MATH 3113 Notes #4

Dr. Day

3/15/19

1 Group presentations

1.1 Generators and Relations

We have worked with the symmetric group S_3 (order six, nonabelian) in the following guise: we let $a = (1, 2, 3)$ and let $b = (1, 2)$, and write the elements of S_3 as $\{1, a, a^2, b, ab, a^2b\}$. Computing in S_3 this way is aided by remembering the following equations: $a^3 = 1$, $b^2 = 1$, and $ba = a^2b$. Using these equations, any finite-length product of a, b, a^{-1}, and b^{-1} can be rewritten as one of the six elements above.

What we have secretly done is this: we have built a *group presentation* for S_3. We record this using the following notation:

$$S_3 = \langle a, b \,|\, a^3 = 1, b^2 = 1, ba = a^2b\rangle.$$

We say that the right side of the equation above is a *presentation* for S_3. The elements a and b are the *generators* in this presentation, and the equations $a^3 = 1, b^2 = 1$, and $ba = a^2b$ the *relations* in this presentation. This means the following:

- We have interpretations of a and b as elements of S_3.
- Every element of S_3 can be written as a finite-length product involving only the generators and their inverses.
- The relations are all true equations in S_3.
- Every true equation in S_3 is a consequence of the relations. This means that if two different finite-length products of generators represent the same element of S_3, then we can deduce this by repeatedly substituting the relations, and by using the usual rules for groups (associativity, $xx^{-1} = 1$, and $1x = x$).

As we have seen, it is much more convenient to compute in S_3 using these generators and relations, as opposed to simply computing using cycles to represent permutations. This is the point of presentations: they provide a simple framework for computing in a given group. Presentations can also be used to define and communicate examples of groups, and to perform many of tasks that we do in group theory (finding subgroups, checking for isomorphisms, building homomorphisms, and describing quotient groups). This motivates the following definitions.

Definition 1.1. Let G be a group, and let S be a subset of G. The *subgroup generated by* S, denoted $\langle S\rangle$, is the subset containing 1 and containing all finite-length products of elements of S and their inverses. If $\langle S\rangle = G$, then S is a *generating set* for G. Elements of a generating set are called *generators*.

It is straightforward to use the subgroup criterion to prove that, for any G and S as above, $\langle S\rangle$ is a subgroup of G.

In the following, we use S in a slightly different way. We think of S not as a set of group elements, but simply as a set. We think of the elements of S as being letters. Given a letter a, we can introduce a new symbol a^{-1} that we call the *formal inverse* of a. We are not thinking of a as being in a specific group, and we are not thinking of a^{-1} as denoting the inverse in that group. Rather, we think of a simply as being a symbol, and a^{-1} as being another symbol. Note: the formal inverse of a formal inverse is what we started with $(a^{-1})^{-1} = a$.

Definition 1.2. Let S be a set of letters. Let $S^{\pm 1} = S \cup \{a^{-1} \,|\, a \in S\}$, the union of S with the set of formal inverses of elements of S. A *word* in $S^{\pm 1}$ is a finite sequence of elements of $S^{\pm 1}$, written as a finite product (a *formal product*). By convention, the sequence of length zero is also a word, called the *empty word*, and is denoted by 1 or by ϵ.

A *relation* in S is an equation, where both sides of the equation are words in $S^{\pm 1}$. A *group presentation* with generators S and relations R is a pair $\langle S|R\rangle$, where R is a set of relations in S.

Now let G be a group. A *presentation for G* is a group presentation $\langle S|R\rangle$ together with an interpretation of S as elements of G, such that

- when thought of as elements of G, we have $\langle S\rangle = G$,
- every relation in R is a true equation in G, and
- every true equation in G, when written as an equation between words in $S^{\pm 1}$, follows from $1 = 1$ using group laws, multiplying both sides by the same element, and substitutions from equations in R.

Technically, an "interpretation" is a function $f\colon S \to G$, and the first condition means $\langle f(S)\rangle = G$. However, in practice, we simultaneously use S both to mean a set of letters and some elements of G.

Definition 1.3. A group G is *finitely generated* if there is a finite subset $S \subseteq G$ with $G = \langle S\rangle$.

A group G is *finitely presentable* if there is a presentation $G = \langle S|R\rangle$, where S and R are finite sets.

Many important groups are not finitely generated (for example, $\mathbb{Q}$ with $+$ is not finitely generated). There are also some groups that are finitely presentable but not finitely generated, but it is difficult to build such examples.

We give a list of examples of finite presentations for most of the finitely presentable groups that we have encountered so far. It is difficult to prove that a particular presentation for a particular group is correct, so we will postpone this until later.

