Journal of Examples and Computations

William Jones

August 30, 2023

For better or for worse, my perspective on mathematics leans towards the abstract—and as such, I sometimes avoid the (important) task of working carefully through examples, as well as coming up with concrete scenarios which both specialize and illustrate general proofs. To help me unlearn these habits, I was inspired by [?] and [?] to start an at-least-weekly record of concrete matters. As the project goes on, the flavor of the entries might change; right now I am trying to explicitly do some computations which I take for granted.

Since I learn best through teaching, I'm writing these entries as though someone is reading them. If someone actually is... hello! Apologies in advance ;-)

Contents

1 August 26, 2023: A Presentation of the Modular Group and Explicitly Computing a Free Subgroup

I've been learning some group theory; here's an example to make sure I understand what I've been learning. In this entry, I reproduce a half-remembered proof about the finite generation of $PSL(2, \mathbf{Z})$, and an interesting application of the theory of covering spaces to the theory of groups. The argument is from Stillwell '80, which among other things has taught me that this line of reasoning harks from the 1930's!

A Mobius transformation is a function $z \mapsto (az+b)/(cz+d)$ on $\mathbf{C} \cup \{\infty\}$; transformations satisfying $ad-bc = 1$ preserve the closed upper-half plane, so the group G of Mobius transformations modulo negation acts naturally on $\mathbf{H}$, the open upper-half plane of $\mathbf{C}$. Requiring a, b, c, d be in $\mathbf{Z}$ restricts our attention to a subgroup of G known as the **modular group**, often called $PSL(2, \mathbf{Z})$ as $SL(2, \mathbf{Z})/-SL(2, \mathbf{Z})$ acts via these transformations.

I've heard the following argument (or a sibling of it) is due to Serre, by which we will show that $PSL(2, \mathbf{Z})$ is generated by two elements: a translation and an involution:

$$T(z) = z + 1 \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad V(z) = \frac{-1}{z} \sim \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

To see why this is true, consider $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2, \mathbf{Z})$. The relation $ad - bc = 1$ implies that c and d are coprime, so we may use T to reduce d mod c so that the image of d is smaller than c. After all, $(T^k M)_{2,2} = d + kc$. We can then use V to switch $T^k M$'s columns (inverting the second, but this is no issue) and reduce c mod d'. Each step of this process strictly reduced the magnitude of the bottom-right entry of the matrix-at-hand and preserved coprimality of the bottom-row entries, so we can continue this process until $(T^{k_1} V T^{k_2} S \dots V T^{k_n} M)_{2,2} = 1$ (if this process produces a -1 entry, recall that we work in $PSL(2, \mathbf{Z})$, not $SL(2, \mathbf{Z})$). One more switch and translation yields:

$$T^{k_0} V T^{k_1} V T^{k_2} S \dots V T^{k_n} M = \begin{pmatrix} \alpha & \beta \\ 1 & 0 \end{pmatrix}$$

Since all these transformations preserve the magnitude of the determinant, it follows that $\beta = \pm 1$. If $\beta = 1$, a switch, translation, and switch reduces the matrix to I. If $\beta = -1$, a switch, translation, and switch reduces the matrix to V.

We have shown that every matrix in $PSL(2, \mathbf{Z})$ is row-reducible to either I or V using only T and V, which is exactly what we desired. These elements are famous for inducing a slick presentation of the modular group, namely:

$$PSL(2, \mathbf{Z}) \cong \left\langle T, V \,;\, V^2, (VT)^3 \right\rangle \cong C_2 * C_3$$

where $C_i = \langle a \,;\, a^i \rangle$. After all, in the presence of V the implied generator VT implies T. As such, it follows that we can construct a two-dimensional surface complex $\mathcal{C}$ whose fundamental group is $PSL(2, \mathbf{Z})$ whose 1-skeleton is two loops a and b based at a single vertex, then adjoining two 2-cells with boundaries a^2 and b^3. To construct a covering complex $\widetilde{\mathcal{C}}$ whose fundamental group is a subgroup H of $\pi_1(\mathcal{C})$, we start with a 0-skeleton of the cosets mod H, adjoining them in the 1-skeleton by the lifts of the loops of $\mathcal{C}$, and then attaching 2-cells as lifts of the 2-cells in $\mathcal{C}$.

