Combinatorial Group Theory

Group Theory via Generators and Relations

B Sury

B Sury is with the School of Mathematics, TIFR, Mumbai.

Group theory revolutionized not only mathematics but also other sciences. A combinatorial way of describing groups is by what are called *generators and relations*. In this article, our purpose is to discuss this combinatorial way of describing groups and some of the immediate applications.

Introduction

The concept of groups surfaced with the fundamental works of the great mathematicians Evariste Galois and Niels Henrik Abel. The advent of group theory revolutionized not only mathematics but also the other sciences.

All of us learn in school, the method of 'completing squares' to solve quadratic equations and perhaps the more precocious ones get to see the formulae for cubic and biquadratic (i.e. fourth degree) equations too. The concept of *groups* surfaced with the fundamental works of the great mathematicians Evariste Galois and Niels Henrik Abel who showed that there is no such *general formula* to solve equations of degree higher than four. It is no exaggeration to say that their ideas revolutionized mathematics and shaped the future direction of algebra. Groups arise in a variety of situations as the group of symmetries of some system. In other words, they arise as the group of transformations of the objects of a system which leave the system as a whole invariant. Fifty years after Galois and Abel, the mathematician Felix Klein introduced his *Erlänger Programm* on the occasion of his admission to the University of Erlangen in 1872, towards a realisation of the fact that any geometry can be characterised by its group of transformations. Sophus Lie, a contemporary of Klein sought to throw light on the solutions of an ordinary differential equation which was invariant under a

group of continuous transformations. This theory, known as the theory of Lie groups has applications in numerous branches of mathematics. The advent of group theory revolutionized not only mathematics but also the other sciences. It was not long before it was realized that if groups are studied for their own sake, they would pay heavy dividends. A combinatorial way of describing groups is by what are called 'generators and relations'. This was first developed by W Van Dyck, a student of Klein. In this article, our purpose is to discuss this combinatorial way of describing groups and some of the immediate applications. For unexplained terminology and notation in what is to follow, the reader is encouraged to look up any standard book, such as Herstein's book on elementary algebra (See Suggested Reading).

The fact that all permutations of a set of objects are obtainable from successive interchanges of pairs of objects, can be restated as saying that a symmetric group is generated by its subset of transpositions.

Generators and Relations

A group G is *generated* by a subset S of its elements if every element of G is expressible as a product of elements from S and their inverses i.e. has an expression of the form $g_1^{a_1} \cdots g_k^{a_k}$ with $a_i = \pm 1$ and $g_i \in S$.

For instance, the fact that all permutations of a set of objects are obtainable from successive interchanges of pairs of objects, can be restated as saying that a symmetric group is generated by its subset of transpositions. Obviously, any group has a trivial set of generators viz. itself, but this is hardly of any use; one would like to have a nicer set of generators, preferably a finite set, if one exists. In the latter situation, one calls the group *finitely generated.*

Of course, a finite group is finitely generated. But, there are also several interesting infinite groups that are finitely generated. An obvious example is the additive group $\mathbb{Z}$ of integers; it is generated by the singleton $\{1\}$ (or $\{-1\}$, if you prefer it!)

More generally, for any n, the (so-called) free abelian group of rank n is the additive group $\mathbb{Z}^n := \{(a_1, \cdots, a_n) :$

$a_i \in \mathbb{Z}\}$; this is generated by the usual *basis vectors* $(1,0,\cdots,0),\cdots,(0,0,\cdots,1)$. This is an abelian group[1].

[1] The nomenclature abelian is after Abel and is another word for commutative.

But, there are also infinite nonabelian groups which are finitely generated. For example, look at the subgroup G generated by the matrices $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$ inside the group of all 2×2 invertible matrices. G is infinite as the powers $\begin{pmatrix}1 & 2n\\ 0 & 1\end{pmatrix}$ of $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ are distinct. G is clearly not abelian since $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$ do not commute(Here the group operation is matrix multiplication.).

