{n_i})_{1 \leq i \leq r} \longmapsto \overline{\sum_{j=1}^r k_j u_j \frac{n}{n_j}}^n$ où l'on a choisit $(u_j)_{1 \leq j \leq r}$ tels que $\sum_{j=1}^r u_j \frac{n}{n_j} = 1$.*

Soient $n, m \geq 2$.

Application 16. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations $\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors

- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 17. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k \in \mathbb{Z}}$.

ANNEXE

Algorithme d'EUCLIDE

Soit A un anneau euclidien. L'algorithme d'EUCLIDE détermine le PGCD de deux éléments :

Entrée : $a, b \in A, b \neq 0$
Sortie : d, u, v tels que $au + bv = d$ et $d = a \wedge b$
Algorithme : $u_0 = 1, u_1 = 0, v_0 = 0, v_1 = 1, r_0 = a, r_1 = b, i = 1$
Tant que $r_i \neq 0$:
$r_{i+1} \leftarrow r_{i-1} - q_i r_i$ (division euclidienne de r_{i-1} par r_i)
$u_{i+1} \leftarrow u_{i-1} - q_i u_i$
$v_{i+1} \leftarrow v_{i-1} - q_i v_i$
$i \leftarrow i + 1$
Renvoyer $r_{i-1}, u_{i-1}, v_{i-1}$

Algorithme d'EUCLIDE étendu

SPEECH

L'objectif est de généraliser les notions de PGCD et de PPCM connue sur $\mathbb{N}$ à des anneaux.

QUESTIONS

Q En quoi le lemme des noyaux est une application du théorème de BÉZOUT ?

Q Dans le cas des anneaux euclidiens, retrouve-t-on exactement les mêmes résultats que dans $\mathbb{Z}$?

R Dans $\mathbb{Z}$ on a unicité de la division euclidienne. Dans A euclidien, il faudrait imposer une condition supplémentaire pour l'avoir.

Q Quelle est la complexité de l'algorithme d'EUCLIDE ?

R $\mathcal{O}(\ln(a)/\ln(b))$.

Q Connaissez-vous un algorithme plus simple que l'algorithme d'EUCLIDE ?

R On a $a \wedge b = (a - b) \wedge b$ pour $a, b \in \mathbb{N}$.
Tant que a sont b sont non nuls, on remplace le $\max(a, b)$ par $\max(a, b) - \min(a, b)$.
Une autre possibilité récursive :
- si a et b sont pairs, $\mathrm{PGCD}(a, b) = 2\,\mathrm{PGCD}(a/2, b/2)$,
- si a est pair et b impair, $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(a/2, b)$,
- si les deux sont impairs, on regarde s'ils sont divisibles par 3 …

Q Montrer que $\mathbb{Z}[\sqrt{5}] \simeq \mathbb{Z}[X]/(X^2 - 5)$. Calculer $d = 9 \wedge 3(2 + i\sqrt{5})$.

R $z = a + \sqrt{5}b$, $N(z) = a^2 + 5b^2$. z inversible correspond à $N(z) = 1$ ou encore $z \in \{\pm 1\}$.
3 est un diviseur commun donc $3 \mid d$. On a $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$
Si $zz' = 2 + i\sqrt{5}$, on a $N(z)N(z') = 9$

Q Que dire des orbites de l'action de $\mathrm{GL}_2(\mathbb{Z})$ sur $\mathbb{Z}^2$?

R $(a\,b) \sim (c\,d)$ si $a \wedge b = c \wedge d = e$ (si $e = au + bv$: $\begin{pmatrix} u & v \\ -b/e & a/e \end{pmatrix}\begin{pmatrix} a \\ -b/e \end{pmatrix} = \begin{pmatrix} e \\ b \end{pmatrix}$).
Réciproquement, deux vecteurs dans la même orbite ont même PGCD par transitivité.

Q Et pour l'action de $\mathrm{GL}_n(\mathbb{Z})$ sur $\mathbb{Z}^n$?

R On espère le même résultat. Par le théorème BÉZOUT, on a $\sum_i a_i u_i = d$ mais on ne va pas pouvoir trouver explicitement la matrice correspondante.
En revanche, si $V = \mathbb{Z}(u_1, \ldots, u_n)^\top$ et $W = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \sum a_i x_i = 0\}$, alors $W \cap V = 0$ et donc $W \simeq \mathbb{Z}^{n-1}$ est un sous-groupe d'un groupe abélien libre donc est un groupe abélien libre. On a donc la matrice qu'il nous faut via cet isomorphisme.

BIBLIOGRAPHIE

[Com98] F. COMBES : *Algèbre et géométrie*. Bréal, 1998.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.