Leçon 123 : Corps finis. Applications.

Développements :

Algorithme de Berlekamp, Polynômes irréductibles sur F_q.

Bibliographie :

Gozard, Escofier, Rombaldi, Tauvel (corps commutatifs et théorie de Galois), Perrin, Ortiz, Papini, Berhuy, OA, Gourdon, Zavidovic,

Rapport du jury :

Une construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Les injections des divers Fq doivent être connues et les applications des corps finis (y compris pour Fq avec q non premier !) ne doivent pas être oubliées : citons par exemple l'étude de polynômes à coefficients entiers et de leur irréductibilité. Le calcul des degrés des extensions et le théorème de la base téléscopique sont incontournables. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont envisageables. S'ils le désirent, les candidats peuvent aller plus loin en détaillant des codes correcteurs.

Intro

Les corps finis ayant la propriété d'être constructibles de façon effective, ils sont très utilisés en cryptographie et pour les codes correcteurs d'erreurs.

1 Existence et construction des corps finis

1.1 Caractéristique et sous-corps premiers

Définition 1. *On appelle corps fini un corps ayant un nombre fini d'éléments.*

Proposition 2 (Gozard p3)**.** *$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

Exemple 3 (Escofier p554)**.** *$F_p[X]/(f)$ où f est irréductible est un corps de cardinal p^d.*

Remarque 4 (Gozard p3)**.** *[Romb p415] Pour p premier, on note $\mathbb{Z}/p\mathbb{Z}$, F_p.*

Définition 5 (Romb p415)**.** *Caractéristique d'un corps.*

Proposition 6 (Romb p415)**.** *La caractéristique d'un corps fini est un nombre premier.*

Définition 7 (Perrin p72)**.** *[Romb p416] Sous-corps premier.*

Proposition 8 (Tauvel CM p7)**.** *Si K est un corps fini de caractéristique p alors sont sous-corps premier est isomorphe à F_p.*
(K est une F_p algèbre de dimension finie en tant que F_p-ev.)

Remarque 9. *On identifiera le sous-corps premier avec F_p.*

Proposition 10 (Tauvel CM p8)**.** *Soit K un corps fini de card q. Alors il existe p premier et $n \in \mathbb{N}$ tels que $q = p^n$ et si q est premier alors K est isomorphe à F_q.*

Remarque 11. *Il n'existe pas de corps fini de cardinal* 6 *ou* 105*.*

Définition 12 (Romb p416)**.** *[Gozard p85] Morphisme de Frobenius. C'est un F_p morphisme de corps qui fixe F_p. C'est un automorphisme si K fini, (Perrin p73), c'est l'identité sur un corps premier.*

Application 13 (Gozard p85)**.** *Dans un corps fini de caractéristique p, chaque élément admet exactement une racine p-ième.*

Application 14 (Gozard p85)**.** *Petit théorème de Fermat.*

1.2 Existence des corps finis

Proposition 15 (Gozard p86)**.** *Il existe un unique corps de cardinal q, à isomorphisme près.*

Remarque 16. *On peut le réaliser comme le corps de décomposition du polynôme $X^q - X$ sur F_p. Ou (Hindry p4], Les éléments de F_q sont les racines du polynôme $X^q - X \in F_p[X]$.*

Application 17 (Gozard p86)**.** *Théorème de Wilson.*

rema[Annette Paugam p174] Une particularité des corps finis est que l'on peut trouver un facteur irréductible P de $X^q - X$ dont le corps de rupture $K = F_p[X]/(P)$ est un corps de décomposition de tous les facteurs irréductibles de $X^q - X$. rema

Proposition 18. *Si F et F' sont deux corps à q éléments ils sont F_p-isomorphes.*

1.3 Construction des corps finis

Proposition 19 (Perrin p74)**.** *F_q^* est un groupe cyclique de cardinal $q - 1$.*

Exemple 20 (Ortiz)**.**

Définition 21 (Papini p69). *Un générateur de K^* est appelé racine primitive de K.*

Corollaire 22 (Elément primitif, Papini p69). *[Papini p69] Si α est un générateur de F_q^* alors $F_q = F_p(\alpha)$.*

