Reidemeister-Schreier Rewriting Process for Group Presentations

Levi Casey

A 501 paper presented for the degree of
Master of Mathematics

Under the direction of
J. Caughman (adviser)
and
P. Latiolais (reader)

Fariborz Maseeh Department of Mathematics and Statistics
Portland State University
December 8th, 2017

Contents

1 Introduction

This 501 project was inspired by the paper *Cryptosystems Using Linear Groups* by Baumslag, Fine, and Xu (see [1]). During the course of reading that paper, it became clear that it would be beneficial to have an exposition of a tool that is integral to their work, namely the Reidemeister-Schreier rewriting process. To this end, we found *Combinatorial Group Theory* by Magnus, Karras, and Solitar extremely helpful (see [2]). Subsequently, the goal of this project became to provide a clear and (relatively) succinct explanation of the Reidemeister-Schreier rewriting process. To this end, we briefly cover the foundational ideas of free groups and group presentations, mostly to have the necessary definitions and symbolic language. In addition, we present a number of arguments and theorems leading up to the Reidemeister-Schreier rewriting process along with a selection of illustrative running examples, to see the ideas displayed in practice. We assume a basic familiarity with the notation and definitions of groups, as one might typically find in an introductory text like Gallian [[5], Ch. 1-2].

2 Group Presentations

2.1 Free Groups

It should be sufficient for our purposes to have a working definition of free groups without defining them abstractly using universal properties, category theory, or some other method. Indeed, there are plenty of other sources that describe free groups in this way far better than this author could hope to. For example, [2], [3], and [4] are helpful resources on this topic.

Accordingly, for our purposes, a **free group, F, with (possibly infinite) generating symbols**

$$\{a_\nu\} = \{a, b, c, \dots\}$$

is the group generated by $\{a_\nu\}$, *together with* the identity and inverses defined below, under the group operation "concatenation". Elements of F are equivalence classes of expressions we call **words**, and in particular, a word in F might look like

$$w = x_1 x_2 \cdots x_r,$$

where $x_i \in \{a_\nu\}$ for all i. We include the word in F written with no symbols of $\mathcal{A}$, called the **empty word**. Clearly "concatenation" is associative, since, if $*$ stands for concatenation, $a_1 * (a_2 * a_3) = a_1 * (a_2 a_3) = a_1 a_2 a_3 = (a_1 a_2) * a_3 = (a_1 * a_2) * a_3$. If we let $()$ be the empty word in F then $() = e$, the identity, since $w * () = w = () * w$ for all words in F. Lastly, if x_i is a generator of F, then we define the inverse of x_i as simply x_i^{-1}. Including these symbols we arrive at the complete definition of elements of F, namely if $w \in F$, then

$$w = x_1 x_2 \cdots x_r,$$

where either $x_i \in \{a_\nu\}$ or x_i is the empty word or one of the inverses described above. By associativity, any sequence of identical symbols in $\{a_\nu\}$,

$$\underbrace{a_i \cdots a_i}_{m \text{ times}}$$

can be rewritten as a_i^m. We say that two words, w_1 and w_2 are **freely equal** if we can rewrite w_1 into the same word as w_2 or vice versa, using a (possibly empty) sequence of steps involving either of the following:

(i) Either inserting or deleting words of the form $a_i a_i^{-1}$ or $a_i^{-1} a_i$ (which are equivalent to the empty word e).

(ii) Either collapsing or expanding words of the form $\underbrace{a_i \cdots a_i}_{m \text{ times}}$ or a_i^m.

Thus $a_i^{-1} a_i$ and $a_i a_i^{-1}$ are freely equal to the empty word. Also, if $w = x_1 x_2 \cdots x_r$, then $w^{-1} = x_r^{-1} x_{r-1}^{-1} \cdots x_1^{-1}$, since

$$\begin{aligned} ww^{-1} &= (x_1 x_2 \cdots x_r)(x_r^{-1} x_{r-1}^{-1} \cdots x_1^{-1}) \\ &= x_1 x_2 \cdots x_{r-1}(x_r x_r^{-1}) x_{r-1}^{-1} \cdots x_2^{-1} x_1^{-1} \end{aligned}$$

which is freely equal to the empty word by repeatedly applying (i) above. Just to be sure,

$$\begin{aligned} w^{-1}w &= (x_r^{-1} x_{r-1}^{-1} \cdots x_1^{-1})(x_1 x_2 \cdots x_r) \\ &= x_r^{-1} x_{r-1}^{-1} \cdots x_2^{-1}(x_1^{-1} x_1) x_2 \cdots x_{r-1} x_r \end{aligned}$$

which again is freely equal to the empty word by successive iterations of (i).

2.2 Presentation of a Group

In this section, we introduce some helpful terminology and notation that we will want to use often in the later sections.

2.2.1 Group Presentations

First we want to modify the way we present free groups in order to describe how we can present other groups in a similar manner.

Let D_4 represent the usual dihedral group, which corresponds to the symmetries of a square. It is common to give a group presentation for D_4 by picking a generating set of group elements, say $\{r, f\}$ (where r represents a rotation, and f represents a flip), along with information of the order of these elements, and how they commute. This is often shown thusly:

$$D_4 = \langle r, f \mid r^4 = e, f^2 = e, rf = fr^3 \rangle. \tag{1}$$

To emphasize the abstract generality of the presentation, we may wish to use generic symbols other than r and f, which bear the association with rotations and flips. In particular, under the mapping $r \mapsto a$ and $f \mapsto b$, we have

$$D_4 = \langle a, b \mid a^4 = e, b^2 = e, ab = ba^3 \rangle \tag{2}$$

which we can describe as a free group on the two symbols a and b, where e stands for the empty word, but with additional rules on which type of words can be reduced to the empty word. For example, we already know that words like aa^{-1} reduce to the empty word, and, in fact, we wish to continue all reductions allowed in free groups whenever words are freely equal. But now, we also wish to say that words like a^4 and b^2 can be reduced to the empty word in our group D_4. We call equations, such as those to the right of "$|$" in (1) and (2) above, **relations**. When the right hand side of a relation is e, we call the expression on the left side of the relation a **relator**. We often put all relations in this form and only write down the list of relators in our presentation. Notice that every relation can be turned into a relator. Thus we can write D_4 in terms of its generators and relators:

$$D_4 = \langle a, b \mid a^4, b^2, abab \rangle. \tag{3}$$

We call this a **presentation** of the group D_4 with **generating symbols** a, b and **defining relators** $a^4, b^2, abab$.

It turns out that every group has a presentation (see [2] for more details), and every finite group has a finite presentation. In this paper, we will see that *the Reidemeister-Schreier rewriting process is a method for finding the presentation of a specific subgroup H, of a known group G, where the presentation of G is also known.* In order to explore this process further, we need some additional ideas.

2.2.2 Group Presentations and Their Corresponding Free Groups

Suppose G has the following presentation:

$$G = \langle a, b, c, \ldots \mid P, Q, R, \ldots \rangle. \tag{4}$$

In this expression, we may view $a, b, c, \ldots$ as the generating symbols of a free group F and $P, Q, R, \ldots$ as the elements of F that are not freely equal to the empty word, the identity in F, that we now want to be considered the identity in a new group G, obtained from F. We do this by letting N be the normal subgroup of F generated by $P, Q, R, \ldots$, the relators in the presentation of G. This means that N contains $P, Q, R, \ldots$ along their inverses, and all products thereof. But, this isn't enough. In order to ensure that N is normal, we must also include all elements of the form $wPw^{-1}, wQw^{-1}, wRw^{-1}, \ldots$, and their inverses, where w is any word in F. Constructing N in this way, the factor group F/N will look much like the group G. In fact, by Corollary 2.1 in [2], G is isomorphic to

$$F/N = \langle a, b, c, \ldots \mid P, Q, R, \ldots \rangle,$$

under the appropriate natural isomorphism. In this way, group presentations identify the corresponding groups as quotient groups of an associated free group.

2.2.3 Proving a List of Relators is Sufficient

Finally, say we are given a list of relators $P, Q, R, \ldots$ for a group G. We must do the following to show that $P, Q, R, \ldots$ form a sufficient set of relators for G, i.e. to show that $P, Q, R, \ldots$ are defining relators for G. Show that

(i) the list of relations are, in fact, relations, and

(ii) show that any valid relation in G can be derived from the given list of $P, Q, R, \ldots$ relators.

