Implementation of the Todd-Coxeter Algorithm to Finitely Presented Groups

Tomas Reed

Advisor: Prof. Arne Meurman

The mathematician, carried along on his flood of symbols, dealing apparently with purely formal truths, may still reach results of endless importance for our description of the physical universe.
Karl Pearson

Popular Science Description

Symmetry is something humans comprehended thousands of years ago. It appears in all aspects of our lives; in art, architecture, poetry, carpets and rugs, music and nature. The human eye is attracted to symmetry and objects that look symmetric. The perfect mirror image and the order, we cannot resist it.

If we would like to take the notion of symmetry, and define it mathematically, how can we do that? It was the ingenuity of the French mathematician Évariste Galois, who invented a language which is needed for showing that a polynomial of degree five and above does not possess a "nice" solution using the mathematical operations we know from school (addition, subtraction, multiplication, division, and taking the nth root). The new language that emerged is what we have today as "group theory". In some sense, Galois studied the "symmetry of the equations", and the reason such a solution is not possible is because the equations have "the wrong kind of symmetry" as Ian Stewart says in [Ste08]. It is necessary to say that mathematicians before Galois had already got results in group theory, but Galois was the one to understand the structure and to use it for his attack on the problem of polynomial solutions. As Israel Herstein writes in [Her64]:

> Very often in mathematics the crucial problem is to recognize and to discover what are the relevant concepts; once this is accomplished the job may be more than half done.

Group theory is the language of mathematics to describe and measure the notion of symmetry. We all have the understanding of what symmetry is, but a concrete, down to earth, way of describing it is:

> Symmetry is not a number or a shape, it is a *transformation* - a way to move an object. If the object looks the same after being transformed, then the transformation concerned is a symmetry.
> [Ste08]

Think about a square. Now rotate the square 90 degrees counterclockwise. Do it again. Is there any visual difference between what we have started with and what we finished with? Hopefully you answer this questions with "no". The rotation of 90 degrees counterclockwise you did is called a transformation. The object looks the same after the transformation. So the transformation concerned is a symmetry. In a similar way, we can draw an imaginary horizontal line right in the middle of the square. If we take the upper half of the square and the lower half of the square and switch their places, we will get the same figure of a square. This is again a symmetry.

The group structure in mathematics allows us to study objects in which symmetry is built into them. In some sense, this is the simplest structure we have. We take a set of objects (does not need to be numbers or functions. It can be anything, including puppies and kittens), and allowing one operation on the elements of the set, such that they satisfy some axioms. This is very simple and yields a beautiful theory.

It turns out that group theory has a deep connection with other physical sciences. For example, in chemistry, symmetry is used in order to classify molecules by their shape. Moreover, chemists use symmetry in studying crystals (See Dan Shechtman, awarded the 2011 Nobel Prize in Chemistry). Physicists also use group theory, for example, in quantum mechanics. Biologists use group theory in molecular systems biology.

While there is a formal mathematical definition for the group structure, usually it is the case where we need to show that a certain structure is a group. However, in some cases we would like to take an arbitrary set of objects and from them **to build** a group in which some elements may or may not satisfy conditions we dictate. So how do we do it? Here comes the phrase "presentation of a

group". Presentation of a group is exactly the way to solve this problem. We take elements that we want to generate (to "create") the group and adding (if we want) some prescribed conditions on these elements. Of course, it requires more details to build it which can be found in this work.

Abstract

This work presents the notion of free groups and the definition of a group using generators and relations. We use the Todd-Coxeter Algorithm in order to solve the coset enumeration problem for the finitely presented groups: D_4, A_4, A_5, S_3, S_4, S_5, $PSL_2(7)$, $PSL_2(9)$. Then we use these presentations in order to prove the exceptional isomorphisms $A_5 \cong PSL_2(5) \cong SL_2(4)$, $PSL_2(9) \cong A_6$ and $SL_3(2) \cong PSL_2(7)$.

To my family

acknowledgment

I would like to express my special thanks of gratitude to my advisor, Prof. Arne Meurman, who introduced me to the wonderful world of combinatorial group theory. I would also like to thank him for the guidance, patience, help and for contributing from his abundance experience, knowledge and wisdom. It was an honor for me to get a glimpse to his world and way of thinking.

Contents

"Being a mathematician is a bit like being a manic depressive: you spend your life alternating between giddy elation and black despair."
Steven G. Krantz, A Primer of Mathematical Writing

1 Introduction

The concept of group theory was first grasped and used by Galois (although without definition), who used it in a paper explaining the conditions for a polynomial to be solvable by radicals. The (axiomatized) definition we use today is due to Heinrich Weber and Walther von Dyck. Except an interesting research area in mathematics (not just in algebra, but also, for example, in topology), groups are used in physics, chemistry, material science and computer science. Groups, in some sense, are the mathematical way of describing symmetry. So not many words are needed to understand the abundance of groups in our lives.

During the first half of the 20^{th} century there were two meanings of the term 'abstract group':

(1) The axomatized definition (associativity, identity and inverses).

(2) Definition using generators and defining relations.

The second meaning was due to Walther von Dyck. Von Dyck published a paper in 1882 named "Gruppentheoretische Studien" (studies in group theory), [Dyc82], where he first introduced the notion of a group defined by generators and relations (however, did not prove the existence of such a group). This marked the rise of the subject called Combinatorial Group Theory. Combinatorial group theory can be thought of as the study of free groups and groups defined by generators and relations, or shorter, by a presentation.

A presentation of a group consists of a set X and a set R of relations on the elements of X. The elements of X are called generators and the elements of R are called relators. It is denoted as $\langle X \mid R \rangle$. The presentation is called finite if both X and R are finite sets, and we say that the group is finitely presented. This way of representing a group has a few advantages, including an easy way of understanding the relations between the elements, for calculation purposes and compact view of the group. In addition, we can create groups that satisfy some relations that we dictate, so we have some power (although it might be that unintentionally we created the trivial group or other well-known groups). However, given a presentation, it is almost impossible to analyze the group and answer questions such as "is the group finite? infinite?", "is it Abelian?" or "is it the trivial group?". We shall see an example later.