Note that evidently a group must, at the least, be countable to be finitely generated. Even then, a finite set of generators is not guaranteed.

For instance, the additive group $\mathbb{Q}$ of rational numbers is infinitely generated. For, if $\frac{p_1}{q_1},\ldots,\frac{p_r}{q_r}$ is any finite set in $\mathbb{Q}$, the number $\frac{1}{2q_1\ldots q_r}$ is *not* in the group generated by $\frac{p_1}{q_1},\ldots,\frac{p_r}{q_r}$. (Why?)

Free Groups and the Ping-Pong Lemma

Any (finite) group can be viewed as a subgroup of the group of permutations of a (finite) set. Another way of viewing a group is as a quotient group of a *free group.*

Any (finite) group can be viewed as a subgroup of the group of permutations of a (finite) set. Another way of viewing a group is as a quotient group of a *free* group.

What is a free group? With a given set X of symbols, we first associate a bijective, disjoint set X' of symbols, whose elements will be denoted by x^{-1}. An expression of the form $x_1 \cdots x_n$ with $x_i \in X \cup X'$ is called a reduced word, if no x in X appears as a neighbour of x^{-1}. The set of reduced words can be multiplied in a natural way to get a group structure (for $u = x_1 \cdots x_n$ and $v = y_1 \cdots y_m$, the product $u \cdot v$ is obtained by writing the expression for v after that for u and cancelling off, successively, all pairs of the form xx^{-1} or $x^{-1}x$ occurring as neighbours). We get, then, the *free group* $F(X)$ *on the set* X where the empty word is the identity element. The cardinality of

X is called the rank of the free group. The rank is an invariant of the group i.e. free groups $F(X), F(Y)$ on sets X, Y are isomorphic if, and only if, the cardinalities of X and Y coincide, and is called the rank of the common group.

Now, for any group G, start with a set X of generators. It is easy to see that G is a quotient group of $F(X)$ i.e. that there is a surjective homomorphism from $F(X)$ onto G. For instance, the group $\mathbb{Z}^n$ of n-tuples of integers mentioned above, is the quotient of the free group F_n of rank n by its commutator subgroup. Recall that the commutator subgroup $[G, G]$ of any group G is defined as the subgroup of G generated by the *commutators* $[x, y] := xyx^{-1}y^{-1}$ of elements in G. Obviously, $\frac{G}{[G,G]}$ is an abelian group; it is called the abelianisation of G.

In the two examples of finitely generated, infinite groups above, the first one of $\mathbb{Z}^n$ is free only for $n = 1$ (as free groups are abelian only in rank one), while the second one is the free group of rank 2, on the two matrices there.

The proof that the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ generate a free group is easy and is a consequence of the following trick due to Klein generally known as *the Ping-Pong lemma*:

Suppose there are two nonempty subsets S_1, S_2 and a point p outside them such that two matrices g and h act as transformations on the set $S_1 \cup S_2 \cup \{p\}$ in such a way that $g(S_2 \cup p) \subset S_1$ and $h(S_1 \cup p) \subset S_2$. Then, no nonempty reduced word in g and h acts trivially on p i.e. g and h 'play ping-pong with the point p' between S_1 and S_2 !. Since the group generated by g and h is free precisely when no word in them is the identity word, it would follow that $< g, h >$ (the group generated by g and h)is free.

In our case, we can take $S_1 = \{z \in \mathbb{C} : -1 < Re(z) < 1\}$, $S_2 = \{z \in \mathbb{C} : \mid z \mid < 1\}$ and p any point outside the unit circle and with real part between -1 and 1, where the action of any 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is by the fractional

linear transformation $z \mapsto \frac{az+b}{cz+d}$. Thus, the two matrices above generate the free group of rank 2.

