GROUPES ALÉATOIRES
[d'après Misha Gromov,...]

par **Étienne GHYS**

INTRODUCTION

La *théorie combinatoire des groupes* traite pour l'essentiel des groupes de *présentation finie*, c'est-à-dire des groupes fondamentaux des polyèdres finis. Les méthodes employées, d'abord combinatoires et topologiques [CM82], ont pris par la suite un aspect métrique, en particulier sous l'impulsion de M. GROMOV. Aujourd'hui, on préfère parfois la terminologie « *théorie géométrique des groupes* » [Ha00]. Une place considérable est faite à des exemples remarquables qui sont analysés en détail : groupes libres, groupes fondamentaux de surfaces, groupes arithmétiques, etc. Par ailleurs, quelques classes de groupes sont mises en évidence, comme celles des groupes nilpotents, polycycliques, résolubles, moyennables etc., mais à l'évidence il ne s'agit que de classes très particulières qui n'illustrent pas le « comportement typique » d'un groupe de présentation finie. Dans une série d'articles étalés sur une vingtaine d'années, M. GROMOV propose une vision globale des propriétés des groupes « génériques » ou « aléatoires », dans un sens que nous préciserons plus loin. Cet exposé fait le point sur la question. Comme souvent dans ce séminaire, il n'est pas possible en quelques pages d'entrer dans les détails de preuves longues et difficiles et il nous faudra malheureusement nous contenter d'un survol superficiel.

Le rôle joué par les objets génériques par rapport aux exemples spécifiques dépend du domaine des mathématiques considéré. Dans la théorie des systèmes dynamiques par exemple, l'étude des dynamiques génériques est absolument fondamentale alors que la géométrie algébrique accorde peut-être moins d'importance aux variétés algébriques « génériques ». Les méthodes présentées dans cet exposé permettent une première approche aléatoire en théorie géométrique des groupes. L'avenir dira si cette approche est féconde et si une véritable « théorie des groupes aléatoires » est destinée à se développer (à l'instar de la théorie des graphes aléatoires?). Quoi qu'il en soit,

nous verrons que ces méthodes permettent d'ores et déjà de montrer l'existence de groupes aux propriétés surprenantes.

Je remercie THOMAS DELZANT, DAMIEN GABORIAU, YANN OLLIVIER, LIOR SILBERMAN, ALAIN VALETTE et ANDRZEJ ŻUK pour leur aide, et MISHA GROMOV pour ses belles mathématiques.

1. QUELQUES ÉNONCÉS

Pour que notre « marche aléatoire parmi les groupes aléatoires » [Gr03] ne soit pas trop désordonnée, je voudrais présenter d'abord quelques énoncés que nous rencontrerons dans cet exposé et qui serviront de repères.

Soit Γ un groupe engendré par une partie finie S symétrique (*i.e.* $S = S^{-1}$). Pour chaque γ de Γ , on note $|\gamma|_S$ sa *norme*, longueur minimale d'un mot en les éléments de S qui représente γ . Si γ_1 et γ_2 sont deux éléments de Γ , on note $d_S(\gamma_1, \gamma_2) = |\gamma_1^{-1}\gamma_2|_S$. Ceci munit Γ de la *métrique des mots*, invariante par translations à gauche. Il est souvent utile de plonger Γ dans son *graphe de CAYLEY*, dont les sommets sont les éléments du groupe et les arêtes connectent les éléments à distance 1. On prolonge naturellement la distance d_S au graphe (ou plus précisément à sa réalisation géométrique), de manière à ce que chaque arête soit isométrique à l'intervalle $[0, 1]$. Un *segment géodésique* est un plongement isométrique d'un intervalle $[0, n]$ dans le graphe de CAYLEY ; on confond souvent un tel segment avec son image. Le groupe Γ est *hyperbolique* s'il existe une constante $\delta_S \geq 0$ telle que pour tout triplet d'éléments γ_i ($i = 1, 2, 3$) et tout triplet de segments géodésiques c_i les connectant deux à deux, tout point de chacun des c_i est à distance inférieure à δ_S de la réunion des deux autres (finesse des triangles géodésiques). Cette propriété ne dépend pas du choix de la partie génératrice S (même si la valeur de δ_S en dépend). Les groupes hyperboliques, introduits par M. GROMOV dans [Gr81, Gr84, Gr87, Gr93], jouissent de nombreuses propriétés remarquables et ont fait l'objet de nombreux travaux (voir par exemple [Gh90, GhH90, CDP90, Al91] pour les fondements de la théorie) : on peut dire aujourd'hui qu'ils sont bien compris. L'un des thèmes essentiels de cet exposé est qu'en un certain sens la majorité des groupes de présentation finie sont hyperboliques.