Free groups are groups of the form $\langle X \mid \rangle$; that is, with no nontrivial relations between the generators. A nontrivial relation is not a relation that comes from the axioms of a group, such as $xx^{-1} = e$. We start by defining free groups and then show that they indeed exist. Free groups are important, as we prove that every group is isomorphic to a factor group of a free group.

We all know that a subgroup of a group induces a partition of this group, and by Lagrange's theorem all the pieces of this partition (i.e. cosets) are of the same cardinality. Now, let us look at the following problem: Given a finite group (presented by generators and relations), with unknown order, and given a subgroup of this group in which the order is known, how can we find the order of the group? Coset enumeration (counting the cosets) is a solution to this problem. If we know the number of pieces comprising the group, and each has the same size, it is easy to calculate the order of the group. In this work, we chose subgroups in which we thought we can calculate their order. As we said, it is almost impossible to analyze a group by its presentation, so by taking a subgroup we could only conjecture its order and in the worst case to get an upper bound to the order of the group.

The method we used for the coset enumeration is the Todd-Coxeter Algorithm. This is not the only method that exist for coset enumeration. However, as Todd and Coxeter write in their paper [TC36] from 1936:

> "... in fact, the method can be reduced to a purely mechanical process, which becomes a useful tool with a wide range of application".

A coin has two sides, so the Todd-Coxeter Algorithm. One of the main reasons for the title of this thesis is given as a Theorem 3.4 in [Coh99]:

Theorem. Suppose the index of H in G is finite. Any Todd-Coxeter coset enumeration procedure in which it is taken care of that

(i) each row of each table is completely filled (or deleted) after a finite number of steps, and

(ii) there are only finitely many steps between two scannings of the tables for coincidences,

will terminate.

An additional problem is that the algorithm does not give any maximum limit for the number of steps required to achieve the goal. In fact, even for finite groups, in practical terms, it can happen that the machine will run out of memory or just break down before the procedure ends! However, it is unfair to blame the algorithm for that, since no algorithm can decide in a finite number of steps if a finite presentation is the trivial group, a problem that has been proved to be undecidable.

Then we use the presentations we found in order to prove some special and intriguing isomorphisms. These proofs become easier once our target is to show that these groups have the same presentation. This is thanks to Theorem 2.3, called Von Dyck Theorem, that says that a group defined by generators and relations is the largest possible such group, and thus, yields a **surjective homomorphism** on any group with the same number of generators and satisfying the same relations.

The work is concluded with an appendix on the GAP software. We give a basic and non-extensive explanation on how to use the GAP software to obtain a coset table. GAP uses the Todd-Coxeter Algorithm for finitely presented groups to enumerate the cosets. GAP also has additional package for interactive Todd-Coxeter Algorithm and one can see the process step-by-step. The interested reader can find the package and a manual file at *https://www.gap-system.org/Packages/itc.html*. We thought it will be appropriate to add the appendix since doing the enumeration by hand, even for relatively small groups, is time-consuming, prone to errors and generally a difficult task (the author can testify).

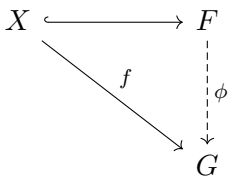
"If you don't like your analyst, see your local algebraist!".
Gert Almkvist (founder and director of The Institute for Algebraic Meditation)

2 Free Groups

A useful way of specifying a group G is by generators and relations. In this case, we are given a list of generators such that the group consists of products of powers of these generators, with a list of equations (called relations) that the generators must satisfy. However, in order to define the notion of presentation of a group by generators and relations, we must do some groundwork.

Definition 1. If X is a subset of a group F, then F is a **free group with basis** X if for every group G and any function $f : X \to G$ there is a unique homomorphism $\phi : F \to G$ such that $\phi(x) = f(x)$, $\forall x \in X$.

Using a commutative diagram, the definition can be seen as



Having a definition is nice but it does not mean that such an object exists. We would like to show that a free group indeed exists, and we shall do it using the following construction: Given a set X. If $X = \emptyset$, then F is defined to be the trivial group $\{e\}$. If $X \neq \emptyset$, let X^{-1} be a set with the same cardinality as X and be disjoint from X, i.e., $X \cap X^{-1} = \emptyset$. Choose a bijection from X to X^{-1} and denote the image of $x \in X$ by x^{-1}. Finally, choose a singleton that is disjoint from $X \cup X^{-1}$ and denote this element by 1.

Definition 2. A **word** on X is a sequence $(a_1, a_2, \ldots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that for some $n \in \mathbb{Z}^+$ we have $a_k = 1$, $\forall k \geq n$. The constant sequence $(1, 1, \ldots)$ is called the **empty word** and is denoted by 1.

Definition 3. A word $(a_1, a_2, \ldots)$ is said to be **reduced** if:

- $\forall x \in X$, the elements x and x^{-1} are not adjacent.
- If $a_n = 1$ then $a_k = 1$ for all $k \geq n$.

In particular, the empty word is reduced.

Now, every non-empty reduced word is of the form $(x_1^{\lambda_1}, \ldots, x_n^{\lambda_n}, 1, \ldots)$ where $n \in \mathbb{Z}^+$ and $\lambda_i = \pm 1$, $i = 1, \ldots, n$. Let us use a shortened and easier way to write such a reduced word. We shall write such a word as $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$.

Note: Two reduced words $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ and $y_1^{\delta 1} y_2^{\delta_2} \cdots y_m^{\delta_m}$ are equal if and only if $m = n$ and $x_i = y_i$, $\lambda_i = \delta_i$, $i = 1, 2, \ldots n$, or they are both 1. Thus, we can say that the map from X to $F(X)$ with $x \mapsto x^1$ is injective. From now on we shall identify X with its image and treat X as a subset of $F(X)$.