Presentations of Groups

We talked about generators but we did not say anything about the uniqueness of expressing an element in terms of a generating set. If $g = g_1^{a_1} \cdots g_k^{a_k} = h_1^{b_1} \cdots h_l^{b_l}$ are two different expressions in terms of elements g_i, h_i in a generating set S, there is, obviously, a relation of the form $s_1^{c_1} \cdots s_m^{c_m} = e$ among some elements s_i of S. Clearly, every finite group has relations among any generating set viz. the relation $s^{O(G)} = e$ for any s, where $O(G)$ denotes the number of elements in G.

Let us look at a group G defined by a finite set X of generators and a finite set of relations among them; we write $G =< X; R >$. One has to be careful while talking about *the set of relations.*

If $w = e$ is a relation (where w is a word in the generators), then, so are $w^k = e$ or $xwx^{-1} = e$. But, the latter are consequences of the former. It is in this sense that we say that a set R is a set of defining relations. In the language of free groups, $G =< X; R >$ means that $G \cong F(X)/N$ where N is the subgroup generated by all conjugates[2] of elements of R (i.e. N is called the *normal* subgroup generated in $F(X)$ by the set R). We call $< X; R >$ a *presentation* of G. If both X and R are finite, the group is said to be *finitely presented.* We have to bear in mind that there can be several presentations of the same group.

[2] Elements x and y of a group G are said to be conjugate if there exists z in G such that $x = zyz^{-1}$

Let $F = F(X)$ be a free group on a set X. If H is a subgroup of F, it is also free as can be proved naturally by the methods of algebraic topology. It was also proved by combinatorial group-theoretic methods by Nielsen and Schreier. The proofs also show that if X is a finite set of n elements, and if H is of finite index m in F, then the rank of H is $mn - (m - 1)$.

If $G =< X; R >$ is any group with X, R finite sets,

and H is a subgroup of G of finite index, does H have a finite presentation too, and, if so, how does one find it? Let $\{x_i\}_1^m$ be a set of left-coset representatives for H in G i.e. $G = \cup_1^m x_i H$, a disjoint union. Write $X = \{s_1, \cdots, s_n\}$ and $R = \{w_1, \cdots, w_r\}$ where w_i are words in the s_j. Now $G = F(X)/N$ where N is the normal subgroup of $F(X)$ generated by R. So, $H = E/N$ where $F(X) \supset E \supset N$. Since $[G : H] = [F(X) : E] = m$, E is a free group of rank $mn - (m-1)$ by the Nielsen-Schreier theorem. Thus, H itself is generated by $mn - (m-1)$ elements. It is also obvious that $H = E/M$ where M is the normal subgroup of E generated by the set $\{x_j^{-1} w_i x_j; j \leq m; i \leq r\}$ i.e. H has mr relations.

There is also a beautiful algorithm due to Coxeter, Moser and Todd to write down a presentation for H from one for G. The interested reader might refer to the book *Presentations of groups* by Johnson, published as lecture notes by the London Math. Society (See Suggested Reading).

If G is finitely generated and is also abelian, a fundamental structure theorem of Dedekind says that G is isomorphic to the group

$$\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$$

where the integers d_i divide d_{i+1} and are uniquely determined.

Here we adopt the convention that if $d = 1$, by $\mathbb{Z}/d$ we mean (0), and if $d = 0$, by $\mathbb{Z}/d$ we mean $\mathbb{Z}$. In particular, if G is any finitely generated group, the abelian group $G^{ab} := \frac{G}{[G,G]}$ has the structure asserted above.