Choisissons deux entiers $g \geq 2$ et $r \geq 1$ et considérons les présentations de groupes à g générateurs et r relateurs de la forme $\Gamma = \langle a_1, a_2, \dots, a_g \mid m_1, m_2, \dots, m_r \rangle$ où les m_j sont des mots cycliquement réduits en les lettres $a_i^{\pm 1}$ (un mot est *réduit* s'il ne contient pas deux lettres consécutives inverses et *cycliquement réduit* si de plus la première et la dernière lettre ne sont pas inverses). Si l'on fixe g et les longueurs ℓ_j des relateurs m_j ($j = 1, \dots, r$), il n'y a qu'un nombre fini $N(g; \ell_1, \dots, \ell_r)$ de telles présentations. Notons $N_{hyp}(g; \ell_1, \dots, \ell_r)$ le nombre de celles qui définissent un groupe hyperbolique *non élémentaire* (c'est-à-dire infini et ne contenant pas de sous-groupe infini cyclique d'indice fini). Le théorème suivant a été énoncé par M. GROMOV dans

[Gr87] puis démontré indépendamment par C. CHAMPETIER [Ch91, Ch93, Ch94, Ch95] et Y. OL'SHANSKIĬ [Ols92a].

THÉORÈME A. — *La probabilité $N_{hyp}(g; \ell_1, \dots, \ell_r)/N(g; \ell_1, \dots, \ell_r)$ pour qu'une présentation de groupe à g générateurs et r relateurs définisse un groupe hyperbolique non élémentaire tend vers 1 lorsque les longueurs $\ell_1, \dots, \ell_r$ des relateurs tendent vers l'infini.*

Nous verrons que la difficulté principale dans la preuve de ce théorème est dans le cas où les ℓ_j ont des ordres de grandeur différents. Une autre approche a été proposée par la suite par M. GROMOV dans [Gr93]. Il s'agit encore de fixer le nombre de générateurs mais de *faire tendre le nombre de relateurs vers l'infini, en les gardant tous de la même longueur ℓ* (tendant également vers l'infini). Plus précisément, choisissons encore un entier $g \geq 2$ et une constante $c \geq 1$ et considérons l'ensemble $S(\ell - c, \ell + c)$ des mots réduits en les lettres $a_i^{\pm 1}$ ($i = 1, \dots, g$) dont les longueurs sont comprises entre $\ell - c$ et $\ell + c$. Chaque partie $R \subset S(\ell - c, \ell + c)$ peut être considérée comme un ensemble de relateurs et définit donc un groupe, quotient du groupe libre par le sous-groupe normal engendré par R . Fixons un réel $d \in [0, 1]$ et une constante $c' > 1$ et considérons l'ensemble des parties $R \subset S(\ell - c, \ell + c)$, dites de *densité d* , dont le cardinal est compris entre $c'^{-1}|S(\ell - c, \ell + c)|^d$ et $c'|S(\ell - c, \ell + c)|^d$ (nous notons $|X|$ le cardinal d'un ensemble fini X). La preuve du théorème suivant a été esquissée par M. GROMOV dans [Gr93] puis précisée par Y. OLLIVIER [Oll03a, Oll03b, Oll03c].