- If G is the finite cyclic group of order n, then $G = \langle a \,|\, a^n = 1\rangle$. Here a can be any element of G that generates G as a cyclic group.
- If G is an infinite cyclic group, then $G = \langle a|\varnothing\rangle$. This means that G has a as a generator and has an empty set of relations. The equations using a that are true in G are exactly the ones that are consequences of the group axioms. Again, we must identify a with one of the two generators of G.
- The non-cyclic group of order 4 has the presentation
  $$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a, b \,|\, a^2 = 1, b^2 = 1, ab = ba\rangle.$$
  Here we identify a and b with $(1, 0)$ and $(0, 1)$ (although there are other choices that will work).
- We have
  $$\mathbb{Z} \times \mathbb{Z} = \langle a, b \,|\, ab = ba\rangle.$$
  Again, we identify a and b with $(1, 0)$ and $(0, 1)$ (although again, there are other choices that will work).
- For every n, the dihedral group D_n (of order $2n$) has the presentation
  $$D_n = \langle a, b \,|\, a^n = 1, b^2 = 1, ba = a^{-1}b\rangle.$$
  Here a is an order-n rotation of the regular n-gon, and b is a reflection through the center of the regular n-gon (there are n choices for b that will work).
- The quaternion group Q_8 of order 8 has the presentation
  $$Q_8 = \langle i, j \,|\, i^4 = 1, j^2 = i^2, ij = ji^{-1}\rangle.$$

The examples above are good for computation because the sets of generators and relations are small. Sometimes it can be useful to know about a presentation, even if that presentation is too large to use for computation. For example, the following proposition immediately implies that every finite group is finitely presentable.

Proposition 1.4. *Let G be a group with identity e. Let $S = G \setminus \{e\}$ and let R be the set of true relations in S of the forms $ab = c$ or $ab = 1$, where $a, b, c \in S$. (So R records the entire multiplication table of G.) Then $G = \langle S|R\rangle$.*

Proof. Since $S \subset G$, we use the natural interpretation of each element of G as being itself. Notice that $\langle S \rangle = G$, since every nontrivial element of G can be written as a product of length 1 (and the identity is aa^{-1} for any $a \in S$). All the relations in R are true.

Finally, we want to show that all true equations in G are consequences of R. Let $u = v$ be such an equation. First we note that we can assume that all the letters appearing in u and v are in S (and not formal inverses). We do this by substituting equations of the form $ab = 1$ to replace any formal inverse with a letter from S.

The length $|w|$ of a word w is the total number of letters appearing in the word, counting repeats. (Note: the length of 1 is 0, since it represents the empty word.) We work by induction on $\max\{|u|, |v|\}$ to show that $u = v$ is a consequence of R. If this maximum is 1 or 0, then the equation is trivial, and therefore a consequence of R (trivially). This is the base case of the induction.

For the general case, we assume that the maximum length is 2 or more. Again we assume that all letters are in S. Then we can find a subword of the longer of u or v of the form ab, where $a, b \in S$. Then we find $c \in S \cup \{1\}$ with $ab = c$ in R, and substitute to replace ab with c. Since the length of the longer word has gone down, we inductively assume that the new equation is a consequence of R. Then the original equation was also a consequence of R. □

Proposition 1.5. *Fix a positive integer n. Let S be set of transpositions in S_n, and let R be the set of equations of the following forms:*

- *If $\sigma \in S$, then $\sigma^2 = 1$.*
- *If $\sigma, \tau \in S$ and σ and τ are disjoint, then $\sigma\tau = \tau\sigma$.*
- *If $\sigma, \tau \in S$, and there are numbers i, j, k with $\sigma = (i, j)$ and $\tau = (i, k)$, then $\sigma\tau = (j, k)\sigma$.*

Then $S_n = \langle S | R \rangle$.

The method used to prove Theorem 2.3.11 in the book can be used to prove this proposition. The fact that all the relations in R above have even length implies that the parity (even versus odd) of a permutation in S_n is well defined. The symmetric groups do have shorter presentations than the one in this proposition, but this presentation is still sometimes useful.

1.2 Trouble with presentations

Suppose somebody gives you an example of a group by writing down a presentation. Should you believe that such a group exists? In fact, such groups always exist, as we show in Theorem 3.2 in the last section below. However, it can be difficult to determine basic facts about a group by using a presentation. For one thing, it can be difficult to determine when different words represent different elements of a group. As a silly example of this, consider the presentation $\langle a, b \,|\, a = b \rangle$. Then a and b are different letters, but both represent the same element of this group (this is a presentation for $\mathbb{Z}$). Further, ab^{-1} is a word representing the identity, but is not the empty word.

A more serious problem is that it can often be difficult to tell whether a group with a given presentation is the trivial group or not. For example, the following is a non-obvious presentation for the trivial group:

$$G = \langle a, b \,|\, a^2 = b^3, a^3 = b^5 \rangle.$$

To see this, we compute:

$$a = a^{10}a^{-9} = (a^2)^5(a^3)^{-3} = (b^3)^5(b^5)^{-3} = b^{15}b^{-15} = 1.$$

Similarly,

$$b = b^{10}b^{-9} = (b^5)^2(b^3)^{-3} = (a^3)^2(a^2)^{-3} = a^6a^{-6} = 1.$$

Since G is generated by a and b, and since these relations force a and b to be different names for 1, it follows that $G = \{1\}$. There are many other examples of non-obvious presentations for the trivial group. There is a technical sense in which it is impossible to always be able to tell if a presentation gives a nontrivial group.

