P. Maurer
ENS Rennes

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

Devs :

- Critère d'Eisenstein
- Décomposition de Dunford

Références :

1. Gourdon, Algèbre
2. Perrin, Cours d'algèbre
3. Combes, Algèbre et géométrie
4. Saux-Picart, Cours de calcul formel : algorithmes fondamentaux
5. Colmez, Eléments d'analyse et d'algèbre
6. Objectif Agrégation

On se donne un anneau A unitaire, commutatif et intègre, et k un corps.

1 PGCD et PPCM dans un anneau factoriel

1.1 Généralités

Définition 1. *On note $A^\times$ le groupe des inversibles de A, aussi appelés unités.*

Définition 2. *Soit $a, b \in A$. On dit que a divise b si il existe $r \in A$ tel que $b = ar$.*
Un élément $d \in A$ est appelé diviseur commun de $n_1, \dots n_m \in A$ si d divise n_i pour tout i.
Un élément $m \in A$ est appelé multiple commun de $n_1, \dots, n_m \in A$ si n_i divise m pour tout i.

Définition 3. *Un élément $p \in A$ est dit irréductible si p n'est ni nul ni inversible et si $p|ab \Longrightarrow p|a$ ou $p|b$ pour tout $a, b \in A$.*

Définition 4. *On dit que $a, b \in A$ sont associés s'il existe $u \in A^\times$ tel que $a = ub$.*
On montre que a et b sont associés si et seulement si $(a) = (b)$.

Définition 5. *Soit A un anneau intègre. On dit que A est factoriel si tout élément $a \in A$ peut s'écrire, de manière unique à permutation de facteurs près, de la forme :*

$$a = u p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$$

Où $u \in A^\times$ et $p_1, \dots, p_\ell \in A$ sont irréductibles et $\alpha_1, \dots, \alpha_\ell \in \mathbb{N}$.

Exemple 6. $\mathbb{Z}[i]$ est factoriel. $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel car $3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$.

Dans ce qui suit, on suppose que A est factoriel.

Définition 7. *Soit $a, b \in A$, écrit sous la forme $a = u \prod p^{v_p(a)}$ et $b = v \prod p^{v_p(b)}$.*

- *On appelle plus petit multiple commun de a et b l'élément* $\operatorname{ppcm}(a, b) := \prod p^{\sup(v_p(a), v_p(b))}$.
- *On appelle plus grand diviseur commun de a et b l'élément* $\operatorname{pgcd}(a, b) := \prod p^{\inf(v_p(a), v_p(b))}$.

Le ppcm et le pgcd sont définis à un inversible près.

Remarque 8. Le ppcm et le pgcd peuvent ne pas exister si l'anneau n'est pas factoriel. Par exemple, dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2 + i\sqrt{5}$ n'ont pas de ppcm tandis ce que 9 et $3(2 + i\sqrt{5})$ n'ont pas de pgcd.

1.2 Contenu d'un polynôme

Définition 9. *Pour $P \in A[X]$ non nul, on appelle contenu de P, noté $c(P)$ le plus grand diviseur commun de ses coefficients. L'élément $c(P)$ est défini modulo $A^\times$ (à un inversible près).*
Un polynôme est dit primitif si $c(P) = 1$.

Lemme 10. *(Gauss)*
On a $c(PQ) = c(P)\, c(Q)$ modulo $A^\times$.

Théorème 11. *Si A est factoriel, $A[X]$ est factoriel.*

Développement 1 :

Théorème 12. *(Critère d'Eisenstein). Soit A un anneau factoriel. On note $K = \mathrm{Frac}(A)$. Les polynômes de $A[X]$ irréductibles sont :*

i. Les constantes $p \in A$ irréductibles dans A

ii. Les polynômes de degré plus grand que 1 primitifs et irréductibles dans $K[X]$

Soit $P = \sum_{i=1}^{n} a_i X^i \in A[X]$, et p un élément irréductible de A tel que $p \nmid a_n$, $p^2 \nmid a_0$ et $p | a_i$ pour tout $i \in [\![0, n-1]\!]$. Alors P est irréductible dans $K[X]$.