Let us now define a binary operation on the set $F(X)$: the empty word 1 is to act as the identity element; that is, $w \cdot 1 = 1 \cdot w = w$, $\forall w \in F(X)$. The natural way to define the product on two non-empty reduced words $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$ and $y_1^{\delta 1} y_2^{\delta_2} \cdots y_m^{\delta_m}$ is by concatenation. However, it might be that the product in this case will not yield a reduced word. For example, $x_1 x_2 x_3$ and $x_3^{-1} x_2^{-1} x_4$ yield $x_1 x_2 x_3 x_3^{-1} x_2^{-1} x_4$, which is not reduced. We need to be careful and take care of such cases. Thus, our definition of such product will still be by concatenation but with solution to such a case:

if $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$ and $y_1^{\delta 1}y_2^{\delta_2}\cdots y_m^{\delta_m}$ are two non-empty reduced words, assuming $n \leq m$, let k be the largest integer $(0 \leq k \leq n)$ such that $x_{n-j}^{\lambda_{n-j}} = y_{j+1}^{-\delta_{j+1}}$ for $j = 0, 1, \ldots, k-1$. Then define:

$$(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n})(y_1^{\delta 1}y_2^{\delta_2}\cdots y_m^{\delta_m}) := \begin{cases} x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_{n-k}^{\lambda_{n-k}}y_{k+1}^{\delta_{k+1}}\cdots y_m^{\delta_m} & \text{if} \quad k < n \\ y_{n+1}^{\delta_{n+1}}\cdots y_m^{\delta_m} & \text{if} \quad k = n < m \\ 1 & \text{if} \quad k = n = m \end{cases}$$

If $n > m$, then the product defined analogously. The definition insures that the product of reduced words is again a reduced word.

We are now ready to prove that the set $F(X)$ that we have constructed is a group.

Theorem 2.1. If X is a non-empty set and $F(X)$ is the set of all reduced words on X, then $F(X)$ is a group under the product we defined above. Moreover, $F(X) = \langle X \rangle$.

Proof. Since 1 is the identity element, and each element $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$ has an inverse, $x_n^{-\lambda_n}\cdots x_1^{-\lambda_1}$, all we have to prove is that the operation is associative. For proving this, we are going to present a bijection from $F(X)$ to a group, which satisfies that homomorphism property. This will enforce associativity in $F(X)$.
For each $x \in X$ and $\delta = \pm 1$, let α_{x^δ} be the map from $F(X)$ to $F(X)$ with $1 \mapsto x^\delta$ and

$$x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n} \mapsto \begin{cases} x^\delta x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n} & \text{if} \quad x^\delta \neq x_1^{-\delta_1} \\ x_2^{\lambda_2}\cdots x_n^{\lambda_n} & \text{if} \quad x^\delta = x_1^{-\delta_1} \end{cases}$$

Since $\alpha_{x^\delta} \circ \alpha_{x^{-\delta}} = 1_{F(X)} = \alpha_{x^{-\delta}} \circ \alpha_{x^\delta}$, then each α_{x^δ} is a bijection (permutation) of $F(X)$.
Let F_0 be the group generated by $\{\alpha_x \mid x \in X\}$. The map $\phi : F(X) \to F_0$ given by $1 \mapsto 1$ and $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n} \mapsto \alpha_{x_1^{\delta_1}} \circ \cdots \circ \alpha_{x_n^{\delta_n}}$ is surjective, with the homomorphism property. Assume ϕ is not injective. Then it sends a word $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n} \neq 1$ to the identity map of $F(X)$. The image of the word $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$ is $\alpha_{x_1^{\delta_1}} \circ \cdots \circ \alpha_{x_n^{\delta_n}}$ which maps 1 to $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n} \neq 1$, so it is not the identity map of $F(X)$. Thus, ϕ is injective. From the discussion we see that ϕ is bijection. In addition, since ϕ satisfies the homomorphism property, then $\phi(a(bc)) = \phi(a)\phi(bc) = \phi(a)(\phi(b)\phi(c))$, and since F_0 is a group, we can apply its associativity into the last term to get $\phi(a)(\phi(b)\phi(c)) = (\phi(a)\phi(b))\phi(c) = \phi((ab)c)$, and since ϕ is injective, then $a(bc) = (ab)c$, which proves the associativity in $F(X)$. □

After showing that $F(X)$ is a group, all we have to do is to show that it is a free group on the set X.

Theorem 2.2. $F(X)$ is a free group on the subset X.

Proof. Let G be any group and let $f : X \to G$ be a set-map. We want to show that there exists a unique homomorphism from $F(X)$ to G that when restricted to X it agrees with $f(x), \forall x \in X$. Define $\bar{f} : F \to G$ by $\bar{f}(1) = 1$, and if $x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}$ is a non-empty reduced word on X, define $\bar{f}(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}) := f(x_1)^{\lambda_1}\cdots f(x_n)^{\lambda_n}$. It is obvious that $\bar{f}$ is homomorphism from $F(X)$ to G, and $f, \bar{f}$ agree on all $x \in X$. Let us now show that $\bar{f}$ is unique. Assume $g : F(X) \to G$ is another homomorphism that agrees with f on all $x \in X$. Then we have $g(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n}) = g(x_1^{\lambda_1})\cdots g(x_n^{\lambda_n}) = g(x_1)^{\lambda_1}\cdots g(x_n)^{\lambda_n} = f(x_1)^{\lambda_1}\cdots f(x_n)^{\lambda_n} =: \bar{f}(x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_n^{\lambda_n})$. Thus, $\bar{f}$ is unique. □

Corollary 2.2.1. Every group G is the homomorphic image of a free group.

