Leçon 142 PGCD et PPCM, algorithmes de calcul, exemples

Dorian Cacitti-Holland

2020-2021

Références.

1. Eléments de théorie des anneaux de Josette Calais
2. Les contre-exemples en mathématiques de Bertrand Hauchecorne
3. Cours d'algèbre de Daniel Perrin
4. Algèbre et géométrie de Jean-Etienne Rombaldi
5. Cours de calcul formel de Saux et Picart
6. Théorie des nombres de Daniel Duverney
7. Oraux X-ENS Algèbre 1
8. Elements d'analyse et d'algèbre de Pierre Colmez

Développements.

1. Critère d'irréductibilité d'Eisenstein
2. Théorème de Sophie Germain
3. Théorème de structure des groupes abéliens finis

Table des matières

1 PGCD et PPCM dans un anneau factoriel

1.1 A partir de la divisibilité

(Chapitres 5.3.A et 5.4 de Eléments de théorie des anneaux de Josette Calais)
On considère A un anneau intègre unitaire.

1. Définition : Soit $a_1, ..., a_n \in A$, alors on appelle PGCD de $a_1, ..., a_n$ tout élément $d \in A^*$ tel que $d \mid a_i$ et $c \mid a_i \Rightarrow c \mid d$
2. Proposition : Soit $a_1, ..., a_n \in A$, d un PGCD de $a_1, ..., a_n$ et $d' \in A^*$, alors d' est un PGCD de $a_1, ..., a_n$ si et seulement si d et d' sont accociés (il existe $c \in A^\times, d = cd'$)
3. Exemple : X et $2X$ sont des PGCD de $X(X-1), X(X+1)$ dans $\mathbb{R}[X]$
4. Remarque : Dans ce cas on note $a_1 \wedge ... \wedge a_n$ la classe d'équivalence des PGCD
5. Proposition : Soit $a_1, a_2, a_3 \in A$ admettant un PGCD, alors $a_1 \wedge a_2 \wedge a_3 = (a_1 \wedge a_2) \wedge a_3 = a_1 \wedge (a_2 \wedge a_3) = (a_1 \wedge a_2) \wedge (a_2 \wedge a_3)$
6. Corollaire : Toute famille de n éléments de A admettent un PGCD si et seulement si toute famille de 2 éléments de A admettent un PGCD
7. Remarque : L'exitence de PGCD n'est pas toujours vérifiée
8. Exemple : Si $A = \mathbb{Z}[i\sqrt{5}]$, soit $p = 2 + i\sqrt{5}, q = 2 - i\sqrt{5}, a = pq = 9, b = 3p = 6i3\sqrt{5}$, alors a et b n'admettent pas de PGCD (Exemple 3.28 des Contre-exemples en mathématiques de Bertrand Hauchecorne)
9. Définition : Soit $a_1, ..., a_m \in A$, alors on appelle PPCM de $a_1, ..., a_n$ tout élément $m \in A^*$ tel que $a_i \mid m$ et $a_i \mid l \Rightarrow m \mid l$
10. Remarque : Les résultats précédents s'adaptent avec les PPCM
11. Théorème : Soit $a, b \in A$ admettant un PGCD d, alors a, b admettent un PPCM m tel que $md = ab$

1.2 Dans un anneau factoriel

(Chapitres 5.6.A et 5.6.B de Eléments de théorie des anneaux de Josette Calais et II.3.c du Cours d'algèbre de Daniel Perrin)
On suppose de plus A factoriel.

1. Définition : On dit que A est factoriel si :
   — (E) Tout $a \in A^*$ non inversible s'écrit $a = r_1...r_n$ avec r_i irréductible dans A
   — (U) Si $a = r_1...r_n = r'_1...r'_p$ alors $n = p$ et il existe $\sigma \in S_n$ tel que r_i et $r'_{\sigma(i)}$ soient associés
2. Exemple : $\mathbb{Z}$ est factoriel
3. Proposition : Les PGCD et PPCM existent, plus précisément soit $a = ur_1^{n_1(a)}...r_p^{n_p(a)}, b = vr_1^{n_1(b)}...r_p^{n_p(b)}$, alors, en notant $\alpha_i = min(n_i(a), n_i(b)), \beta_i = max(n_i(a), n_i(b))$, $d = r_1^{\alpha_1}...r_p^{\alpha_p}$ est un PGCD de a, b et $m = r_1^{\beta_1}...r_p^{\beta_p}$ est un PPCM de a, b
4. Exemple : Dans $\mathbb{Z}$, on a $314 = 2 \times 157$ et $666 = 2 \times 3^2 \times 37$, donc un PGCD de 314 et 666 est 2 et un PPCM est $2 \times 3^2 \times 37 \times 157$