Intuitively, the second step can be understood thusly: Consider the set $\{a_\nu\}$ of generators in the presentation of some group G. Any valid relation, $\mathcal{R}$, in G can be written in the form

$$a_{n_1}^{\alpha_1} a_{n_2}^{\alpha_2} \cdots a_{n_r}^{\alpha_r} = a_{m_1}^{\beta_1} a_{m_2}^{\beta_2} \cdots a_{m_s}^{\beta_s}$$

which then can be rewritten as the following relator:

$$a_{n_1}^{\alpha_1} a_{n_2}^{\alpha_2} \cdots a_{n_r}^{\alpha_r} a_{m_s}^{-\beta_s} \cdots a_{m_1}^{-\beta_1}.$$

If we can reduce this relator, showing it to be freely equal to the empty word using the additional insertion or deletion of $P, Q, R, \ldots$, then we could rebuild this relator from $P, Q, R, \ldots$ in reverse order, and hence we can rebuild the original relation from the given list $P, Q, R, \ldots$ of relators. Since our choice of relation $\mathcal{R}$ was arbitrary, this would show that the given list $P, Q, R, \ldots$ of relators is sufficient to express any relation for the group. Hence the given list $P, Q, R, \ldots$ of relators is a set of defining relators for G.

3 Rewriting Process

3.1 Definition of a Rewriting Process

Let G be a group with presentation

$$G = \langle a, b, c, \ldots \mid P, Q, R, \ldots \rangle, \tag{5}$$

and let H be a subgroup of G.

Definition 3.1. Suppose that H has generators $\{j_i\}$, which are words in the symbols $\{a_\nu\}$. For each i, identify each word of $\{j_i\}$ with a single new symbol s_i. Call this new set of symbols $\{s_i\}$. A **rewriting process for *H* with respect to generators $\{j_i\}$** is a map, τ, from words in the symbols $\{a_\nu\}$ that define elements of H to words in the symbols $\{s_i\}$, such that these two words, one written in the symbols $\{a_\nu\}$ and the other in the symbols $\{s_i\}$, define the same element of H.

Since $\{j_i\}$ is a set of generators for H then for any $h \in H$ there is some $t \in \mathbb{Z}$ such that,

$$h = j_{n_1}^{\epsilon_1} \cdots j_{n_t}^{\epsilon_t} \qquad (\epsilon_j = \pm 1). \tag{6}$$

This is not the only way to write h as a product of the generators j_i, but any such expression will suffice for our purposes, so let us make use of this particular one. Note that, in this form, h is a word in $\{a_\nu\}$, since each j_i is a word in $\{a_\nu\}$. Now a rewriting process is a map τ that identifies each j_i with a single symbol s_i, and maps the words in H accordingly. In other words

$$\tau(h) = \tau(j_{n_1}^{\epsilon_1} \cdots j_{n_t}^{\epsilon_t}) = s_{n_1}^{\epsilon_1} \cdots s_{n_t}^{\epsilon_t}. \tag{7}$$

Therefore $\tau(h)$ is the *same group element* as h, but h is a word in $\{a_\nu\}$ while $\tau(h)$ is a word in $\{s_i\}$.

3.2 Simple Example of a Rewriting Process

For example, let us return to the dihedral group with eight elements:

$$D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

or, as a presentation:

$$D_4 = \langle a, b \mid a^4, b^2, abab\rangle.$$

Here, we are using a and b as generators of the whole group. Recall that the Klein 4-group, V, is a subgroup of D_4, and in fact there is more than one subgroup of D_4 that is isomorphic to the Klein 4-group. One possibility is

$$V = \{e, a^2, a^2b, b\}.$$

In this case, V is generated by the set $\{a^2, b\}$. Let us make the following identifications: $x = a^2$ and $y = b$. Then a rewriting process for V could be the following map:

$$\begin{aligned} e &\xrightarrow{\tau} e \\ a^2 &\xrightarrow{\tau} x \\ a^2b &\xrightarrow{\tau} xy \\ b &\xrightarrow{\tau} y. \end{aligned}$$

In terms of the notation in the definition of a rewriting process, the set $\{j_i\}$ is $\{a^2, b\}$, and the set $\{s_i\}$ is $\{x, y\}$. Say, $j_1 = a^2$, $j_2 = b$ and $s_1 = x$, $s_2 = y$. So then for $a^2b \in V$, we have that $a^2b = j_1j_2$ and

$$\tau(a^2b) = \tau(j_1^1j_2^1) = s_1^1s_2^1 = xy.$$

We will use this group again to illustrate various general concepts, so we designate it as a running example below.

Definition 3.2. (**Running Example 1**) Let G_1 have the following presentation

$$G_1 = D_4 = \langle a, b \mid a^4, b^2, abab\rangle$$

and let us designate the following subgroup:

$$H_1 = V = \{e, a^2, a^2b, b\}.$$

In this case, note that $G_1/H_1 = \{H, Ha\} = \{\{e, a^2, a^2b, b\}, \{a, a^3, ab, a^3b\}\}$.

3.3 The Simple Example Becomes Unwieldy

As we will see, we can obtain a presentation for H_1 using the above rewriting function! At this point it will be fairly cumbersome, but the Reidemeister rewriting function simplifies it, and then the Reidemeister-Schreier process simplifies it even more. Continuing with Running

Example 1 for now, a presentation for H_1 can be obtained using the generators $\{x, y\}$, and using the following relations (as will be proved in the next section):

$$x = \tau(a^2) \text{ and } y = \tau(b) \tag{8}$$

$$\tau(h) = \tau(h') \tag{9}$$

where h and h' are any freely equal words in V (written as words in a, b), and

$$\tau(h_i \cdot h_j) = \tau(h_i) \cdot \tau(h_j) \tag{10}$$

where h_i and h_j are any elements of V (written as words in a, b), and

$$\tau(wR_\mu w^{-1}) = e \tag{11}$$

where $\{R_\mu\}$ are the relators of G_1, and w is any word in a, b.

The reason this presentation is cumbersome is because we have infinitely many relations here! So even with our simple example of H_1 as a subgroup of G_1, we cannot expect to completely write this down explicitly. Nevertheless, let us attempt to see at least a finite selection of these relations to 1) get a sense of why we need a simpler way of obtaining a presentation of subgroups and 2) feel somewhat convinced that these relations do in fact generate H. Later on we will prove it in general. The following are selections of relations of the form (8)

$$x = \tau(a^2) \tag{12}$$
$$y = \tau(b), \tag{13}$$

and of the form (9)

$$\tau(ea^4e^{-1}) = \tau(a^4) \tag{14}$$
$$\tau(eb^2e^{-1}) = \tau(b^2), \tag{15}$$

and of the form (10)

$$\tau(a^2b) = \tau(a^2)\tau(b) \tag{16}$$
$$\tau(b^2) = \tau(b)\tau(b) \tag{17}$$
$$\tau(a^4) = \tau(a^2)\tau(a^2) \tag{18}$$
$$\tau(a^2ba^2b) = \tau(a^2)\tau(b)\tau(a^2)\tau(b), \tag{19}$$

and, finally, of the form (11)

$$\tau(ea^4e^{-1}) = e \tag{20}$$
$$\tau\big((ab^{-1}a^{-1})abab(ab^{-1}a^{-1})^{-1}\big) = e \tag{21}$$
$$\tau\big((ab^{-1})abab(ab^{-1})^{-1}\big) = e \tag{22}$$
$$\tau(ab^2a^{-1}) = e \tag{23}$$
$$\tau(eb^2e^{-1}) = e \tag{24}$$
$$\tau(ea^4e^{-1}) = e. \tag{25}$$

As long as τ is a rewriting process, these, along with all other relations of this form, are the basis for the relators in a presentation of a subgroup H.

3.4 Reducing to a More Familiar Presentation

Note that there are infinitely many possible relations of the form (8) through (11). In this case we already know a presentation of V, so the relations (12) through (25) were carefully chosen in order to show that we can obtain the usual relators known in a presentation of V. In fact, we know that the generators x and y along with the relators $x^2, y^2,$ and $xyxy$ form a presentation of V. In other words, it is known that

$$V = \langle x, y \mid x^2, y^2, xyxy \rangle$$

is a presentation of V. In practice, we may not know the presentation of a subgroup, H, before hand (the whole point of this process after all is to *obtain* a presentation of H), so it would likely be much more difficult to weed through infinitely many relations and select a finite (much less, minimally finite) collection of relations that are sufficient for a presentation of H.