There are other questions about groups that cannot be computed using presentations, however, there are certain tasks that become much easier using presentations. For example, presentations make it easy to build homomorphisms between groups, and to describe quotients of groups.

2 Working with presentations

2.1 Building and bootstrapping presentations

We verify the presentation of an infinite cyclic group, and then look into several tricks for finding presentations.

Proposition 2.1. *The presentation $\mathbb{Z} = \langle a | \varnothing \rangle$ is correct.*

Proof. We identify a with 1. Since $\langle 1 \rangle = \mathbb{Z}$, the statement about generators in the definition of presentation is true. There are no relations, so it is vacuously true that every relation is a true equation. Finally, suppose $u = v$ is an equation in words in $\{a, a^{-1}\}$ that is true in $\mathbb{Z}$. This means that the sums of the exponents of a in u equals the sums of the exponents of a in v. Then by using associativity and cancelling inverses, we can change the equation into $a^k = a^k$. Since this equation follows from $1 = 1$ by multiplying both sides by a^k, we are done. □

Proposition 2.2. *If G is isomorphic to H and $\langle S|R \rangle$ is a presentation for G, then $\langle S|R \rangle$ is also a presentation for H.*

Proof. Let $\phi\colon G \to H$ be such an isomorphism. The interpretation of S in G is a function $f\colon S \to G$. We use the function $\phi \circ f\colon S \to H$ to interpret S with in

H. Since $\langle f(S)\rangle = G$ and ϕ is an isomorphism, we have $\langle \phi \circ f(S)\rangle = H$. Since ϕ is an isomorphism, the true equations in G are exactly the same as the true equations in H. Therefore the presentation is correct. □

Proposition 2.3. *Suppose G is a group with presentation $\langle S|R\rangle$, and G has a normal subgroup N. Suppose $T \subset N$ with $\langle T\rangle = N$. We write each $a \in T$ as a word w_a in $S^{\pm 1}$. Let R' consist of all the equations $w_a = 1$ for $a \in T$. Then $\langle S|R \cup R'\rangle$ is a presentation for G/N.*

Proof. The interpretation of elements of S in G/N comes via the quotient projection $\pi\colon G \to G/N$. Since π is a surjective homomorphism, $\langle \pi(S)\rangle = G/N$. Since π is a homomorphism, all the equations in R are true in G/N. Every equation in R' is of the form $w_a = 1$ for $a \in T$. This $a \in T$ is in N, and therefore $\pi(a) = 1$. So $a = 1$ is true, interpreted in G/N.

Now suppose $u = v$ is a true equation in G/N. Interpreting S in G, we get that $v^{-1}u$ is an element of G. Then $\pi(v^{-1}u) = 1$, since $u = v$ in G/N, This means that $v^{-1}u \in N$ (since N is the kernel of π). We express $v^{-1}u$ as a product $a_1 \cdots a_k$ of elements of $T^{\pm 1}$, which is possible since $\langle T\rangle = N$. Then $u = vw_{a_1} \cdots w_{a_k}$ is a true equation in G. Since $\langle S|R\rangle$ is a presentation for G, this equation is a consequence of R. Since $u = v$ is a consequence of R' and $u = vw_{a_1} \cdots w_{a_k}$, it follows that $u = v$ is a consequence of $R \cup R'$, and the presentation for G/N is correct. □

In fact, the condition that T generates N can be weakened to the condition that T *normally generates* N in G. This means that N is generated by the set of all elements of the form bab^{-1}, where $a \in T$ and $b \in G$.

As a quick consequence of Proposition 2.3 and Proposition 2.1, we see that $\mathbb{Z}_n$ has the presentation $\langle a|a^n = 1\rangle$ for each positive integer n.

Next we consider how to build a presentation for a group if we know presentations for a normal subgroup and its quotient. Suppose G is a group and N is a normal subgroup of G. Let $\pi\colon G \to G/N$ be the quotient projection. Suppose N has the presentation $\langle S_N|R_N\rangle$, and G/N has the presentation $\langle S_Q|R_Q\rangle$.

To build a presentation for G out of this, we start by *lifting* generators from S_Q to G. This means, for each $a \in S_Q$, thought of as an element of G/N, we select an element $\tilde{a} \in G$ such that $\pi(\tilde{a}) = a$. Of course, this can be the element that we originally used to write the coset, or it can be any of the other elements of the coset. We define S'_Q to be the collection of lifts we selected, one for each element of S_Q. We write $\tilde{a}$ for our chosen lift of a. Our generators for our presentation will be $S_N \cup S'_Q$.

