Un peu de géométrie des groupes

Les groupes discrets apparaissent dans tous les domaines des mathématiques, et même chez Escher. Ils sont définis algébriquement, mais on les comprend souvent mieux en les faisant agir sur des objets géométriques. De plus en plus, on les considère comme des êtres géométriques à part entière. Leurs propriétés sont particulièrement remarquables lorsque la courbure est négative.

QUELQUES GROUPES

Nous considérons un groupe G, en général non commutatif (encadré). Nous le noterons multiplicativement, l'élément neutre étant noté 1_G ou seulement 1. Les groupes qui nous intéresseront le plus seront *de type fini*, c'est-à-dire pouvant être engendrés par un nombre fini d'éléments. Voyons quelques exemples.

- Le groupe abélien libre $\mathbf{Z}^2$, ou $\mathbf{Z}\times\mathbf{Z}$, ou $\mathbf{Z}\oplus\mathbf{Z}$, est l'ensemble des couples d'entiers (m,n), avec l'addition $(m,n)+(m',n')=(m+m',n+n')$. Pour le noter multiplicativement, posons $a=(1,0)$, $b=(0,1)$, et voyons $\mathbf{Z}^2$ comme l'ensemble des $a^m b^n$ muni de la multiplication $(a^m b^n)(a^{m'} b^{n'}) = a^{m+m'} b^{n+n'}$. L'élément neutre $a^0 b^0$ est noté 1, l'inverse de $a^m b^n$ est $a^{-m} b^{-n}$.
- Considérons sur la droite réelle $\mathbf{R}$ le groupe affine $\mathrm{Aff}(\mathbf{R})$ formé des homothéties et des translations, c'est-à-dire les transformations de la forme $x \mapsto ax+b$ avec a, b réels et $a \neq 0$, le produit étant la composition $(f\circ g)(x) = f(g(x))$. C'est un groupe « continu » (groupe de Lie), mais nous pouvons considérer des sous-groupes de type fini, par exemple le groupe G_1 engendré par $t : x \mapsto x+1$ et $h : x \mapsto 2x$. On vérifie que G_1 est l'ensemble des transformations φ_{mnp} de la forme $\varphi_{mnp}(x) = 2^m x + \dfrac{n}{2^p}$, avec m, n, p entiers (encadré).
- Le groupe $GL(n,\mathbf{R})$ des matrices $n\times n$ à coefficients réels qui sont inversibles (c'est-à-dire de déterminant $\neq 0$) est aussi un groupe de Lie. Les matrices à coefficients entiers ne forment pas un sous-groupe car le déterminant apparaît au dénominateur quand on calcule l'inverse d'une matrice. Mais $SL(n,\mathbf{Z})$, l'ensemble des matrices à coefficients entiers et de déterminant 1, est un sous-groupe et nous considérons le groupe $G_2 \subset SL(2,\mathbf{Z})$ engendré par $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

GROUPES LIBRES

Dans un espace vectoriel V sur un corps K, le sous-espace vectoriel engendré par $\{v_1,\dots,v_k\}$ est l'ensemble des combinaisons linéaires $\sum_{i=1}^k \lambda_i v_i$, avec $\lambda_i \in K$. Les éléments $v_1,\dots,v_k$ sont indépendants si deux combinaisons linéaires différentes représentent toujours des éléments différents de V ou, de façon équivalente, s'il n'existe pas de relation $\sum_{i=1}^k \lambda_i v_i = 0$ avec les λ_i non tous nuls. Le sous-espace engendré est alors de dimension k, il est isomorphe à K^k.

Dans un groupe G, le sous-groupe engendré par $\{g_1,\dots,g_k\}$ est l'ensemble des éléments de G pouvant s'écrire comme un *mot réduit* $g_{i_1}^{n_1}\dots g_{i_p}^{n_p}$, où les n_i sont des entiers non nuls et $i_j \neq i_{j+1}$. Par exemple, a^2, $b^{-1}c$, $c^{-3}a^3b^2acb^{-5}$ sont des mots en a, b, c. On prend garde de ne pas oublier le mot vide, noté 1, qui représente le neutre 1_G. La *longueur* $|W|$ d'un mot W est le nombre total de lettres, en tenant compte des puissances ; ainsi $|c^{-3}a^3b^2acb^{-5}| = 15$.

