Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications.

1 Généralités

Définition 1. Soient $a, b \in A$.

1. On dit que a divise b noté $a|b$ lorsqu'il existe $c \in A$ tel que $b = ac$. C'est équivalent à dire $(b) \subset (a)$.
2. On dit que a et b sont associés noté $a \sim b$ lorsque $a|b$ et $b|a$. c'est équivalent à dire $(a) = (b)$.

Proposition 2. *Dans un anneau intègre, $\sim$ est une relation d'équivalence. Pour tout $a, b \in A$ on a $a \sim b$ si et seulement si il existe $u \in A^\times$ tel que $a = bu$.*

Définition 3. Soient $a_1, \dots, a_m \in A \setminus \{0\}$.

1. L'élément $p \in A$ est appelé un Plus Petit Multiple Commun (PPCM) de $a_1, \dots, a_m$ lorsque pour tout $i \in [\![1, m]\!]$ on a $a_i|p$ et pour tout autre élément $q \in A$ vérifiant cette propriété on a $p|q$.
2. L'élément $d \in A$ est appelé un Plus Grand Diviseur Commun (PGCD) de $a_1, \dots, a_m$ lorsque pour tout $i \in [\![1, m]\!]$ on a $d|a_i$ et pour tout autre élément $q \in A$ vérifiant cette propriété on a $q|d$.

Remarque 4. Ces éléments n'existent pas obligatoirement dans tous les anneaux. Lorsqu'ils existent ils ne sont pas uniques mais sont toujours associés.

Proposition 5. *Soient $a, b \in A \setminus \{0\}$, $c \in A$ est un PPCM de a et b si et seulement si $(a) \cap (b) = (c)$.*

Proposition 6. *Pour A intègre, $a, b \in A \setminus \{0\}$ et $d \in A$, les propriétés suivantes sont équivalentes :*

- *$d|a$, $d|b$ et il existe $u, v \in A$ tels que $d = au + bv$,*
- *$d \sim pgcd(a, b)$ et il existe $u, v \in A$ tel que $d = au + bv$,*
- *$(a, b) = (a) + (b) = (d)$.*

2 PGCD dans un anneau factoriel

2.1 Généralités

Définition 7. Un anneau A est dit factoriel lorsqu'il est intègre et si pour tout élément $a \in A$ non inversible et non nul il existe une décomposition $a = q_1 q_2 \dots q_r$ avec les q_i irréductibles qui est unique a permutation près et à multiplication par in inversible près.

Théorème 8. *Soit A un anneau intègre, les propositions suivantes sont équivalentes :*

- *A est factoriel,*
- *Tout élément non nul non inversible possède une décomposition en produit d'irréductibles et tout élément irréductible est premier,*
- *Tout élément non nul, non inversible de A est produit d'éléments premiers.*

Proposition 9. *Si A est factoriel alors $A[X]$ est factoriel.*

Définition 10. Dans un anneau factoriel tout élément $a \in A$ possède une unique décomposition $a = u_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $u_a \in A^\times$, $\mathcal{P}$ un système de représentants des éléments premiers et $v_p(a)$ des entiers presque tous nuls.

Proposition 11. *Soit A factoriel et $a, b \in A$ non nuls alors un PGCD et un PPCM existent et on a :*

- *$a|b \iff v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathcal{P}$.*
- *$\prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$ est un PGCD de a et de b.*
- *$\prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$ est un PPCM de a et de b.*

Théorème 12. *Tout anneau principal est factoriel.*

Remarque 13. La réciproque est fausse $\mathbb{Z}[i\sqrt{5}]$ est factoriel non principal.

2.2 Applications aux polynômes

Définition 14. Pour $P = a_nX^n + \cdots + a_0 \in A[X]$ on définit le contenu de P noté $c(P) = \text{pgcd}(a_0, \ldots, a_n)$ modulo les inversibles de A. On dit que P est primitif lorsque $c(P) = 1$.

Lemme 15. *Pour $P, Q \in A[X]$ on a $c(PQ) = c(P)c(Q)$ modulo les inversibles.*

Proposition 16. *Soit $P \in A[X]$ non constant, si P est réductible dans $\mathbb{K}[X]$, alors il existe $Q, R \in A[X]$ non constants tels que $P = QR$.*

Proposition 17. *Soient $P, Q \in \mathbb{K}[X]$ unitaires non constants tels que $PQ \in A[X]$ alors $P, Q \in A[X]$.*

Théorème 18. *(Critère d'Eisenstein) Soit A anneau factoriel et $\mathbb{K}$ son corps des fractions. Soit $P(X) = a_nX^n + \cdots + a_0 \in A[X]$ et $p \in A$ irréductible. Si on a les conditions suivantes :*

1. *$p \nmid a_n$,*
2. *$p \mid a_i$ pour $i \in \{0, \ldots, n-1\}$,*
3. *$p^2 \nmid a_0$*

Alors P est irréductible dans $\mathbb{K}[X]$ (donc si pgcd$(a_i) = 1$ il l'est dans $A[X]$).

