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

Développements :

Algorithme de Berlekamp, Décodage des codes BCH.

Bibliographie :

Naudin et Quité, Perrin, Rombaldi, Demazure, Combes, Papini.

Rapport du jury :

Il est bien clair que le champ d'étude ne peut se limiter au cas de Z ; il s'agit de définir et manipuler les notions de PGCD et PPCM dans un anneau factoriel et comme générateurs de sommes/intersections d'idéaux dans un anneau principal. Le candidat devra prendre soin de différencier le cadre théorique des anneaux factoriels ou principaux dans lequel sont définis les objets et dans lequel s'appliquent les énoncés des théorèmes proposés et le cadre euclidien fournissant les algorithmes. Bien sûr, la leçon peut opportunément s'illustrer d'exemples élémentaires d'anneaux euclidiens, comme Z et $K[X]$. La leçon doit accorder une part substantielle à la présentation d'algorithmes : algorithme d'Euclide, algorithme binaire, algorithme d'Euclide étendu. Dans le cas des polynômes, on étudiera l'évolution de la suite des degrés et des restes. Il est important de savoir évaluer le nombre d'étapes de ces algorithmes dans les pires cas et on pourra faire le lien avec les suites de Fibonacci. La leçon abordera des applications élémentaires : calcul de relations de Bézout, résolutions d'équations diophantiennes linéaires, inversion modulo un entier ou un polynôme, calculs d'inverses dans les corps de ruptures, 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 pourra évoquer le rôle de algorithme d'Euclide étendu dans de nombreux algorithmes classique en arithmétique (factorisation d'entiers, de polynômes, etc). Décrire l'approche matricielle de l'algorithme d'Euclide et l'action de $SL2(Z)$ sur $\mathbb{Z}^2$ est tout à fait pertinent. On pourra établir l'existence d'un supplémentaire d'une droite dans Z^2, ou d'un hyperplan de Z^n, la possibilité de compléter un vecteur de Z^n en une base. La leçon peut amener à étudier les matrices à coefficients dans un anneau principal ou euclidien, la forme normale d'Hermite et son application à la résolution d'un système d'équations diophantiennes linéaires. 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 candidats familiers de ces notions, à décrire le calcul de PGCD dans $Z[X]$ et $K[X,Y]$, avec des applications à l'élimination de variables. On pourra 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.

Remarque 1. *Cadre : Les anneaux sont supposés intègres.*

1 Autour du PGCD et du PPCM

1.1 Divisibilité et éléments irréductibles

Définition 2 (Perrin p45). *[Naudin Q p109] Eléments inversibles.*

Définition 3 (Naudin p109). $a|b$.

Proposition 4 (Perrin p46). $b|a$ *si et seulement si* $(a) \subset (b)$.

Définition 5 (Perrin p46). *Eléments associés.*

Définition 6 (Naudin p109). *Elément irréductible.*

Exemple 7. *Dans un corps, pas d'éléments irréductibles. Dans* $\mathbb{C}[X]$, *les polynômes de degré* 1.

Définition 8 (Romb p207). *Elément premier (?).*

Proposition 9 (Romb p207). *Premier implique irréductible.*

Contre exemple 10 (Rombaldi). 2 *dans* $\mathbb{Z}[i\sqrt{n}]$.

1.2 Définitions et propriétés du PGCD et du PPCM

Définition 11 (Romb p237). *pgcd.*

Contre exemple 12 (Naudin p114). *[Perrin p61] Dans* $\mathbb{Z}[\sqrt{-5}]$, 6 *et* $2+2\sqrt{-5}$ *n'admettent pas de pgcd.*

Proposition 13 (Romb p237). *Associativité du pgcd. (se placer dans un anneau à pgcd)*

Définition 14 (Romb p240). *ppcm.*

Contre exemple 15 (Perrin p61). 3 *et* $2+i\sqrt{5}$ *dans* $\mathbb{Z}[\sqrt{-5}]$ *n'ont pas de ppcm.*

Proposition 16 (Romb p240). *Associativité du ppcm.*

Proposition 17 (Ulmer...). *c est un ppcm de a et b si et seulement si $(a) \cap (b) = (c)$. Donc (a) et (b) admettent un ppcm si et seulement si $(a) \cap (b)$ est principal.*

Proposition 18 (Ulmer ...). *Existence du pgcd.*

Proposition 19 (Naudin p116). *Relation de Bezout : Si $(d) = (a) + (b)$ alors d est un pgcd de a et b.*

Définition 20 (Romb p239). *Eléments étrangers (Naudin p113).*

Proposition 21 (Romb p239). *$d = pgcd(a_1, .., a_r)$ si et seulement si $1 = pgcd(b_1, .., b_r)$ où $a_i = db_i$.*

Théorème 22 (Romb p239). *Théorème de Gauss.*

Proposition 23 (Romb p240). *Deux éléments admettent un pgcd si et seulement si ils admettent un ppcm et on a $ab = pgcd(a, b)ppcm(a, b)$.*

