112 - Corps finis. Applications.

Prérequis : caractéristique d'un anneau, extension de corps. Si K/k est une extension de corps, alors k est un k-ev (même une k-algèbre. En effet, si i est l'injection de k dans K, on définit l.x comme i(l)*x). On admet le théorème de Steinitz qui garantit l'existence d'une clôture algébrique pour tout corps.

I) Construction des corps finis [Goz]

1) Sous corps premier [Goz 7]

Déf : un corps est dit premier si il n'admet pas d'autre sous corps que lui-même.

Ex : Q est premier (tout sous corps de Q contient 1 donc Q entier)

Prop : Z/pZ est un corps premier. On note Fp ce corps (en effet un sous corps est en particulier un sg additif)

Déf : soit K un corps. Le sous corps premier de K est le corps engendré par 1.

Prop : K un corps, P sous sous corps premier. Alors la caractéristique de P est soit 0, et P est isomph à Q, soit un nombre premier p, et P est isomorphe à Fp *(rappel : la caractéristique est 0 ou p car Z/carac(K)Z est isomorphe à Im(f)⊂K donc est intègre, donc carac(K)=0 ou p. Par ce mph caractéristique, on peut injecter Z/pZ=Fp dans K, c'est donc le sous corps premier. Si la caract est 0, on prolonge le mph caracté sur Q en f(z/d)=(z.1)(d.1)^-1. Ce prolongement est injectif car non trivial (mph de corps) donc c'est bon, Q s'injecte dans K)*

Prop : p premier. Tout corps fini de cardinal p est isomorphe à Fp *(car il est de caract p, donc contient Fp, donc égal)*

2) Propriétés des corps finis [Goz]

Prop : soit K un corps fini. Alors sa caractéristique est un nb premier p, et il existe n tq #K=p^n *(si on avait caract=0, il contiendrait Q, or il est fini. Don caract=p. Son sous corps est donc isomph à Fp. K est donc un Fp espace vectoriel. Comme il est de dimension fini, K est isomorphe à Fp^n en tant qu'ev, donc #K=p^n)*

Rq : la réciproque est fausse. Fp(X) est infini de caractéristique p.

Th (Wedderburn) : tout corps fini est commutatif

Th : K un corps commutatif. Tout sg fini de K* est cyclique

Cor : K un corps fini. Alors K* est cyclique

3) Existence et unicité d'un corps de cardinal p^n [Goz]

Déf : automph de Frobenius

Th : p un nb premier, n entier non nul. On note q=p^n. Il existe un corps à q éléments, et c'est le corps de décomposition de X^q-X. Il est unique à isomph près. On note ce corps F_p^n=F_q *(soit K le corps de décomposition de X^q-X. Soit k l'ensemble des racines dans K. L'application g:t→t^q de k dans K est le Frobenius itéré n fois, c'est donc un automph de K. k est l'ensemble des invariants de ce mph, donc un sous corps de K. Donc k contient Fp. X^q-X est premier avec sa dérivée donc il a q racines, donc k est un corps à q élements. On a donc k=K=corps de décomp du poly. Unicité : K un corps à q élément. Carac K divise q donc c'est p. K* a q-1 éléments donc pour tout x de K, x^q=x. Or X^q-X a au plus q racines, donc K est bien son corps de décomposition)*

4) Sous corps d'un corps fini

Prop : K sous corps de Fq => il existe d diviseur de n tq #K=p^d. Réciproquement, pour tout diviseur d de n, il existe un unique sous corps de cardinal p^d *(Fq est un K-ev donc Fq est isomorphe à K^e qui est isomorphe à Fp^n. Pour l'existence, on regarde le corps de décomp de X^p^d-X)*

Exemple : les sous corps de F64=F2^6 sont F2, F4, F8, F64. F16 n'est pas un sous corps de F64.

5) Clôture algébrique d'un corps fini [Goz]

Th : la clôture alg de Fp est $\bigcup F_{p^i} = \bigcup F_{p^{i!}}$ *(on montre la 2e égalité. Un sens trivial et pour l'autre, i divise i! donc Fp^i⊂Fp^i!. Montrons la première égalité. On mq que l'union est bien un corps. Soit P un polynôme à coeff dans l'union. P a un nb fini de coeff, chacun étant dans un des Fp^i, donc P est entier dans un Fp^n. Soit f un facteur irred de P. En quotientant, on a un corps de rupture plus grand, et il reste dans l'union, donc elle est algébriquement close. Est-ce que l'union est une extension algébrique ? Si on prend x dans C, il est dans un Fq donc c'est bon)*

II) Polynômes sur corps finis [Goz] + [FG]

1) Polynômes irréductibles [Goz] + [FG]