In our case, it would be nice to be able to derive the relators $x^2, y^2,$ and $xyxy$ from (12) through (25). To this end, note that (12), (14), (18), and (25) yield $x^2 = e$, while (13), (15), (17), and (24) yield $y^2 = e$. More difficult to see is the following:

$$\begin{aligned}
e &= e \cdot e \cdot \boldsymbol{e^{-1}} \\
&= \tau\big((ab^{-1}a^{-1})abab(ab^{-1}a^{-1})^{-1}\big)\tau\big((ab^{-1})abab(ab^{-1})^{-1}\big)\boldsymbol{\tau((ab^2a^{-1})^{-1})} && * \\
& && \text{by } (21), (22), \text{ and } (23) \\
&= \tau\big((ab^{-1}a^{-1})abab(ab^{-1}a^{-1})^{-1}(ab^{-1})abab(ab^{-1})^{-1}(ab^2a^{-1})^{-1}\big) \\
& && \text{by } (10) \\
&= \tau(ab^{-1}a^{-1}abababa^{-1}ab^{-1}ababba^{-1}ab^{-2}a^{-1}) \\
& && \text{by } (9) \\
&= \tau(a^2ba^2b) \\
& && \text{by } (9) \\
&= xyxy \\
& && \text{by } (12), (13), \text{ and } (19).
\end{aligned}$$

($*$ Note that we will show $\tau(h^{-1}) = \tau(h)^{-1}$ in the next section, a fact used to get from the first bold factor to the second in the first two lines.)
Thus we obtain the desired relators $x^2, y^2, xyxy$ in a known presentation of V from the carefully chosen relations (12) through (25) of the infinitely many relations of the form (8) through (11).

From this exploration it is easy to suspect that the collection of relations of the form (8) through (11) do in fact give us a defining set of relators, along with many redundant relators. We prove this fact in more generality now in the next section.

3.5 A First Presentation for a subgroup H

Thanks to Reidemeister and Schreier, we can find a simpler presentation for our subgroup H. We obtain this simpler presentation by choosing special generators for H and using the following tools, a **right coset representative function** (defined in Section 5) and a **Schreier transversal** (defined in Section 6.3.1). In the meantime, let us prove that relations of the form (8)-(11) do in fact give presentations of subgroups more generally. To show this, recall the two steps from Section 2.2.3 for showing that a list of relators is a presentation of a group G.

Theorem 3.1. *Let G have the presentation*

$$G = \langle a_1, \ldots, a_n \mid R_\mu, \ldots \rangle$$

and let H be a subgroup of G. If $\{j_i\}$ is a set of generators of H and τ is a rewriting process for H with respect to the generators $\{j_i\}$, then a presentation for H under the mapping $j_i \to s_i$ is obtained by using the symbols s_i as generating symbols and using the following equations as defining relations:

$$s_i = \tau(j_i) \tag{26}$$

$$\tau(h) = \tau(h') \tag{27}$$

$$\tau(h_i \cdot h_j) = \tau(h_i) \cdot \tau(h_j) \tag{28}$$

$$\tau(wR_\mu w^{-1}) = e \tag{29}$$

where h, h', h_i, and h_j words in the generators of G which define elements of H, and h, h' are freely equal. Also, R_μ is a defining relator in the presentation of G and w is any word in the generators of G.

Proof.

(i) First we show that (26)-(29) are relations.

(26) This is a relation under the identification $s_i \Rightarrow j_i$.

(27) This is a relation since if h and h' are freely equal words, then they are the same group element of H. Also h and $\tau(h)$ denote the same group element for all $h \in H$ by definition of the rewriting process. Thus $\tau(h)$ and $\tau(h')$ denote the same group element of H.

(28) This is a relation since, again, h and $\tau(h)$ denote the same group element for all $h \in H$, thus

$$\tau(h_i h_j) = h_i h_j = \tau(h_i)\tau(h_j).$$

The equality here is understood to mean "as group elements".

(29) This is a relation since $wR_\mu w^{-1}$ is the identity in G, and hence the identity in H. In other words, $wR_\mu w^{-1} \in H$, thus we can use the fact that h and $\tau(h)$ denote the same group element for all h to say

$$\tau(wR_\mu w^{-1}) = wR_\mu w^{-1} = e.$$

(ii) Next we show that any arbitrary relator can be reduced to the empty word using (26)-(29).

Let
$$s_{n_1}^{\epsilon_1} \cdots s_{n_r}^{\epsilon_r} \qquad (\epsilon_i = \pm 1) \tag{30}$$
be any relator. We must show we can reduce this to the empty word using (26)-(29). First, let us derive a few consequences of (26)-(29):

(a) We have $\tau(e) = e$. This follows from (28) by letting $h_i = h_j = e$:
$$\tau(e) \cdot \tau(e) = \tau(e \cdot e) = \tau(e).$$
And since $\tau(e)$ is a group element, we can multiply both sides by $\tau(e)^{-1}$ to obtain the desired result.

(b) We also have that $\tau(h^{-1}) = \tau(h)^{-1}$. To see this, we again using (28) and the result from (a), which gives
$$\tau(h^{-1})\tau(h) = \tau(h^{-1}h) = \tau(e) = e.$$
Multiplying both sides by $\tau(h)^{-1}$ yields the desired result.

(c) Thus for any product of elements, $h_1^{\epsilon_1} \cdots h_q^{\epsilon_q}$ such that $\epsilon_i = \pm 1$ for all i, we have by (3) and (b)
$$\tau(h_1^{\epsilon_1} \cdots h_q^{\epsilon_q}) = \tau(h_1^{\epsilon_1}) \cdots \tau(h_q^{\epsilon_q}) = \tau(h_1)^{\epsilon_1} \cdots \tau(h_q)^{\epsilon_q}.$$

Now we have the tools for the following reduction of (30) to the empty word (let $\eta_i = \pm 1$ for all i):
$$\begin{aligned}
s_{n_1}^{\epsilon_1} \cdots s_{n_r}^{\epsilon_r} &= \tau(j_1)^{\epsilon_1} \cdots \tau(j_r)^{\epsilon_r} && (31)\\
&= \tau(j_1^{\epsilon_1} \cdots j_r^{\epsilon_r}) && (32)\\
&= \tau\left((w_1 R_{\mu_1} w_1^{-1})^{\eta_1} \cdots (w_t R_{\mu_t} w_t^{-1})^{\eta_t}\right) && (33)\\
&= \tau\left(w_1 R_{\mu_1} w_1^{-1}\right)^{\eta_1} \cdots \tau\left(w_t R_{\mu_t} w_t^{-1}\right)^{\eta_t} && (34)\\
&= e^{\eta_1} \cdots e^{\eta_t} && (35)\\
&= e \cdots e && (36)\\
&= e && (37)
\end{aligned}$$

I imagine for most of us, the most mysterious step is from (32) to (33) (it certainly was for me!). But step by step:

(31) is by relation (26).

(32) is by (c) above.

(33) is by the fact that since s_i and j_i denote the same group element, and since $s_{n_1}^{\epsilon_1} \cdots s_{n_r}^{\epsilon_r} = e$, then we also have $j_1^{\epsilon_1} \cdots j_r^{\epsilon_r} = e$. In particular, this tells us that $j_1^{\epsilon_1} \cdots j_r^{\epsilon_r}$ is the identity in G. By Corollary 2.1 in [2], if a word is the identity in G, then that word is an element of the normal subgroup of the free group, F, on $\{a_\nu\}$,

that is generated by the relations in the presentation of G. A normal subgroup containing these relations must also contain their conjugates and the inverses of their conjugates (in order to be normal), thus a word that is the identity in G can always be written as we see in the argument of τ in (33).

(34) is by (c) again.

(35) is by (29).

(36) and (37) should be obvious.

Thus, any relation satisfied by the generators of H can be reduced to the empty word using (26)-(29). Therefore (26)-(29), along with the generators $\{s_i\}$ do in fact form a presentation for H. In other words, we can present H thusly:

$$H = \langle s_1, s_2, \cdots \mid s_i = \tau(j_i), \tau(h) = \tau(h'), \tau(h_i \cdot h_j) = \tau(h_i) \cdot \tau(h_j), \tau(wR_\mu w^{-1}) = e\rangle$$

for all h, h', h_i, and h_j words in the generators of G which define elements of H, where h, h' are freely equal, and where R_μ is any defining relator in the presentation of G, and w is any word in the generators of G. □

4 Searching for a Second Running Example

Let

$$G = \langle a, b, c \mid a^4,\ b^2, c^2,\ baba,\ caca^3,\ bcbc\rangle.$$

Alternatively, we could rewrite the relators as relations, which might make the underlying structure of G a little more clear:

$$G = \langle a, b, c \mid a^4 = b^2 = c^2 = e,\ ba = a^3b,\ ac = ca,\ bc = cb\rangle.$$

Thus we can see, for example, that a, c and b, c commute but not a, b. This group G has order 16 and is isomorphic to the external direct product $D_4 \times \mathbb{Z}_2$, where we use the notation D_n to denote the symmetry group of a regualar n-gon, i.e. the dihedral group of order $2n$.