On dira que $g_1,\dots,g_k$ sont *indépendants* (ou forment une *famille libre*) si deux mots réduits différents représentent toujours deux éléments différents de G ou, de façon équivalente, s'il n'existe pas de relation non triviale $g_{i_1}^{n_1}\dots g_{i_p}^{n_p} = 1$. Ainsi la famille $\{g\}$ (constituée du seul élément g) est libre si et seulement si il n'y a pas de relation non triviale $g^n = 1$, c'est-à-dire si g est d'ordre infini. Dans les exemples ci-dessus, les familles $\{a,b\} \subset \mathbf{Z}^2$ et $\{h,t\} \subset G_1$ ne sont pas libres, à cause des relations $ab = ba$ et $hth^{-1} = t^2$. Nous allons en revanche montrer, en utilisant la technique dite du ping-

– *Gilbert Levitt, laboratoire de mathématiques Nicolas Oresme – UMR 6139 CNRS – Université de Caen, BP 5186, 14032 Caen cedex.*
levitt@math.unicaen.fr

Encadré

GROUPES

Un groupe est un ensemble dans lequel on peut multiplier et inverser les éléments. Le produit doit être associatif : on a $(xy)z = x(yz)$*, et on note simplement* xyz*. En revanche, le produit n'est pas forcément commutatif : on peut avoir* $xy \neq yx$*. L'inverse de* x *est noté* x^{-1}*. Il vérifie* $xx^{-1} = x^{-1}x = 1$*, où* 1 *désigne l'élément neutre, caractérisé par* $1x = x1 = x$*.*
Par exemple, l'ensemble des permutations d'un ensemble à n *éléments est un groupe fini, le groupe symétrique* S_n *; le produit de deux permutations* σ *et* τ *est la permutation composée, définie par* $(\sigma \circ \tau)(i) = \sigma(\tau(i))$*. Les matrices* $n \times n$ *à coefficients réels qui sont inversibles (c'est-à-dire de déterminant* $\neq 0$*) forment un groupe pour le produit matriciel.*
Si X *est un ensemble quelconque muni d'une certaine structure, les transformations inversibles préservant la structure forment un groupe (le produit étant toujours la composition, consistant à appliquer les transformations successivement). Si par exemple* X *est le plan euclidien (muni de la distance habituelle), on obtient le groupe des isométries, qui contient en particulier les rotations, les translations, les symétries orthogonales par rapport à des droites.*

SOUS-GROUPES

Une partie A *d'un groupe* G *est un* sous-groupe *si c'est elle-même un groupe pour le produit de* G*. Il faut et il suffit pour cela que* ab *et* a^{-1} *soient dans* A *chaque fois que* a *et* b *y sont. Si* A *n'est pas un sous-groupe, il existe un plus petit sous-groupe contenant* A*, c'est le* sous-groupe engendré *par* A*. Lorsque le sous-groupe engendré par* A *est* G *tout entier, on dit que* A engendre G*. Le groupe* G *est* de type fini *s'il peut être engendré par une partie finie.*
Montrons par exemple que le sous-groupe G_1 *engendré par* $t : x \mapsto x + 1$ *et* $h : x \mapsto 2x$ *dans le groupe* $Aff(\mathbf{R})$ *des transformations affines de* $\mathbf{R}$ *se compose des* φ_{mnp} *de la forme* $\varphi_{mnp}(x) = 2^m x + \dfrac{n}{2^p}$*, avec* m, n, p *entiers. Les formules*

$$(\varphi_{mnp}\varphi_{m'n'p'})(x) = \varphi_{mnp}(\varphi_{m'n'p'}(x)) = 2^{m+m'}x + \frac{2^{m+p}n' + 2^{p'}n}{2^{p+p'}} = \varphi_{m''n''p''}(x)$$

avec $m'' = m + m'$*,* $n'' = 2^{m+p}n' + 2^{p'}n$*,* $p'' = p + p'$*, et* $\varphi_{mnp}^{-1} = \varphi_{m'n'p'}$ *avec* $m' = -m$*,* $n' = -n$*, et* $p' = m + p$*, montrent que l'ensemble des* φ_{mnp} *est un sous-groupe. Il contient* h *et* t*, et c'est le plus petit car* $\varphi_{mnp} = h^{-p}t^n h^{m+p}$ *appartient à tout sous-groupe contenant* h *et* t*.*
Si G *est un groupe fini, et* A *est un sous-groupe, le cardinal de* A *divise celui de* G*. Le quotient est le nombre de classes de* G *modulo* A*, appelé* indice *de* A*. Ce nombre est encore défini lorsque* G *est infini, mais il peut être infini. S'il existe un entier* N *tel que, à chaque fois que l'on se donne* $g_0, g_1, \ldots, g_N \in G$*, on peut trouver* $i \neq j$ *avec* $g_i g_j^{-1} \in A$*, alors le plus petit de ces entiers* N *est l'indice de* A*. Sinon, l'indice de* A *est infini. Par exemple, l'ensemble des entiers multiples de* d *forme un sous-groupe de* $\mathbf{Z}$ *qui est d'indice* d *pour* $d > 0$*, alors que* $A = \{0\}$ *est d'indice infini.*