Proof. Let X be a set of generators of G and let F be the free group on X. By Theorem 2.2 the inclusion map $X \to G$ induces a unique homomorphism $\bar{f} : F \to G$ such that $x \mapsto x \in G$. Since $G = \langle X \rangle$, the function $\bar{f}$ constructed in Theorem 2.2 is a surjective homomorphism onto G. □

From Corollary 2.2.1 and the first isomorphism theorem we get that

Corollary 2.2.2. Every group is isomorphic to a factor group of a free group.

So, in order to describe a group $G = \langle X \rangle$ up to isomorphism, all we need is the set X, the free group $F(X)$ and the kernel of the epimorphism $F \twoheadrightarrow G$ of Corollary 2.2.1, call it N. Now, if $w = x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} \in F$ is a generator of N, then under the epimorphism $F \twoheadrightarrow G$, we get that $w \mapsto x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} = e \in G$. The equation $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} = e \in G$ is called a **relation** on the generators x_i. So, a given group G can be completely described by a set of generators of G and a suitable set of relations on these generators. This description will not be unique as we can have different choices for X and different choices for the set of (suitable) relations.

Conversely, if we get a set X and a set Y of reduced words on X, we can find a group G with X as generators and all the relation $w = e \in G$, $w \in Y$ are satisfied. Let F be the free group on X and N the normal subgroup generated by Y (normal closure). Let G be the factor group F/N and identify X with its image in F/N under the natural homomorphism $F \twoheadrightarrow F/N$. Then G is a group generated by X, and by our construction all the relations $w = e\,(w \in Y)$ are satisfied since $w = x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} \in Y \implies x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} \in N \implies x_1^{\lambda_1} N x_2^{\lambda_2} N \cdots x_n^{\lambda_n} N = N$, which means that $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} = e \in G = F/N$.

Finally, we have arrived at the desired definition:

Definition 4. Let X be a set, and Y a set of reduced words on X. A group G is said to be the **group defined** by **generators** $x \in X$ **and relations** $w = e\,(w \in Y)$ provided that $G \cong F/N$, where F is the free group on X and N the normal subgroup of F generated by Y. We say that $\langle X \mid Y \rangle$ is a **presentation** of G.

The following theorem, by Walther von Dyck, tells us that a group defined by generators and relation is the maximal group in certain sense.

Theorem 2.3 (Von Dyck)**.** Let X be a set, Y a set of reduced words on X, and G the group defined by the generators $x \in X$ and relations $w = e\,(w \in Y)$. If H is any group such that $H = \langle X \rangle$ and H satisfies all the relations $w = e\,(w \in Y)$, then there is an epimorphism $G \twoheadrightarrow H$.

Proof. See [Hun80] (Theorem 9.5). □

"I'm afraid that the following syllogism may be used by some in the future.

Turing believes machines think
Turing lies with men
Therefore machines do not think

Yours in distress,
Alan"
From a letter sent by Alan Turing to Norman Routledge, February 1952

3 The Todd-Coxeter Algorithm

The time has arrived to describe the algorithm presented by Todd and Coxeter in 1936, [TC36]. This is an algorithm for solving the coset enumeration problem. In a coset enumeration problem we try to find the index of a finitely generated subgroup in a finitely presented group. In theory, if the index is finite, the process stops at some point. If the procedure succeeds and the process stops, this method also gives us, implicitly, a permutation representation of G on the right cosets of H. Moreover, if G is finite, we can get an upper bound for the order of G. In their original paper, Todd and Coxeter discuss the method for a finite group, although the finiteness of the group does not impact the success of the procedure.

Let G be the finitely presented group

$$G := \langle g_1, g_2, \ldots, g_n \mid r_1(g_1, g_1, g_2, \ldots, g_n) = e, \ldots, r_m(g_1, g_1, g_2, \ldots, g_n) = e \rangle$$

or shorter $G := \langle E \mid R \rangle$ where $E := \{g_1, g_2, \ldots, g_n\}$ and $R := \{r_i(g_1, g_1, g_2, \ldots, g_n) \mid i = 1, 2, \ldots m\}$ where each relator $r_i(g_1, g_1, g_2, \ldots, g_n)$ is a *word* in $g_1, g_2, \ldots, g_n$ and e is the identity of G, and let H be the subgroup of G generated by the set S of *words*,

$$S := \{s_1(g_1, g_1, g_2, \ldots, g_n), \ldots, s_p(g_1, g_1, g_2, \ldots, g_n)\}$$

that is, $H := \langle S \rangle$.

The algorithm is based on two simple facts:

1. If $s \in S$, then $Hs = H$.
2. If $r(g_1, \ldots, g_n)$ is a relator, then for any coset $Hx, x \in G$ we have $Hxr(g_1, \ldots, g_n) = Hx$. So if $r(g_1, \ldots, g_n) = g_{i_1} \ldots g_{i_t}$ where each g_{i_j} is a generator or an inverse of a generator, then: $H_0 := Hx, H_1 := H_0 g_{i_1}$, $H_2 := H_1 g_{i_2}$, $\ldots$, $H_j := H_{j-1} g_{i_j}$ is defined, then $H_t = H_0$.

Now, for the procedure itself: for each word that generates the subgroup H we maintain a one-line table, called a **subgroup table**. The row is labeled as 1 for the coset H itself. The columns are labeled by the factors of the generator of the word. That is, if $s_j = g_{i_1} \ldots g_{i_k}$ is a generator of H, then we have $k + 1$ columns.

Subgroup Table

g_{i_1}	g_{i_2}	$\cdots$	g_{i_k}
1			1

If we look at the table as a matrix of order $1 \times (k + 1)$, then the entry $(1, g_{i_j})$ in the table, if defined, is the number of the coset we get from the multiplication $1 \cdot g_{i_1} \cdots g_{i_j}$.