The following is a nice way to find the invariants d_i. Let $G =< X; R >$ with $X = \{x_1, \cdots, x_m\}$ and $R = \{w_1, \cdots, w_n\}$. Now, each w_i is a word in the x's. Write M for the $m \times n$ integer matrix whose (i,j)-th entry m_{ij} is the sum of the powers of x_i occurring in the expression of w_j. Let $h_i(M)$ denote the G.C.D of all the $i \times i$ minors of M, for $i \leq k := min(m,n)$. Let $d_1 = h_1(M)$ and $d_i(M) = \frac{h_i(M)}{h_{i-1}(M)}$ $\forall i > 1$. Then, the invariants

What can one say about a finitely generated group where each element has finite order? Is such a group necessarily finite? This is the famous Burnside problem and the answer is negative even when the orders of all the elements are bounded by a fixed number.

of $\frac{G}{[G,G]}$ are $d_1, \cdots, d_k, 0, 0, \ldots, 0$ where $k = min(m,n)$ and 0 is repeated $m-k$ times. In other words, $\frac{G}{[G,G]} \cong \mathbb{Z}^{m-k} \times \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_k$. In particular, we notice that if $m > n$, then $m > k$ and so, $\frac{G}{[G,G]}$ is infinite.

This shows also that if $G =< X; R >$ is a *finite* group, then $m \leq n$ i.e. *the number of generators in any presentation of a finite group is at the most the number of relations* !

The Burnside Problem

What can one say about a finitely generated group where each element has finite order? Is such a group necessarily finite? This is the famous Burnside problem [3] and the answer is negative even when the orders of all the elements are bounded by a fixed number. However, it is very difficult to give such an example of a finitely generated, infinite group all of whose elements are of orders less than some fixed r.

But, there are positive results too. For instance, a group all of whose (nontrivial) elements are of order 2 is clearly abelian (because $x^2 = 1$ for all x means $x = x^{-1}$ i.e. $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$). So, if such a group were finitely generated also, then all the elements of the group are found among the finite set $x_1^{\pm 1} \cdots x_n^{\pm 1}$ where $x_1, \cdots, x_n$ is a set of generators for G.

Even those finitely generated groups all of whose elements have order ≤ 3 are necessarily finite (although nonabelian in general).

Consider a finitely generated group G consisting of matrices with entries in the complex field. If all matrices in G have finite orders, G is necessarily finite. The proof uses some sophisticated methods and we don't comment on it here. On the other hand, if the entries of the matrices in G are integers, instead of complex numbers, the proof is quite easy as we show now.

Note first that since $\det(g)$ and $\det(g^{-1}) = (\det(g))^{-1}$ are

[3] Work on problems related to this earned E I Zelmanov the Fields Medal in 1994.

both integers, we have $\det(g) = \pm 1$ for all $g \in G$. Call $GL(\mathrm{n}, \mathbb{Z}) := \{g : g_{ij} \in \mathbb{Z}, det(g) = \pm 1\}$.[4] So, our group G is a subgroup of $GL(\mathrm{n}, \mathbb{Z})$. Observe that if $g \in GL(n, \mathbb{Z})$ has order r, its eigen values are r-th roots of unity and, so, the minimal polynomial $P(X)$ of g divides the polynomial $X^r - 1$. As a result, it has distinct roots.; so g can be conjugated (by some complex matrix) to a diagonal matrix $\mathrm{diag}(\lambda_1, \cdots, \lambda_n)$ where λ_i are r-th roots of 1. (Why ?) Thus, the trace of g satisfies

$$\mid Tr(g) \mid = \mid \sum \lambda_i \mid \leq \sum \mid \lambda_i \mid = n$$

As $Tr(g)$ is an integer, the condition $\mid Tr(g) \mid \leq n$ implies that the possible values of $Tr(g)$ are among $\{n, n-1, \cdots, 0, -1, \cdots, -n\}$. To summarise, *any matrix of finite order* in $GL(n, \mathbb{Z})$ has trace in the finite set $\{0, \pm 1, \cdots, \pm n\}$. Let p be a prime not dividing $(2n)!$. Consider the finite group $GL(n, \mathbb{Z}/p)$ of $n \times n$ invertible matrices with entries in $\mathbb{Z}/p$. Look at the natural homomorphism obtained by reducing each entry mod p