pong, que *les matrices* A et B *sont indépendantes* dans $SL(2, \mathbf{Z})$.

Pour cela, faisons agir $SL(2, \mathbf{Z})$ sur $P = \mathbf{R} \cup \{\infty\}$ (la droite projective réelle) en associant à $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ l'homographie $h_M : x \to \dfrac{ax + b}{cx + d}$ (avec les conventions usuelles, en particulier $h_M\left(-\dfrac{d}{c}\right) = \infty$ et $h_M(\infty) = \dfrac{a}{c}$ si $c \neq 0$). La définition est faite pour que $h_{MN} = h_M h_N$.

Soit $P_A =]-1, 1[$, et soit P_B le complémentaire de $[-1, 1]$. On a $h_A(x) = x + 2$ et par conséquent $h_A^n(P_A) \subset P_B$ pour tout $n \neq 0$. On a de même $h_B(x) = \dfrac{x}{2x + 1}$ et $h_B^n(P_B) \subset P_A$ pour $n \neq 0$. Nous allons maintenant jouer au ping-pong avec P_A et P_B.

Pour montrer l'indépendance de A et B, considérons un mot réduit non trivial, par exemple $W = B^2AB^{-3}A^5$. Appliquons $h_W = h_B^2 h_A h_B^{-3} h_A^5$ à P_A. L'élément h_A^5 l'envoie dans P_B, l'élément h_B^{-3} le renvoie dans P_A, etc. et finalement $h_W(P_A)$ est contenu dans P_A, sans lui être égal. Cela empêche h_W d'être l'identité et donc W d'être égal à 1 dans $SL(2, \mathbf{Z})$, cqfd. Ce raisonnement s'applique à tout mot W commençant par une puissance de B et se terminant par une puissance de A. Les autres cas se traitent de manière analogue : si W commence et se termine par une puissance de A, on a $h_W \neq id$ car

$h_W(P_A) \subset P_B$; si W se termine par une puissance de B, on applique h_W à P_B.

Puisque A et B sont indépendants, tout élément de G_2 s'écrit *de façon unique* comme un mot réduit en A et B. A ce point, on peut oublier que A et B sont des matrices, et voir G_2 comme l'ensemble $F(A, B)$ des mots réduits en deux symboles abstraits A et B. La multiplication consiste à juxtaposer et réduire ; par exemple $(B^2AB^{-3}A^5)(A^{-5}BA^4) = B^2AB^{-2}A^4$, et l'inverse de $B^2AB^{-3}A^5$ est $A^{-5}B^3A^{-1}B^{-2}$. On dit que G_2 est le *groupe libre de rang 2*, souvent noté F_2. On définit de même F_n, le groupe libre de rang n, pour $n > 2$.

Beaucoup de groupes contiennent des groupes libres. On montre par exemple que deux rotations de la sphère prises au hasard engendrent un groupe libre, les transformations $x \mapsto x + 1$ et $x \mapsto x^3$ sur $\mathbf{R}$ aussi.

Le groupe F_2 contient des familles libres arbitrairement grandes : on voit facilement que la famille infinie $\{A^nBA^{-n}\}_{n\in\mathbf{N}}$ est libre, car les B ne se simplifient pas quand on multiplie ces éléments. Le groupe libre de rang 2 contient donc des groupes libres de rang quelconque et même des groupes qui ne sont pas de type fini. Le théorème de Nielsen-Schreier garantit que tout sous-groupe d'un groupe libre est libre, c'est-à-dire qu'il est engendré par une famille libre.