For each relator, $r(g_1, \ldots, g_n)$ we have a **relation table**. Relation tables will give us information in case two cosets which have numbered differently are the same. If a relation acts on two cosets in exactly the same way, then these cosets must be identical. The rows of the relation tables are labeled with the numbering we defined for the cosets. Similarly to the subgroup table, given a relator $r_i = g_{i_1} \cdots g_{i_k}$, we have $k + 1$ columns.

Relation table for $r_i = g_{i_1} \cdots g_{i_k}$

g_{i_1}	g_{i_1}	$\cdots$	g_{i_k}
1			1
2			2
$\vdots$			$\vdots$
t			t
$\vdots$			$\vdots$

As in the subgroup table, the entry (n, g_{i_j}) if defined, is the coset we get from the multiplication $n \cdot g_{i_1} \cdot g_{i_2} \cdots g_{i_j}$. Since we know that $r_i = g_{i_1} \cdots g_{i_k} = e$, we get that $Hxr_i = Hx$. So the entry (n, g_{i_k}) is n.

Finally, we would like to have a table that keeps track for us on the result of multiplications. This table is the **coset table**. The rows will be labeled with the numbers of the cosets, and the columns will be labeled by the generators of G and their inverses (unless a generator is an involution). The entry (n, g_i), if defined, is $n \cdot g_i$ for the coset n and the generator g_i.

When the last entry in a row of a relation table or a subgroup table is filled in, we get an extra piece of information, in the form of $n \cdot g = l$, for some cosets n, l and a generator g. This extra piece of information is called a **deduction**. When getting a deduction we can face three situations:

(i) The entries (n, g) and (l, g^{-1}) are still empty. In this case, we just fill the number l in the entry (n, g) and the number n in the entry (l, g^{-1}). We also insert this information into all other relevant places in the other tables.

(ii) The entry (n, g) is already filled with the number l. In this case, the deduction brings no new information.

(iii) At least one of the entries (n, g) or (l, g^{-1}) in the coset tables is filled with a number different from l or n, respectively. In this case, we conclude that we have two different numbers to the same coset. This phenomenon is called a **coincidence**. When a coincidence is found, we replace both numbers by the smaller one in all places they occur.

The process terminates when all the entries of the coset, relation and subgroup tables are filled. From now on we shall refer to the Todd-Coxeter Algorithm as TCA.

We would like to give a detailed example of the TCA for the group S_4, using generators and relations, as follows:

$$G := \langle a, b, c \mid a^2 = b^2 = c^2 = e,\ (ab)^3 = e,\ (bc)^3 = e,\ (ac)^2 = e \rangle \tag{1}$$

and taking the subgroup

$$H := \langle a, b \rangle.$$

However, before we begin the example, let us prove some useful proposition that we shall use throughout the text:

Lemma 3.1. The set of transpositions $\{(1, k) \mid 1 \leq k \leq n\}$ generate S_n, for $n \geq 2$.

Proof. We know that every element in S_n can be written as a product of transpositions. So it is enough to show that every transposition in S_n can be written as an element of the group $\langle \{(1k) \mid 1 \leq k \leq n\} \rangle$. So let (i, j), $i \neq j$ be a transposition in S_n. Then we have that $(i, j) = (1, j)(1, i)(1, j)$ as desired. □

Proposition 3.1. The set of transpositions $\{(12), (23), \ldots, (n-1, n)\}$ generate S_n, for $n \geq 2$.

Proof. Since by Lemma 3.1 the set $\{(1k) \mid 1 \leq k \leq n\}$ generates S_n, it is enough to show that for all $1 \leq k \leq n$, the transposition $(1,k) \in \langle (12),(23),\ldots,(n-1,n)\rangle$ for all $1 \leq k \leq n$. For $k = 1$ we get the identity which is obviously in the group, and for $k = 2$ we get $(1,2)$ which is also in the group. Assume that $(1,k)$ is in $\langle (12),(23),\ldots,(n-1,n)\rangle$, where $1 \leq k < n$, and let us show that $(1,k+1) \in \langle (12),(23),\ldots,(n-1,n)\rangle$. Then, $(1,k+1) = (1,k)(k,k+1)(1,k)$, as desired. □

First, we define three cosets and try to fill in the tables. Then we will be able to see whether we need to define more cosets in order to complete the tables, or not.
We define:

$$1 := H,\ 2 := 1c,\ 3 := 2b.$$

The subgroup tables are already closed, and as expected, we did not gain any additional information from them.

Subgroup Tables

a	
1	1

b	
1	1

However, from the definitions and the relations in the group G, we can immediately derive the following: $2c = 1,\ 3b = 2$, as b and c are of order 2. We should note that there are a few possible ways to fill in the tables. One can start from the left or from the right and then can continue using and any combination of them. Nevertheless, eventually one arrives at the same result.

Now, let us start filling in the coset and relation tables:

Coset table

	a	b	c
1	1	1	2
2	2	3	1
3		2	3

Relation tables for $a^2 = e,\ b^2 = e,\ c^2 = e$

a	a	
1	1	1
2	2	2
3		3

b	b	
1	1	1
2	3	2
3	2	3

c	c	
1	2	1
2	1	2
3	3	3

Relation table for $(ab)^3 = e$

a	b	a	b	a	b	
1	1	1	1	1	1	1
2	2	3			3	2
3			3	2	2	3

Relation table for $(ac)^2 = e$

a	c	a	c	
1	1	2	2	1
2	2	1	1	2
3			3	3

Relation table for $(bc)^3 = e$

b	c	b	c	b	c	
1	1	2	3	3	2	1
2	3	3	2	1	1	2
3	2	1	1	2	3	3

In the process of filling in the tables we have received the following deductions, $2a = 2$, $3c = 3$, which we have underlined in the table, in the place we got them.