2 Expression du pgcd et du ppcm dans certains anneaux

2.1 Anneaux factoriels

Définition 24. *Anneau factoriel. (Produit d'irréductibles ou système de représentants ?)*

Exemple 25. *$\mathbb{Z}$, $K[X]$ et systèmes de représentants.*

Théorème 26 (Romb p217). *A est factoriel si et seulement si il est intègre, toute suite croissante d'idéaux principaux est stationnaire et tout élément irréductible de A est premier.*

Exemple 27 (Romb p219). *Les anneaux $\mathbb{Z}[i\sqrt{n}]$ ne sont pas factoriels pour $n \geq 3$ puisque 2 y est irréductible non premier.*

Proposition 28 (Romb p238). *[Perrin p48] Toute famille d'éléments d'un anneau factoriel admet un pgcd et un ppcm. Les donner.*

2.2 Anneaux principaux et relation de Bezout

Définition 29. *Anneau principal.*

Proposition 30 (Perrin p49). *Un anneau principal est factoriel.*

Proposition 31 (Romb p237, 242). *Dans un anneau principal, il existe δ non nul tel que $(a, b) = (a) + (b) = (\delta)$ et $\delta = au + vb$ où $u, v \in A$ et δ est un pgcd de a et b. C'est la relation de Bezout.*
Il existe m non nul tel que $(a) \cup (b) = (m)$ et m est un ppcm de a et b.

Proposition 32 (Romb p241). *Deux éléments a et b sont premiers entre eux si et seulement si il existe u, v tels que $au + bv = 1$.*

Contre exemple 33 (Perrin p49). *Le théorème de Bezout tombe en défaut dans un anneau factoriel non principal. $k[X, Y]$ est factoriel et X et Y sont premiers entre eux mais $(X) + (Y) = (X, Y) \neq 1$.*

Application 34 (Romb p241). *Dans un anneau principal, si c est premier avec a alors $pgcd(a, b) = pgcd(a, bc)$.*

Application 35 (Romb p241). *Dans un anneau principal, si c est premier avec chacun des a_i alors il est premier avec leur produit. (Faux dans un anneau factoriel ?)*

Proposition 36 (Romb p242). *Si les a_i dans un anneau principal sont premiers entre eux deux à deux alors $ppcm(a_1, .., a_n) = \prod a_i$.*

Remarque 37 (Naudin p131). *L'égalité $(a) + (b) = (d)$ assure donc l'existence d'un pgcd sans toutefois fournir de moyen de calcul de ce pgcd. La différence notoire entre anneaux principal et euclidien réside dans la calculabilité des objets. Il faut tout de même noter qu'il existe des anneaux principaux non euclidiens pour lesquels on dispose d'algorithmes de calcul du pgcd et même des coefficients de Bezout. (Certains anneaux d'entiers de corps quadratiques)*

Exemple 38. *$(2, X)$ non principal dans $\mathbb{Z}[X]$ et $pgcd(2, X) = 1$.*

3 Anneaux euclidiens et point de vue effectif

3.1 Anneaux euclidiens

Définition 39 (Romb p257). *Anneau euclidien.*

Exemple 40 (Rmb p262). *$\mathbb{Z}$ est euclidien pour $||$.*
L'anneau $\mathbb{Z}[i]$ est euclidien pour la norme.
L'anneau $K[X]$ est euclidien pour le degré.

Proposition 41 (Romb p257). *Un anneau euclidien est principal.*

Contre exemple 42. *$\mathbb{Z}[(1 + i\sqrt{19})/2]$ est principal non euclidien.*

3.2 Algorithme d'Euclide

Proposition 43 (Romb p260). *En notant r le reste de la division euclidienne de a par b, on a $pgcd(a, b) = b$ si $r = 0$, $pgcd(b, r)$ sinon.*

Proposition 44 (Romb p261). *Algorithme d'Euclide : le pgcd est le dernier reste non nul la suite finie de divisions euclidiennes. (Penser à échanger a et b si on n'est pas dans le bon ordre.)*

Définition 45 (Demazure p38). *[Naudin p133] Suite de Fibonacci.*

Proposition 46 (Naudin p133). *[Demazure p38][Cohen p13] Coût de l'algorithme.*

Proposition 47 (Demazure p36). *Algorithme d'Euclide binaire.*

Proposition 48 (Demazure p37). *Coût de l'algorithme binaire.*

3.3 Algorithme d'Euclide étendu

Remarque 49 (Naudin p142). *Calculer les coefficients de Bezout.*

Proposition 50 (Naudin p142). *Soient* $(r_i), (u_i), (v_i)$ *définies pas*
$r_0 = a$, $r_1 = b$, $u_0 = 1$, $u_1 = 1$, $v_0 = 0$, $v_1 = 1$. *Pour tout* $i \geq 1$, *tant que* $r_i \neq 0$,
$r_{i+1} =$ *reste de* (r_i, r_{i-1}), $q_{i+1} =$ *quotient* (r_i, r_{i-1}), $u_{i+1} = u_{i-1} - q_{i+1}u_i$, $v_{i+1} = v_{i-1} - q_{i+1}v_i$.
Soit N *tel que* $r_N = 0$. *Alors*

1. $r_N = pgcd(a, b)$
2. $r_i = au_i + bv_i$
3. u_i *et* v_i *sont premiers entre eux.*

Remarque 51 (Demazure p43). *Dans le cas de* $K[X]$, *on a aussi* $deg(v_i) = deg(a) - deg(r_{i-1})$.