5. Lemme d'Euclide : Soit $p \in A$ irréductible, $a, b \in A$ tels que $p \mid ab$, alors $p \mid a$ ou $p \mid b$
6. Théorème de Gauss : Soit $a, b, c \in A$ tels que $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$

1.3 Application à $A[X]$ avec A anneau factoriel

(Chapitres 5.6.C de Eléments de théorie des anneaux de Josette Calais et II.4.a du Cours d'algèbre de Daniel Perrin)

1. Définition : Soit $f \in A[X] \backslash A$, alors le contenu de f est $c(f)$ un PGCD des coefficients de f (défini à association près), et on dit que f est primitif si 1 est un PGCD des coefficients de f
2. Remarque : Soit $f \in A[X] \backslash A$, alors il existe $f_0 \in A[X] \backslash A$ primitif tel que $f = c(f) f_0$, de plus tout polynôme unitaire est primitif
3. Lemme de Gauss : Soit $f, g \in A[X]$, alors $c(fg) = c(f)c(g)$
4. Proposition : Soit K le corps des fractions de A, soit $r \in A[X]^*$, alors :
   — r est irréductible dans $A[X]$ et $deg(r) = 0$ si et seulement si r est irréductible dans A
   — r est irréductible dans $A[X]$ et $deg(r) > 0$ si seulement si r primitif dans $A[X]$ et irréductible dans $K[X]$
5. Théorème : $A[X]$ est factoriel
6. Exemple : $\mathbb{Z}[X]$ est factoriel
7. Théorème : Critère d'irréductiblité d'Eisenstein : Soit $f \in A[X]$, tel que $n = deg(f) > 0$, s'il existe $p \in A$ premier tel que $\forall i \in [\![0, n-1]\!], p \mid a_i$, p^2 ne divise pas a_i et p ne divise pas a_n alors f est irréductible dans $K[X]$, si de plus f est primitif alors f est irréductible dans $A[X]$
8. Exemple : Dans $\mathbb{Z}[X]$, $X^5 + 4X^3 + 15X + 2$ est irréductible dans $\mathbb{Z}[X]$, $\sum_{i=0}^{p-1} X^i$ également

2 PGCD et PPCM dans un anneau plus "petit"

2.1 Dans un anneau principal

(Chapitres 8.1 et 19.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi et II.3.d du Cours d'algèbre de Daniel Perrin)

On suppose de plus A principal.

1. Définition : On dit que A est principal si tout idéal de A est principal, ie engendré par un seul élément de A
2. Exemple : $\mathbb{Z}$ et $K[X]$ sont principaux, un corps est un anneau principal
3. Théorème : A factoriel
4. Remarque : Un anneau factoriel est non nécessairement principal
5. Exemple : $\mathbb{Z}[X]$ est factoriel non principal, $(2, X)$ n'est pas un idéal principal

6. Théorème : Soit $a_1, ..., a_n \in A$, alors $a_1, ..., a_n$ admettent un PGCD d tel que $(d) = (a_1, ..., a_n)$, de même $a_1, ..., a_n$ admettent un PPCM m tel que $(m) = (a_1) \cap ... \cap (a_n)$
7. Remarque : Dans le cas $n = 2$, on a $a, b \in A$ admettent un PGCD d et un PPCM m tels que $(d) = (a, b), (m) = (a) \cap (b)$
8. Corollaire : Théorème de Bézout : Soit $a, b \in A$ premiers entre eux, alors il existe $u, v \in A$ tels que $1 = au + +bv$, appelé identité de Bézout
9. Remarque : Dans le cas $n > 2$, soit $a_1, ..., a_n \in A$, alors $a_1, ..., a_n$ premiers entre eux si et seulement s'il existe $u_1, ..., u_n \in A$ tels que $1 = \sum_{k=1}^{n} a_k$
10. Exemple : $-\frac{1}{2}(X-1) + \frac{1}{2}(X+1) = 1$, donc $X-1$ et $X+1$ sont premiers entre eux
11. Application : Lemme des noyaux : Soit $P_1, ..., P_r \in K[X]^*$ deux à deux premiers entre eux, $P = \prod_{k=1}^{r} P_k$ et $u \in End(E)$ avec E un K-espace vectoriel, alors $ker(P(u)) = \bigoplus_{k=1}^{p} ker(P_k(u))$, de plus les projecteurs $\pi_k : ker(P(u)) \longrightarrow ker(P_k(u))$ sont des polynômes en u

2.2 Dans un anneau euclidien

(Chapitres 9.1 et 9.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 5.5.B de Eléments de théorie des anneaux)

On suppose de plus A euclidien.

