108 - Exemples de parties génératrices d'un groupe. Applications.

Plan général, on proposera des applications tout au long. Ces applications peuvent se ranger en plusieurs catégories :
- Connaître les générateurs d'un groupe permet de mieux connaître sa structure
- Prouver la surjectivité de morphismes (ou des problèmes proches (ex : si on a un p cycle et une transpo dans le groupe de Galois, alors G=Sp)
- Montrer qu'un groupe est simple (An, SO(3))
- On peut vérifier une ppté seulement sur les générateurs et ça se transmet au groupe entier

Définition : groupe engendré par une partie

Exemple : D(G) est le groupe engendré par les commutateurs de G

Rq : si f est un morphisme de G dans un groupe abélien A alors D(G) est inclus dans Ker(f).

I) Groupes abéliens de type fini

1) 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) Groupes abéliens de type fini

Déf : groupe abélien engendré par un nombre fini d'éléments

Ex : groupes cycliques et groupes monogènes. Z/4Z, Z.

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)*

II) Exemples de groupes finis non abéliens

1) Groupe diédral

Définition : isométries qui conservent un n-gone

Prop : isomorphe à un psd

Générateurs : a,b tq a tq a^n=b²=…

2) Groupe symétrique [Del]

Prop : toute permutation se décompose de façon unique en un produit de cycles à support disjoint *(algorithme : s une permutation. On cherche l'image de 1, puis l'image de cette image, etc, jusqu'à retomber sur 1, ça donne un 1er cycle. Ensuite on prend le plus petit entier qui n'est pas apparu et on recommence. Jusqu'à ce qu'il n'y ait plus d'entier. On obtient des cycles à support disjoints. Unicité ? Un cycle contenant un entier doit contenir toutes ses images successives par s, si il ne contient pas la k-ème image, on a un problème lorsqu'on élève s à la puissance k. Par le même argument, l'ordre des elts ds un cycle est uniquement déterminé)*

Prop : tout r-cycle se décompose en un produit de transpo. Sn est donc engendré par les transpo *((i,j,k,l)=(i,j)((j,k)(k,l))*

Appl : Iso+(T)=S4 *(on montre l'injectivité, puis la surj en mq il y a toutes les transpos)*

Prop : plusieurs systèmes de générateurs de Sn : (1,i), (i,i+1), (1,..,n) et (1,2) *((i,j)=(1,i)(1,j)(1,i) ; pareil pour les autres)*

Prop : si p est premier, alors Sp est engendré par un p-cycle et une transpo (pour Galois) [Goz 177] *(on suppose que la transpo t=(1,2) et le cycle c=(1,a,b,c,…). Il existe k tq c^k(1)=2. On remplace c par c^k. c^k est un p-cycle (c'est là qu'intervient l'hup p premier) et c^k=(1,2x_3,x_4,….). Il existe u dans Sp tq u(1)=1, u(2)=2, u(3)=x_3, u(4)=x_4… Quitte à remplacer c par u^-1*c*u, on a c=(1,2,3,4…,p). On se retrouve donc avec (1,2) et (1,2,…,p) qui génère Sp entier. Hum pas clair, on a eu besoin d'un u inconnu)*

Prop : An est engendré par les 3 cycles (\ge 3)

Prop : An est engendré par les (1,2,i)

Appl : A5 est simple [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)*

Cor : An est simple *(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)*

Appl : D(Sn)=An *(le groupe dérivé est inclus dans An par signature, et il est distingué dans Sn donc c'est An)*

Appl : le seul mph non trivial de Sn dans C* est la signature *(le groupe dérivé est inclus dans le noyau d'un tel morphisme, donc An est inclus dans le noyau du mph f, donc Sn/An={+-1}est une surjection sur Imf, donc Imf={1} ou Im(f)=+-1. Reste à mq le seul mph non trivial de Sn dans {+1} est la signature)*

Appl : le groupe de Galois de X^5-4X+2 est isomorphe à S5, donc non résoluble [Gozard 178] *(en effet, il a exactement 2 racines non réelles, la conjugaison correspond donc à une transposition, et comme on est dans S5, par Sylow, il existe un élément d'ordre 5 (ie un 5 cycle), donc le groupe de Galois est S5 tout entier. En effet, un lemme dit que si H un sg de Sp contient une transpo et un p-cycle alors H=Sp [Goz 177]).*