Consider the subgroup

$$H = \{e,\ a^3bc\}.$$

Note that H is a subgroup, since if we expand and move c to the end, and simplify using the relations, we have:

$$\begin{aligned}(a^3bc)^2 = aaabcaaabc &= aa(\boldsymbol{aba})aab(\boldsymbol{cc})\\ &= aa\boldsymbol{b}aab\boldsymbol{e}\\ &= a(\boldsymbol{aba})ab\\ &= a\boldsymbol{b}ab\\ &= (aba)b\\ &= bb\\ &= e\end{aligned}$$

Also, $[G:H]=8$, since the cosets are given by $G/H=$

$$\left\{\begin{array}{ll} H_0=H=\{e,a^3bc\}, & H_4=Ha^2=\{a^2,abc\}, \\ H_1=Ha=\{a,a^2bc\}, & H_5=Hab=\{ab,a^2c\}, \\ H_2=Hb=\{b,a^3c\}, & H_6=Hac=\{ac,a^2b\}, \\ H_3=Hc=\{c,a^3b\}, & H_7=Ha^3=\{a^3,bc\} \end{array}\right\}$$

We will define this example below.

Definition 4.1. (Running Example 2) Let G have presentation

$$G=\langle a,b,c \mid a^4,\ b^2,c^2,\ baba,\ caca^3,\ bcbc\rangle$$

and let H denote the following subgroup of G:

$$H=\{e,\ a^3bc\}.$$

5 Some Special Generators of H

Let $\mathcal{K}$ be a complete set of distinct representatives of G/H **that contains e**, called here, for short, a **transversal**. One possibility for $\mathcal{K}$ in Running Example 2 is

$$\mathcal{K}=\{e,\ a,\ a^3c,\ c,\ abc,\ ab,\ a^2b,\ a^3\},$$

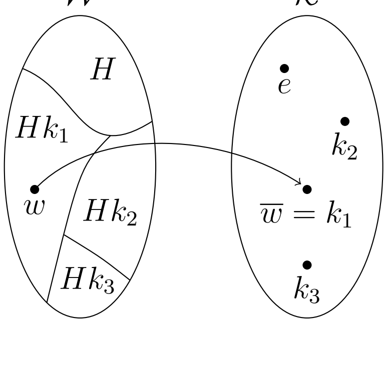
which we get by picking one element from each coset in our complete list of cosets at the end of the previous section. In this case, there are $2^7=128$ possible transversals for G/H that contain e.

Definition 5.1. Right Coset Representative Function
Let $\mathcal{W}$ be the set of words in $\{a_\nu\}$, where $\{a_\nu\}$ are the generators of G, and let $\mathcal{K}$ be any transversal for the cosets of a subgroup H. Define the function $\overline{}:\mathcal{W}\to\mathcal{K}$ by the rule

$$w\mapsto\overline{w} \text{ where } \overline{w} \text{ is the element of } \mathcal{K} \text{ such that } w\in H\overline{w}.$$

We call this function a **right coset representative function for G (on the generators a_ν) modulo a subgroup H.**

Visualization of an element being mapped under a right coset representative function for a situation in which $[G:H]=4$:



In the above diagram, we can think of each "Hk_i" as all words that, as group elements of G, are elements of Hk_i. Also, the transversal being used is $\mathcal{K} = \{e, k_1, k_2, k_3\}$.

Theorem 5.1. *With the above notation, the subgroup H is generated by the set of words*

$$S = \left\{ ka_\nu \overline{ka_\nu}^{-1} \mid k \in \mathcal{K} \textit{ and } a_\nu \textit{ is any generator of } G \right\}.$$

In other words, any element of H can be written as a product of elements, or the inverses of elements, in S.

The proof of this relies on the following lemma:

Lemma 5.2. *With the above notation,*

(i) $\overline{w} = e$ *if and only if* w *defines an element of* H*;*

(ii) whenever w *is freely equal to* v*, we have* $\overline{w} = \overline{v}$*;*

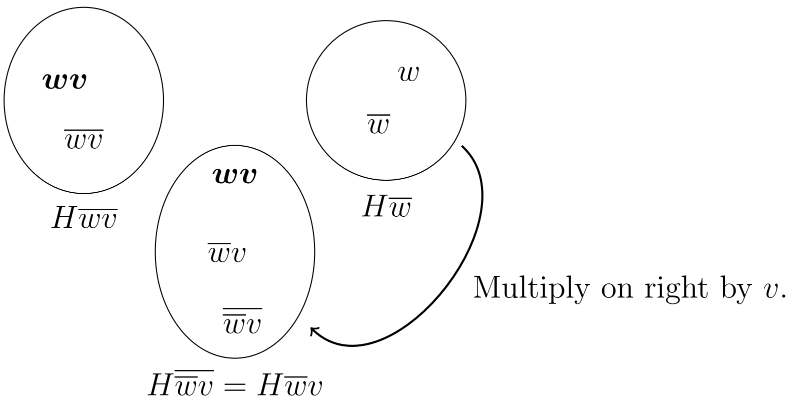
(iii) $\overline{\overline{w}} = \overline{w}$*;*

(iv) $\overline{wv} = \overline{\overline{w}v}$*.*

Proof. (i) If $\overline{w} = e$, then $w \in H\overline{w} = He = H$ by definition. On the other hand, if $w \in H$, then $Hw = H$. Since we defined $\mathcal{K}$ to contain e, and since $e \in H$, then we only have one choice for $\overline{w}$, namely e.

(ii) Since w and v are freely equal, they define the same group element, thus $Hw = Hv$. Hence $H\overline{w} = Hw = Hv = H\overline{v}$. Since $\overline{w}$ and $\overline{v}$ define the same coset of H, and each element of $\mathcal{K}$ represents a *distinct* coset of G/H, then $\overline{w} = \overline{v}$.

(iii) By definition, $\overline{\overline{w}}$ is the element of $\mathcal{K}$ such that $\overline{w} \in H\overline{\overline{w}}$. Note that $\overline{w} \in H\overline{w}$ as well. Thus $\overline{w} \in H\overline{\overline{w}} \cap H\overline{w}$ which implies $H\overline{\overline{w}} = H\overline{w}$, since cosets can only be disjoint or equal. Since there is one and only one representative for each coset in $\mathcal{K}$, it must be that $\overline{\overline{w}} = \overline{w}$. Visual aid for (iv):



(iv) By definition, $wv, \overline{wv} \in H\overline{wv}$, and $\overline{w}v, \overline{\overline{w}v} \in H\overline{\overline{w}v}$. Similarly $w, \overline{w} \in H\overline{w}$. Multiplying every element of $H\overline{w}$ on the right by v results in the coset $H\overline{w}v$, which is the same as $H\overline{\overline{w}v}$. Since $w \in H\overline{w}$, we now have $wv \in H\overline{\overline{w}v}$.Thus $wv \in H\overline{wv} \cap H\overline{\overline{w}v}$ which implies $H\overline{wv} = H\overline{\overline{w}v}$, from which the conclusion $\overline{wv} = \overline{\overline{w}v}$ follows, since each coset has one and only one representative in $\mathcal{K}$.

□

Now we have enough to prove Theorem 5.1:

Proof. First, two preliminary facts: note that $ka_\nu\overline{ka_\nu}^{-1} \in H$ for all $k \in \mathcal{K}$ and all generators $\{a_\nu\}$ of G. This is because $Hka_\nu = H\overline{ka_\nu}$ by definition, so $Hka_\nu\overline{ka_\nu}^{-1} = H$. Thus there exists an $h \in H$ such that $h = ka_\nu\overline{ka_\nu}^{-1}$.

Less obviously, note the fact that $ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}$ is the inverse of $\overline{ka_\nu^{-1}}a_\nu\overline{\overline{ka_\nu^{-1}}a_\nu}^{-1}$, the latter of which we can see is an element of S (after staring at it for a week or so). Obvious, right? Well, not for me, so let's work it out:

$$\begin{aligned}
\left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right) \cdot \left(\overline{ka_\nu^{-1}}a_\nu\overline{\overline{ka_\nu^{-1}}a_\nu}^{-1}\right) &= \left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right) \cdot \left(\overline{ka_\nu^{-1}}a_\nu\overline{ka_\nu^{-1}a_\nu}^{-1}\right) && \text{by (iv)} \\
&= \left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right) \cdot \left(\overline{ka_\nu^{-1}}a_\nu\overline{ke}^{-1}\right) \\
&= \left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right) \cdot \left(\overline{ka_\nu^{-1}}a_\nu k^{-1}\right) && \text{by (i)} \\
&= \left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right) \cdot \left((a_\nu k^{-1})^{-1}\left(\overline{ka_\nu^{-1}}\right)^{-1}\right)^{-1} \\
&= \left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right) \cdot \left(ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}\right)^{-1} \\
&= e
\end{aligned}$$

So now anytime we see something of the form $ka_\nu^{-1}\overline{ka_\nu^{-1}}^{-1}$, we know it is the inverse of something in S.