1. Définition : On dit que A est euclidien s'il existe un stathme $\varphi : A^* \longrightarrow \mathbb{N}$ tel que pour tout $(a, b) \in A \times A^*$, il existe $q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $\varphi(r) < \varphi(b)$
2. Exemple : $\mathbb{Z}$ et $K[X]$ sont des anneaux euclidiens avec comme stathmes $|\cdot|$ et deg, l'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien de stathme $N(z) = z\overline{z}$, une division euclidienne de $4 + 7i$ par $8 - i$ donne $q = i$ et $r = 3 - i$
3. Théorème : A est principal, plus précisément, pour I idéal non nul de A, $I = (a_0)$ avec $a_0 \in I^*$ tel que $\varphi(a_0) = \underset{a \in I^*}{min} \varphi(a)$
4. Corollaire : Si A est euclidien alors A est factoriel, donc tout $a, b \in A$ admettent un PGCD et un PPCM
5. Remarque : La réciproque est fausse, en général un anneau principal n'est pas euclidien
6. Exemple : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ principal non euclidien

2.3 Algorithmes de calcul

(Chapitres 9.1 et 9.2 d'Algèbre et géométrie de Jean-Etienne Rombaldi, 5.5.B de Eléments de théorie des anneaux, III.4.2 du Cours de calcul formel de Saux et Picart et Exercice III.2 du Cours de calcul formel de Saux et Picart)

1. Lemme : Soit $a, b \in A^*$ et r le reste de la division euclidienne de a par b, alors $a \wedge b = 0$ si $r = 0$ et $a \wedge b = b \wedge r$ sinon

2. Théorème : Algorithme d'Euclide : Soit $a, b \in A^*$, alors on considère les divisions euclidiennes de r_i par r_{i+1} avec r_i les restes successifs de cette algorithme en commençant par $r_0 = b$, ainsi il existe un plus petit $p \in \mathbb{N}^*$ tel que $r_p = 0$, d'où r_{p-1} est un PGCD de a et b
3. Exemple : Dans l'anneau des entiers de Gauss euclidien $\mathbb{Z}[i]$, on obtient $(4+7i) \wedge (8-i) = 1 - 2i$
4. Corollaire : Algorithme d'Euclide étendu pour une relation de Bézout : Par récurrence on a construite $u_k, v_k \in A$ tels que $r_k = au_k + bv_k$, donc on obtient une identité de Bézout $r_{p-1} = au_{p-1} + bv_{p-1}$
5. Exemple : Par l'algorithme d'Euclide étendu on obtient que 120 et 23 sont premiers entre eux avec comme relation de Bézout $1 = -9 \times 120 + 47 \times 23$
6. Proposition : Soit $a, b \in \mathbb{Z}$, alors le nombre n de divisions euclidiennes à réaliser pour déterminer $a \wedge b$ vérifie $n \leq 2Ent(log_2(a)) + 1$
7. Théorème : Calcul binaire de PGCD d'entiers : Soit $a, b \in \mathbb{N}^*$, alors $f(a, b)$ définie en annexe vérifie $f(a, b) = a \wedge b$

3 Utilisations des PGCD et PPCM dans l'anneau $\mathbb{Z}$

3.1 Equations diophantiennes

(Chapitres 4.3 de Théorie des nombres de Daniel Duverney et Exercice 4.39 de Oraux X-ENS Algèbre 1)