L'ALTERNATIVE DE TITS

Nous avons déjà remarqué que G_1 n'est pas libre, car ses générateurs vérifient $hth^{-1} = t^2$. Pour obtenir d'autres relations, remarquons que dans Aff($\mathbf{R}$), et donc dans G_1, tout *commutateur* $[g_1, g_2] = g_1g_2g_1^{-1}g_2^{-1}$ est une translation, et que deux translations commutent. On a donc $[g_1, g_2][g_3, g_4] = [g_3, g_4][g_1, g_2]$ pour tous $g_1, g_2, g_3, g_4 \in G_1$. Cette relation « universelle » exprime que G_1 est *métabélien*, ou encore *résoluble de classe* 2.

Plus généralement, on dit que G est *résoluble* de classe $\leqslant p$ si le sous-groupe engendré par tous les commutateurs $[g_1, g_2]$ est résoluble de classe $\leqslant p - 1$, c'est-à-dire si 2^p éléments quelconques de G vérifient une certaine identité formée à partir de commutateurs itérés. Les groupes résolubles sont ceux que l'on peut obtenir par extensions à partir de groupes commutatifs. La non-résolubilité par radicaux des équations algébriques de degré 5 est due à la non-résolubilité du groupe symétrique S_5 (théorie de Galois).

On vérifie facilement que, pour tout corps K, le sous-groupe de $GL(n, K)$ formé des matrices triangulaires supérieures inversibles est résoluble (de classe n). La célèbre *alternative de Tits* (1972) affirme que, si le groupe de type fini G est linéaire, c'est-à-dire isomorphe à un sous-groupe d'un $GL(n, K)$, alors ou bien G contient un sous-groupe isomorphe à F_2, ou bien un sous-groupe d'indice fini de G (encadré) est résoluble. Autrement dit, ou bien G contient des familles libres arbitrairement grandes, ou bien (à indice fini près) les éléments de G vérifient une relation universelle. L'alternative de Tits a été étendue à d'autres groupes ; ainsi Bestvina, Feighn et Handel l'ont récemment montrée pour les sous-groupes du groupe $Out(F_n)$ des automorphismes d'un groupe libre de rang fini, modulo les conjugaisons.

RELATIONS ET PRÉSENTATIONS

Si un groupe G n'est pas libre, des mots réduits différents peuvent représenter le même élément : on dit qu'ils sont *équivalents*. Le *problème du mot* consiste à décider (algorithmiquement) si deux mots donnés sont ou non équivalents. Il suffit en fait de savoir décider quels mots sont *triviaux*, c'est-à-dire représentent l'élément neutre 1_G.

C'est facile dans $\mathbf{Z}^2$, qui est commutatif. Il est par exemple immédiat pour nous que $a^{100}b^{100}a^{-100}b^{-100} = 1$. Mais une machine qui ne saurait qu'appliquer mécaniquement la relation de base $ab = ba$ (et, soyons généreux, les relations $a^{\pm1}b^{\pm1} = b^{\pm1}a^{\pm1}$) trouverait pénible de montrer cette égalité : il lui faudrait en effet faire passer séparément chacun des cent a^{-1} à gauche de chaque b, soit 10 000 opérations pour un mot de longueur 400. De manière générale, le nombre d'opérations nécessaires pour montrer la trivialité d'un mot de longueur n est, dans le pire des cas, de l'ordre de n^2 pour n grand. On parle pour $\mathbf{Z}^2$ d'*inégalité isopérimétrique quadratique*.

L'interprétation géométrique est la suivante (figure). Quadrillons le plan par un grillage dont les barreaux horizontaux sont orientés vers la droite et portent la lettre a, les barreaux verticaux étant orientés vers le haut et portant b. Fixons un sommet E de ce graphe comme origine.

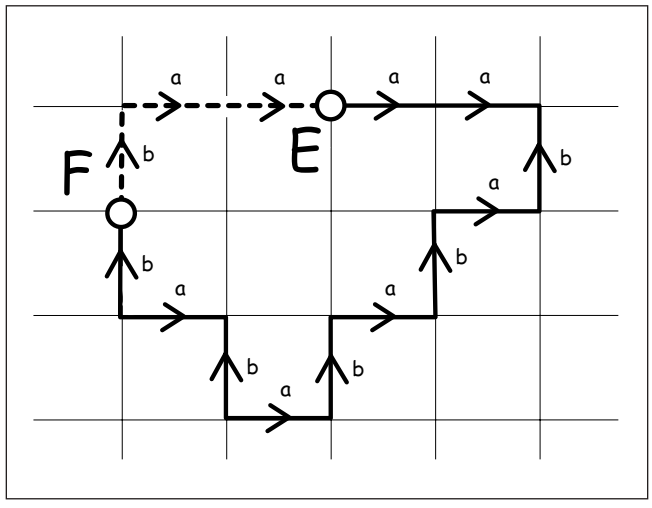

Figure 1 - *Les mots $a^2b^{-1}a^{-1}b^{-1}a^{-1}b^{-1}a^{-1}ba^{-1}b$ et $a^{-2}b^{-1}$ représentent le même élément de $\mathbf{Z}^2$: les chemins associés ont la même extrémité F.*

Un mot en a et b se représente alors comme un chemin issu de E, par exemple $a^2b^{-1}a^{-1}b^{-1}$ fait aller deux unités vers la droite, une vers le bas, une vers la gauche et une vers le bas.

