Leçon 122 : Anneaux principaux. Applications.

Développements :

Décodage des codes BCH, Théorème des deux carrés.

Bibliographie :

Rombaldi, Escoffier, Perrin, Combes, Gourdon, OA, Papini.

Rapport du jury :

Cette leçon n'est pas uniquement théorique, Il est possible de présenter des exemples d'anneaux principaux classiques autres que Z et KrXs (décimaux, entiers de Gauss ou d'Eisenstein), accompagnés d'une description de leurs irréductibles. Les applications en algèbre linéaire ne manquent pas et doivent être mentionnées. Par exemple, les notions de polynôme minimal sont très naturelles parmi les applications. Les anneaux euclidiens représentent une classe d'anneaux principaux importante et l'algorithme d'Euclide a toute sa place dans cette leçon pour effectuer des calculs. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant à l'étude des réseaux, à des exemples d'anneaux non principaux, mais aussi à des exemples d'équations diophantiennes résolues à l'aide d'anneaux principaux. A ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. De même, le calcul effectif des facteurs invariants de matrices à coefficients dans certains anneaux peut être fait.

A désigne un anneau commutatif unitaire et intègre. K désigne un corps. $A^\times$ désigne l'ensemble des inversibles de A.

1 Notion de principalité

1.1 Idéaux et anneaux principaux

Définition 1 (Perrin p42). *Idéal principal.*

Exemple 2. *$n\mathbb{Z}$ est un idéal principal de $\mathbb{Z}$.*

Contre exemple 3 (Romb p252). *$(2, X)$ n'est pas principal dans $\mathbb{Z}[X]$.*

Définition 4 (Romb p229). *Anneau principal.*

Exemple 5 (Romb p229). *Un corps est un anneau principal.*

Proposition 6 (Romb p229). *$\mathbb{Z}$ est principal. Tous ses idéaux sont de la forme $n\mathbb{Z}$.*

Proposition 7 (Romb p231). *Tout sous-anneau du corps $\mathbb{Q}$ est principal. (Utilise Bezout mais sur $\mathbb{Z}$.)*

Exemple 8 (Romb p231). *L'anneau des nombres décimaux est principal.*

Proposition 9 (Romb p231). *Si A est principal alors $S^{-1}A$ est principal.*

Exemple 10 (Romb p231). *Avec $A = K[X]$ et $S = \{X^n, n \in \mathbb{N}\}$, l'anneau $D = \{\frac{P(X)}{X^n}, P \in K[X], n \in \mathbb{N}\}$ est principal.*

Proposition 11 (Romb p232). *Si un anneau est isomorphe à un anneau principal alors il est principal.*

Exemple 12 (Francinou Gianella p70). *$\mathbb{C}[X, Y]/(X - Y^2)$ est principal car isomorphe à $\mathbb{C}[X]$.*

1.2 Exemple des anneaux euclidiens

Définition 13 (Romb p257). *Anneau euclidien.*

Définition 14 (Romb p258). *Stathme croissant.*

Proposition 15 (Romb p258). *Tout anneau euclidien admet un stathme croissant.*

Proposition 16 (Romb p257). *Un anneau euclidien est principal.*

Exemple 17 (Romb p262). *$\mathbb{Z}$ est euclidien, tout corps est euclidien.*

Proposition 18 (Perrin p50). *Division euclidienne dans $A[X]$.*

Proposition 19 (Romb p372). *Si K est un corps, $K[X]$ est euclidien.*

Proposition 20 (Romb p236). *$A[X]$ est principal si et seulement si A est un corps.*

Application 21. *$K[X_1, , X_n]$ est un corps si et seulement si $n = 1$.*

Exemple 22 (Romb p236). *$K[X, Y] = K[X][Y]$ n'est pas principal car $K[X]$ n'est pas un corps.*

Application 23 (Rombp249). *$K[x, Y]/(Y - X^2)$ est principal.*

Application 24 (Romb p245). *Si $\alpha \in L$ est algébrique sur K alors il existe un unique polynôme unitaire $\mu \in K[X]$ tel que $\{P \in K[X], P(\alpha) = 0\} = (\mu)$ et ce polynôme est l'unique polynôme unitaire irréductible de $K[X]$ qui annule α.*

Proposition 25 (Romb p269). *$\mathbb{Z}[\frac{1 + i\sqrt{19}}{2}$ est principal mais pas euclidien.*

Proposition 26 (Perrin). $\mathbb{Z}[i]$ *l'anneau des entiers de Gauss est euclidien pour le module au carré.*

Proposition 27 (Romb p263). *L'anneau des nombres décimaux est euclidien.*

Proposition 28 (Romb p266). *Si* $n = 1$ *ou* $n = 2$, $\mathbb{Z}[i\sqrt{n}]$ *est euclidien .*

Proposition 29 (Romb p268). $\mathbb{Z}[w]$ *est un anneau si et seulement si* w *est un entier quadratique, ie une racine d'un polynçome de degré* 2 *unitaire à coefficients entiers et il existe un nombre complexe* $w' = x' + iy'$ *tel que* $x' \in [0, 1[, y' > 0$ *et* $\mathbb{Z}[w] = \mathbb{Z}[w']$ *et* $w' = i\sqrt{n}$ *ou* $w' = 1/2 + i\dfrac{\sqrt{4n-1}}{2}$ *avec* $n \in \mathbb{N}^*$.