Finding relations is a little more difficult. First of all, relations in R_N are still true in G, and we will include them in our presentation. For a relation $u = v$ in R_Q, we can lift both sides to get an element $\tilde{v}^{-1}\tilde{u}$ in G. (This means that for each $a \in S_Q$ appearing in u or v, we substitute $\tilde{a} \in S'_Q$.) Although $\pi(\tilde{v}^{-1}\tilde{u}) = v^{-1}u = 1$ in G/N, it may be that $\tilde{v}^{-1}\tilde{u}$ is a nontrivial element of G. However, we know $\tilde{v}^{-1}\tilde{u}$ is in the kernel of π, which is N. So to get a relation for G, we pick a word $w_{u,v}$ in $S_N^{\pm 1}$ representing $\tilde{v}^{-1}\tilde{u}$. Then the equation $\tilde{u} = \tilde{v}w_{u,v}$

will be true in G. We carry this out for every relation in R_Q, and collect these relations together in a set we call R'_Q.

Still, it turns out that $R_N \cup R'_Q$ is not enough relations for G. Since N is a normal subgroup of G, whenever we conjugate an element of S_N by an element of $(S'_Q)^{\pm 1}$, we get a new element of N. For each $a \in S_N$ and each $b \in (S'_Q)^{\pm 1}$, we choose a word $u_{a,b}$ in $S_N^{\pm 1}$ with $bab^{-1} = u_{a,b}$, and we record all these equations as relations in a set R''.

Proposition 2.4. *Suppose N is a normal subgroup of G with $N = \langle S_N | R_N \rangle$ and $G/N = \langle S_Q | R_Q \rangle$. Select lifts S'_Q of S_Q in G and select relations R'_Q and R'' as described in the preceding paragraphs. Then*

$$G = \langle S_N \cup S'_Q \,|\, R_N \cup R'_Q \cup R'' \rangle.$$

Proof. First we explain why $S_N \cup S'_Q$ generates G. Let $g \in G$. Then $\pi(g) \in G/N$. Since S_Q generates G/N, there is a word v_g in $S_Q^{\pm 1}$ that represents $\pi(g)$. Let $\tilde{v}_g$ be the corresponding lifted word in $(S'_Q)^{\pm 1}$. Then $\pi(\tilde{v}_g) = v_g$, so $g\tilde{v}_g^{-1}$ is in N, the kernel of π. Since S_N generates N, $g\tilde{v}_g^{-1}$ is equal to a word in $S_N^{\pm 1}$, and it follows that g can be expressed as a word in $(S_N \cup S'_Q)^{\pm 1}$.

It is easy to see from the definitions above that all the relations in $R_N \cup R'_Q \cup R''$ are true in G.

Next we explain why every true equation in G is a consequence of these relations. (This part is a little sketchy; you can fill in the details yourself.) Suppose $u = v$ is a true equation using letters in $S_N \cup S'_Q$. By replacing u with $v^{-1}u$, we can assume that $v = 1$, so that our equation has the form $u = 1$. We use relations from R'' to move generators from $S_N^{\pm 1}$ to the left, until we have rewritten our equation as $u_N \tilde{u}_Q = 1$, where u_N is a word in $S_N^{\pm 1}$ and $\tilde{u}_Q$ is a word in $(S'_Q)^{\pm 1}$. The map π sends $u_N \tilde{u}_Q$ to the word u_Q in $S_Q^{\pm 1}$, where $\tilde{u}_Q$ is the lift of u_Q, since u_N is in N and π sends N to 1. So $u_Q = 1$ is a true equation in G/N, and is a consequence of the relations in R_N. Applying the lifts of these relations to $u_N \tilde{u}_Q = 1$ will change it into an equation of the form $u_N v = 1$, where v is a word in $S_N^{\pm 1}$. Then finally, $u_N v = 1$ is a true equation in N, and is therefore a consequence of relations in R_N. □

We can use Proposition 2.4 to get a presentation for S_3. Let $N = \langle (1,2,3) \rangle$. Since N has index 2 in S_3, N is a normal subgroup of S_3. Since $|N| = 3$ and 3 is prime, we know that $N = \langle a | a^3 = 1 \rangle$. Here we interpret a as $(1,2,3)$. Since $|S_3/N| = 2$ and 2 is prime, we know that $S_3/N = \langle c | c^2 = 1 \rangle$.Here we interpret c as the coset $(1,2)N$.

We use the procedure above to find a presentation for S_3. (In the notation above, $S_N = \{a\}$, $R_N = \{a^3 = 1\}$, $S_Q = \{c\}$, and $R_Q = \{c^2 = 1\}$.) We pick $b = (1,2)$ as our lift of c. We lift the relation $c^2 = 1$ to the relation $b^2 = 1$ (this is valid because $(1,2)^2 = 1$ in S_3). We must also add relations for conjugation. We check that $(1,2)(1,2,3)(1,2)^{-1} = (1,3,2)$ and $(1,2)^{-1}(1,2,3)(1,2) = (1,3,2)$. Rewriting these equations in terms of a and b, we get the following presentation:

$$S_3 = \langle a, b \,|\, a^3 = 1, b^2 = 1, bab^{-1} = a^2, b^{-1}ab = a^2 \rangle.$$

This presentation is correct, but it has an extra equation that we don't need. We explain how to get rid of this in the next section.

