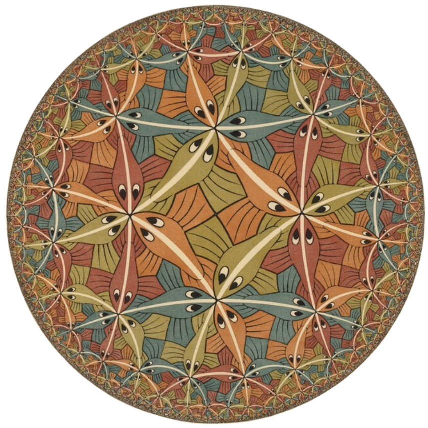
A Bit of Geometric Group Theory

by Gilbert Levitt



Maurits Cornelis Escher, *Circle Limit III*, Print, 1959

Discrete groups appear in every area of mathematics — and even in Escher's art. Even if they are defined algebraically, we often understand them better by their action on geometric objects. More and more often, they are viewed as geometric entities in their own right. Their properties are especially striking when the curvature is negative.

1. A Few Examples of Groups

We consider a group G, generally non-commutative. We will write it multiplicatively, with the neutral element denoted $\mathbf{1}_G$ or simply $\mathbf{1}$. Groups that will interest us most are finitely generated —that is, that is they can be generated by a finite number of elements. Let's take a look at a few examples.

- The *free abelian group* $\mathbb{Z}^2$, or $\mathbb{Z} \times \mathbb{Z}$, or $\mathbb{Z} \oplus \mathbb{Z}$, is the set of pairs of integers (m, n), with addition defined by $(m, n) + (m', n') = (m + m', n + n')$. To write it multiplicatively, let $a = (1, 0)$, $b = (0, 1)$, and view $\mathbb{Z}^2$ as the set of elements $a^m b^n$, equipped with the multiplication rule $(a^m b^n)(a^{m'} b^{n'}) = a^{m+m'} b^{n+n'}$. The neutral element $a^0 b^0$ is denoted $\mathbf{1}$, and the inverse of $a^m b^n$ is $a^{-m} b^{-n}$.
- Let us consider the group $\mathrm{Aff}(\mathbb{R})$ acting on the real line $\mathbb{R}$ by homotheties and translations — that is, the transformations of the form $x \mapsto a \cdot x + b$ with $a, b \in \mathbb{R}$ and $a \neq 0$, the product being given by composition $(f \circ g)(x) = f(g(x))$.

  This is a "continuous" group (a Lie group), but we can consider finitely generated subgroups, for example the group G_1 generated by $t : x \mapsto x + 1$ and $h : x \mapsto 2x$. One can deduce that G_1 is the set of transformations φ_{mnp} of the form $\varphi_{mnp}(x) = 2^m x + n2^p$, with $m, n, p \in \mathbb{Z}$ (see box).
- The group $\mathrm{GL}(n, \mathbb{R})$ of invertible (with determinant $\neq 0$) $n \times n$ matrices with real coefficients is also a Lie group.

  The matrices with integer entries do not form a subgroup, because the determinant appears in the denominator when computing the inverse of a matrix. However, $\mathrm{SL}(n, \mathbb{Z})$, the set of matrices with integer entries and determinant 1, is a subgroup.

We will consider the group $G_2 \subset \mathrm{SL}(n, \mathbb{Z})$ generated by

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

2. Free Groups

In a vector space V over a field K, the *vector subspace* generated by vectors $\{v_1, \ldots, v_k\}$ in V is the set of all linear combinations

$$\sum_{i=1}^{k} \lambda_i v_i,$$

with $\lambda_i \in K$. The elements $v_1, \ldots, v_k$ are *linearly independent* if any two different linear combinations represent different elements of V, or equivalently, if there is no relation

$$\sum_{i=1}^{k} \lambda_i v_i = 0$$

with the λ_i not all zero. The subspace generated has then dimension k and is isomorphic to K^k.

In a group G, the subgroup generated by $g_1, \ldots, g_k$ is the set of all elements of G that can be written as a reduced word $g_{i_1}^{n_i} \ldots g_{i_p}^{n_p}$, where the n_j are nonzero integers and $i_j \neq i_{j+1}$. For example, a^2, $b^{-1}c$, and $c^{-3}a^3b^2acb^{-5}$ are reduced words in a, b, c. Care must be taken not to forget the empty word, denoted 1, which represents the identity element 1_G. The length $|W|$ of a word W is the total number of letters, taking exponents into account, for example $|c^{-3}a^3b^2acb^{-5}| = 15$.

