104 - Groupes finis : exemples et applications.

I) Généralités

1) Premières propriétés

Th : Lagrange

Prop : G est fini ssi il a un nb fini de sg [Del 4] *(si G a un nb fini de sg, il y a un nb fini de sg du style <x>. RpA : G est infini. Comme il y a un nb fini de sg monogènes et que leur union vaut G, il y a un sg monogène infini inclus dans G, et ce groupe a une infinité de sg, abs)*

2) Actions de groupes

Déf : action de G sur X [Del 59]

Déf : stabilisateur, orbite, transversale [Del 60]

Prop : bijection entre O(x) et G/Gx [Del 61] *(on explicite la bijection : g.Gx->gx et on vérifie)*

Ex : G agit sur lui-même par translation à gauche [Del 59]

Csq : théorème de Cayley.

Ex : si H est un sg de G, G agit sur G/H par translation

Appl : si p est le plus petit nombre premier dans la décomposition de n, et si H est un sg de G d'indice p, alors H est distingué dans G [Del 74] *(Le noyau de l'action est un sg distingué N. On mq N est inclus dans H. Alors G/N est isomorphe à un sq de Sp donc l'indice de N dans G divise p !, mais il divise aussi #G donc c'est 1 ou p. Si c'est 1 alors N=G impossible donc c'est p donc N=H)*

Th : équation aux classes [Del 63] *(on montre que les orbites forment une partition de X en montrant qu'on a une relation d'équivalence)*

Csq : tout corps fini est commutatif (Wedderburn) [Perrin 82] *(Z le centre de k, de cardinal q. On mq k est d'ordre q^n. On supp que k n'est pas commutatif, on fait agir k* sur k* par conjugaison. On écrit la formule des classes. Les polynômes cyclotomiques nous aident à trouver une contradiction avec les cardinaux et la divisibilté)*

Csq 2 : Un p groupe est un groupe fini d'ordre p^r (p nombre premier). Si G est un groupe d'ordre p^rm où p ne divise pas m, un p Sylow de G est un sg de G d'ordre p^r. Alors le centre d'un p-groupe n'est pas trivial [Del 63] *(G agit sur lui-même par conjugaison, équation des classes, considérations de divisibilité)*

Th : formule de Burnside [Del 64] *(E l'ensemble ds couples (g,x) tq gx=x. Alors #E=sum(#Fix(g)). D'autre aprt, #E=sum(#Gx). De cette dernière égalité, on déduit que si A est une transversale, #E est la somme des #Gx.#O(x) pour x dans A, ce qui vaut #A.#G. On conclut)*

Appl : on compte le nombre de roulettes à n secteurs et p couleurs [Del p.64] *(S_n agit sur l'ensemble des coloriages, donc en particulier, si s est la permutation (1,…,n), <s> agit sur les coloriages. Deux roues sont égales ssi elles sont dans la même orbite. Il faut donc compter le nb d'orbites, donc Burnside. Il reste juste à trouver #Fix(g) pour g une permutation. On décomp la permut en k cycles, le coloriage doit être fixe sur chaque cycle, il y en a donc p^k. Reste à trouver le nb de cycles ds la decomp de s^m. Il y en a pgcd(m,n) (cf [Del 47]))*

3) Théorèmes de Sylow [Perrin p.18-19]

Th : Sylow [Del 72]
(n=p^km. 1er th : il existe un p Sylow, ie un groupe d'ordre p^k. On appelle X l'ensemble des SOUS ENSEMBLES à p^k éléments. G agit sur X par translation à gauche. On calcule le cardinal de X, on voit qu'il n'est pas divisible par B, ça veut