THÉORÈME B

— *Si $d > 1/2$, la probabilité pour qu'une partie $R \subset S(\ell - c, \ell + c)$ de densité d définisse le groupe trivial tend vers 1 lorsque la longueur ℓ tend vers l'infini.*

— *Si $d < 1/2$, la probabilité pour qu'une partie $R \subset S(\ell - c, \ell + c)$ de densité d définisse un groupe hyperbolique non élémentaire tend vers 1 lorsque la longueur ℓ tend vers l'infini.*

Ces théorèmes ont d'importantes généralisations dans lesquelles on remplace le groupe libre engendré par les a_i par un groupe hyperbolique non élémentaire quelconque. Il s'agit alors de considérer le quotient de ce groupe par le sous-groupe normalement engendré par un nombre fini d'éléments de grandes longueurs. En itérant le procédé on construit une suite de groupes hyperboliques et un passage à la limite donne des exemples intéressants de groupes de *type fini*. Une manière agréable de présenter ce genre de limite consiste à introduire une topologie sur l'ensemble $\mathcal{G}r_g$ des sous-groupes normaux du groupe libre F_g à g générateurs ou, ce qui revient au même, sur l'ensemble des groupes équipés d'une famille génératrice à g éléments. Dans cette topologie, deux sous-groupes normaux sont proches si leurs intersections avec une grande boule de F_g coïncident. Cette topologie (introduite par R. GRIGORCHUK [Gri85]) fait de $\mathcal{G}r_g$ un espace métrisable compact. Soit $\mathcal{H}yp_g \subset \mathcal{G}r_g$ la partie définie par les groupes hyperboliques non élémentaires (dénombrable car ceux-ci sont de

présentation finie) et $\overline{\mathcal{H}yp_g}$ son adhérence dans $\mathcal{G}r_g$. Enfin, on note $\overline{\mathcal{H}yp_g^{st}}$ l'adhérence des groupes hyperboliques non élémentaires sans torsion. Le théorème suivant est exprimé dans le vocabulaire de C. CHAMPETIER [Ch91, Ch93, Ch94, Ch95, Ch00] mais on trouverait des énoncés du même genre dans l'article de Y. OLSHANSKIÏ [Ols92b].

THÉORÈME C. — *Il existe un G_δ dense dans l'adhérence des groupes hyperboliques non élémentaires $\overline{\mathcal{H}yp_g}$ formé de groupes infinis dont tous les éléments sont d'ordre fini.*

Il existe un G_δ dense dans $\overline{\mathcal{H}yp_g^{st}}$ formé de groupes infinis Γ qui :

- possèdent la propriété (T) de KAZHDAN (voir [HV89]) et sont donc non moyennables,
- ne contiennent pas de sous-groupe non abélien libre,
- n'ont aucun quotient fini non trivial,
- possèdent une partie génératrice à deux éléments.

Enfin, nous donnerons une idée générale de la démonstration par M. GROMOV du théorème suivant [Gr03].

THÉORÈME D. — *Il existe un groupe de présentation finie Γ qui ne se plonge pas de manière uniforme dans un espace de HILBERT $\mathcal{H}$, autrement dit pour lequel il n'existe aucun plongement $i : \Gamma \rightarrow \mathcal{H}$ vérifiant $F(d_S(\gamma_1, \gamma_2)) \leq \|i(\gamma_1) - i(\gamma_2)\| \leq d_S(\gamma_1, \gamma_2)$ pour tous γ_1, γ_2 dans Γ , avec $F : \mathbb{N} \rightarrow \mathbb{N}$ tendant vers l'infini à l'infini.*

L'intérêt de ce concept de plongement provient du fait qu'un théorème de YU affirme que tous les groupes qui se plongent uniformément dans un espace de HILBERT vérifient la conjecture de BAUM-CONNES « grossière » (coarse) (et donc celle de NOVIKOV) [Yu00]. Ces groupes sont aussi caractérisés par l'existence d'une action moyennable sur un espace compact [HR00]; c'est le cas pour tous les groupes hyperboliques [Se92]. On pourra consulter à ce sujet l'exposé de G. SKANDALIS dans ce séminaire [Sk00]. Le théorème D permet la construction de contre-exemples à des versions généralisées de la conjecture de BAUM-CONNES [HLS02].

Dans cet exposé, la lettre ℓ désignera toujours un entier destiné à tendre vers l'infini. Un événement aléatoire dépendra de ℓ et se réalisera avec une probabilité dépendant également de ℓ . Lorsque cette probabilité tend vers 1 quand ℓ tend vers l'infini, nous dirons que l'événement se réalise très probablement.