Exemple 19. Pour p premier dans $\mathbb{N}$, $X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Z}$.
Pour tout $n \in \mathbb{N}^*$ le polynôme $X^n - 2$ est irréductible sur $\mathbb{Z}$.

Remarque 20. Le deuxième exemple nous donne l'existence d'extensions de $\mathbb{Q}$ de n'importe quel degré puis l'existence des nombres transcendants sur $\mathbb{R}$.

3 Existence et unicité dans un anneau principal

Proposition 21. *Dans un anneau principal, tout idéal premier non nul est maximal.*

Définition 22. Deux éléments non nuls $a, b \in A$ sont dits premiers entre eux si et seulement si tout diviseur commun est inversible. C'est équivalent à dire que $\text{pgcd}(a, b) \sim 1$.

Théorème 23. *(Bézout) Dans un anneau principal A, le PGCD et le PPCM d'éléments non nuls $a_1, \ldots, a_m$ existent. Un PGCD d de cette famille est générateur de $(a_1, \ldots, a_m)$. Un PPCM b de cette famille est générateur de $(a_1) \cap \cdots \cap (a_m)$. En particulier d peut s'écrire comme combinaison linéaire des a_i c'est à dire $d = a_1b_1 + \cdots + a_mb_m$ avec $b_i \in A$.*

Remarque 24. Dans un anneau factoriel non principal c'est faux. Dans $\mathbb{K}[X, Y]$ on a $\text{pgcd}(X, Y) = 1$ mais $(X) + (Y) = (X, Y) \neq (1)$.

Lemme 25. *(Euclide) Soit A principal, $a, b \in A$ premiers entre eux et $c \in A$, si $a|bc$ alors $a|c$.*

Lemme 26. *(Gauss) Soit A principal, $a, b \in A$ premiers entre eux et $c \in A$, si $a|c$ et $b|c$ alors $ab|c$.*

On considère A est principal, $(a_1, \ldots, a_r) \in A$ non nuls et non inversible et $a = \prod_{k=1}^{r} a_k$. Pour tout $j \in [\![1, r]\!]$ on pose π_j la surjection canonique de A sur $A/(a_j)$ et π celle sur $A/(a)$. Enfin on pose pour tout $j \in [\![1, r]\!]$ l'élément $b_j = a/a_j$.

Lemme 27. *Si pour tout $j \in [\![1, r]\!]$, les a_j sont deux à deux premiers entre eux alors les b_j sont premiers entre eux dans leur ensemble.*

Théorème 28. *(Chinois) Supposons que pour tout $j \in [\![1, r]\!]$, les a_j sont 2 à 2 premiers entre eux, alors l'application*

$$\varphi : x \in A \mapsto (\pi_j(x))_{1 \leqslant j \leqslant r} \in \prod_{j=1}^{r} A/(a_j)$$

est un morphisme d'anneau surjectif de noyau $\ker(\varphi) = (a)$ *et induit un isomorphisme d'anneau*

$$\overline{\varphi} : \pi(x) \in A/(a) \mapsto (\pi_j(x))_{1 \leqslant j \leqslant r} \in \prod_{j=1}^{r} A/(a_j)$$

dont l'inverse est

$$\overline{\varphi}^{-1} : (\pi_j(x_j))_{1 \leqslant j \leqslant r} \in \prod_{j=1}^{r} A/(a_j) \mapsto \overline{\sum_{i=1}^{r} x_i u_i b_i} \in A/(a)$$

où les $(u_j)_{1 \leqslant j \leqslant r}$ *vérifient* $\sum_{j=1}^{r} u_j b_j = 1$.

4 Anneaux euclidiens

Proposition 29. *Tout anneau euclidien est principal.*

Remarque 30. La réciproque est fausse, par exemple $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$.

Théorème 31. *Si* $\mathbb{K}$ *corps, alors* $\mathbb{K}[X]$ *est un anneau euclidien de stathme le degré. Il y a de plus unicité du quotient et du reste.*

Corollaire 32. *Les assertions suivantes sont équivalentes :*

1. *A est un corps ;*
2. *A*$[X]$ *est euclidien ;*
3. *A*$[X]$ *est principal.*

Lemme 33. *Soit A euclidien de stathme* ν, $a, b \in \mathbb{A} \setminus \{0\}$ *et r un reste de la division euclidienne de a par b, alors soit* $r = 0$ *et pgcd*$(a, b) = b$, *soit pgcd*$(a, b) =$ *pgcd*(b, r).

Théorème 34. *(Algorithme d'Euclide) Soit A euclidien de stathme* ν *et* $a, b \in \setminus \{0\}$ *tels que* $\nu(a) \geqslant \nu(b)$, *on définit une suite* $(r_k)_k$ *décroissante par :*

- $r_0 = b$,
- r_1 *est un reste de la division euclidienne de a par b donc* $\nu(r_1) \leqslant \nu(r_0)$,
- *Pour* $k \geqslant 2$ *si* $r_{k-1} = 0$ *alors* $r_k = 0$ *sinon c'est un reste de la division euclidienne de* r_{k-2} *par* r_{k-1}.

Alors pgcd(a, b) *est le dernier reste non nul de cette suite.*

Remarque 35. On peut remonter l'algorithme d'Euclide pour obtenir les coefficients de Bézout, on parle d'algorithme d'Euclide "étendu".