Proposition 30 (Romb p269). *L'anneau des séries formelles est euclidien.*

2 Arithmétique dans les anneaux principaux

2.1 Divisibilité, éléments premiers et irréductibles

Définition 31 (Perrin p46). $a|b$.

Proposition 32 (Perrin p46). $a|b$ *si et seulement si* $(b) \subset (a)$.

Définition 33 (Romb p206). *Eléments associés.*

Proposition 34 (Perrin p 46). $(a) = (b)$ *si et seulement si* a *et* b *sont associés.*

Proposition 35 (Romb p206). *Les inversibles de* A *sont les éléments associés à* 1.

Exemple 36 (Romb p356). $K[X]^\times = K^*$. $\mathbb{Z}^\times = \{1, -1\}$, $A[X]* = A*$.

Définition 37 (Romb p206). $p \in A$ *irréductible,* p *premier.*

Définition 38 (Romb p215). *Idéal premier.*

Définition 39 (Romb p215). *Idéal maximal.*

Proposition 40 (Romb p207). *Premier implique irréductible.*

Proposition 41 (Romb p216). *Si* (p) *est maximal alors* p *est irréductible.*

Contre exemple 42. (XY) *n'est pas maximal mais* XY *est irréductible.*

Exemple 43. X *est premier et irréductible dans* $A[X]$ *avec* A *intègre.* X^2 *n'est ni premier, ni irréductible.*

Soit $A \subset K[X, Y]$ *le sous-anneau engendré par les monômes de degré pair. Alors* XY *est irréductible non premier.*

Proposition 44 (Perrin p46). *Si* A *n'est pas un corps,* p *irréductible si et seulement si* (p) *est maximal.*

Définition 45 (Romb p207). $p \in A$ *premier.*

Proposition 46 (Romb p216). p *est premier si et seulement si* (p) *est premier.*

Proposition 47 (Romb p235). *Dans un anneau principal, premier si et seulement si irréductible.*

Proposition 48 (Romb p235). *Dans un anneau principal,* (p) *premier si et seulement si* p *est premier si et seulement si* p *est irréductible si et seulement si* (p) *est maximal.*

Exemple 49 (Romb p235). $\mathbb{Z}[i\sqrt{n}]$ *n'est pas principal pour* $n \leq 3$ *puisque* 2 *est irréductible non premier. Donner les inversibles.*

Théorème 50 (Romb p258). *Si* A *est un anneau euclidien avec un stathme croissant alors* $A^\times = \{a \in A^*, \phi(a) = \phi(1)$.

Exemple 51 (Romb p263). *Inversibles de l'anneau des nombres décimaux.*

Proposition 52 (Romb p236). *Soit* A *un anneau principal. L'anneau* $A/(p)$ *est corps si et seulement si* p *est premier ou irréductible.*

Exemple 53 (Combes p251). *Construction de* $\mathbb{C}$ *ou construction des corps de rupture.*

2.2 PGCD, PPCM et relation de Bezout

Définition 54 (Romb p237, 240). *Admettre un pgcd, admettre un ppcm.*

Exemple 55 (Escoffier p463). *pgcd et ppcm n'existent pas toujours :* $\mathbb{Z}[i\sqrt{5}]$.

Remarque 56 (Romb p237). *Les pgcd sont associés.*

Définition 57 (Romb p237). *Anneau à pgcd.*

Proposition 58. *ppcm existe si et seulement si* $(a) \cap (b)$ *est principal.*

Définition 59 (Romb p237). *Un anneau principal est un anneau à pgcd et identité de Bezout.*

Définition 60 (Romb p239). *Eléments étrangers.*

Théorème 61 (Romb p239). *Théorème de Gauss.*

Théorème 62 (Romb p241). *Théorème de Bezout.*

Proposition 63 (Romb p261). *Algorithme d'Euclide étendu pour déterminer la relation de Bezout dans un anneau euclidien.*

Exemple 64 (Escofier p227).

Application 65 (Gourdon p175). *Lemme des noyaux.*

Exemple 66 (Escofier p232). *Calcul de l'inverse : 583 dans* $\mathbb{Z}/679\mathbb{Z}$.

Application 67. *Résolution des équations diophantiennes* $ax + by = c$.