III) Exemples dans le groupe linéaire

E un K-ev de dimension n

1) GL(E) et SL(E)

Déf : transvection, dilatation [Szp 298]

Prop : les transvections sont conjuguées si n≥3
Th : Les transvections engendrent SL(E) [Szp] *(on commence par montrer un lemme qui dit que si on a x,y dans E, alors y est l'image de x par une transvection ou un produit de 2 transvections. On a aussi besoin du lemme qui dit que di H1 et H2 sont deux hyperplans distincts et que si on prend x qui est pas dans leur intersection, alors il y a une transvection qui envoie x sur x et H1 sur H2 (on se sert du lemme précédent). Pour le th faut alors une récurrence sur n. On fixe u dans SL(E) et x. On prend H un hyperplan contenant pas x. Par les lemmes, on peut supposer u(H)=H et u(x)=x, quitte à remplacer u par u*transvections. On écrit la matrice de u dans une base adaptée. On applique l'hypothèse de récurrence à u restreint à H et c'est bon)*

Rq : tout élément de SLn(K) est engendré par au plus n transvections (n+1 si c'est une homothétie). Démo difficile

Th : GL(E) est engendré par les transvections et les dilatations *(u dans GL(E), v une dilatation de rapport 1/det(u), vu est dans SL(E) bref c'est ok)*

Appl : le centre de GLn(K) est l'ensemble des homothéties, celui de SLn(K) est l'ensemble des homothéties de déterminant 1 *(on montre que utu^-1=t pour toute transvection, donc u fixe toutes les droites donc c'est bon. Pareil pour SLn(K))*

Déf : PGLn(K), PSLn(K)

Th : PSLn(K) est simple si n≥3 *(on regarde un sg normal non trivial de PSLn(K), son image réciproque par la proj canonique, qui doit être un sg distingué de SLn(K). On mq qu'il contient une transvection, et comme elles sont toutes conjuguées pour n≥3, il les contient toutes, donc c'est SLn(K) entier)*

2) Groupe O(q)

Déf : réflexion, retournement

Prop : les retournements sont conjuguées si n≥3

Th : Cartan Dieudonné [Szp 317]

Corollaire : si n≥3 alors tout élément de SO(q) s'écrit comme le produit d'au plus n retournements *(en effet, un élément de SO(q) est produit d'un nb pair de réflexions. Or un lemme nous dit que si r1 et r2 sont des reflexions, on peut trouver des retournements s1 et s2 tq r1r2=s1s2. Preuve du lemme : si n=3, on change r_i en –r_i et ça marche. Sinon on note H1 et H2 les hyperplans de r1 et r2. On suppose r1=r2. Il faut trouver un sev non isotrope de H1 de dim n-3, on écrit alors E comme F+F^orth. On peut écrire r1 et r2 comme pdt de deux renversements sur F^orth car de dim 3, on prolonge par Id sur le reste et ça marche. Si r1 et r2 sont différents, on montre que l'intersection de H1 et H2 contient un sev non isotrope de dim n-3 et on conclut pareil)*

Appl : SO(3) est simple

Appl : SU(2)/{+-1}=SO3(R) [Per 164] *(on note G l'ens des quaternions de module 1. G opère sur H par conjugaison, ce qui donne un morphisme S de G dans GL(4,R). Conservation de la norme qui est une fq de sgn (4,0) donc S va de G dans O(4). Si on regarde la restriction sur l'orthogonal de R dans H, on a un mph de G dans O(3), et même SO(3) par connexité. Reste à montrer la surjectivité en montrant qu'on a tous les retournements)*

Développements :
An simple [Per 26] (***)
Théorème de Cartan Dieudonné [Szp 317] (***)
Iso+(T) et Iso+(C) [Aless 62] (**)
SO(3) est simple [???] (**)

Bibliographie :
Delcourt
Combes
Perrin
Szp
Gozard
BR

Pas parlé :
Groupes libres, présentation de groupes, PSL2(Z) ([FGN1 60])

Rapport du jury : peu de candidats voient l'utilité des parties génératrices dans l'analyse des morphismes de groupes. Il est important de réfléchir à l'utilisation des générateurs d'un groupe pour établir des propriétés de certains morphismes (automorphismes du groupe diédral par exemple). La leçon ne se limite pas aux groupes finis (on peut penser à certains groupes libres) ou à la simplicité de An, $n > 4$.