2. MODÈLE À DENSITÉ

Densités

Commençons par donner une définition simple qui permet d'obtenir des estimations intuitives sur la combinatoire d'ensembles finis dont la taille tend vers l'infini. Soit X

un ensemble fini de référence, dont le cardinal tendra par la suite vers l'infini. Si A est un ensemble fini non vide, nous dirons (suivant [Gr93]) que la *densité* de A (sous-entendu par rapport à X) est $\text{dens}(A) = \log |A| / \log |X|$. Lorsque A est une partie de X , sa *codensité* est définie par $\text{codens}(A) = 1 - \text{dens}(A)$. Si X est un espace vectoriel de dimension finie sur un corps fini et A est un sous-espace vectoriel, alors la densité est bien sûr le rapport des dimensions $\dim(A) / \dim(X)$. La codimension de l'intersection de deux sous-espaces en position générale est la somme de leurs codimensions, sauf si cette somme est supérieure à la dimension ambiante, auquel cas l'intersection est triviale. Il est remarquable que cette propriété s'étende aux parties d'un ensemble fini, sans aucune structure additionnelle, lorsque le cardinal tend vers l'infini. Plus précisément, fixons deux nombres cod_1 et cod_2 dans l'intervalle $[0, 1]$ et un $\varepsilon > 0$. Considérons l'ensemble (fini) des couples de parties A_1, A_2 de X dont les codensités sont respectivement dans les intervalles $[\text{cod}_1 - \varepsilon, \text{cod}_1 + \varepsilon]$ et $[\text{cod}_2 - \varepsilon, \text{cod}_2 + \varepsilon]$. Parmi ces couples de parties (A_1, A_2) on peut compter la proportion de ceux qui sont tels que la codensité de l'intersection vérifie $|\text{codens}(A_1 \cap A_2) - (\text{cod}_1 + \text{cod}_2)| \leq 3\varepsilon$. Dans cette dernière inégalité, nous convenons d'attribuer n'importe quelle codensité supérieure ou égale à 1 à l'ensemble vide. Il se trouve que lorsque le cardinal de X tend vers l'infini, cette proportion tend (rapidement) vers 1. En particulier, si $\text{cod}_1 + \text{cod}_2 > 1$ et si ε est assez petit, la probabilité pour que $A_1 \cap A_2$ soit vide tend vers 1. La preuve est bien sûr facile mais nous en retiendrons qu'il est souvent possible d'estimer le nombre de solutions d'« équations aléatoires » dans un ensemble fini de grande taille en « comptant les équations ». Voici un autre exemple : la non injectivité d'une application $f : A \rightarrow X$ revient à l'existence de solutions non triviales à l'équation $f(x) = f(y)$ à deux inconnues dans A et à valeurs dans X ; si d désigne la densité de A , on s'attend donc à ce qu'une application aléatoire f soit injective si $2d - 1 < 0$ et non injective si $2d - 1 > 0$. Formellement, cela signifie que si les cardinaux de deux ensembles finis A_ℓ et X_ℓ tendent vers l'infini avec une limite $d = \lim_\ell \log |A_\ell| / \log |X_\ell|$, et si $2d - 1 < 0$ (resp. $2d - 1 > 0$) alors une application $f : A_\ell \rightarrow X_\ell$ est *très probablement* injective (resp. non injective). On reconnaît le *principe des tiroirs probabiliste* (aussi connu comme le paradoxe des dates d'anniversaire) : si on met $\ell^{1/2+\varepsilon}$ objets au hasard dans ℓ tiroirs, très probablement l'un des tiroirs contient au moins deux objets.

Dans le théorème B, nous utilisons un concept de « partie R de $S(\ell - c, \ell + c)$ de densité d » qui ne coïncide pas exactement avec celui que nous venons de définir mais il est clair que la densité de R dans notre nouveau sens tend vers d quand ℓ tend vers l'infini et ce changement de terminologie n'a aucune importance.

Diagrammes

Avant d'esquisser la preuve du théorème B, il nous faut faire quelques rappels. Soit Γ un groupe possédant une présentation de la forme $\langle a_1, \dots, a_g \mid m_1, \dots, m_r \rangle$. Par définition, cela signifie que Γ est le quotient du groupe libre F_g de base les a_i par le