2.2 Rewriting presentations

The following rules for rewriting presentations are called *Tietze transformations.* Suppose we have a presentation $G = \langle S|R\rangle$, and we want to build a new presentation $\langle S'|R'\rangle$ for the same group G.

1. *Adding a generator.* Suppose g is an element of G. Find a word w in $S^{\pm 1}$ representing g, and pick a letter t not appearing in S. We may then add t to S and add the relation $t = w$ to R; so $S' = S \cup \{t\}$ and $R' = R \cup \{t = w\}$.

2. *Deleting a generator.* Suppose $t \in S$ and t appears in exactly one relation in R. Further suppose that this relation has the form $t = w$ for some word w not involving t or t^{-1}. Then we may delete t from S and delete $t = w$ from R; so $S' = S \setminus \{t\}$ and $R' = R \setminus \{t = w\}$.

3. *Adding a relation.* Suppose $v = w$ is any relation using S that is a true equation in G. Then we may add it to R, so that $S' = S$ and $R' = R \cup \{v = w\}$.

4. *Deleting a relation.* Suppose $v = w$ is a relation in R and $v = w$ is a consequence of relations in $R \setminus \{v = w\}$. Then we may delete it from R, so that $S' = S$ and $R' = R \setminus \{v = w\}$.

Proposition 2.5. *Suppose $G = \langle S|R\rangle$, and $\langle S'|R'\rangle$ comes from $\langle S|R\rangle$ from one of the four Tietze transformations above. Then $\langle S'|R'\rangle$ is another presentation for G.*

Proof. In each case, the setup quickly implies that the second presentation satisfies the definition for a presentation of G. We show this only for the third case (adding a relation). In this case, $S = S'$, so S' generates G because S does. Every relation in R' is in R, except for the relation $v = w$. Since $\langle S|R\rangle$ is a presentation for G, this means that all the other relations of R' are true equations in G, and $v = w$ is one by hypothesis. So all relations in R' are true equations. Now suppose that $w_1 = w_2$ is a true equation in G. Since this is a consequence of R, and $R \subset R'$, this is also a consequence of R'.

The remaining cases are exercises. □

To illustrate these transformations, we first simplify the presentation for S_3 above. We start with

$$S_3 = \langle a, b \,|\, a^3 = 1, b^2 = 1, bab^{-1} = a^2, b^{-1}ab = a^2\rangle.$$

First we notice that the last relation is a consequence of the preceding relations. Start with the third relation $bab^{-1} = a^2$. By the second relation, we can insert a b^2 or a b^{-2} wherever we like. So we derive $b^{-2}bab^{-1}b^2 = a^2$, which simplifies to the last relation. So by a Tietze transformation, we can delete it, and get:

$$S_3 = \langle a, b \,|\, a^3 = 1, b^2 = 1, bab^{-1} = a^2 \rangle.$$

Next we point out that the third relation is easily equivalent to the equation $ba = a^2b$ (multiply both sides on the right by b to get this). Since $ba = a^2b$ follows from the relations, it is a true equation, and we can add it to the presentation. After adding it, we have that $bab^{-1} = a^2$ is a consequence of $ba = a^2b$, and so we can delete it. This gives us our preferred form of the presentation:

$$S_3 = \langle a, b \,|\, a^3 = 1, b^2 = 1, ba = a^2b \rangle.$$

As a second example, we turn this presentation into one that looks really different. First we add a generator by letting the letter t (which does not appear in this presentation) denote the element ab (which is $(1, 2, 3)(1, 2)$, or just $(1, 3)$). So we have

$$S_3 = \langle a, b, t \,|\, a^3 = 1, b^2 = 1, ba = a^2b, t = ab \rangle.$$

Then $a = tb^{-1} = tb$, so we add the relation $a = tb$. Then $t = ab$ is a consequence of this, so we can delete it. We add $(tb)^3 = 1$ and $btb = tbt$, which come from the first and third relations after substituting $a = tb$ (and we use $b^2 = 1$ to simplify after we substitute). Since $a^3 = 1$ and $ba = a^2b$ are then easy consequences of these relations, we can delete them. We get

$$S_3 = \langle a, b, t \,|\, (tb)^3 = 1, b^2 = 1, btb = tbt, a = tb \rangle.$$

Since a appears in only one relation, where a is expressed in terms of other generators, we can delete it. We make one last change to the presentation. Note that in the presence of $(tb)^3 = 1$ and $b^2 = 1$, we have

$$btb = tbt \iff btbbtb = (tb)^3 \iff btbbtb = 1 \iff tb^2t = b^{-2} \iff t^2 = 1.$$

So we can add $t^2 = 1$ to the presentation and delete $btb = tbt$. We finally get

$$S_3 = \langle b, t \,|\, b^2 = 1, t^2 = 1, (tb)^3 = 1 \rangle.$$

This is a presentation for S_3 that looks really different from the one we found earlier.