Let $h \in H$, and write h in the following way:

$$h = a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\ldots a_{\nu_r}^{\epsilon_r} \qquad (\epsilon_i = \pm 1),$$

where a_{ν_i} is not necessarily distinct from a_{ν_j} when $i \neq j$. For example, pick $h = a^3bc$ from Running Example 2. We would write h in the above way as

$$h = aaabc \text{ or } a^{-1}bc.$$

If we could find $W_1, \ldots, W_r$ such that

$$h = \overline{W_1}a_{\nu_1}^{\epsilon_1}\overline{W_1a_{\nu_1}^{\epsilon_1}}^{-1} \cdot \overline{W_2}a_{\nu_2}^{\epsilon_2}\overline{W_2a_{\nu_2}^{\epsilon_2}}^{-1} \cdot \cdots \cdot \overline{W_r}a_{\nu_r}^{\epsilon_r}\overline{W_ra_{\nu_r}^{\epsilon_r}}^{-1}, \tag{38}$$

then since $\epsilon_i = \pm 1$ for all i, and by property (iv) above, we will have written h in terms of S or the inverses of S. In other words, when $\epsilon_i = 1$ then $\overline{W_i}a_{\nu_i}\overline{W_ia_{\nu_i}}^{-1} = \overline{W_i}a_{\nu_i}\overline{\overline{W_i}a_{\nu_i}}^{-1} \in S$

and when $\epsilon_i = -1$ then $\overline{W_i}a_{\nu_i}^{-1}\overline{W_ia_{\nu_i}^{-1}}^{-1} = \overline{W_i}a_{\nu_i}^{-1}\overline{\overline{W_i}a_{\nu_i}^{-1}}^{-1} \in S^{-1}$, the set of inverses of S, since $\overline{W_i}a_{\nu_i}^{-1}\overline{\overline{W_i}a_{\nu_i}^{-1}}^{-1}$ is of the form $ka_{\nu}^{-1}\overline{ka_{\nu}^{-1}}^{-1}$.

The following choices for $W_1, \dots, W_r$ will rewrite h as a product in the form of (38). Let

$$W_1 = e,\ W_2 = a_{\nu_1}^{\epsilon_1},\ W_3 = a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2},\ \dots,\ W_r = a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\dots a_{\nu_{r-1}}^{\epsilon_{r-1}}.$$

We call these choices for W_j the $(j-1)^{\text{st}}$ **initial segments** of h. Let's see how this works:

$$\begin{aligned}
&\overline{W_1}a_{\nu_1}^{\epsilon_1}\overline{W_1a_{\nu_1}^{\epsilon_1}}^{-1}\cdot\overline{W_2}a_{\nu_2}^{\epsilon_2}\overline{W_2a_{\nu_2}^{\epsilon_2}}^{-1}\cdots\overline{W_r}a_{\nu_r}^{\epsilon_r}\overline{W_ra_{\nu_r}^{\epsilon_r}}^{-1}\\
&\qquad = \overline{e}a_{\nu_1}^{\epsilon_1}\overline{ea_{\nu_1}^{\epsilon_1}}^{-1}\cdot\overline{a_{\nu_1}^{\epsilon_1}}a_{\nu_2}^{\epsilon_2}\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}}^{-1}\cdots\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\dots a_{\nu_{r-1}}^{\epsilon_{r-1}}}a_{\nu_r}^{\epsilon_r}\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\dots a_{\nu_{r-1}}^{\epsilon_{r-1}}a_{\nu_r}^{\epsilon_r}}^{-1}\\
&\qquad = \overline{e}a_{\nu_1}^{\epsilon_1}\left(\overline{a_{\nu_1}^{\epsilon_1}}^{-1}\overline{a_{\nu_1}^{\epsilon_1}}\right)a_{\nu_2}^{\epsilon_2}\left(\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}}^{-1}\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}}\right)\cdots\\
&\qquad\qquad\qquad \left(\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\dots a_{\nu_{r-1}}^{\epsilon_{r-1}}}^{-1}\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\dots a_{\nu_{r-1}}^{\epsilon_{r-1}}}\right)a_{\nu_r}^{\epsilon_r}\overline{a_{\nu_1}^{\epsilon_1}a_{\nu_2}^{\epsilon_2}\dots a_{\nu_{r-1}}^{\epsilon_{r-1}}a_{\nu_r}^{\epsilon_r}}^{-1}\\
&\qquad = \overline{e}a_{\nu_1}^{\epsilon_1}(e)a_{\nu_2}^{\epsilon_2}(e)\cdots(e)a_{\nu_r}^{\epsilon_r}\overline{h}^{-1}\\
&\qquad = \overline{e}h\overline{h}^{-1}\\
&\qquad = ehe^{-1} && \text{by (i)}\\
&\qquad = h
\end{aligned}$$

□

Truly awesome! Let's see how this works with a concrete example, using Running Example 2. Let $h = a^3bc$. Now write it in the form $h = aaabc$. Thus we have

$$W_1 = e,\ W_2 = a,\ W_3 = aa,\ W_4 = aaa,\ \text{ and } W_5 = aaab.$$

Then we proceed as follows:

$$\begin{aligned}
&\overline{W_1}a\overline{W_1a}^{-1}\cdot\overline{W_2}a\overline{W_2a}^{-1}\cdot\overline{W_3}a\overline{W_3a}^{-1}\cdot\overline{W_4}b\overline{W_4b}^{-1}\cdot\overline{W_5}c\overline{W_5c}^{-1}\\
&\qquad = \overline{e}a\overline{ea}^{-1}\cdot\overline{a}a\overline{aa}^{-1}\cdot\overline{aa}a\overline{aaa}^{-1}\overline{aaa}b\overline{aaab}^{-1}\cdot\overline{aaab}c\overline{aaabc}^{-1}\\
&\qquad = \overline{e}a\left(\overline{ea}^{-1}\overline{a}\right)a\left(\overline{aa}^{-1}\overline{aa}\right)a\left(\overline{aaa}^{-1}\overline{aaa}\right)b\left(\overline{aaab}^{-1}\overline{aaab}\right)c\overline{aaabc}^{-1}\\
&\qquad = \overline{e}\left(aaabc\right)\overline{aaabc}^{-1}\\
&\qquad = \overline{e}h\overline{h}^{-1}\\
&\qquad = h.
\end{aligned}$$

Cool! Ok, now I have to try it with the second way I wrote h, namely $h = a^{-1}bc$ just to see that it works! In this case

$$W_1 = e,\ W_2 = a^{-1},\ W_3 = a_1^{-1}b.$$

So then we have:

$$\begin{aligned}
&\overline{W_1}a^{-1}\overline{W_1a^{-1}}^{-1} \cdot \overline{W_2}b\overline{W_2b}^{-1} \cdot \overline{W_3}c\overline{W_3c}^{-1} \\
&\qquad = \overline{e}a^{-1}\overline{ea^{-1}}^{-1} \cdot \overline{a^{-1}}b\overline{a^{-1}b}^{-1} \cdot \overline{a^{-1}b}c\overline{a^{-1}bc}^{-1} \\
&\qquad = \overline{e}a^{-1}\left(\overline{a^{-1}}^{-1}\overline{a^{-1}}\right)b\left(\overline{a^{-1}b}^{-1}\overline{a^{-1}b}\right)c\overline{a^{-1}bc}^{-1} \\
&\qquad = \overline{e}a^{-1}(e)b(e)c\overline{a^{-1}bc}^{-1} \\
&\qquad = \overline{e}h\overline{h}^{-1} \\
&\qquad = h
\end{aligned}$$

Notably this delightfully matches our results above.

Indeed, at this point we have found a generating set for H, so now we can prove the following result:

Theorem 5.3. *If G is finitely generated and H is a subgroup of G of finite index, then H is finitely generated.*

Proof. Recall that we have a (possibly infinite) list of generators for H, namely the set

$$S = \{ka_\nu\overline{ka_\nu}^{-1} \mid k \in \mathcal{K} \text{ and } a_\nu \text{ is any generator of } G\}.$$

Since G is finitely generated, we can say G has n generators, for some $n \in \mathbb{N}$. Likewise, since H is a subgroup of finite index, we can say $[G : H] = j$, for some $j \in \mathbb{N}$. Then $|\mathcal{K}| = j$. Accordingly, for elements of S, there are n choices for a_ν and j choices for k, thus $|S| \leq nj$ (nothing we've said so far necessitates that $k_ia_{\nu_i}\overline{k_ia_{\nu_i}}^{-1} \neq k_ta_{\nu_t}\overline{k_ta_{\nu_t}}^{-1}$ when $i \neq t$). Thus H is generated by a finite set; hence H is finitely generated. □