Corollaire 23 (Papini p74). *Il existe un polynôme irréductible de degré n sur F_p : le polynôme minimal de α sur F_p.*

Remarque 24. *On peut avoir $F_q = F_p(\alpha)$ sans que α soit générateur de F_q^*.*

Exemple 25 (Escofier p558). *$F_2[X]/(X^4+X^3+X^2+X+1) = F_2[\overline{X}]$ et $\overline{X}$ est d'ordre 5.*

Proposition 26 (Papini p74). *Tout corps fini de cardinal p^n est isomorphe à $F_p[X]/(P)$ où P est un polynôme irréductible de degré n sur F_p.*

Exemple 27 (Rombaldi p438). *F_8, F_16.*

Exemple 28 (Papini). *F_9.*

Exemple 29 (Berhuy p659). *Exemple d'isomorphismes.*

2 Structure et clôture algébrique

2.1 Sous-corps

Théorème 30 (Romb p417). *Tout sous-corps de F_p^n est de cardinal p^d où $d|n$. Réciproquement, pour tout diviseur d de n, il existe un unique sous-corps de F_{p^n} de cardinal p^d à savoir le corps $\{x \in F_{p^n}, x^{p^d} = x\}$.*

Proposition 31 (Gozard p92). *F_{p^n} est un sous corps de F_{p^m} si et seulement si $n|m$.*

Exemple 32. *Treillis d'extension de F_2.*

Proposition 33. *Théorème de la base télescopique.*

2.2 Automorphismes

Théorème 34 (Romb p426). *[Dema p212] Le groupe $Aut(F_{p^n})$ est cyclique d'ordre n engendré par l'automorphisme de Frobenius.*

Corollaire 35. *$Aut(F_{p^n}) \simeq \mathbb{Z}/n\mathbb{Z}$.*

2.3 Clôture algébrique sur les corps finis

Définition 36 (Gozard p62). *Un corps K est algébriquement clos si tout polynôme non constant admet une racine dans K.*

Proposition 37 (Gozard p62). *Un corps fini n'est pas algébriquement clos. (F_{p^n} n'est pas algébriquement clos car $X^{p^n} - X + 1$ n'a pas de racines dans F_{p^n}.*

Proposition 38 (Gozard p92). *La clôture algébrique de F_{p^n} est $\cup_{i\in\mathbb{N}} F_{p^{i!}}$.*

3 Polynômes irréductibles sur $F_q[X]$ et sur $Z[X]$

3.1 Polynômes irréductibles sur F_q

Proposition 39 (Gozard p88). *Décomposition de $X^{p^n} - X$ en fonction des irréductibles.*

Proposition 40 (Gozard p87). *Si $P \in F_p[X]$ est irréductible, son corps de rupture est aussi son corps de décomposition.*

Exemple 41. *F_4.*

Proposition 42. *$p^n = \sum dI(p,d)$.*

Exemple 43 (Gozard). *Calculs de $I(p,2)$, $I(p,3)$.*

Proposition 44 (Gozard). *$I(p,d)$ par inversion de Mobius.*

Proposition 45 (Perrin p78). *P est irréductible sur K si et seulement si P n'a pas de racines dans les extensions L de K telles que $[L:K] \leq n/2$.*

Exemple 46 (Beruy).

Proposition 47 (Perrin p79). *Conservation de l'irréductibilité par extension de corps.*

Proposition 48 (Berhuy p659). *f est irréductible si et seulement si f divise $X^{p^n} - X$ et si $pgcd(f, X^{p^d} - X) = 1$.*

3.2 Factorisation de polynômes

Proposition 49 (OA). *Algorithme de Berlekamp.*

Remarque 50. *Cas où P n'est pas sans facteurs carrés.*

Exemple 51 (Escofier).