Now that we have Tietze transformations, we can prove an easy special case of Proposition 2.4.

Corollary 2.6. *Suppose $G = \langle S_G | R_G \rangle$ and $H = \langle S_H | R_H \rangle$. Define*

$$R = \{ab = ba \,|\, a \in S_G, b \in S_H\}.$$

Then $G \times H = \langle S_G \cup S_H | R_G \cup R_H \cup R \rangle$.

Proof. We have a normal subgroup $N = G \times \{e_H\}$ in $G \times H$. We have $N \cong G$ and $(G \times H)/N \cong H$ (it is easy to prove these facts by the definitions or by using theorems about homomorphisms applied to the first coordinate projection). We carry out the procedure in Proposition 2.4. We lift every generator b in H to $\tilde{b} = (e_G, b)$ in $G \times H$. We interpret every generator a in G as (a, e_H) in $G \times H$. Our relations in R_H lift to the same relations in $G \times H$ (we do not need to modify them by an element of the kernel). This is because $\tilde{w}$ is (e_G, w), and $\tilde{w}$ is trivial if and only if w is. For every $b \in S_H$ and $a \in S_G$, we have $a\tilde{b}a^{-1} = \tilde{b}$ and $a^{-1}\tilde{b}a = \tilde{b}$. These relations must be added to the presentation, but then using Tietze transformations, we can add relations $a\tilde{b} = \tilde{b}a$, and delete the conjugation relations. The corollary follows by simply relabeling each $\tilde{b}$ as b. □

Given what we have already said, this corollary immediately implies the presentations

$$\mathbb{Z} \times \mathbb{Z} = \langle a, b | ab = ba \rangle \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a, b | a^2 = 1, b^2 = 1, ab = ba \rangle.$$

2.3 Presentations and homomorphisms

Proposition 2.7. *Let $G = \langle S | R \rangle$ and let H be another group. Suppose $f \colon S \to H$ is a function. Suppose that for every relation $u = v$ in R, we get a true equation in H when we substitute $f(a)$ for a for every $a \in S$. Then there is a unique homomorphisms $\phi \colon G \to H$, such that $\phi(a) = f(a)$ for every $a \in S$.*

Proof. We define ϕ on $g \in G$ as follows. Since S generates g, we can find $a_1, \ldots, a_k \in S$ and $p_1, \ldots, p_k \in \{1, -1\}$ such that $g = a_1^{p_1} \cdots a_k^{p_k}$. We define $\phi(g) = f(a_1)^{p_1} \cdots f(a_k)^{p_k}$.

We first need to show that ϕ is well defined. Suppose $b_1, \ldots, b_m \in S$ and $q_1, \ldots, q_m \in \{1, -1\}$ such that $g = b_1^{q_1} \cdots b_m^{q_m}$. Then $a_1^{p_1} \cdots a_k^{p_k} = b_1^{q_1} \cdots b_m^{q_m}$ is a true equation in G, and therefore is a consequence of relations in R. We then substitute $f(a_i)$ for each a_i and $f(b_i)$ for each b_i. By our hypothesis, this gives us a true equation in H for each relation, and therefore $f(a_1)^{p_1} \cdots f(a_k)^{p_k} = f(b_1)^{q_1} \cdots f(b_m)^{q_m}$ is a true equation in H. But this says that $\phi(g)$ is the same, no matter which word we use to represent g.

Now suppose $g, h \in G$. We write $g = a_1^{p_1} \cdots a_k^{p_k}$ and $h = b_1^{q_1} \cdots b_m^{q_m}$, where these are words in $S^{\pm 1}$. Then $gh = a_1^{p_1} \cdots a_k^{p_k} b_1^{q_1} \cdots b_m^{q_m}$. By the definition of ϕ, we have that both $\phi(gh)$ and $\phi(g)\phi(h)$ are $f(a_1)^{p_1} \cdots f(a_k)^{p_k} f(b_1)^{q_1} \cdots f(b_m)^{q_m}$. This shows that ϕ is a homomorphism.