Exemples

Prop : Fq=Fp/(P) où P est un polynôme de degré n irred sur Fp *(un sens OK. L'autre : soit x un générateur de Fq*. Alors Fq=Fp(x). P le poly minimal de x sur Fp. Fp[X]/(P)=Fp(x) donc le degré de P est n)*

Cor : il existe des polynômes irred de tout degré sur Fq

Déf : fonction de Möbius

Prop : mu est multiplicative (facile)

Th : formule d'inversion de Möbius [FG 93]

Appl : lien entre les deux fonctions *(appliquer la formule d'inversion à Phi)*

Th : dénombrement des polynômes irréductibles de Fq[X] [FG 189]

2) Construction des corps finis [Goz]

Prop : P un poly irred sur Fp, de degré n (existe bien). x une racine de P. Alors $Fp[X]/(P) \cong Fp(x) \cong Fq$.

Ex : F4.

3) Réduction modulo p [Goz 12]

Th : P un polynôme de Z[X]. Soit p premier qui divise pas le coeff dominant. Si la réduction de P modulo p est irréductible dans Fp, alors P est irréductible sur Q.

Exemple : $X^3-127X^2+3608X+19$ modulo 2.

III) Equations sur Fp [Goz]

On veut résoudre des équations de degré 2 sur Fp. Pour cela, il sera important de savoir si un élément de Fp est un carré ou pas (tout comme sur C on veut savoir si le discriminant est un carré ou pas, ie s'il est positif ou non). Ici on supposera toujours p différent de 2.

1) Symbole de Legendre [Goz]

Notation : Fq^2

Déf : symbole de Legendre

Prop : critère d'Euler

Cor : le symbole de Legendre est un mph de groupe.

Csq : il suffira de connaitre les valeurs (p,q) du symbole de Legendre.

2) Loi de réciprocité quadratique [Goz]

Loi de réciprocité quadratique version Caldero

Version pour p=2

Appl : exemple de calculs pour voir si c'est un carré ou pas.

Appl : test de Pépin. Un nd de Fermat Fn est premier ssi 3^(Fn-1)/2+1 congru à 0 modulo 3 *(on remarque que 2^2 congru à 1 modulo 3, donc 2^2^n congru à 1 mod 3. Donc Fn et 3 sont pee. Supp la congruence du test vérifiée. On note w l'ordre de 3 dans (Z/FnZ)*, on mq w=Fn-1, ce qui donne que Fn est premier. Si on supp Fn premier, par la LRQ, on a que (3,Fn)=(Fn,3). Fn congru à 2 mod 3 donc (Fn,3)=(2,3)=-1. Donc (3,Fn)=-1=3^(Fn-1)/2 donc c'est bon)*

IV) L'espace vectoriel Fq [Perr] + [Szp] + [FGN Alg1]

1) Dénombrement et isomph exceptionnels [Perr]

Isomph exceptionnels

2) Sous groupes de GLn(Z) [Ø]

G un sg fin ide GLn(Z). Alors G s'injecte dans GLn(Fp) (donc cardinal majoré)

3) Formes quadratiques sur Fq [Szp] + [FGN Alg1]

Déf discriminant

Deux formes quadratiques sont équivalentes ssi elles ont même discriminant

Exemple

SO2(Fq) [FGN Alg1]

Développements :
1 - Loi de réciprocité quadratique via les fq [???] (**)
2 - Isomorphismes exceptionnels [Perr 105] (**)
3 - Dénombrement des polynômes irréductibles sur Fq [FG 189] (**)
SO2(Fq) [FGN Alg1 17] (***)

Bibliographie :
[Goz]
[FG]
[Perr]
[Szp]
[FGN Alg1]

Commentaires :
- pas mis Frobenius Zolotarev

- nb d'automph diagonalisables sur un corps fini [FGN1][Gourdon]
- cardinal grassmannienne

Rapport du jury : le théorème de Wedderburn ne doit pas constituer le seul développement de cette leçon. En revanche, les applications des corps finis ne doivent pas être négligées. Le théorème de l'élément primitif, s'il est énoncé, doit pouvoir être utilisé. Les constructions des corps de petit cardinal doivent avoir été pratiquées. Il convient de montrer comment l'utilisation des corps de rupture permet de prouver l'irréductibilité d'un polynôme. Comprendre les sous-corps de F_64 est un bon exercice, en particulier F_16 n'est pas un sous-corps de F_64. Il faut savoir construire un corps de petit cardinal : F_4, F_8, F_9…, et mener des calculs dans ce corps.

Question du jury 2010 :
- q=p^n. soit a un générateur de Fq*. Quel est le degré de a sur Fp ?
- Combien y a-t-il de polynômes minimaux possibles pour a ?
- Quel est le polynôme caractéristique du morphisme de Fq dans Fq qui à x associe x^p ?