2.3 Caractère factoriel d'un anneau principal

Définition 68 (Romb p217). *Anneau factoriel.*

Proposition 69 (Romb p219). *Dans un anneau factoriel,un élément est irréductible si et seulement si il est premier.*

Contre exemple 70 (Romb p218). $\mathbb{Z}[i\sqrt{5}]$ *non factoriel.*

Proposition 71 (Romb p219). *Un anneau principal est factoriel.*

Exemple 72. $\mathbb{Z}$, $K[X]$, $\mathbb{Z}/p\mathbb{Z}$ *sont factoriels.*

Contre exemple 73. $\mathbb{Z}[X]$.

Proposition 74 (Romb p238). *Expression du pgcd de deux éléments.*

Exemple 75. $P = (x-1)(X+1)^2$, $Q = (X-1)^3(X^2+7)$, *alors* $pgcd(P,Q) = X-1$.

Application 76. *Irréductibles de* $\mathbb{C}[X]$ *et* $\mathbb{R}[X]$.

Proposition 77 (FG ALG1). *Un anneau factoriel qui vérifie le théorème de Bezout est principal.*

Proposition 78. *Si A est factoriel alors* $A[X]$ *l'est.*

Contre exemple 79. $\mathbb{Z}[X]$ *factoriel non principal.*

2.4 Lemme chinois

Proposition 80 (FG ALG 1 p50). *[Romb p243] Soit A un anneau principal et* $a_1...a_n$ *des éléments de A premiers entre eux deux à duex. Alors* $A/(a_1..a_n) \simeq A/(a_1)...A/(a_n)$.

Exemple 81 (Combes p249). *Résolution d'un système de congruences.*

Application 82. $Aut(\mathbb{Z}/n\mathbb{Z}) = ...$

Application 83 (OA). *Algorithme de Berlekamp. Factoriser des polynômes à coefficients dans un corps et sans facteurs carrés*

Proposition 84 (Saux Picart calcul formel). *Algorithme de Newton.*

Définition 85. *Indicatrice d'Euler.*

3 Utilisation de la principalité

3.1 Algèbre linéaire

Application 86 (Gourdon p176). *[OA] Si* $f \in L(E)$, $\{P \in K[X], P(f) = 0\}$ *est un idéal de* $K[X]$ *donc engendré par P appelé polynôme minimal de f.*

Application 87. *Si* $f \in L(E), x \in E$, $\{P \in K[X], P(f)(x) = 0\}$ *est un idéal de* $K[X]$ *donc engendré par* P_x *appelé polynôme minimal de f en x.*

Proposition 88. *Il existe* $x \in E$ *tel que* $\pi_u = \pi_{u,x}$.

Application 89. *Invariants de similitude.*

3.2 Entiers de Gauss et équations diophantiennes

Proposition 90. *Inversibles de* $\mathbb{Z}[i]$.

Proposition 91. $p \in \Sigma$ *si et seulement si p n'est pas réductible dans* $\mathbb{Z}[i]$.

Proposition 92. *Un nombre premier est somme de deux carrés si et seulement si il est égal à 2 pi est congru)* 1 *modulo* 4.

Théorème 93 (Romb p266). *Un entier n est somme de deux carrés si et seulement si les éventuels diviseurs premiers de n congrus à* 3 *mod* 4 *qui apparaissent dans sa décomposition en facteurs premiers ont un exposant pair.*

Proposition 94. *Les irréductibles de* $\mathbb{Z}[i]$ *sont les p premiers tels que* $p = 2, 3mod4$ *et les* $a + ib$ *tels que* $a^2 + b^2$ *est premier.*

L'équation diophantienne $x^2 + y^2 = n$ *admet des solutions si et seulement si pour tout p premier tel que* $p = 3mod4$, $v_p(n)$ *est pair.*

Exemple 95. $x^2 + 2y^2 = 49$, *seule solution* $(7, 0)$ *car* 7 *est irréductible dans* $\mathbb{Z}[i\sqrt{2}]$.

3.3 Codes correcteurs cycliques

Remarque 96. *—OA p190] But : Détecter voire corriger les erreurs dues au canal de transmission.*

Définition 97 (OA p191). *Code correcteur linéaire. Code correcteur cyclique.*

Définition 98 (OA p192). *Distance de Hamming. Distance minimale.*

Proposition 99. *Un code linéaire de distance minimale d peut détecter jusqu'à* $d-1$ *erreurs et corriger jusqu'à* $E((d-1)/2)$.

Théorème 100 (OA p192). *Borne de singleton.*

Proposition 101 (OA p194). *Les codes cycliques sont les idéaux de l'anneau* $F_q[X]/(X^n - 1)$.

Proposition 102 (OA p194). $F_q[X]$ *étant principal, se donner un code cyclique de longueur n revient à se donner un polynçome unitaire P divisant* $X^n - 1$. *Ce polynôme est appelé polynôme générateur du code.*

Application 103 (OA p194). *Construction et décodage des codes BCH.*

Remarque 104. *Mieux construit dans Papini.*

3.4 Extensions de corps

Polynôme minimal, éléments transcendants, algébriques et exemples.