It is immediate from the definition that $\phi(a) = f(a)$ for every $a \in S$. To show uniqueness, suppose ψ is another homomorphism with this property. Then for any $g \in G$, we write $g = a_1^{p_1} \cdots a_k^{p_k}$, and then $f(a_1)^{p_1} \cdots f(a_k)^{p_k}$ equals both $\phi(g)$ and $\psi(g)$. This means $\phi = \psi$. □

Proposition 2.7 can be useful to show that a presentation represents a nontrivial group. For example, consider

$$G = \langle a, b \,|\, a^7 = 1, b^3 = 1, bab^{-1} = a^2 \rangle.$$

By using the relations, we can rewrite any element of this group as one of the 21 elements $\{1, a, \ldots, a^6, b, ba, \ldots, ba^6, b^2, b^2a, \ldots, b^2a^6\}$. However, nothing about this guarantees that the any of these elements are nontrivial—in theory, there could be an equation $a = 1$ that is a consequence of the relations in a complicated way. So to be sure that these elements are nontrivial, we build a nontrivial homomorphism to another group.

Using Proposition 2.7, there is a homomorphism $\phi\colon G \to \mathrm{GL}_2(\mathbb{Z}_7)$ defined by

$$\phi(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \phi(b) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

This defines a homomorphism because, working in $\mathbb{Z}_7$, the following equations are true:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^7 = I_2, \quad \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}^3 = I_2, \text{ and } \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2.$$

Since all 21 of the elements listed above map to nontrivial matrices, the homomorphism ϕ is injective. So the group given by this presentation is a nonabelian group of order 21 that isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}_7)$.

Corollary 2.8. *Suppose groups G and H have the same presentation. Then G and H are isomorphic.*

Proof. Use Proposition 2.7 to build homomorphisms $G \to H$ and $H \to G$ that are inverses of each other. □

3 Existence of a group with a given presentation

This section isn't needed for any of the homework problems, but you should read it if you are curious about why presentations exist. Given a presentation $\langle S|R\rangle$, there is always a group with this presentation, even though we might never be able to identify this group.

Let M be the set of all words in $S^{\pm 1}$. This M has a binary product given by *concatenation*: if $w = s_1 s_2 \cdots s_n$ and $v = t_1 t_2 \cdots t_m$ are two different words in $S^{\pm 1}$, then the concatenation wv is the word

$$wv = s_1 s_2 \cdots s_n t_1 t_2 \cdots t_m.$$

Concatenation is well defined (as a function $M \times M \to M$) because the output of any concatenation is a word in M and there are no choices in the definition. Concatenation is associative because, for any $u, v, w \in M$, the words $(uv)w$ and $u(vw)$ are given by the same finite sequence of letters. The empty word is an identity element for concatenation, since attaching the sequence of length zero to the beginning or the end of a sequence does not change it. However, M is not a group, because nontrivial words do not have inverses under concatenation.

To make M a group, we take a quotient of M (as a set) and deduce that concatenation descends to a binary operation on this quotient that makes it a group. For the first step, we define a relation $\sim$ on M as follows: for $w, v \in M$, we say $w \sim v$ if $w = v$, or if we can turn w into v by inserting or deleting subwords ss^{-1} or $s^{-1}s$, for $s \in S^{\pm 1}$, finitely many times. This means that $w \sim v$ if there is $s \in S^{\pm 1}$ and $u_1, u_2 \in M$ with $w = u_1 u_2$ and $v = u_1 x x^{-1} u_2$. However, it is also possible that $w \sim v$, and we need to add and delete these inverse pairs several times to get from w to v.

It is straightforward to show that $\sim$ is an equivalence relation on M. We define F to be the quotient $M/\sim$ (so in other words, F is the set of equivalence classes of M under $\sim$). Define a binary product on F by $[w][v] = [wv]$, so that the product is induced by concatenation. It is not obvious that this product is well defined. However, if we assume that it is, then it is easy to show that F is a group: the product is associative because concatenation is, the class of the empty word is the identity, and $[s_1 \cdots s_n]^{-1} = [s_n^{-1} \cdots s_1^{-1}]$.

Proposition 3.1. *The product on F is well defined.*

Proof. Suppose $[w] = [u]$ in M, and $[v] \in M$. We show that $[wv] = [uv]$. The independence of $[w][v]$ on the choice of v would then follow by a similar argument.

Since $[w] = [u]$, we have $w \sim u$, and by the definition of $\sim$, we can turn w into u by doing a finite number of insertions and deletions of inverse pairs of generators. We induct on the number of times inverse pairs are inserted and deleted. The base case is when $w = u$, in which case $[wv] = [uv]$ automatically. So for the inductive step, we assume that $w \sim w' \sim u$, we can get from w' to u by inserting or deleting a single inverse pair, and we assume that $[wv] = [w'v]$. In one case, we can get from w' to u by deleting a single inverse pair. Then $w' = u_1 s s^{-1} u_2$ and $u = u_1 u_2$ for some $s \in S^{\pm 1}$. Then $w'v = u_1 s s^{-1} u_2 v$ and $uv = u_1 u_2 v$, so that $[w'v] = [uv]$. Then $[wv] = [uv]$, as we wanted to show. The case where we get from w' to u by inserting an inverse pair is similar. □

We have created a group F, which is equivalence classes of words in M, under the operation induced by concatenation. It is not hard to show that F has the presentation $F = \langle S | \varnothing \rangle$. Such an F is called a *free group.* If $|S| = 1$, then $F \cong \mathbb{Z}$. If $|S| > 1$, then F is a nonabelian infinite group that is not isomorphic to any group we have studied before.