On remarque que deux mots sont équivalents si et seulement si les chemins associés ont la même extrémité : par exemple $a^2b^{-1}a^{-1}b^{-1}a^{-1}b^{-1}a^{-1}ba^{-1}b$ est équivalent à $a^{-2}b^{-1}$. En particulier, les sommets du graphe s'identifient avec les éléments de $\mathbf{Z}^2$ et un mot est trivial si et seulement si le chemin associé est un lacet (il se referme en E). Ainsi $a^{100}b^{100}a^{-100}b^{-100}$ représente le bord d'un carré de côté 100. Appliquer la relation $a^{\pm1}b^{\pm1} = b^{\pm1}a^{\pm1}$ revient à faire traverser au lacet une maille du grillage, et 10 000 est simplement l'aire du carré.

L'exposant 2 obtenu plus haut est ainsi celui par lequel s'exprime l'aire d'un carré en fonction de son côté. On voit l'analogie avec l'inégalité isopérimétrique classique majorant l'aire bordée par une courbe plane par le *carré* de sa longueur (divisé par 4π, mais peu importe ici).

Revenant à l'algèbre, nous allons maintenant expliquer comment résoudre le problème du mot dans G_1 en utilisant uniquement la relation $hth^{-1}t^{-2} = 1$. Grâce aux équations $ht^{\pm1} = t^{\pm2}h$ et $t^{\pm1}h^{-1} = h^{-1}t^{\pm2}$, on peut dans un mot faire passer toutes les puissances positives de h à la droite du mot et toutes les puissances négatives à gauche. En d'autres termes, un mot quelconque W est équivalent dans G_1 à un mot de la forme $h^{-m}t^nh^p$ avec $m, p \geqslant 0$. Un tel mot représente la transformation $x \mapsto 2^{p-m}x + 2^{-m}n$, qui est l'identité si et seulement si $n = 0$ et $p = m$, c'est-à-dire si le mot est vide. Donc $W = 1$ dans G_1 si et seulement si le mot $h^{-m}t^nh^p$ associé à W est le mot vide : le problème du mot est résolu.

Ce raisonnement montre en fait que toutes les relations vérifiées par h et t se déduisent formellement de la relation $hth^{-1}t^{-2} = 1$. On dit que G_1 est présenté par les éléments h et t soumis à la relation $hth^{-1}t^{-2} = 1$.

De manière générale, on dit que

$$G = < g_1, \ldots, \ g_k^{-1} \ / \ r_1, \ldots, r_q >,$$

où les r_j sont des mots en les g_i, est une présentation de G si G est engendré par des éléments g_i vérifiant les relations $r_j = 1$, et si toute relation entre les g_i se déduit formellement des relations $r_j = 1$ (plus précisément, G est isomorphe au quotient du groupe libre $F(g_1, \ldots, g_k)$ par le sous-groupe formé des produits de conjugués des r_j et de leurs inverses).

Fixons un entier m et demandons maintenant à une machine de montrer la relation $[h^mth^{-m}, t] = 1$ à partir de $hth^{-1}t^{-2} = 1$. C'est facile pour nous, qui pouvons voir que $h^mth^{-m} = t^{2^m}$. Mais pour la machine, le nombre d'opérations sera de l'ordre de 2^m, donc une fonction exponentielle de la longueur de $[h^mth^{-m}, t]$ (égale à $4m + 4$). Les mots $[h^mth^{-m}, t]$ étant représentatifs du cas général, G_1 vérifie une *inégalité isopérimétrique exponentielle*.