6 More Practical Presentations of H

6.1 The Reidemeister Rewriting Process

We can find a rewriting process using the generators, $S = \{ka_\nu\overline{ka_\nu}^{-1}\}$, for any subgroup H. Let's first explore the Reidemeister rewriting process with our running example. The element $a^{-1}bc$ is an element of H, written in terms of the generators of G, and we actually rewrote it previously as

$$\begin{aligned}
a^{-1}bc &= \left(\boldsymbol{\overline{e}a^{-1}\overline{ea^{-1}}^{-1}}\right)\left(\overline{a^{-1}}b\overline{a^{-1}b}^{-1}\right)\left(\overline{a^{-1}b}c\overline{a^{-1}bc}^{-1}\right) \\
&= \left(\boldsymbol{\overline{a^{-1}}a\overline{e}^{-1}}\right)^{\boldsymbol{-1}}\left(\overline{a^{-1}}b\overline{a^{-1}b}^{-1}\right)\left(\overline{a^{-1}b}c\overline{a^{-1}bc}^{-1}\right) \\
&= \left(\boldsymbol{\overline{a^{-1}}a\overline{a^{-1}a}^{-1}}\right)^{\boldsymbol{-1}}\left(\overline{a^{-1}}b\overline{a^{-1}b}^{-1}\right)\left(\overline{a^{-1}b}c\overline{a^{-1}bc}^{-1}\right)
\end{aligned}$$

where each element in parenthesis, on the final line, is a generator of H, not G. Notice how the first bold factor begins in the form $k'a^{-1}\overline{k'a^{-1}}^{-1}$. Recall from the previous section that something in this form is the inverse of a generator of H, i.e. the inverse of an element of S. Thus we know there is a $k \in \mathcal{K}$ such that $k'a^{-1}\overline{k'a^{-1}}^{-1} = \left(ka\overline{ka}\right)^{-1}$. And, in fact

$$k' = \overline{e} \text{ and } k = \overline{k'a^{-1}} = \overline{\overline{e}a^{-1}} = \overline{a^{-1}}.$$

In even more excruciating detail, this is how we get from $k'a^{-1}\overline{k'a^{-1}}^{-1}$ to $\left(ka\overline{ka}\right)^{-1}$:

$$\begin{aligned}\left(k'a^{-1}\overline{k'a^{-1}}^{-1}\right)^{-1} &= \overline{k'a^{-1}}a(k')^{-1} \\ &= \overline{k'a^{-1}}a\overline{k'}^{-1} && \text{by (iii) from §5} \\ &= \overline{k'a^{-1}}a\overline{k'a^{-1}a}^{-1}.\end{aligned}$$

Then taking the respective inverses of both sides yields

$$\begin{aligned}k'a^{-1}\overline{k'a^{-1}} &= \left(\overline{k'a^{-1}}a\overline{k'a^{-1}a}^{-1}\right)^{-1} \\ &= \left(ka\overline{ka}^{-1}\right)^{-1} && \text{for } k = \overline{k'a^{-1}}.\end{aligned}$$

In practice it might be simpler to deal with a specific element, rather than in this generality, like we did with the example at the beginning of this section with

$$\left(\overline{e}a^{-1}\overline{ea^{-1}}^{-1}\right) = \left(\overline{a^{-1}}a\overline{a^{-1}a}^{-1}\right)^{-1},$$

but it's kind of nice to know the relationship between k' and k. So there it is!

If generalized, this basically becomes the Reidemeister rewriting process. But first, some new notation for the elements of S. We'll say that

$$s_{k,a_\nu} \in S \text{ means } s_{k,a_\nu} = ka_\nu\overline{ka_\nu}^{-1}.$$

Using this new notation in the above example yields

$$\begin{aligned}a^{-1}bc &= \left(\overline{a^{-1}}a\overline{a^{-1}a}^{-1}\right)^{-1}\left(\overline{a^{-1}}b\overline{a^{-1}b}^{-1}\right)\left(\overline{a^{-1}b}c\overline{a^{-1}bc}^{-1}\right) \\ &= s_{k_1,a}^{-1} \cdot s_{k_2,b} \cdot s_{k_3,c},\end{aligned}$$

where $k_1 = \overline{a^{-1}}, k_2 = \overline{a^{-1}},$ and $k_3 = \overline{a^{-1}b}$.

With this notation, we are now ready to define the Reidemeister rewriting function.

The Reidemeister Rewriting Process

Let $h = a_{\nu_1}^{\epsilon_1} a_{\nu_2}^{\epsilon_2} \dots a_{\nu_r}^{\epsilon_r}$ $(\epsilon_j = \pm 1)$ *be a word in the generators of* G *that defines an element of* H*. Define the mapping* τ *in the following way:*

$$\tau(h) = s_{k_1, a_{\nu_1}}^{\epsilon_1} s_{k_2, a_{\nu_2}}^{\epsilon_2} \cdots s_{k_r, a_{\nu_r}}^{\epsilon_r}$$

where

$$k_j = \begin{cases} \overline{a_{\nu_1}^{\epsilon_1} a_{\nu_2}^{\epsilon_2} \dots a_{\nu_{j-1}}^{\epsilon_{j-1}}} & \text{if } \epsilon_j = 1 \\ \overline{a_{\nu_1}^{\epsilon_1} a_{\nu_2}^{\epsilon_2} \dots a_{\nu_j}^{-1}} & \text{if } \epsilon_j = -1 \end{cases}$$

We say that τ *is a Reidemeister rewriting process.*

In order to prove that τ is in fact a rewriting process, we need to show that h and $\tau(h)$ are the same group element in H. To do this, recall from before equation (38):

$$h = \overline{W_1} a_{\nu_1}^{\epsilon_1} \overline{W_1 a_{\nu_1}^{\epsilon_1}}^{-1} \cdot \overline{W_2} a_{\nu_2}^{\epsilon_2} \overline{W_2 a_{\nu_2}^{\epsilon_2}}^{-1} \cdot \dots \cdot \overline{W_r} a_{\nu_r}^{\epsilon_r} \overline{W_r a_{\nu_r}^{\epsilon_r}}^{-1}$$

where W_j is defined as:

$$W_j = a_{\nu_1}^{\epsilon_1} a_{\nu_2}^{\epsilon_2} \dots a_{\nu_{j-1}}^{\epsilon_{j-1}}.$$

We saw from before that the right hand side defines the same group element as the left hand side. Now we have two cases to consider (note: I make free use of property (iv) of Lemma 5.1 without reference):

Case 1 ($\epsilon_j = 1$):

$$\begin{aligned} s_{k_j, a_{\nu_j}} &= k_j a_{\nu_j} \overline{k_j a_{\nu_j}}^{-1} = \overline{W_j} a_{\nu_j} \overline{W_j a_{\nu_j}}^{-1} \qquad \text{by definition of } k_j \text{ and } W_j \\ &= \overline{W_j} a_{\nu_j}^{\epsilon_j} \overline{W_j a_{\nu_j}^{\epsilon_j}}^{-1}. \end{aligned}$$

Case 2 ($\epsilon_j = -1$):

$$\begin{aligned} s_{k_j, a_{\nu_j}}^{-1} &= \left(k_j a_{\nu_j} \overline{k_j a_{\nu_j}}^{-1} \right)^{-1} \\ &= \left(\overline{W_j a_{\nu_j}^{-1}} a_{\nu_j} \overline{W_j a_{\nu}^{-1} a_{\nu_j}}^{-1} \right)^{-1} \qquad \text{since } k_j = \overline{W_j a_{\nu_j}^{-1}} \text{ in this case} \\ &= \overline{W_j} a_{\nu_j}^{-1} \overline{W_j a_{\nu_j}^{-1}}^{-1} \\ &= \overline{W_j} a_{\nu_j}^{\epsilon_j} \overline{W_j a_{\nu_j}^{\epsilon_j}}^{-1}. \end{aligned}$$

Thus, in either case, we have $s_{k_j, a_{\nu_j}}^{\epsilon_j} = \overline{W_j} a_{\nu_j}^{\epsilon_j} \overline{W_j a_{\nu_j}^{\epsilon_j}}^{-1}$. Hence

$$\begin{aligned} \tau(h) &= s_{k_1, a_{\nu_1}}^{\epsilon_1} s_{k_2, a_{\nu_2}}^{\epsilon_2} \cdots s_{k_2, a_{\nu_r}}^{\epsilon_r} \\ &= \overline{W_1} a_{\nu_1}^{\epsilon_1} \overline{W_1 a_{\nu_1}^{\epsilon_1}}^{-1} \cdot \overline{W_2} a_{\nu_2}^{\epsilon_2} \overline{W_2 a_{\nu_2}^{\epsilon_2}}^{-1} \cdot \dots \cdot \overline{W_r} a_{\nu_r}^{\epsilon_r} \overline{W_r a_{\nu_r}^{\epsilon_r}}^{-1} \\ &= h \end{aligned}$$

as was shown before.