At this point, we finally use the relations R. Each relation in R has the form $u = v$, and is equivalent to a relation $v^{-1}u = 1$. So we rewrite our presentation to assume that every relation in R has the form $w = 1$ for some w in M. We define N to be the smallest normal subgroup of F that contains all the elements $[w]$, for all relations $w = 1$ from R. (Formally N is the subgroup generated by all the conjugates of elements $[w]$. N is generated by an infinite set, but it still exists.) We define G to be the quotient F/N.

Theorem 3.2. *Given a presentation $\langle S|R \rangle$, the group $G = F/N$ as constructed above is a group with presentation $G = \langle S|R \rangle$.*

Proof. For each a in S, we interpret a as the element $[a]N$ in $G = F/N$. Since S generates F, it follows that S generates G. Each relation $w = 1$ in R has

$[w] \in N$, so it follows that $[w]N = 1$ in G. In particular, $w = 1$ is a true equation in G. Conversely, suppose $u = v$ is a true equation in G. Then the element $[v^{-1}u]$ in F is in N. Then $v^{-1}u$ is a product of conjugates of elements $\{w | (w = 1) \in R\}$. This means that $u = v$ is a consequence of relations in R. □

4 Exercises

1. Prove that for any group G and any subset S of G, the subset $\langle S \rangle$ is a subgroup of G.

2. Let G be a group and S a subset of G. We want to show that $\langle S \rangle$ is the "smallest subgroup of G containing S." To make this meaningful, we do the following parts.

    (a) Let G be a group. Let I be an index set, and let $\{H_\alpha\}_{\alpha \in I}$ be a collection of subgroups of G indexed over I. Let $H = \bigcap_{\alpha \in I} H_\alpha$. Use the subgroup criterion to show that H is a subgroup of G. (Warning: I is not necessarily finite or even countable, so don't assume this in your proof.)

    (b) Now let S be a subset of G. Let $\{H_\alpha\}_{\alpha \in I}$ be the collection of all subgroups of G that contain S (so for all $\alpha \in I$, $S \subset H_\alpha$). Let $H = \bigcap_{\alpha \in I} H_\alpha$. Show that $H \subset \langle S \rangle$.

    (c) With G, H and S as in part (b), show that $\langle S \rangle \subset H$. Conclude that $\langle S \rangle$ is the smallest subgroup of G containing S.

3. Prove that the Tietze transformation for adding a generator always produces a new presentation for the same group.

4. Prove that the Tietze transformation for deleting a generator always produces a new presentation for the same group.

5. Prove that the Tietze transformation for deleting a relation always produces a new presentation for the same group.

6. Let $G = \langle a, b | a^5 = 1, b^3 = 1, ba = a^2 b \rangle$. Show that $G \cong \mathbb{Z}_3$. (Hint: show that $a = 1$ and use Tietze transformations to rewrite the presentation).

7. Verify the presentation $D_4 = \langle a, b \,|\, a^4 = 1, b^2 = 1, ba = a^3 b \rangle$ by taking the following steps.

    (a) Use $D_4 \leq S_4$ given by

    $$D_4 = \{(1), (1,2,3,4), (1,3)(2,4), (1,4,3,2),$$
    $$(1,3), (1,4)(2,3), (2,4), (1,2)(3,4)\}.$$

    Let $N = \langle (1,2,3,4) \rangle$. Prove that N is a normal subgroup of D_4, that N is cyclic of order 4, and that D_4/N is cyclic of order 2.

(b) Use propositions from Section 2.1 to prove that D_4 has the presentation

$$D_4 = \langle a, b | a^4 = 1, b^2 = 1, bab^{-1} = a^3, b^{-1}ab = a^3 \rangle.$$

(c) Use Tietze transformations to simplify the presentation from the previous part.

8. Use the presentation from the previous problem and Tietze transformations to derive the presentation $D_4 = \langle r, s | r^2 = 1, s^2 = 1, (rs)^4 = 1 \rangle$.

9. Verify the presentation for Q_8 using $N = \langle i \rangle$ as a normal subgroup with $N \cong \mathbb{Z}_4$ and $Q_8/N \cong \mathbb{Z}_2$.

10. Verify the presentation for $\mathbb{Z}_2 \times \mathbb{Z}_2$ by writing down a presentation whose relations are the entire multiplication table (like in Proposition 1.4), and then using Tietze transformations to turn it into a presentation with two generators and three relations.

11. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, let $a = (1, 0)$, and let $b = (0, 1)$.

    (a) Show that every function $f : \{a, b\} \to G$ defines a homomorphism $\phi : G \to G$ with $\phi(a) = f(a)$ and $\phi(b) = f(b)$.

    (b) List all the isomorphisms $G \to G$.