Application 13. Le polynôme cyclotomique $\Phi_{\mathbb{Q},p}(X) = \prod_{\zeta \in \mu_p^*} (X - \zeta) = \sum_{i=1}^{p-1} X^i$ est irréductible sur $\mathbb{Q}$, où p est un nombre premier et μ_p^* désigne l'ensemble des racines primitives $p^{\text{èmes}}$ de l'unité.

1.3 Cas des anneaux principaux

Définition 14. *On dit que A est principal si tout idéal de A est principal, c'est-à-dire engendré par un seul élément.*

Exemple 15. $\mathbb{Z}$ et $k[X]$ sont des anneaux principaux.

Théorème 16. *(Théorème de Bézout)*
Soit A un anneau principal et $a, b \in A$. On note $d = \text{pgcd}(a,b)$. Alors $(a)+(b)=(d)$. Autrement dit, il existe $u, v \in A$ tels que $au+bv=d$.

Corollaire 17. *Soit A un anneau principal et $a, b \in A\setminus\{0\}$ premiers entre eux. Alors $(a)+(b)=(1)$, i.e il existe $u, v \in A$ tels que $au+bv=1$.*

Remarque 18. Le théorème de Bézout est mit en défaut dans un anneau factoriel non principal. Par exemple, l'anneau $k[X,Y]$ est factoriel et X et Y sont premiers entre eux, mais on a $(X)+(Y)=(X,Y)\neq(1)$.

Exemple 19. (Lemme des noyaux)
Soit E un k-espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$. Soit $P_1, \dots, P_r \in K[X]$ deux à deux premiers entre eux. Alors $\text{Ker}\, P(f) = \text{Ker}\, P_1(f) \oplus \cdots \oplus \text{Ker}\, P_r(f)$.

Développement 2 :

Proposition 20. *Soit $f \in \mathcal{L}(E)$ et $F \in k[X]$ un polynôme annulateur de f. Soit $f = \beta M_1^{\alpha_1} \cdots M_s^{\alpha_s}$ la décomposition en facteurs irréductibles de $k[X]$ du polynôme F.*
Pour $i \in [\![1,s]\!]$, on note $N_i = \text{Ker}\, M_i^{\alpha_i}(f)$. On a alors $E = N_1 \oplus \cdots \oplus N_s$, et pour tout $i \in [\![1,s]\!]$, la projection sur N_i parallèlement à $\bigoplus_{\substack{1\leq j\leq s \\ j\neq i}} N_j$ est un polynôme en f.

Théorème 21. *(Réduction de Dunford)*
Soit $f \in \mathcal{L}(E)$ un endomorphisme dont le polynôme caractéristique χ_f est scindé sur k. Alors il existe un unique couple $(d,n) \in \mathcal{L}(E)^2$ tel que

1. *Les endomorphismes d et n commutent et $d+n=f$.*
2. *L'endomorphisme d est diagonalisable et l'endomorphisme n est nilpotent.*

De plus, les endomorphismes d et n sont des polynômes en f.

2 Algorithmes de calcul dans un anneau euclidien

2.1 Obtention du PGCD et des relations de Bézout

Définition 22. *Un anneau intègre A est dit euclidien si il existe une application $f: A\setminus\{0\} \to \mathbb{N}$ telle que pour tout $(a,b) \in A \times A\setminus\{0\}$, il existe un couple $(q,r) \in A^2$ vérifiant $a = bq+r$ et $(r=0$ ou $f(r)<f(b))$.*

Proposition 23. *Si A est euclidien, le couple (q,r) obtenu pour tout $(a,b) \in A \times A\setminus\{0\}$ ci-dessus est unique.*

Exemple 24. L'anneau $\mathbb{Z}$ muni de l'application $f(n)=|n|$ est euclidien. L'anneau $k[X]$ muni de l'application $f(P)=\deg(P)$ est euclidien.

Théorème 25. *(Algorithme d'Euclide)*
Soit a et b deux éléments non nuls d'un anneau euclidien A, soit $(r_i)_i$ la suite d'éléments définie par $r_0=a$, $r_1=b$, puis, pour $r \geq 2$, $r_i = \text{rem}(r_{i-2}, r_{i-1})$, où $\text{rem}(x,y)$ désigne la fonction qui a (x,y) associe le reste dans la division de x par y dans A.
Alors la suite $(r_i)_i$ est finie : il existe un entier $n+1$ pour lequel $r_{n+1}=0$ et $\text{pgcd}(a,b)=r_n$.