To apply this theory, we claim that a subgroup of $PSL(2, \mathbf{Z})$ is $F_2 = \langle a, b \,;\, \varnothing \rangle$. Using the complex $\mathcal{C}$, we let G be $PSL(2, \mathbf{Z})$'s commutator (normal!) subgroup, and construct a covering complex $\widetilde{\mathcal{C}}$ so that $\pi_1(\widetilde{\mathcal{C}}) = G$. A presentation of $PSL(2, \mathbf{Z})$ allows us to easily describe G: it is all words in $PSL(2, \mathbf{Z})$ whose total a-exponent-sum is a multiple of two, and whose total b-exponent-sum is a multiple of three (elements of G are exactly those elements which are 0 mod G, which are those elements in $PSL(2, \mathbf{Z})$ which vanish if we pretend they commute). As such, there are six minimal coset representatives of G mod $PSL(2, \mathbf{Z})$:

$$\{1, a, b, b^2, ab, ab^2\}$$

These are the vertices of $\widetilde{\mathcal{C}}$. Adjoining the edges a, b, a^{-1} and b^{-1} to $\widetilde{\mathcal{C}}$'s vertices so that the edge x goes from g to gx, we obtain two b-cycle triangles adjoined at each vertex vertically by an a-cycle. To complete the complex, we adjoin cells on each cycle to obtain the covering complex $\widetilde{\mathcal{C}}$ in full. Immediate inspection shows that $\widetilde{\mathcal{C}}$ has a deformation retract to a bouquet of two circles, so we obtain the remarkable fact that we have sought: the commutator subgroup of $PSL(2, \mathbf{Z})$ is free of rank 2.

One final note: this result is massively generalized by the Kurosh Subgroup Theorem, which is why I chose it as an example to work out concretely.

2 August 28th, 2023: The Commutator of A Free Product of Cyclic Groups

This write-up is inspired by the previous one.

Let $C_n = \langle a \,;\, a^n \rangle$ be the cyclic group of order n. The commutator $[G, G]$ of a specified froup G has many equivalent definitions; one nice one is that $[G, G]$ is the smallest normal subgroup N of G for which G/N is commutative. In particular, if $G \cong \langle S \,;\, R \rangle$ and $[S, S]$ is the set of commutators of elements of S, then $[G, G] \cong \langle S \,;\, R \cup [S, S] \rangle$.

Proof. If $\langle\!\langle - \rangle\!\rangle$ denotes the normal closure, recall that $\langle S \,;\, R \cup T \rangle \cong \langle S \,;\, R \rangle / \langle\!\langle T \rangle\!\rangle$ (this could also be the definition of relators in a presentation). As such, we need only show that $[G, G] = \langle\!\langle [S, S] \rangle\!\rangle$; namely, that $\langle\!\langle [S, S] \rangle\!\rangle$ is the smallest normal subgroup whose quotient is commutative.

Suppose $N \triangleleft G$ has a commutative quotient. Then for each $s_1, s_2 \in S$, the commutator $[s_1, s_2] = 1$ in G/N, so is in N. It follows that $[S, S] \subseteq N$, so $\langle\!\langle [S, S] \rangle\!\rangle \triangleleft N$. Since $G/\langle\!\langle [S, S] \rangle\!\rangle$ is commutative:

$$\langle\!\langle [S, S] \rangle\!\rangle \subseteq \bigcap \{N : G/N \text{ is commutative}\} \subseteq \langle\!\langle [S, S] \rangle\!\rangle$$

So $[G, G] = \langle\!\langle [S, S] \rangle\!\rangle$.