6.2 A Simplified Presentation for H

6.2.1 Reidemeister's Presentation

Using the Reidemeister rewriting process, we can obtain a presentation for H with a more manageable, i.e. finite, list of relations. The following theorem states this fact formally:

Theorem 6.1. *Let τ be a Reidermeister rewriting process for a subgroup H of a group G. If G has the presentation $G = \langle a_\nu, \cdots \mid R_\mu, \dots \rangle$, then H has the presentation*

$$H = \langle s_{k,a_\nu}, \cdots \mid s_{k,a_\nu} = \tau(ka_\nu \overline{ka_\nu}^{-1}), \dots, \tau(kR_\mu k^{-1}), \dots \rangle$$

under the mapping $s_{k,a_\nu} \to ka_\nu \overline{ka_\nu}^{-1}$, where $k \in \mathcal{K}$.

6.2.2 Example of Reidemeister's Presentation

Although it is fairly routine to verify that the Reidemeister presentation gives a valid presentation (just using the checklist provided in Section 2.2.3), it is more illuminating to work through a concrete example in detail. For this purpose, we return to Running Example 1. In this case we have

$$G/H = \{H, Ha\}$$

where $H = \{e, a^2, a^2b, b\}$ and $Ha = \{a, a^3, ab, a^3b\}$. Thus a possible transversal for G/H could be:

$$\mathcal{K} = \{e, ab\}.$$

Referring to Theorem 6.1, H will have the following list of generators:

$$\{s_{e,a}, s_{e,b}, s_{ab,a}, s_{ab,b}\}.$$

Some of whose relations are of the form $s_{k,a_\nu} = \tau(ka_\nu \overline{ka_\nu}^{-1})$ seen below.

$$s_{e,a} = \tau(ea\overline{ea}^{-1}) = \tau(a\overline{a}^{-1}) = \tau(a(ab)^{-1}) = \tau(ab^{-1}a^{-1}) = s_{e,a}s_{ab,b}^{-1}s_{e,a}^{-1} \tag{39}$$

$$s_{e,b} = \tau(eb\overline{eb}^{-1}) = \tau(b) = e \tag{40}$$

$$s_{ab,a} = \tau((ab)a\overline{(ab)a}^{-1}) = \tau(aba) = s_{e,a}s_{ab,b}s_{ab,a} \tag{41}$$

$$s_{ab,b} = \tau((ab)b\overline{(ab)b}^{-1}) = \tau(abbb^{-1}a^{-1}) = s_{e,a}s_{ab,b}s_{ab,b}s_{ab,b}^{-1}s_{e,a}^{-1}. \tag{42}$$

The details, for all but line (39), are left to the reader. To evaluate τ above, we are using the fact that τ is a Reidemeister rewriting process, and using the definition from Section 6.1.

According to Theorem 6.1, we also have relations of the form $\tau(kR_\mu k^{-1}) = e$, shown below.

$$e = \tau(ea^4e^{-1}) = \tau(aaaa) = s_{e,a}s_{ab,a}s_{e,a}s_{ab,a} \tag{43}$$

$$e = \tau(eb^2e^{-1}) = \tau(bb) = s_{e,b}s_{e,b} \tag{44}$$

$$e = \tau(eababe^{-1}) = \tau(abab) = s_{e,a}s_{ab,b}s_{ab,a}s_{e,b} \tag{45}$$

$$e = \tau((ab)a^4(ab)^{-1}) = \tau(abaaaab^{-1}a^{-1}) = s_{e,a}s_{ab,b}s_{ab,a}s_{e,a}s_{ab,a}s_{e,a}s_{ab,b}^{-1}s_{e,a}^{-1} \tag{46}$$

$$e = \tau((ab)b^2(ab)^{-1}) = \tau(abbbb^{-1}a^{-1}) = s_{e,a}s_{ab,b}s_{ab,b})s_{ab,b}s_{ab,b}^{-1}s_{e,a}^{-1} \tag{47}$$

$$e = \tau((ab)abab(ab)^{-1}) = \tau(abababb^{-1}a^{-1}) = s_{e,a}s_{ab,b}s_{ab,b}s_{e,b}s_{e,a}s_{ab,b}s_{ab,b}^{-1}s_{e,a}^{-1}. \tag{48}$$

By canceling group elements when possible and cleaning things up (for instance, eliminating $s_{e,b}$, since (40) says that $s_{e,b} = e$), we get the following list of relations:

$$
\begin{align}
s_{e,a}s_{ab,b} &= e \tag{49}\\
s_{ab,a}s_{ab,b} &= e \tag{50}\\
s_{ab,b}s_{e,a} &= s_{e,a}s_{ab,b} \tag{51}\\
(s_{e,a}s_{ab,a})^2 &= e \tag{52}\\
s_{e,a}s_{ab,b}s_{ab,a} &= e \tag{53}\\
(s_{ab,a}s_{e,a})^2 &= e \tag{54}\\
s_{ab,a}^2 &= e \tag{55}\\
s_{ab,a}s_{e,a}s_{ab,b} &= e. \tag{56}
\end{align}
$$

6.2.3 Reducing to a More Familiar Presentation

The relations (49) through (56) might not look like what we'd expect as a set of relations for the presentation of the Klein-4 group, V, the subgroup used in Running Example 1. If x and y are generators of V, then a familiar presentation of V could be

$$V = \langle x, y, z \mid x^2, y^2, (xy)^2 \rangle.$$

Notice that by combining (54) and (56), we obtain $s_{ab,b}^2 = e$. By (55), we see that $s_{ab,a}^2 = e$. I'll leave the details to the reader, but it is possible to then derive $(s_{ab,b}s_{ab,a})^2 = e$ from the relations (49) through (56) as well. Thus, under the identification $s_{ab,b} \Rightarrow x$ and $s_{ab,a} \Rightarrow y$ the relations (49) through (56) reduce to the familiar relations for V seen above.

6.3 Reidemeister's Presentation using a Schreier Transversal

6.3.1 Schreier Transversal

Recall from Section 5 the initial segments of a word. For example, if $w = a^2bc$, then the initial segments of w, in order, are $e, a, a^2, a^2b,$ and a^2bc. A **Schreier transversal** is simply a transversal that is closed under initial segments. Some hypothetical transversals that are Schreier include

$$\{e, a, b, c, ac\}, \{e, a, a^2, a^2b\}.$$

Hypothetical transversals that would not be Schreier include

$$\{e, a, b, cd\}, \{e, c, ab, b\}, \{e, x, y, x^2y\}.$$

The following lemma states that, when G is finitely generated, a Schreier transversal always exists.

Lemma 6.2. *Let $G = \langle a_1, \ldots, a_n \mid P, Q, R, \ldots \rangle$ and let H be a subgroup of G. Then there is a Schreier transversal for G/H.*

Proof. We call the **length of a coset** of G/H the length of the shortest word in it. Let us use $\ell(w)$ to represent the length of the word w. The function ℓ is additive. For example $\ell(a^2b) = 3 = \ell(a) + \ell(ab) = 1 + 2$, etc. We will prove Lemma 6.2 inductively on the length of the cosets G/H.

For each coset in G/H, we want to choose a representative in the transversal whose length is equal to the length of the coset. In particular, note that this implies $\ell(\overline{w}) \leq \ell(w)$ for all $w \in H\overline{w}$. Choose e as the representative for H, the coset with length zero. If H_1 is any coset with length one, choose any word of length one to represent it. Suppose H_2 is any coset with length two. Let x_1x_2 be any word of length two in H_2, where x_i is a generator, or the inverse of a generator, in the presentation of G. By Lemma 5.2, part (iv), $\overline{x_1}x_2 \in H_2$. Since H_2 is length two, then $\ell(\overline{x_1}x_2) \geq 2$, by which we have the following inequality:

$$2 \leq \ell(\overline{x_1}x_2) = \ell(\overline{x_1}) + \ell(x_2) = \ell(\overline{x_1}) + 1.$$

Thus, $\ell(\overline{x_1}) \geq 1$. But $\ell(\overline{x_1}) \leq \ell(x_1) = 1$, so we conclude that $\ell(\overline{x_1}) = 1$. This means that, on the one hand, $\overline{x_1}x_2$ has length two, and on the other hand, that $\overline{x_1}$ is the representative of a coset of length one, and hence has already been chosen! We choose $\overline{x_1}x_2$ as our representative of H_2 in the transversal.