Proposition 26. *En gardant les mêmes notations, on a $n \leq 2\log_2(a)+1$. En particulier, le nombre de divisions à réaliser pour calculer $\text{pgcd}(a,b)$ est majoré par $2\log_2(a)$.*

Proposition 27. *Le calcul du pgcd de a et b par l'algorithme d'Euclide a une complexité de $O(\log(a)\log(b))$ opérations binaires, dans le pire des cas.*

Exemple 28. $\text{pgcd}(X^m-1, X^k-1) = X^{\text{pgcd}(m,k)}-1$.

Théorème 29. *(Algorithme d'Euclide étendu)*
Si $a, b \in A\setminus\{0\}$, on définit :

$$W_0 = \begin{pmatrix} a \\ 1 \\ 0 \end{pmatrix},\ W_1 = \begin{pmatrix} b \\ 0 \\ 1 \end{pmatrix},\ W_i = \begin{pmatrix} r_i \\ u_i \\ v_i \end{pmatrix}$$

Où pour $i \geq 2$, r_i est le reste de la division euclidienne (q_i, r_i) de r_{i-2} par r_{i-1}, u_i et v_i étant définis par $u_i = u_{i-2} - q_i u_{i-1}$ et $v_i = v_{i-2} - q_i v_{i-1}$.
Alors pour tout i, $r_i = au_i + bv_i$: en particulier, $\text{pgcd}(a,b) = au_n + bv_n$, où n est le plus petit indice pour lequel $r_{n+1}=0$.

2.2 Théorème chinois et résolution effective

Théorème 30. *(Théorème chinois)*
Soit I et J des idéaux de A tels que $I+J=A$. L'application φ: $\begin{cases} A/I\cap J & \to & (A/I)\times(A/J) \\ \hat{x} & \mapsto & (\bar{x}, \check{x}) \end{cases}$ est un isomorphisme d'anneau.

Corollaire 31. *Soit A un anneau principal, $m \in A$ et $n \in A$ premiers entre eux. Considérons $u \in A$, $v \in A$ tels que $1 = um+vn$. L'application ψ: $\begin{cases} A/mnA & \to & (A/mA)\times(A/nA) \\ \hat{x} & \mapsto & (\bar{x}, \check{x}) \end{cases}$ est un isomorphisme d'anneau.*

L'isomorphisme réciproque associe à $(\bar{a},\check{b})\in(A/mA)\times(A/nA)$ la classe $\hat{x}\in A/mnA$ de $x=vna+umb$.

Remarque 32. Si m et n sont premiers entre eux, le corollaire montre que le système

$$\begin{cases} k &\equiv a \pmod{mA} \\ k &\equiv b \pmod{nA} \end{cases}$$

a une unique solution modulo mnA. Si A est euclidien, on peut déterminer une relation de Bézout via l'algorithme d'Euclide pour obtenir une solution x. Les autres solutions s'obtiennent en ajoutant à x un multiple de mn.

Exemple 33. Le système de congruences dans $\mathbb{Z}$ $\begin{cases} x\equiv 2 \pmod 4 \\ x\equiv 3 \pmod 5 \\ x\equiv 1 \pmod 9 \end{cases}$ a pour solutions $x=838+180k$ et $x=118+180k'$ pour $k,k'\in\mathbb{Z}$.

3 Applications

3.1 Résolution d'équations diophantiennes

Proposition 34. *Soit $a,b\in\mathbb{Z}$. L'équation $ax=b$ admet des solutions si et seulement si $a|b$, et dans ce cas, l'unique solution est donnée par $x=\frac{b}{a}$.*

Proposition 35. *Soit $a,b\geq 2$ deux entiers premiers entre eux. L'équation $ua-vb=1$ admet pour uniques solutions les couples $(u+kb,v+ka)$ où le couple (u,v) est donné par le théorème de Bézout et k est un entier relatif.*

Remarque 36. En pratique, on obtient u et v grâce à l'algorithme d'Euclide.

Exemple 37. L'équation $47u+111v=1$ a pour solutions $(26+111k,-11+47k)$ pour $k\in\mathbb{Z}$.