Now, one can define one more coset and continue, or to define a few more at once. As we shall see, it is enough to define only one more coset, namely, $4 := 3a$ to complete all the tables. However, since we would like to demonstrate the notion of "coincidences" we shall take the latter approach: we shall define three more cosets at once: $4 := 3a$, $5 := 4b$, $6 := 4c$. Continuing filling in the tables gives

a	b	a	b	a	b	
1	1	1	1	1	1	1
2	2	3	4^*	4^*	3	2
3	4	5^*	3^*	2	2	3
4	3	2	2	3	5	4
5	3	2	2	3	4	5
6	3	2	2	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	4_5	2	3
4	3	5_4	6
5	3	4	
6			4

From this relation table we receive the following deductions: $4b = 4$ and $5a = 3$. However, as we see in the coset table, the place of $4b$ is already filled with 5. Therefore, we get a **coincidence**: cosets 4 and 5 are the same coset of H in the group G. Similarly, the place of $3a$ is already filled with 4 in the coset table, which means, as have already discovered, that 4 and 5 are the same coset. We note that coincidences are marked in the tables with asterisk(*). Equipped with the previous information, let us continue to the other relation tables.

a	c	a	c	
1	1	2	2	1
2	2	1	1	2
3	4	6^*	3^*	3
4	3	3	4	4
5	3	3	4	5
6	3	3	4	6

	a	b	c
1	1	1	2
2	2	3	1
3	$4_{5,6}$	2	3
4	3	5_4	6
5	3	4	
6	3		4

From this relation table we get the information that $6a = 3$ or, equivalently, $3a = 6$. This yields another **coincidence**: this time we get that cosets 4 and 6 are the same cosets of H in G. So, from the last two coincidences we have $4 = 5 = 6$. These coincidences yield full information about the multiplication of all the elements we have, or in other words, we filled in the whole coset table, and thus can fill in the rest of the tables completely. As we said in the description of the algorithm, we take the smallest integer in a coincidence to represent the equal cosets.

	a	b	c
1	1	1	2
2	2	3	1
3	$4_{5,6}$	2	3
4	3	5_4	6_4
5	3	4	4
6	3	4	4

	a	a
1	1	1
2	2	2
3	4	3
4	3	4
5	3	5
6	3	6

	b	b
1	1	1
2	3	2
3	2	3
4	5	4
5	4	5
6	4	6

	c	c
1	2	1
2	1	2
3	3	3
4	6	4
5	4	5
6	4	6

	b	c	b	c	b	c	
1	1	2	3	3	2	1	
2	3	3	2	1	1	2	
3	2	1	1	2	3	3	
4	4	4	4	4	4	4	
5	4	4	4	4	4	5	
6	4	4	4	4	4	6	

Eventually, we receive four different cosets of H in G, which are 1,2,3 and 4. This means that $[G : H] = 4$, and since $|H| \leq 6$ then we get an upper bound to the order of G, that is, $|G| \leq 24$. On the other hand, by Proposition 3.1 we see that the three transpositions $(12), (23), (34)$, of which the generators of G act on the cosets 1,2,3 and 4, generate S_4 and by Theorem 2.3 we get an epimorphism from G onto S_4 (or equivalently, S_4 is a homomorphic image of G), which means that $|G| \geq 24$. All in all, we get that $|G| = 24$ and thus $G \cong S_4$. We have just proved the following theorem:

Theorem 3.1. The group S_4 has the presentation using generators and relation given in (1).

However, there is a problem. Given an arbitrary presentation of a group using generators and relations, it is sometimes unclear with which group we are dealing with. Using TCA may not help in this case. Indeed, if we take a subgroup of the abstract group, and the index of it in the abstract group is not finite, then there is no guarantee that the TCA stops. Another disadvantage of arbitrary presentations is that we might waste our time dealing with a complicated presentation of the trivial group, as seen in the following examples.

Taking the presentation $G := \langle a, b, c \mid a^3 = b^3 = c^4 = e, ac = ca^{-1}, aba^{-1} = bcb^{-1} \rangle$ (from [MKS04]) with the subgroup $H := \langle a, b \rangle$. Defining the cosests $1 := H$, $2 := 1c$, $3 := 2b$, $4 := 3c$, $5 := 4c$, $6 := 5a$, $7 := 4a$, $8 := 3b$ yields a total collapsing immediately after a few steps. In fact, the above presentation of the trivial group is not unique. Another presentation of the trivial group, taken from [Fra03], is the presentation $\langle x, y \mid y^2x = y, yx^2y = x \rangle$ (take the subgroup H defined by $H := \langle x \rangle$ and the cosets: $1 := H$, $2 := 1y$, $3 := 2y$, $4 := 3y$ to verify by the TCA). Also, the presentations $G := \langle a, b \mid a^2ba^{-1} = e, ab^{-1}a^{-1} = e \rangle$ (from [Pei97]) and $G := \langle a, b \mid aba^{-1} = b^2, bab^{-1} = a^2 \rangle$ (from [Löh17]) are the trivial group. So we have already four presentations of the trivial group!

3.1 Identifying groups with their presentations

We shall now use the TCA to identify more groups with their presentation using generators and relations. For obvious reasons of saving space, the environment and laziness of the author, we should give only our coset definitions, the (full) coset table and list of deductions and coincidences. The reader is warmly advised to do the process on their own, or to use a computerized algebra software, for example, GAP.

(1) $D_4 \cong G := \langle a, b \mid a^2 = e, b^4 = e, (ab)^2 = e \rangle$

Let us recall that the group D_n is the group of symmetries of a regular n-gon, called the n**th dihedral group**. This is a finite group of order $2n$ (n rotations and n reflections). We consider the case $n = 4$. Then we have the group of symmetries of a square. There are 4 rotations and 4 reflections.