LA FONCTION DE DEHN

Étant donné une présentation finie

$$G = < g_1, \ldots, \ g_k^{-1} \ / \ r_1, \ldots, r_q >,$$

nous allons définir la *fonction de Dehn* $\varphi(n)$, dont la croissance détermine l'inégalité isopérimétrique vérifiée par G. Un remplacement tel que $a^{\pm1}b^{\pm1} \mapsto b^{\pm1}a^{\pm1}$ ou $ht^{-1} \mapsto t^{\pm2}h$ revient à multiplier le mot par un conjugué d'un $r_j^{\pm1}$, et un mot W est trivial dans G si et seulement si dans le groupe libre $F(g_1, \ldots, g_k)$ on peut écrire $W = \prod_{m=1}^{s} u_m r_{j_m}^{\pm1} u_m^{-1}$. Pour chaque mot trivial W, on considère le plus petit s possible, et $\varphi(n)$ est le maximum de ces s pour tous les mots triviaux de longueur $\leqslant n$.

La fonction de Dehn dépend de la présentation, mais la manière dont elle croît (quadratique, exponentielle, etc.) ne dépend que de G. Nous avons dit que φ est quadratique pour $\mathbf{Z}^2$ et exponentielle pour G_1 ; voici un exemple de φ linéaire.

Soit G_3 le groupe de présentation $< a, b, c, d \ | aba^{-1}b^{-1}cdc^{-1}d^{-1} >$ (groupe fondamental de la surface fermée orientable de genre 2). Étant donné un mot W en a, b, c, d, nous pouvons le raccourcir s'il contient plus de la moitié de la relation, ou de son inverse, à permutation circulaire près. On peut ainsi remplacer $aba^{-1}b^{-1}c$ par dcd^{-1}, $d^{-1}c^{-1}bab^{-1}$ par $c^{-1}d^{-1}a$, $dc^{-1}d^{-1}ab$ par $c^{-1}ba$, etc. On réduit alors le mot obtenu (si l'on peut) et on recommence autant que possible.

Dehn a montré (vers 1910) que dans G_3 cet algorithme, dit *algorithme de Dehn*, résoud le problème du mot : W représente 1 si, mais surtout *seulement si*, l'algorithme aboutit au mot vide. La longueur du mot diminuant à chaque itération, le nombre d'opérations est majoré par la longueur du mot : G_3 vérifie une *inégalité isopérimétrique linéaire*.

Les groupes dans lesquels le problème du mot se résoud par l'algorithme de Dehn (raccourcir le mot s'il contient plus de la moitié d'une relation) ont une fonction de Dehn au plus linéaire. Réciproquement, on montre qu'un groupe à fonction de Dehn au plus linéaire admet une présentation pour laquelle l'algorithme de Dehn s'applique. Ces groupes sont en fait les *groupes hyperboliques* définis par Gromov vers 1985 ; nous évoquerons ci-dessous leurs aspects géométriques.

Si G n'est pas hyperbolique, on montre que sa fonction de Dehn est au moins quadratique. Il n'y a en revanche pas de trou au-delà de l'exposant 2 : Brady et Bridson ont récemment montré que l'ensemble des α tels qu'il existe un groupe de fonction de Dehn équivalente à n^α est dense dans $[2, +\infty[$ (on notera que l'ensemble des classes d'isomorphisme de groupes de présentation finie est dénombrable, donc l'ensemble de ces α aussi).

Connaître explicitement la fonction de Dehn d'un groupe de présentation finie permet la résolution algo-

rithmique du problème du mot dans ce groupe : pour savoir si un mot W de longueur n est trivial, il suffit de le comparer à toutes les expressions $\prod_{m=1}^{s} u_m r_{j_m}^{\pm 1} u_m^{-1}$ avec $s \leqslant \varphi(n)$, qui sont en nombre fini (la longueur des mots u_m peut être bornée *a priori*). Inversement, un algorithme résolvant le problème permet de calculer φ.

On sait qu'il existe des groupes de présentation finie dans lesquels le problème du mot ne peut pas être résolu algorithmiquement, car la fonction de Dehn n'est pas récursive : elle croît tellement vite qu'aucun algorithme ne peut la calculer. Donc en toute généralité, on ne peut rien dire d'un groupe donné par générateurs et relations (même pas savoir si le groupe est trivial ou non...). Mais le plus souvent, toute information algébrique ou géométrique sur G, même minime, permet de l'analyser.