Cadre 38. *Soit $n,m\in\mathbb{N}$, $A\in\mathcal{M}_{m,n}(\mathbb{Z})$ et $B\in\mathcal{M}_{m,1}(\mathbb{Z})$. On souhaite résoudre l'équation $AX=B$.*

Proposition 39. *On suppose que $A=\operatorname{diag}(d_1,\dots,d_r,0,\dots,0)$ avec $d_1,\dots,d_r\in\mathbb{Z}$. Alors l'équation $AX=B$ a des solutions si et seulement si $d_i|b_i$ pour tout $i\in[\![1,r]\!]$ et $b_{r+1}=\dots=b_m=0$, et dans ce cas, les solutions sont les n-uplets $\left(\frac{b_1}{d_1},\dots,\frac{b_r}{d_r},k_{r+1},\dots,k_n\right)$ avec $k_{r+1},\dots,k_n\in\mathbb{Z}$.*

Théorème 40. *(Invariants de similitude). Soit $A\in\mathcal{M}_{m,n}(\mathbb{Z})$. Il existe une famille $(d_1,\dots,d_r)$ d'entiers non nuls tels que $d_1|\dots|d_r$ telle que A soit équivalente à $\operatorname{diag}(d_1,\dots,d_r,0,\dots,0)$.*

Remarque 41. On obtient les invariants de similitude de A de manière algorithmique, sur une méthode similaire au pivot de Gauss, en utilisant des divisions euclidiennes successives.

Proposition 42. *Soit $P\in\mathrm{GL}_m(\mathbb{Z})$ et $Q\in\mathrm{GL}_n(\mathbb{Z})$ tels que $PAQ=D$, où D est de la forme du théorème 8. Alors X est solution de $AX=B$ si et seulement si $Q^{-1}X$ est solution de $DQ^{-1}X=PB$.*

Remarque 43. Ceci donne une méthode de résolution pour les équations diophantiennes linéaires à n variables.

3.2 Une application en théorie des groupes

On considère G un groupe abélien fini.

Définition 44. *On appelle ordre d'un élément $g\in G$ et on note $\operatorname{ord}(g)$ le plus petit entier $d\in\mathbb{N}^*$ tel que $g^d=1$.*

Proposition 45. *Pour $g\in G$, on a $\operatorname{ord}(g)=d\iff g^d=1$ et $\forall k\in\mathbb{N}^*\quad g^k=1\Rightarrow d|k$.*

Proposition 46.

1. *Si $x\in G$ est d'ordre a et si $y\in G$ est d'ordre b, et si $\operatorname{pgcd}(a,b)=1$, alors xy est d'ordre ab.*
2. *Si $a,b\in\mathbb{N}^*$ et si G contient des éléments d'ordre a et b, alors il contient un élément d'ordre $\operatorname{ppcm}(a,b)$.*
3. *Soit N le maximum des ordres des éléments de G. Alors on a $x^N=1$ pour tout $x\in G$. On dit que N est l'exposant du groupe G.*

Définition 47. *On appelle caractère linéaire de G un morphisme de groupes $\chi:G\to\mathbb{C}^*$, et on note $\hat{G}$ l'ensemble des caractères linéaires de G.*

Proposition 48. *Muni du produit $(\chi_1\chi_2)(g):=\chi_1(g)\,\chi_2(g)$, l'ensemble $\hat{G}$ des caractères linéaires de G est un groupe commutatif. On l'appelle le groupe dual de G.*

Lemme 49. *Soit G un groupe abélien fini. Alors G est isomorphe à $\hat{\hat{G}}$.*

Lemme 50. *Soit G un groupe abélien fini. Alors G et $\hat{G}$ ont le même exposant.*

Théorème 51. *(Théorème de structure des groupes abéliens finis, existence)*
Soit G un groupe abélien fini. Alors il existe $r\in\mathbb{N}$ et des entiers $N_1,\dots,N_r$, où N_1 est l'exposant de G et qui vérifient $N_{i+1}|N_i$ pour tout $i\leq r-1$, et qui sont tels que

$$G\simeq\prod_{i=1}^{r}\mathbb{Z}/N_i\mathbb{Z}.$$