□

It follows that the quotient of $C_n * C_m$ by its commutator is nothing but $C_n \times C_m$. This allows us to prove:

Theorem. *The commutator of $C_n * C_m$ is free of rank $(n-1)(m-1)$.*

Proof. Let K be the commutator of $C_n * Cm$. Let $\mathcal{C}$ be the two-dimensional complex whose 1-skeleton is a bouquet of two loops, with one 2-cell wound about the first loop n times, and the other 2-cell wound about the second loop m times. Of course, $\mathcal{C}$ was chosen so that $\pi_1(\mathcal{C}) \cong C_n * C_m$, so that we may realize a covering complex $\widetilde{\mathcal{C}}$ whose fundamental group is K.

Since K is normal, the 1-skeleton of $\widetilde{\mathcal{C}}$ is nothing but the Cayley diagram of $C_n * C_m$, which we have shown is $C_n \times C_m$. Cayley diagrams of products are products of the diagrams of the factors, so after attaching 2-cells according to the unique lifting requirement of the covering, we obtain a two-dimensional covering complex $\widetilde{\mathcal{C}}$ which is comprised of m copies of an n-gon, adjoined to each other along the vertices of n copies of an m-gon. To find the fundamental group, we observe that the n-gons are homotopy equivalent to points, so we consider an equivalent space of n copies of an m-gon, whose copied vertices

are all adjoined at a point. After contracting the m-gons to paths, it follows that $\widetilde{\mathcal{C}}$ is homotopy equivalent to a multiple-edged path on m vertices, with n edges between every pair of vertices. A spanning tree for this graph is a proper path with $n-1$ edges, so the total number of edges in the graph absent a spanning tree is $m(n-1)-(n-1) = (m-1)(n-1)$, which is the rank of the free fundamental group of the space. $\square$

I tried quickly doing a computation for the rank of the commutator of the free product of many cyclic groups, but that one is gonna take a little more work that I didn't want to do. It's essentially the same argument: construct a covering complex, and find a graph it's homotopy equivalent to. The graph will be an $(n-1)$-dimensional grid graph instead of a path (which is a one-dimensional grid graph), where each "axis" path will have the same multiplicity of edges counted by the order of the generator of the respective cyclic group. Multiply it all up, subtract the number of edges of a spanning tree (which can be found inductively), and you have your rank! There might be an easy algebraic argument to compute this I am not aware of. Maybe if I think of it, it'll be another entry.

3 August 30th, 2023: Applications of Conjugation: Dyck's Theorem and Commutators

I'm starting this entry with a quote from the last.

"If $\langle\langle - \rangle\rangle$ denotes the normal closure, recall that $\langle S \,;\, R \cup T\rangle \cong \langle S \,;\, R\rangle / \langle\langle T \rangle\rangle$"

In my mind, the notation $\langle S \,;\, R\rangle$ really is about a projection from a free group— which makes that "isomorphism" essentially a definition. However, the definition of $\langle S \,;\, R\rangle$ with more solidity is in terms of words and relations; specifically, a **word** in S is a formal product of elements in S and their formal inverses. A **reduced word in S relative to** R is a word in S with no occurrences of elements of R, nor pairs of the form ss^{-1} or $s^{-1}s$. Every word has a unique reduction (provable by induction), and two words can be multiplied by being put in sequence. All of this is to say, the referent of the symbol $\langle S \,;\, R\rangle$ is the collection of reduced words in S relative to R, imbued with a group structure given by word multiplication, followed by reduction.

With this definition, the above isomorphism is not entirely obvious, and will take a little work which I think illustrates a perspective on conjugation I was not given in my undergraduate:

1. Inserting a letter into a word is multiplication by a conjugate of that letter.
2. In particular, switching two consecutive letters in a word is multiplication by a conjugate of their commutator.