Exemple 52 (Naudin p144). $pgcd(1292, 798)$.

Remarque 53. *Complexité : la même que précédemment.*

4 Applications

4.1 Arithmétique et théorème de Bezout

Proposition 54 (Demazure p29). a *est inversible modulo* n *si et seulement si* a *et* n *sont premiers entre eux.*

Exemple 55 (Naudin p144). *Inverse de* 34 *dans* $\mathbb{Z}/235\mathbb{Z}$ *:* $1 = 11 \times 235 - 76 \times 34$ *donc l'inverse de* 34 *modulo* 235 *est donc* $-76 = 159$.

Exemple 56 (Naudin p144). *Dans* $\mathbb{Z}[i]$.

Exemple 57. *Inverse d'un polynôme.*

Application 58 (Combes p264). *Résoudre* $ax = bmod(n)$.

Application 59 (Combes p264). $ax + by = c$ *a des solutions si et seulement si* $pgcd(a, b)|c$.

Exemple 60 (Combes p264). *Résolution de* $522x + 2214y = 36$.

Proposition 61 (Romb p244). *Théorème chinois.*

Corollaire 62 (Ulmer...). *Le système de congruence admet une unique solution modulo* $x_1..x_n$.

Proposition 63 (Combes p249). *Méthode pour trouver une solution particulière.*

Proposition 64 (Saux Picart). *Méthode de Newton.*

Exemple 65 (Combes p249). *Exemple d'un système modulaire.*

Corollaire 66 (Ulmer...). *Interpolation de polynômes.*

4.2 Détermination des polynômes irréductibles sur un corps fini

Proposition 67 (Naudin p129). *Soit* $Q \in F_p[X]$ *de degré* n. *Alors* Q *est irréductible si et seulement si pour tout diviseur premier* q *de* n *on a* $Q|X^{p^n} - X$ *et* $pgcd(X^{p^{n/q}} - X, Q) = 1$.

Exemple 68 (Naudin p129). $X^{10} + X^3 + 1$ *est irréductible dans* $F_2[X]$. $X^5 + X^4 + X^3 + X^2 + X - 1$ *est réductible.*

Proposition 69. *Algorithme de Berlekamp.*

4.3 Codes BCH

Définition 70 (p105). *Un code linéaire de longueur* n *sur* K *et de dimension* k *est un sev de* K^n *de dimension* k.

Définition 71 (p105). *Le poids d'un élément est le nombre de ses composantes non nulles.*

Proposition 72 (p105). *La distance minimale d'un code linéaire est le poids minimal des mots non nuls du code.*

Définition 73 (p123). *Un code* C *est dit cyclique si* C *est un code linéaire et si* $(x_1, ..., x_n) \in C$ *alors* $(x_n, x_1, ...x_{n-1}) \in C$.

Définition 74 (p124). *On associe au code* C *l'ensemble* $C(X) = \{\overline{c_0 + c_1X + ... + c_{n-1}X^{n-1}}\} \in F_q[X]/(X^n - 1), (c_0, ..., c_{n-1}) \in C\}$.

Proposition 75 (p125). *Un code* C *est cyclique si et seulement si* $C(X)$ *est un idéal de* $F_q[X]/(X^n - 1)$.

Proposition 76 (p125). *Si* C *est un code cyclique, alors* $C(X)$ *est formé de tous les multiples d'un même polynôme unitaire qui divise* $X^n - 1$, *appelé polynôme générateur.*

Remarque 77 (p125). *Les codes BCH sont des codes cycliques particuliers qui permettent de prévoir la distance minimale avant la construction.*

Définition 78 (p136). *Soit $n \in \mathbb{N}^*$, soit q une puissance de p tel que n et q sont premiers entre eux.Soit m l'ordre de q modulo n et α une racine primitive n-ème de 1. Un code BCH sur F_q de longueur n de distance prescrite δ est un code cyclique dont le générateur est le ppcm des polynômes minimaux de $\alpha^r, \alpha^{r+1}, ...\alpha^{r+\delta-2}$ pour un entier r donné. Si $r = 1$, le code est dit BCH strict.*

Définition 79 (p158). *Soit C un code de longueur n sur F_q et $E \subset F_q^n$. Le code C corrige les erreurs de E si pour tout $y \in F_q^n$, $card\{(x, e) \in C \times E, y = c + e\} \leq 1$.*

Proposition 80 (p158). *C corrige les erreurs si et seulement si pour tout $y \in F_q^n$, la décomposition $y = x + e$ lorsqu'elle existe est unique.*

Définition 81 (p128). *Le code C détecte une erreur si le mot reçu n'appartient pas au code.*