We say that elements $g_1, \ldots, g_k$ of G are *independent*[a] (or form a *free family*) if two different reduced words always represent two different elements of G, or equivalently, if there is no nontrivial relation $g_{i_1}^{n_1} \cdots g_{i_p}^{n_p} = 1$. Thus, the family g (consisting of the single element g) is free if and only if there is no nontrivial relation $g^n = 1$, that is, if g has infinite order.

In the examples above, the families $a, b \subset \mathbb{Z}^2$ and $h, t \subset G_1$ are not free, because of the relations $ab = ba$ and $hth^{-1} = t^2$.

We will, however, show — using the so-called ping-pong technique — that the matrices A and B are independent in $\mathrm{SL}(n, \mathbb{Z})$.

To this end, let us make $\mathrm{SL}(n, \mathbb{Z})$ act on $P = \mathbb{R} \cup \infty$ (the real projective line) by associating to the $\mathrm{SL}(n, \mathbb{Z})$-matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

the *homography* (or *projective transformation*)

$$h_M : x \mapsto \frac{ax + b}{cx + d}$$

---

[a]Often in the literature by indpendence of the collection $g_1, \ldots, g_k$ of elements of a group, another, in general strictly stronger, condition is meant, namely that no element is equal to a reduced word in other elements of the collection.

with the usual conventions, in particular $h_M(-d/c) = \infty$ and $h_M(\infty) = a/c$ if $c \neq 0$. The definition is made so that $h_{MN} = h_M h_N$ for all pairs of $\mathrm{SL}(n,\mathbb{Z})$-matrices M and N.

Let $P_A = (-1,1)$, and let P_B be the complement of $[-1,1]$ in P. We have $h_A(x) = x+2$, and therefore $h_A^n(P_A) \subset P_B$ for all $n \neq 0$. Similarly, $h_B(x) = x/(2x+1)$ and $h_B^n(P_B) \subset P_A$ for $n \neq 0$.[b] Let's now play ping-pong with P_A and P_B.

To show that A and B are independent, consider a nontrivial reduced word, for example $W = B^2AB^{-3}A^5$. Apply $h_W = h_B^2 h_A h_B^{-3} h_A^5$ to P_A. The element h_A^5 sends it into P_B, the element h_B^{-3} sends it back into P_A, and so on, and finally $h_W(P_A)$ is contained in P_A but not equal to it. This prevents h_W from being the identity, and therefore W from being equal to 1 in $\mathrm{SL}(2,\mathbb{Z})$.

This reasoning applies to any word W beginning with a power of B and ending with a power of A. The other cases are treated similarly: if W begins and ends with a power of A, we have $h_W \neq \mathrm{id}$ because $h_W(P_A) \subset P_B$; if W ends with a power of B, we apply h_W to P_B.

Since A and B are independent, every element of G_2 can be written uniquely as a reduced word in A and B. At this point we can forget that A and B are matrices and regard G_2 as the set $F(A,B)$ of reduced words in two abstract symbols A and B. Multiplication consists of concatenation and reduction; for example, $(B^2AB^{-3}A^5)(A^{-5}BA^4) = B^2AB^{-2}A^4$, and the inverse of $B^2AB^{-3}A^5$ is $A^{-5}B^3A^{-1}B^{-2}$.

We say that G_2 is the free group of rank 2, often denoted F_2. Similarly, we define F_n, the free group of rank n, for $n > 2$.

Many groups contain subgroups which are free groups. For example, one can show that two randomly chosen rotations of the sphere generate a free group, as do the transformations $x \mapsto x+1$ and $x \mapsto x^3$ on $\mathbb{R}$.

The group F_2 contains arbitrarily large free families: it is easy to see that the infinite family $A^nBA^{-n}{}_{n\in\mathbb{N}}$ is free, because the B's do not cancel when these elements are multiplied. The free group of rank 2 therefore contains free groups of any rank, and even groups that are not finitely generated. The Nielsen–Schreier theorem guarantees that every subgroup of a free group is free, that is, it is generated by a free family.

---

[b] Note also, that the inclusions $h_A^n(P_A) \subset P_B$ and $h_B^n(P_B) \subset P_A$ are strict.