dire qu'il existe une orbite A qui est pas divisible par p. On pose H le stab d'un élément K de A. L'indice de H est non divisible par p car le cardinal de A ne l'est pas. Donc #H=p^km'. Soit x un élément de K. Pour tout g du stab H, g.x est dans K, et si on a deux g différents dans le stab, gx et gx' sont différents. On a une sorte d'injection du stab dans K, donc #H est plus petit que p^k. Donc #=p^k.
2e th : ils sont conjugués. S un p –Sylow de G, H un p groupe. H agit sur G/S par translation à gche. Le stab d'un élément de G/S est un sg du p groupe H donc son indice est une puissance de p : les orbites sont donc de # une puissance de p. Formule des classes : m=somme(puissances dep), or p divise pas m, donc il doit y avoir une orbite de # p^0=1. Soit xS cette orbite. On a hxS=xS pour tout h de H donc H inclus ds xSx^-1. Si H est un p Sylow on conclut par #.
3e th : nb de p-Sylow. S un p Sylow, il agit sur l'ensemble des p-Sylow par conjugaison. Les orbites sont des puissances de p. Il y a une orbite à un seul élément : {S}. Faut montrer que c'est la seule (RpA) et c'est gagné)

Corollaire : s'il y a un unique p-Sylow, il est distingué [Del 72]

Exemple : un groupe d'ordre pq n'est pas simple [Per p.27] *(raisonner sur les cardinaux)*

II) Groupes finis abéliens

1) Groupes cycliques référence pour les groupes cycliques !

Prop : un groupe cyclique est abélien. Si G est un groupe cyclique d'ordre n alors il est isomorphe à Z/nZ.

Ex : U_n est isomorphe à Z/nZ

Prop : un groupe d'ordre p premier est cyclique.

Prop : générateurs de (Z/nZ,+) [Per 24]

Prop : sous groupes d'ordre d

Prop : Aut(Z/nZ) isomorphe à (Z/nZ)* [Per 24]

Th Chinois [Per 25] *(isomorphisme d'anneau, poser le morphisme, vérifier qu'il est INJ, et SURJ par cardinalité)*

Application : formule pour l'indicatrice d'Euler [Per 25]

2) Décomposition des groupes finis abéliens

Th de structure, invariants [Combes 66] *(récurrence sur l'ordre de G, grosse démo)*
-> D'où l'utilité d'étudier les groupes cycliques

Exemple : Groupe d'ordre 120=2^3*3*5 : (120), (2,30), (2,2,30) *(méthode : on commence par déterminer tous les « diviseurs élémentaires » possibles : 2^3,3,5 ; 2^2,2,3,5 ; 2,2,2,3,5. On fait un tableau dans chaque cas, avec 2,3,5 sur les colonnes. Par exemple, pour le 1er cas 2^3,3,5, ça donne [3,1,1] ; puis on calcule le produit de chaque ligne qui donne (120). 2e cas : 2^2,2,3,5 : [2,1,1 ; 1,0,0] donc (60,2). 3e cas : 2,2,2,3,5 : [1,1,1 ; 1,0,0 ; 1,0,0] qui donne (30,2,2) cf http://pagesperso-orange.fr/cyd60000/cours/Decomposition.pdf p.5)*

Application : le groupe multiplicatif d'un corps fini est cyclique [BR 105] *(par Wedderburn le corps est commutatif. K* est donc commutatif est s'écrit K*=H1x…xHn où Hi cyclique avec #Hi | #Hi+1 ; le cardinal de Hn r est donc tq x^r=e pour tout x. Tous les éléments de K* sont racines de X^r-1, qui a au plus r racines car K corps, donc #K*<r. Mais #Hn=r divise #K* donc on a égalité. Donc K*=Hn)*

III) Exemples de groupes finis

1) Le groupe symétrique Sn

Motivation de l'étude : théorème de Cayley

Prop : toute permutation se décompose de façon unique en cycles à supports disjoints [Del 46]

Prop : S_n est engendré par : [Del 48]
- Les transpositions
- Les transpositions du type (1,i)
- Les transpositions du type (i,i+1)

Déf : morphisme signature (produit des (s(i)-s(j))/(i-j)). C'est un morphisme dont le noyau est noté An

Prop : An est engendré par les 3 cycles [Del 48]