So we have 8 elements in this group. If we take a to be the reflection operator and b to be the rotation operator, then we claim that: $D_4 \cong G := \langle a, b \mid a^2 = e,\, b^4 = e,\, (ab)^2 = e\rangle$ where taking the subgroup $H := \langle a\rangle$. Using the TCA with the definitions $1 := H$, $2 := 1b$, $3 := 2b$, $4 := 3b$, we get the deductions $4b = 1$, $2a = 4$ and $3a = 3$, with no coincidences. The coset table is

	a	b	b^{-1}
1	1	2	4
2	4	3	1
3	3	4	2
4	2	1	3

So we get 4 distinct cosets with at most 2 elements in each one which gives the upper bound 8 for the order of G. We see that the permutation representation is given by $a \mapsto (24) \in S_4$, and $b \mapsto (1234) \in S_4$. It is easy to see that (1234), (24) generate D_4 ((1234) rotates the square by 90 degrees (say counterclockwise), and (24) reflects two vertices). Moreover, $(24)(1234) = (14)(23)$ (we do multiplication from right to left) which has order 2 (disjoint transpositions). Thus, we found generators of D_4 that satisfy the relations of G, so by Theorem 2.3 there is an epimorphism from G onto D_4, which gives now the lower bound of the order of G, namely 8. Therefore, we get that $G \cong D_4$.

(2) $S_3 \cong \langle a, b \mid a^2 = b^2 = e, (ab)^3 = e\rangle$

We have already shown in detail the presentation of the group S_4 in which S_3 is a subset of. Thus, the resemblance of the presentation to that of S_4 is reasonable. We are taking the subgroup H of G to be $H := \langle a\rangle$. With the definition of the cosets $1 := H$, $2 := 1b$, $3 := 2a$, we get the deduction $3b = 3$ and the coset table

	a	b
1	1	2
2	3	1
3	2	3

From the algorithm we have received that $|G| \leq 6$. The permutation representation is given by $a \mapsto (23)$, $b \mapsto (12)$ which by Proposition 3.1 generates S_3, and $(23)(12) = (132)$, so the relations in G are satisfied, and thus by Theorem 2.3 we get $|G| \geq 6$, so $S_3 \cong G$.

(3) $S_5 \cong G$
$G := \langle a, b, c, d \mid a^2 = b^2 = c^2 = d^2 = e,\, (ab)^3 = (bc)^3 = (cd)^3 = e,\, (ac)^2 = (bd)^2 = (ad)^2 = e\rangle$.

We continue with the symmetric groups and arriving at S_5. This is one of the cases when we cannot avoid coincidences. Even after doing the process and trying to present the results as efficient and "engineered" as possible, we must sometime (without knowing) define some redundant cosets.

Taking H to be $H := \langle a, b, c\rangle$, we define the cosets as follows: $1 := H$, $2 := 1d$, $3 := 2c$, $4 := 3d$, $5 := 4b$, $6 := 5a$. Then we get the deductions $4c = 2$, $2b = 2$, $5c = 5$, $6c = 6$, $5d = 5$, $2a = 2$, $3a = 3$, $6b = 6$, $6d = 6$, and the coincidence $3 = 4$.

	a	b	c	d
1	1	1	1	2
2	2	2	3_4	1
3	3	5	2	4_3
4	3	5	2	3
5	6	4_3	5	5
6	5	6	6	6

Here we had to define the coset 4 in order to get the distinct cosets 5 and 6. So, from the process we get that the index $|G : H|$ is 5, which means that our upper bound of $|G|$ is $5 \cdot 24 = 120$. We also get the permutation representation $a \mapsto (45)$, $b \mapsto (34)$, $c \mapsto (23)$ and $d \mapsto (12)$ (do not confuse the numbering of the elements in S_5 with the numbering in the TCA). As we have already proved, the images of a, b, c and d generate S_5. We leave it as an exercise to the reader to check that the relations in G hold for these elements of S_5. Again we use Theorem 2.3 to get a surjective homomorphism which implies the desired isomorphism.

(4) $A_4 \cong G := \langle a, b, c \mid a^2 = b^2 = c^3 = e, ab = ba, ca = abc, cb = ac \rangle$

Recall that A_n is the alternating group on n letters and is a subgroup of S_n whose elements are the even permutations in S_n. The order of A_n is $n!/2$ (the even and odd permutations partition S_n). We define H now to be the coset $H := \langle c \rangle$, and use the following enumeration: $1 := H$, $2 := 1b$, $3 := 1a$, $4 := 3b$. We get the deductions: $4a = 2$, $4c = 3$, $3c = 2$, $2c = 4$ and no coincidences were observed. The coset table looks as follows:

	a	b	c	c^{-1}
1	3	2	1	1
2	4	1	4	3
3	1	4	2	4
4	2	3	3	2

As we see, we have four cosets which give an upper bound of 12 elements. The permutation representation in this case is given by $a \mapsto (13)(24)$, $b \mapsto (12)(34)$, $c \mapsto (243)$. These elements belong to A_4 and generate a subgroup of order $2 \cdot 2 \cdot 3 = 12$, so they generate A_4. If the reader is not tired already (as the author is), then they are invited to check that the relations in G are satisfied by the above elements of A_4.

(5) $A_5 \cong G := \langle a, b \mid a^5 = b^3 = e, (ab)^2 = e \rangle$

Taking $H := \langle a \rangle$, define the following cosets:

$$1 := H,\ 2 := 1b,\ 3 := 1b^{-1},\ 4 = 3a,\ 5 = 4a,\ 6 := 5a,\ 7 := 2a,\ 8 := 7a$$
$$9 := 8a,\ 10 := 9b,\ 11 := 8b^{-1},\ 12 := 10b,\ 13 := 10a^{-1},\ 14 := 12a,\ 15 := 13b$$

	a	b	c	c^{-1}
1	1	2	1	3_7
2	7_3	3_7	6	1
3	4	1	2	2
4	5	6	3	11
5	6	10	4	12
6	2	11	5	4
7	8_4	1	2	2
8	9	6	7	11
9	6	10	8	12
10	11	12	13	9
11	12	8_4	10	6
12	14	9_5	11	10
13	10	15	14	14
14	13	13	12	15
15	15	14	15	13