Exemple 36. On a $\text{pgcd}(1763, 731) = 43 = 5 \times 1763 - 12 \times 731$.

5 Application aux systèmes de congruences

Définition 37. On appelle équation diophantienne dans $\mathbb{Z}$ une équation de la forme $ax \equiv b \mod (n)$ avec $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$.

Théorème 38. *L'équation diophantienne* $ax \equiv b \mod (n)$ *admet des solutions entières si et seulement* $\delta = pgcd(a, n)$ *divise b. Dans ce cas, en notant* $a = \delta a'$, $b = \delta b'$ *et* $n = \delta n'$, *l'ensemble des solutions est alors* $S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$ *où* x'_0 *est une solution de* $a'x \equiv 1 \mod (n')$.

Corollaire 39. *Pour un système d'équations diophantiennes* $k \equiv a_j \mod (n_j)$ *pour* $1 \leqslant j \leqslant r$.. *Lorsque les* $n_1, \ldots, n_r$ *sont deux à deux premiers entre eux, cela revient à trouver l'antécédent dans* $\mathbb{Z}/n\mathbb{Z}$ *de* $(\pi_1(a_1), \ldots, \pi_r(a_r))$ *par l'isomorphisme* ψ *défini dans le théorème Chinois. Cet antécédent est* $\overline{k_0}$ *où* $k_0 = \sum_{i=1}^{r} a_i u_i m_i$. *Les autres solutions sont donc les* $k = k_0 + qn$ *avec* $q \in \mathbb{Z}$.

Exemple 40. Les solutions du système $\begin{cases} k \equiv 2 \mod (4) \\ k \equiv 3 \mod (5) \\ k \equiv 1 \mod (9) \end{cases}$ sont les $k = 118 + 180q$ avec $q \in \mathbb{Z}$.

Dev 1 : Théorème des restes chinois 27, 28 et 40
Dev 2 : Eisenstein 15,16, 17 et 18

Références

[PER96] Daniel PERRIN : Cours d'algèbre. Ellipses, 1996.

[ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

[SP99] Philippe SAUX-PICART : Cours de calcul formel : algorithmes fondamentaux. Ellipses, 1999.

RAPPORT DU JURY :

Le candidat doit prendre soin de différencier le cadre théorique des anneaux factoriels ou principaux dans lequel sont définis les PGCD et PPCM et dans lequel s'appliquent les énoncés des théorèmes proposés et le cadre euclidien fournissant les algorithmes. Le champ d'étude de cette leçon ne peut se limiter au cas de $\mathbb{Z}$, mais la leçon peut opportunément s'illustrer d'exemples élémentaires d'anneaux euclidiens, comme $\mathbb{Z}[X]$ et $\mathbb{K}[X]$. Une part substantielle de la leçon doit être consacrée à la présentation d'algorithmes : algorithme d'Euclide, algorithme binaire, algorithme d'Euclide étendu. Il est possible d'en évaluer le nombre d'étapes dans les pires cas et faire le lien avec les suites de Fibonacci. Des applications élémentaires sont particulièrement bienvenues : calcul de relations de Bézout, résolutions d'équations diophantiennes linéaires, inversion modulo un entier ou un polynôme, calculs d'inverses dans les corps de rupture, les corps finis. On peut aussi évoquer le théorème chinois effectif, la résolution d'un système de congruences et faire le lien avec l'interpolation de Lagrange.

Pour aller plus loin, on peut évoquer le rôle de algorithme d'Euclide étendu dans de nombreux algorithmes classiques en arithmétique (factorisation d'entiers, de polynômes, etc). Décrire l'approche matricielle de l'algorithme d'Euclide et l'action de $SL_2(\mathbb{Z})$ sur $\mathbb{Z}^2$ est tout à fait pertinent. On peut aussi établir l'existence d'un supplémentaire d'une droite dans $\mathbb{Z}^2$, ou d'un hyperplan de $\mathbb{Z}^n$, examiner l'éventuelle possibilité de compléter un vecteur de $\mathbb{Z}^n$ en une base. On peut aussi étudier les matrices à coefficients dans un anneau principal ou euclidien, et, de manière plus avancée, la forme normale d'Hermite et son application à la résolution d'un système d'équations diophantiennes linéaires. De même, aborder la forme normale de Smith, et son application au théorème de la base adaptée, permet de faire le lien avec la réduction des endomorphismes via le théorème des invariants de similitude. La leçon invite aussi, pour des candidates et candidats maîtrisant ces notions, à décrire le calcul de PGCD dans $\mathbb{Z}[X]$ et $\mathbb{K}[X, Y]$, avec des applications à l'élimination de variables. On peut rappeler les relations entre PGCD et résultant et montrer comment obtenir le PGCD en échelonnant la matrice de Sylvester. Sur l'approximation diophantienne, on peut enfin envisager le développement d'un rationnel en fraction continue et l'obtention d'une approximation de Padé-Hermite à l'aide de l'algorithme d'Euclide, la recherche d'une relation de récurrence linéaire dans une suite ou le décodage des codes BCH.