Appl : An est simple pour n>5 [Perrin 28] *(cas n=5 : sit H un sg distingué de A5. Dans A5 il y a des éléments d'ordre 3, 3 et 5. Les 3-cycles sont conjugués dasn A5 et les éléments d'ordre 2, donc si H en contient un il les contient tous. Si H contient un élément d'ordre 5, il contient le 5 Sylow engendré par cet élément, donc tous les 5 Sylow car ils sont conjugués, donc tous les éléments d'ordre 5. On montre alors que H ne peut pas contenir que des éléments d'ordre 2 ou 3 ou 5 pour des raisons de cardinaux, donc il en contient au moins 2 type, donc son cadinal est >35 donc H=A5. Pour n>5 : H sg dist de An, s dans H no ntrivial. On veut fabriquer à partir de s un élément de H qui agit sur un ens à 5 éléments. On prend un élément u particulier de An, et on pose r=[u,s] (commutateur) qui va fixer n-5 éléments, et agit sur un ens F à 5 éléments. A(F) est isomph à A5 et se plonge dans An. Soit H_0 l'ens des permutations de A(F) qui se plongent dans H. H_0 sistingué dans A(F)=A5 donc =A5. Soit t un 3-cycle de A(F)=H0 inclus dans H, H contient un 3 cycle donc tous donc =An)*

Csq : D(Sn)=An [Perrin 28]

Prop : un sous groupe d'ordre n de Sn est isomorphe à Sn-1 [Per 30] *(utilise la simplicité de An et l'action de Sn sur Sn/H par translation)*

2) Le groupe diédral Dn

Déf : groupe des isométries du plan conservant un polygone régulier à n côtés [Per 23]

Prop : #Dn=2n

Prop : générateurs (une rotation + une symétrie)

Prop : non abélien pour n>2. Plus précisément, égal à Zn SD Z2

3) Le groupe quaternionique H8

Définition : définition avec les formules entre i j et k [Per 13]

Prop : tous les sg sont distingués.

IV) Autour de GLn(K) et PGLn(K)

1) Les sous groupes finis de GLn(Z)

Prop : les sous groupes finis de GLn(Z) peuvent s'identifier à des sous groupes de GLn(F_q), pour q>3 *(montrer qu'on a bien une surjection f entre GLn(Z) et GLn(Fp), et que si G est un groupe fini de GLn(Z) alors f est injective sur G. Un élément g de Ker(f) est de la forme Id+pM et son poly caract est Chi_g=p^n.Chi_M((X-1)/p. Montrer (rusé) par récurrence que si P(X)=p^nQ(X-1)/p) alors P=(X-1)^n. On a alors Chi_g=(X-1)^n, et g est diagonalisable donc g =Id).*

Csq : si G est un sous groupe fini de GL2(Z), alors son ordre divise 48.

2) Les sous groupes finis de SO3(R)

Prop : si G est un sg fini de SO(3), G agit sur les pôles des éléments de G [BR 258]

Th : sous groupes finis de SO(3), avec les isomorphismes [BR 258] *(dans le développement, admettre le dernier)*

3) Les groupes PGL_n(Fq)

Les groupes finis sont classes à partir des groupes finis simples. Parmi ceux-ci il y a des séries A_n et PSLn(F_q) mais il y a des isomorphismes entre eux.

Th : Isomorphismes exceptionnels [Perrin 105]

Bibliographie :
Perrin
Bouvier Richard
Delcourt
Combes
Francinou-Gianella

Développements :
1 - Iso+(T) et Iso+(C) [Aless 62] (**)
2 - Isomorphismes exceptionnels [Perr 105] (**)
3 - Groupes d'ordre 12 [FG 19] (**)
An simple [Per 26] (**)
Sous groupes finis de SO_3, 3 cas [Combes] + [BR] (**)

Rapport jury 2005-5009 :
Les exemples doivent figurer en bonne place dans cette leçon. Il semble important de connaitre les classes d'isomorphismes des groupes de petit cardinal (inferieur a 6).Il semble important de connaitre les classes d'isomorphismes des groupes `a 2, 3, 4, 5, 6 éléments et de savoir démontrer que tous les groupes finis se plongent dans un Sn. Un minimum de connaissance est exigible sur les groupes diédraux (description, présentation en terme de générateurs et relation).