LE PLAN HYPERBOLIQUE H^2

Regardons par exemple le groupe G_3 d'un point de vue géométrique (comme le faisait Dehn). Essayons de construire un graphe comme pour $\mathbf{Z}^2$. Le graphe à considérer n'est plus de degré 4, mais de degré 8 : de chaque sommet partent 4 arêtes étiquetées a, b, c, d et il en arrive 4. Les mailles du grillage sont des octogones, correspondant à la relation $aba^{-1}b^{-1}cdc^{-1}d^{-1}$. On peut essayer de dessiner ce graphe, mais on manque très vite de place pour tracer 8 arêtes en chaque sommet : on ne peut pas paver le plan par des octogones réguliers. Ce graphe doit en fait être tracé non dans le plan euclidien mais dans le *plan hyperbolique* H^2.

Imaginons une piscine circulaire (plus mathématiquement, le disque unité ouvert D dans le plan) remplie d'un liquide visqueux, d'autant plus dense que l'on s'approche du bord : le coefficient de viscosité est proportionnel à $\dfrac{1}{1-r^2}$, où r est la distance euclidienne au centre du disque. On définit la distance (hyperbolique !) entre deux points x, y de D comme le temps nécessaire au lecteur pour nager de x à y.

Il existe toujours un plus court chemin de x à y (appelé géodésique), mais il ne nous apparaît pas comme rectiligne : il s'incurve vers le centre du disque pour pouvoir aller plus vite, tout comme un avion prend de l'altitude pour réduire la résistance de l'air. Les géodésiques sont en fait les arcs contenus dans des cercles perpendiculaires au bord de D, ainsi que les diamètres (noter que le bord de D est « à l'infini », on ne peut pas l'atteindre en un temps fini).

Comme le plan euclidien, le plan hyperbolique est un espace métrique homogène : on peut envoyer tout point sur tout autre point par une isométrie (en particulier, le « centre » de D ne joue pas un rôle particulier ; toute homographie du plan complexe qui envoie D sur lui-même induit une isométrie). Mais il est à courbure négative, alors que le plan euclidien est à courbure nulle et la sphère à courbure positive.

Escher a utilisé des pavages de H^2 par exemple, « Limite circulaire III » (figure 2) évoque un pavage par des triangles et quadrilatères réguliers, séparés par des lignes blanches géodésiques.

Figure 2 - *Le plan hyperbolique vu par M.C. Escher.*

Pour étudier G_3, on pave H^2 par des octogones réguliers dont les côtés sont des segments géodésiques de même longueur et dont les angles valent $2\pi/8$ (soit $45°$), de façon que 8 octogones se touchent en chaque sommet. Le graphe associé à un tel pavage est le « grillage » cherché pour G_3.

La fonction de Dehn de G_3 est ainsi linéaire car H^2 vérifie une inégalité isopérimétrique linéaire : on peut borner l'aire bordée par une courbe par une fonction linéaire de sa longueur. Par exemple, un disque de rayon R est d'aire $2\pi sh\, R$, comparable à son périmètre $2\pi(ch\, R - 1)$ (il vaut mieux faire des puzzles dans le plan hyperbolique : quand on a posé le bord, on a placé une proportion non négligeable des pièces).

La géométrie élémentaire dans H^2 réserve d'autres surprises. Ainsi, l'axiome des parallèles d'Euclide n'est pas vrai et la somme des angles d'un triangle ne vaut pas $\pi(= 180°)$: elle est égale à π moins l'aire du triangle (en particulier, l'aire d'un triangle est au plus π).

Une autre propriété fondamentale de H^2 est la finesse des triangles : il existe une constante δ (égale à $\log(\sqrt{2}+1)$) telle que tout point situé sur un côté d'un triangle à bords géodésiques est à distance au plus δ d'un point situé sur l'un des deux autres côtés. Cette propriété s'appelle *δ-hyperbolicité* ou simplement hyperbolicité.

Nous avons vu que le groupe $\mathbf{Z}^2$ « ressemble » au plan euclidien, alors que G_3 « ressemble » au plan hyperbolique. Suivant Gromov, on formalise cela en regardant un groupe G, muni d'un système fini S de générateurs, comme un espace métrique : la distance entre deux éléments g et h de G est la longueur minimale d'un mot (écrit avec les éléments de S) représentant $g^{-1}h$.

On visualise mieux cet espace « discret » en le considérant comme l'ensemble des sommets du *graphe de Cayley* de G : on place une arête entre deux sommets g, h si h s'obtient à partir de g par multiplication à droite par un élément de S, et on décrète que chaque arête est un segment de longueur 1. La distance entre deux points est simplement celle d'un chemin de longueur minimale les joignant (un tel chemin s'appelle encore géodésique).