For our induction hypothesis, assume we have chosen a representative in the transversal for cosets of length less than n in the manner stated in the first sentence of the above paragraph. Suppose that H_n is a coset of length n. In other words, the least length word in H_n is n. Pick an element of H_n with this least length, say $x_1x_2\cdots x_{n-1}x_n$. By Lemma 5.2, part (iv), $\overline{x_1x_2\cdots x_{n-1}}x_n \in H_n$. Thus $\ell(\overline{x_1x_2\cdots x_{n-1}}x_n) \geq n$, which as before implies that $\ell(\overline{x_1x_2\cdots x_{n-1}}) \geq n-1$. By construction we also have that

$$\ell(\overline{x_1x_2\cdots x_{n-1}}) \leq \ell(x_1x_2\cdots x_{n-1}) = n-1.$$

Thus $\ell(\overline{x_1x_2\cdots x_{n-1}}) = n-1$. This means that $\overline{x_1x_2\cdots x_{n-1}}$ is the representative in the transversal of a coset of length $n-1$, and, according to our hypothesis, has already been chosen for the transversal! Thus $\overline{x_1x_2\cdots x_{n-1}}x_n$ has length n, and it's initial segment is already in the transversal, so we choose it as the representative of H_n in the transversal. □

6.3.2 Reidemeister-Schreier's Presentation

Using the Schreier transversal, we get a further simplified presentation for a subgroup H, stated in the following theorem.

Theorem 6.3. *Suppose G has the following presentation:*

$$G = \langle a_1, \ldots, a_n \mid P, Q, R, \ldots \rangle, \tag{57}$$

and let H be a subgroup of G. If τ is a Reidemeister-Schreier rewriting process, then H can be presented as

$$\langle s_{k,a_\nu}, \cdots \mid s_{m,a_\lambda}, \ldots, \tau(kRk^{-1}), \ldots \rangle, \tag{58}$$

where k is an element of a Schreier transversal for G/H, a_ν is any generator of G and R is any relator in (57), and m is a Schreier representative and a_λ a generator such that

$$ma_\lambda \text{ is freely equal to } \overline{ma_\lambda}. \tag{59}$$

6.3.3 Example of Reidemeister-Schreier's Presentation

Here again, it is fairly routine to verify that the Reidemeister-Schreier presentation gives a valid presentation (just using the checklist provided in Section 2.2.3), it is more illuminating to work through a concrete example in detail. For this purpose, we return to Running Example 2.

First, we would like to find a Schreier transversal for H. Using Lemma (6.2) as a guide, let the Schreier representative for H be e. Notice that $H_1, H_2,$ and H_3 all have length one. For each there is only one element of length one, namely $a, b,$ and c, respectively. The length of $H_4, H_5, H_6,$ and H_7 is two. Lemma (6.2) requires that we pick elements of length two to begin finding their respective Schreier representatives, but again there is only one such choice for each. Thus, a Schreier transversal for G/H is

$$\mathcal{K} = \{e,\ a,\ b,\ c,\ a^2,\ ab,\ ac,\ bc\}. \tag{60}$$

Next we need to find for which choices $m \in \mathcal{K}$ and a_λ in the generating set $\{a, b, c\}$ are ma_λ freely equal to $\overline{ma_\lambda}$. To that end, see the following table (note: to save space, $\approx$? stands for "Are they freely equal?"):

ma_λ		$\overline{ma_\lambda}$	$\approx$?	ma_λ		$\overline{ma_\lambda}$	$\approx$?	ma_λ		$\overline{ma_\lambda}$	$\approx$?
ea	$\rightarrow$	a	Y	eb	$\rightarrow$	b	Y	ec	$\rightarrow$	c	Y
aa	$\rightarrow$	a^2	Y	ab	$\rightarrow$	ab	Y	ac	$\rightarrow$	ac	Y
ba	$\rightarrow$	c	N	bb	$\rightarrow$	e	N	bc	$\rightarrow$	bc	Y
ca	$\rightarrow$	ac	N	cb	$\rightarrow$	bc	N	cc	$\rightarrow$	e	N
a^2a	$\rightarrow$	bc	N	a^2b	$\rightarrow$	ac	N	a^2c	$\rightarrow$	ab	N
aba	$\rightarrow$	b	N	abb	$\rightarrow$	a	N	abc	$\rightarrow$	a^2	N
aca	$\rightarrow$	ab	N	acb	$\rightarrow$	a^2	N	acc	$\rightarrow$	a	N
bca	$\rightarrow$	e	N	bcb	$\rightarrow$	c	N	bcc	$\rightarrow$	b	$N.$

So out of the 24 possible expressions of the form ma_λ, only 7 are freely equal to their respective representatives in the Schreier transversal. Note that for the remaining relators, that are of the form $\tau(kRk^{-1})$, there are 8 choices for k and 6 choices for R, so there are a total of 48 relators of this form. This brings the total relators in a presentation for H to 55. At this point it's beginning to seem a little difficult to see how this new presentation is simplifying things. Let us revisit Running Example 1 (defined at the bottom of Section 3.2), and compare it to our results in Section 6.2.2 to get a better sense of this.

Recall that in Running Example 1, $[G : H] = 2$, with $G/H = \{\{e, a^2, a^2b, b\}, \{a, a^3, ab, a^3b\}\} = \{H, Ha\}$. As usual, we choose e as the Schreier representative for H. Notice that Ha has length one, and contains only one element of length one as well, namely a. Thus a Schreier transversal in this case is

$$\mathcal{K} = \{e, a\}.$$

According to Theorem 6.3, the generating symbols for H are of the form s_{k,a_ν}, of which there are the following four:

$$s_{e,a}, s_{e,b}, s_{a,a}, \text{ and } s_{a,b}.$$

Then we have relations of two different types. First, those of the form s_{m,a_λ}, where ma_λ is freely equal to $\overline{ma_\lambda}$. In this case there is only one out of a total possible four that satisfy this relation, as can be seen in the following table:

ma_λ		$\overline{ma_\lambda}$	freely equal?	ma_λ		$\overline{ma_\lambda}$	freely equal?
ea	$\rightarrow$	a	Y	eb	$\rightarrow$	e	N
ab	$\rightarrow$	a	N	ab	$\rightarrow$	a	$N.$

Thus the only relation of this type that we obtain is $s_{e,a} = e$. The second type of relator in Theorem 6.3 is of the form $\tau(kRk^{-1})$, of which we have $2 \cdot 3 = 6$, in this case. Calculating these similar to how we calculated them in 6.2.2 yields

$$\begin{aligned}
s_{e,a}s_{a,a}s_{e,a}s_{a,a} &= e \\
s_{e,b}s_{e,b} &= e \\
s_{e,a}s_{a,b}s_{a,a}s_{e,b} &= e \\
s_{e,a}s_{a,a}s_{e,a}s_{a,a} &= e \\
s_{e,a}s_{a,b}s_{a,b}s_{e,a}^{-1} &= e \\
s_{e,a}s_{a,a}s_{e,b}s_{e,a}s_{a,b}s_{e,a}^{-1} &= e.
\end{aligned}$$

Cleaning this up by cancelling group elements, using the fact that $s_{e,a} = e$, and eliminating one redundant relation, we obtain

$$(s_{a,a})^2 = e \tag{61}$$

$$(s_{e,b})^2 = e \tag{62}$$

$$s_{a,b}s_{a,a}s_{e,b} = e \tag{63}$$

$$(s_{a,b})^2 = e \tag{64}$$

$$s_{a,a}s_{e,b}s_{e,a}s_{a,b} = e. \tag{65}$$

Comparing this cleaned up list of relations to the final list of Section 6.2.2, we have something noticeably more simple.

6.3.4 Reducing to a More Familiar Presentation

As we have already done twice with the previous two presentations, it might be nice to see that the defining set of relations that we get for V from the Reidemeister-Schreier theorem will also derive a common and familiar presentation for V. Recall that the Klein-4 group, V, need only two generators, say x and y, and is often defined by the relators $x^2, y^2,$ and $(xy)^2$. Consider the identifications $s_{a,a} \Rightarrow x$, $s_{e,b} \Rightarrow y$, and $s_{a,b} \Rightarrow z$. Then (61) through (65) from above becomes

$$x^2 = e \tag{66}$$

$$y^2 = e \tag{67}$$

$$zxy = e \tag{68}$$

$$z^2 = e \tag{69}$$

$$xyz = e \tag{70}$$

Notice that (66) and (67) are already two of the familiar relators we want. To get the third, observe that (68) and (69) yield $xy = z$, and by substituting this result into (69), we obtain $(xy)^2 = e$.

References

[1] Gilbert Baumslag, Benjamin Fine, and Xiaowei Xu. *Cryptosystems Using Linear Groups*. Springer-Verlag, 2006.

[2] Wilhelm Magnus, Abraham Karras, and Donald Solitar. *Combinatorial Group Theory*. Dover Publications, INC, Mineola, New York, 1976.

[3] Paolo Aluffi. *Algebra: Chapter 0*. American Mathematical Society, 2009.

[4] Gilbert Baumslag. *Topics in Combinatorial Group Theory*. Birkhäuser, 1993.

[5] Joseph A. Gallian *Contemporary Abstract Algebra*. Cengage, 2017