$$\phi : GL(n, \mathbb{Z}) \rightarrow GL(n, \mathbb{Z}/p)$$

We claim that $G \bigcap Ker(\phi) = \{Id\}$ i.e. that $G \cong \phi(G)$. If $g \in Ker(\phi)$ has finite order, then $\overline{g_{ij}} = \overline{\delta_{ij}}$, where the 'bar' denotes mod p. So, $Tr(g) \equiv n \bmod p$. But $Tr(g) - n$ takes values in $\{0, -1, \cdots, -2n\}$ since $Tr(g)$ takes values in the set $\{0, \pm 1, \cdots, \pm n\}$. By the choice of p, this forces $Tr(g) = n$ i.e. $g = Id$. So, $\phi(G) \cong G$ and, therefore, $\mid G \mid \leq \mid GL(n, \mathbb{Z}/p) \mid$.

[4] Thus $GL(n, \mathbb{Z})$ is the collection of all $n \times n$ matrices with integer entries and determinant either +1 or −1.

Probability of Generating the Integers

We end with a *heuristic* discussion which can be made rigorous.

What is the 'probability' P that two randomly chosen integers generate $\mathbb{Z}$*?* Well, they generate *some* subgroup of $\mathbb{Z}$, at any rate. Overlooking the case that this subgroup is $\{0\}$ (surely an event of probability 0), this subgroup is

of $\mathbb{Z}$, at any rate. Overlooking the case that this subgroup is $\{0\}$ (surely an event of probability 0), this subgroup is $n\mathbb{Z}$ for some $n > 0$. The probability that both the integers belong to $n\mathbb{Z}$ is $\frac{1}{n^2}$. Since $n\mathbb{Z} \cong \mathbb{Z}$, P is also the probability that two elements of $n\mathbb{Z}$ generate it; and so $\frac{P}{n^2}$ is the probability that two random integers generate $n\mathbb{Z}$. Therefore, $\sum_{n=1}^{\infty} \frac{P}{n^2} = 1$ which gives $P = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n^2}}$.

On the other hand, two integers generate $\mathbb{Z}$ exactly when they are coprime. Since every pth integer is divisible by p, the 'probability' of a 'randomly' chosen integer being divisible by p can be taken to be $\frac{1}{p}$. Thus the probability that two independently chosen integers are both divisible by p is $\frac{1}{p^2}$; hence the probability that not both are multiples of p is $1 - \frac{1}{p^2}$. Therefore, the probability that they are coprime is the probability that not both of them are multiples of any prime i.e. $P = \prod_{p \text{ prime}}(1 - \frac{1}{p^2})$. We, thereby, get the 'Euler product formula'

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \prod_{p \text{ prime}} (1 - \frac{1}{p^2})^{-1}$$

However, we know that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, so that we finally have $P = \frac{6}{\pi^2}$.

A similar discussion can be made for any positive integer k in place of two integers. For $k = 1$, this probability is obviously 0 (as only ± 1 generate $\mathbb{Z}$); and is also $\prod_{p \text{ prime}}(1 - \frac{1}{p})$, on the other hand. This shows that $\prod_{p \text{ prime}}(1 - \frac{1}{p})^{-1}$ diverges i.e. the number of primes is infinite.

The discussion above was not rigorous as probability was not defined precisely. All of this can be done precisely, in terms of the notion of the *Haar measure* on a *profinite group* and (hopefully) this will be done in a follow-up article!

Suggested Reading

- I N Herstein. *Topics in Algebra.* Second edition. Vikas Publishing House, 1976.

For the uninitiated reader, who wants to look up standard notation and terminology used in elementary group theory, this book is a good source.

- D L Johnson. *Presentation of groups.* London Math. Soc. Lecture Note Series. No.22. Cambridge University Press.

Address for Correspondence
B Sury
School of Mathematics
Tata Institute of Fundamental Research, Homi Bhabha Road
Mumbai 400 005, India
email: sury@tifrvax.tifr.res.in