The first is illustrated by:

Theorem. *(Dyck's Theorem)* $\langle S \,;\, R\rangle \cong \langle S \,;\, \varnothing\rangle / \langle\langle R \rangle\rangle$.

Proof. Let $\langle S; \varnothing\rangle$ surject onto $\langle S; R\rangle$ by the identity function on words, which descends to an epimorphism φ. Clearly each $r \in \ker\varphi$, so that $\langle\langle R\rangle\rangle \subseteq \ker\varphi$. Conversely, if $\varphi(w) = 1$, there is a sequence of insertions and reductions of elements of R which take w to 1 *in the domain*, which is to say that there is a sequence of insertions of elements of $R \cup R^{-1}$ which takes w to 1 in $\langle S \,;\, \varnothing\rangle$.

Since inserting a letter into a word is multiplication by a conjugate of that letter, the above fact is expressed by the formula:

$$w \prod_{i=1}^{n} w_i r_i^{\epsilon_i} w_i^{-1} = 1$$

where $\epsilon_i = \pm 1$, and $w_i \in \langle S \,;\, \varnothing\rangle$. In other words, $w = \prod_{i=1}^{n} w_i r_i^{-\epsilon_i} w_i^{-1} \in \langle\langle R\rangle\rangle$. □

If we define F_S by its universal property, we obtain that every group is a quotient of a free group with next to no effort, but can't really say much about what we are quotienting by. Dyck's Theorem tells us: if we can find a presentation of a group, the normal closure of the relators is the subgroup of F_S which we quotient by.

The second perspective is also very helpful. In the last entry, I defined the commutator $[G, G]$ of a group G as the smallest subgroup whose quotient is commutative. Similarly to the previous example, we need to dip our toe into the combinatorial swamp to get our hands around what $[G, G]$ actually is.

Theorem. *The following subgroups of $G \cong \langle S; R\rangle$:*

1. $[G, G] := \{[g, h] : g, h \in G\}$
2. $\langle\langle [S, S] \rangle\rangle$
3. *The smallest normal subgroup of G whose quotient is commutative.*

are identical, and are called the commutator subgroup of G.

Proof. We prove that $(1) = (2)$, and $(2) = (3)$. We get that $(3) \subseteq (2)$ for free, and to see the converse we observe that any quotient $\langle S \,; R\rangle / H$ which is commutative must satisfy $[S, S] = \{1\}$. This and Dyck's theorem together imply that $\langle\langle [S, S] \rangle\rangle \subseteq H$, so that $\langle\langle [S, S] \rangle\rangle$ in particular is inside of (3).

We also get $(2) \subseteq (1)$ for free. To finish the proof, we recall that switching consecutive letters in a word amounts to multiplying by a conjugate of their commutator. This has a nice application in expressing commutators of products:

$$\begin{aligned}
[ab, c] &= abca^{-1}b^{-1}c^{-1} \\
&\to (ba)ca^{-1}b^{-1}c^{-1} \\
&\to b(ca)a^{-1}b^{-1}c^{-1} \\
&= bcb^{-1}c^{-1} \\
&\to (cb)b^{-1}c^{-1} \\
&= 1
\end{aligned}$$

where the arrows represent conjugation by a commutator. We unraveling this sequence to derive $[ab, c] = [a, b](b[a, c]b^{-1})[b, a]$, so that $[ab, c] \in \langle\langle [a, b], [a, c] \rangle\rangle$. The precise same reasoning generalize to any finite product of elements; this can be proved by induction in a few different ways.

To prove that $[g, h] \in \langle\langle [S, S] \rangle\rangle$ we write $g = \prod s_i^{\epsilon_i}$ and $h = \prod s_i'^{\epsilon_i'}$ and conclude from the above reasoning that $[g, h] \in \langle\langle [S, S] \rangle\rangle$. □

I got through group theory up to now by thinking of conjugation as the "next-best thing to commutativity;" this is a riff on that notion, but one that had not occurred to me before and one I thought worthwhile and interesting to write down.