Le graphe de Cayley du groupe libre G_2 est un arbre (il n'y a pas de boucle). Celui de $\mathbf{Z}^2$ est le grillage utilisé plus haut, avec la distance dite du chauffeur de taxi new-yorkais (noter qu'il existe en général plusieurs géodésiques entre deux points donnés). Cette distance n'est pas celle du plan euclidien (qui est le vol d'oiseau), mais elle lui est comparable : le rapport des deux distances est compris entre deux constantes strictement positives (ici 1 et $\sqrt{2}$). De même, le graphe de G_3 est formé des géodésiques délimitant les octogones du pavage de H^2 mentionné plus haut, avec une distance comparable à la distance hyperbolique.

On dit que G est un *groupe hyperbolique* s'il existe une constante δ telle que son graphe de Cayley soit δ-hyperbolique, c'est-à-dire si les triangles du graphe de Cayley, comme ceux de H^2, sont fins. Ainsi G_2 et G_3 sont hyperboliques, $\mathbf{Z}^2$ ne l'est pas (G_1 non plus).

Pour présenter nos exemples, nous avons toujours choisi le système de générateurs évident, le plus simple. Mais un groupe de type fini possède une infinité de systèmes générateurs, donc une infinité de graphes de Cayley différents, et il n'est pas évident qu'ils soient tous hyperboliques si l'un d'entre eux l'est.

En fait, tous ces graphes se ressemblent, de même qu'ils ressemblent à l'espace discret G considéré plus haut, tout comme le graphe de Cayley de $\mathbf{Z}^2$ ressemble au plan euclidien et celui de G_3 à H^2, la ressemblance devant être comprise comme une *quasi-isométrie*.

Deux espaces métriques X, Y sont quasi isométriques s'il existe une application $f : X \to Y$ et une constante $\lambda > 1$, telle que f ne distord pas trop les distances des points assez éloignés (le rapport entre $d_Y(f(x), f(x'))$ et $d_X(x, x')$ est compris entre $\frac{1}{\lambda}$ et λ si $d_X(x, x') > \lambda$) et f est presque surjective (toute boule de rayon λ dans Y contient un point de l'image).

Tout espace borné est quasi isométrique à un point, la quasi-isométrie est faite pour capturer des propriétés à l'infini (on dit *asymptotiques*) des espaces. Deux espaces (géodésiques) quasi isométriques sont simultanément hyperboliques ou non, ce qui légitime la définition d'un groupe hyperbolique donnée ci-dessus.

A un groupe de type fini est ainsi associé un espace métrique, bien défini à quasi-isométrie près. On peut en particulier parler de groupes quasi isométriques entre eux. Beaucoup de propriétés algébriques ou géométriques des groupes sont invariantes par quasi-isométrie : par exemple être fini, de présentation finie, contenir un sous-groupe commutatif d'indice fini, être hyperbolique, avoir une fonction de Dehn avec un type de croissance donné. De manière générale, on cherche à classifier les groupes à quasi-isométrie près.

Mentionnons simplement un récent résultat de rigidité dû à Farb et Mosher. Pour n entier $\geqslant 2$, soit H_n le sous-groupe de Aff($\mathbf{R}$) engendré par $x \mapsto x + 1$ et $x \mapsto nx$ (H_2 est donc le G_1 étudié plus haut). Si n est une puissance de m, alors H_n est un sous-groupe d'indice fini de H_m, il lui est donc quasi isométrique. Inversement, Farb et Mosher ont montré que H_n et H_m sont quasi isométriques si et seulement si n et m sont des puissances d'un même entier, et (essentiellement) qu'un groupe de type fini quasi isométrique à un H_n contient un sous-groupe d'indice fini isomorphe à un H_{n^p}.

POUR EN SAVOIR PLUS

Gersten (S.), Introduction to hyperbolic and automatic groups, Summer School in Group Theory in Banff, 1996, 45-70, CRM Proc. *Lecture Notes, 17, Amer. Math. Soc*., *Providence*, RI, 1999.

Ghys (E.), de la Harpe (P.) (éditeurs), Sur les groupes hyperboliques d'après Mikhael Gromov, *Progress in Mathematics 83*, Birhäuser.

Glass (A.), The ubiquity of free groups, *Math. Intelligencer* 14, n° 3, 54-57, 1992.

Valette (A.), Quelques coups de projecteurs sur les travaux de Jacques Tits, *Gazette des Mathématiciens* n° 61, 61-79, 1994.