3.3 Critères d'irréductibilités sur $Z[X]$

Proposition 52 (Gourdon). *Critère d'Eisenstein sur Q.*

Application 53. *Il existe des polynômes irréductibles de tout degré sur Z ($X^n - p$).*

Exemple 54 (Gourdon). *$X^n + ... + 1$*

Proposition 55 (Perrin p77). *Soit $P \in \mathbb{Z}[X]$ et p un nombre premier ne divisant pas le coefficient dominant de P. Si $\overline{P}$ est irréductible dans $F_p[X]$ alors P est irréductible dans $\mathbb{Z}[X]$.*

Exemple 56 (Perrin p77). *$X^p + X + 1$.*

Contre exemple 57 (Perrin p78). *$X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur F_p pour tout premier p.*

Application 58. *Irréductibilité des polynômes cyclotomiques.*

Application 59. *Progression de Dirichlet.*

4 Arithmétique et corps finis

4.1 Résidus quadratiques

Définition 60 (Perrin p74). F_q^2, F_q^{*2}.

Proposition 61 (Perrin p74). *Pour $p = 2$, $F_q^2 = F_q$.*
Sinon, cardinaux.

Proposition 62 (Perrin p75). $x \in F_q^{*2} sietseulementsix^{(p-1)/2} = 1$.

Théorème 63 (Romb p428). *1. Nombre de carrés et de non carrés.*

2. *Les carrés de F_q^* sont les racines de $X^{(q-1)/2} - 1$ et les non carrés sont les racines de $X^{(q-1)/2} + 1$.*

Corollaire 64 (Romb p428). *1. -1 est un carré dans F_q^* si et seulement si q est congru à 1 modulo 4.*

2. *Le produit de deux carrés ou de deux non carrés est un carré. Le produit d'un carré et d'un non carré est un non carré.*
3. *Pour tout $a, b \in F_q^*$ et tout $c \in F_q$, il existe $x, y \in F_q$ tels que $c = ax^2 + by^2$.*

Application 65 (Perrin p76). *Il existe une infinité de nombres premiers de la forme $4m + 1$.*

Application 66. *Le théorème des deux carrés.*

Définition 67 (Romb p429). *[Gozard p155] Symbole de Legendre.*

Proposition 68. *Le symbole de Legendre est une fonction multiplicative.*

Proposition 69. $(\frac{x}{p}) = x^{\frac{p-1}{2}}$.

Exemple 70 (Gozard p155). $(\frac{-1}{p}), (\frac{2}{p})$

Théorème 71. *Loi de réciprocité quadratique.*

Remarque 72. *La loi de réciprocité quadratique, les symboles pour -1 et 2 et la division euclidienne, permettent de calculer les symboles de Legendre.*

Exemple 73 (Gozard p156). $(\frac{23}{59} = -1$.

Corollaire 74. *L'équation $x^2 + 59y = 23$ n'a pas de solutions.*

Application 75 (Escofier p569). *Résolution d'une équation.*

4.2 Système d'équations

Théorème 76 (Zavi). *Chevalley-Warning.*

Application 77. *Zéros de formes quadratiques.*

Application 78 (Zavi). *EGZ.*

5 Codes correcteurs

5.1 Codes cycliques

Définition 79 (p105). *Un code linéaire de longueur n sur K et de dimension k est un sev de K^n de dimension k.*

Définition 80 (p105). *Le poids d'un élément est le nombre de ses composantes non nulles.*

Proposition 81 (p105). *La distance minimale d'un code linéaire est le poids minimal des mots non nuls du code.*

Définition 82 (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 83 (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 84 (p125). *Un code C est cyclique si et seulement si $C(X)$ est un idéal de $F_q[X]/(X^n - 1)$.*

Proposition 85 (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 86 (p126). *La connaissance de tous les diviseurs de $X^n - 1$ permet de trouver tous les codes cycliques de longueur n. Ces diviseurs sont les diviseurs irréductibles de $X^n - 1$ sur F_q.*

5.2 Construction des codes BCH

Remarque 87 (p125). *Les codes BCH sont des codes cycliques particuliers qui permettent de prévoir la distance minimale avant la construction.*

Définition 88 (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 89 (Papini p136). *Codes BCH.*

Théorème 90 (Papini p135). *Théorème des codes BCH (poids minimum d'un code).*

Remarque 91. *On pourra donc corriger t erreurs avec un code BCH de distance prescrite $2t + 1$.*