1. Lemme : Soit $a, b, c \in \mathbb{Z}$, soit $d = PGCD(a, b)$, alors si d ne divise pas c alors $ax+by = c$ n'a pas de solutions dans $\mathbb{Z}^2$, sinon, en notant $a = da', b = db', c = dc'$, alors résoudre $ax + by = c$ revient à résoudre $a'x + b'y = c'$
2. Théorème : Soit $a, b, c \in \mathbb{Z}$, alors $ax+by = c$ d'inconnue $(x, y) \in \mathbb{Z}^2$ admet une solution si et seulement si $d = PGCD(a, b)$ divise c
3. Exemple : Les solutions de $37x+13y = 5$ sont de la forme $(x, y) = (30+13k, -85-37k)$
4. Lemme : Soit p un nombre premier impair tel que $q = 2p + 1$ (appelé nombre premier de Sophie Germain) et $x, y, z \in \mathbb{Z}$ tel que $x^p + y^p + z^p = 0$ mais xyz différent de 0 modulo p, alors on peut supposer x, y, z premiers entre eux et même premiers entre eux deux à deux
5. Théorème de Sophie-Germain : Soit p nombre premier de Sophie Germain, alors il n'existe pas de $x, y, z \in \mathbb{Z}$ tel que $x^p + y^p + z^p = 0$ et xyz différent de 0 modulo p

3.2 Système de congruence

(Chapitre 8.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Lemme : Soit $a_1, ..., a_r$ éléments deux à deux premiers entre eux dans $\mathbb{Z}$ et pour tout k dans $[\![1, r]\!], b_k := \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$ alors les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble

2. Théorème des restes chinois : Avec les notations du lemme précédent, en notant de plus $a := \prod_{k=1}^{r} a_k$ et les surjections canoniques $\pi : A \longrightarrow \mathbb{Z}/(a)$ et $\pi_k : \mathbb{Z} \longrightarrow \mathbb{Z}/(a_k)$ pour $k \in [\![1, r]\!]$, l'application $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/(a_1) \times ... \times \mathbb{Z}/(a_r) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ est un morphisme d'anneaux surjectif, en particulier φ induit un isomorphisme d'anneaux $\overline{\varphi} : \begin{array}{ccc} \mathbb{Z}/(a) & \longrightarrow & \mathbb{Z}/(a_1) \times ... \times \mathbb{Z}/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ d'inverse $\overline{\varphi}^{-1} : \begin{array}{ccc} \mathbb{Z}/(a_1) \times ... \times \mathbb{Z}/(a_r) & \longrightarrow & \mathbb{Z}/(a) \\ (\pi_1(x_1), ..., \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{k=1}^{r} x_k u_k b_k\right) \end{array}$ avec $(u_1, ..., u_r) \in \mathbb{Z}^r$ tel que $1 = \sum_{k=1}^{r} u_k b_k$
3. Application : On considère le système de congruences $\left\{ \begin{array}{rcl} x & \equiv & a[n] \\ x & \equiv & b[m] \end{array} \right.$ d'inconnue $x \in \mathbb{Z}$ et de paramètres $(a, b, n, m) \in \mathbb{Z}^4$ avec n et m premiers entre eux, alors il existe une solution $x \in \mathbb{Z}$ (unique modulo nm) de ce système
4. Exemple : Le système $\left\{ \begin{array}{rcl} x & \equiv & 2[4] \\ x & \equiv & 3[5] \\ x & \equiv & 1[9] \end{array} \right.$ a pour ensemble de solutions $\{838 + 180k, k \in \mathbb{Z}\}$ car on a la relation de Bézout entre 4,5 et 9 : $1 = 1 \times 5 \times 9 + 11 \times 4 \times 9 - 22 \times 4 \times 5$

3.3 Exposant d'un groupe fini

(Chapitres 1.5 et 1.9 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 0.3.2 et I.2.5 de Eléments d'analyse et d'algèbre de Pierre Colmez)

On considère G un groupe fini.

1. Définition : L'exposant de G est l'entier $N(G) = PPCM(o(g), g \in G)$
2. Exemple : Si $G = \mathbb{Z}/4\mathbb{Z}$ alors $N(G) = 2$
3. Définition : Un caractère de G est un morphisme de groupe de G dans $\mathbb{C}^*$, et on note $\hat{G}$ l'ensemble des caractères sur G
4. Exemple : Le morphisme $g \in G \longmapsto 1 \in \mathbb{C}^*$ est la caractère trivial
5. Proposition : Soit H sous-groupe de G et χ caractère de H, alors χ peut se prolonger en un caractère sur G
6. Lemme : $\hat{G}$ est un groupe et G et $\hat{\hat{G}}$ sont isomorphismes
7. Proposition : G et $\hat{G}$ ont le même exposant
8. Théorème : Il existe $g \in G$ d'ordre $N(G)$
9. Théorème de structure des groupes abéliens finis : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ...\mathbb{Z}/d_r\mathbb{Z}$ avec $d_{i+1} \mid d_i$