We get three coincidences which are $3 = 7$, $4 = 8$, $5 = 9$. Thus, we have index 12 of H in G. So our upper bound this time is $5 \cdot 12 = 60$. This time we shall not look for the permutation representation. We are going to find two generators of A_5 which satisfy the relations of G, and which

yield an epimorphism onto A_5. We claim that $\alpha := (12345)$ and $\beta := (153)$ generates A_5. Indeed, the order of $\langle \alpha, \beta \rangle (\leq A_5)$ must be divisible by 3, 5 and 2 (since the order of, for example, $\alpha\beta$ is 2), by Lagrange's theorem. So the order of $\langle \alpha, \beta \rangle$ must be at least 30. However, $\langle \alpha, \beta \rangle$ has a subgroup of order 4 ($\alpha\beta$ has order 2, and γ which we get by defining $\omega = \alpha^2\beta\alpha^{-2}$ and $\gamma = \omega(\alpha\beta)\omega^{-1}$ has order 2), so the order must also must be divisible by 4. So the order is at least 60. But this is the order of A_5. So $|\langle \alpha, \beta \rangle| = 60 \implies \langle \alpha, \beta \rangle = A_5$. We can immediately see that $\alpha^5 = e = \beta^3$ and $\alpha\beta = (23)(45)$ which is of order 2. So our choice of generators is good (obviously), and they satisfy the relations in G. So we can use Theorem 2.3 to get again the desired isomorphism.

So far we have dealt with permutation groups. Let us now look at some different but interesting groups which have matrices as their elements. However, we do what mathematicians like to do, which is to define some notions and then prove some theorems.

Definition 5. Let F be a field. Then the set $GL_n(F) := \{A \in M_n(F) \mid \det(A) \neq 0\}$ is called the **general linear group**. If F is a finite field with q elements, we write $GL_n(q)$. The binary operation in this group is matrix multiplication.

An interesting case is when the determinant of an element in $GL_n(F)$ is 1.

Definition 6. Let F be a field. Then the set $SL_n(F) := \{A \in M_n(F) \mid \det(A) = 1\}$ is called the **special linear group**. The special linear group is a subgroup of $GL_n(F)$.

Theorem 3.2. If F is a finite field with q elements, then

$$|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Proof. From linear algebra we know that a square matrix is invertible if and only if its rows/columns are linearly independent, when seen as vectors in the appropriate space. Let us try to count how many options we have to choose an n linearly independent columns to form a matrix in $GL_n(F)$. The first vector can be any non-zero vector, so we have $q^n - 1$ ways to choose it. The second vector shall not be a multiple of the first vector (including the zero vector), but other than that we have no restrictions, so it can be chosen in $q^n - q$ ways (the field has q elements which yield q multiples of the first vector). Assume now that we have chosen k linearly independent vectors and we want to choose the $k+1$th vector to be linearly independent of the previous vectors. The vector v is linearly *dependent* on the vectors $v_1, \ldots, v_k$ if and only if we can write $v = \alpha_1 v_1 + \cdots \alpha_k v_k$. So in F there are q^k such sums, so we exclude them in our counting to get $q^n - q^k$. Therefore, taking all into account yields $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$ different ways to choose an $n \times n$ invertible matrices. Thus, $|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$. □

Let us now look at $SL_n(q)$. Consider the map $\det : GL_n(q) \to F^* := F \setminus \{0\}$ with $A \mapsto \det(A)$. As we recall from linear algebra, $\det(AB) = \det(A)\det(B)$, so the determinant function is a group homomorphism. Moreover, if we look at the kernel of this homomorphism we discover that $\ker(\det) = SL_n(q)$. Also, it is easy to see that the map det is onto F^*.

Since we are going to deal with 2×2 matrices, let us zoom down from dimension n to 2. We would like to find now the order of $SL_2(q)$. From Theorem 3.2 for matrices of dimension 2 we get $|GL_2(q)| = (q^2 - 1)(q^2 - q)$. Since the map det is onto F^*, we get by Lagrange's theorem that $|GL_2(q) : SL_2(q)| = q - 1$, and thus

$$|SL_2(q)| = \frac{|GL_2(q)|}{q-1} = (q^2 - 1)q = (q-1)q(q+1). \tag{2}$$

We would like to continue our construction, and to arrive at the following

Definition 7. The **centre** of the group G is the set $Z(G) := \{x \in G \mid xg = gx, \forall g \in G\}$. The centre is an Abelian subgroup of G.

We can easily see that the centre of $SL_2(F)$ is $\{I, -I\}$ (when the characteristic of F is not 2, since then $I = -I$), as the identity matrices commute with every other matrix. We have finally arrived at our main definition:

Definition 8. Let $Z(SL_n(F))$ be the centre of $SL_n(F)$. The factor group $SL_n(F)/Z(SL_n(F))$ is called the **projective special linear group** and is denoted by $PSL_n(F)$.

Since the centre is a normal subgroup of $SL_2(q)$, then we know that (assuming $\text{char}(F) \neq 2$)

$$|SL_2(q)/Z(SL_2(q))| = |SL_2(q) : Z(SL_2(q))| = \frac{(q-1)q(q+1)}{2}.$$

In case and $\text{char}(F)=2$, then $Z(SL_2(F))$ is the trivial group and therefore, $SL_2(F) = PSL_2(F)$ and $|PSL_2(F)| = (q-1)q(q+1)$.

(6) $PSL_2(7) \cong G := \langle a, b, w \mid a^7 = b^3 = w^2 = e, bab^{-1} = a^2, (bw)^2 = e, (aw)^3 = e \rangle$

We are in search for finding the generators of $PSL_2(7)$ that satisfy the above relations. We are going to use **Bruhat decomposition** in order to break down $SL_2(7)$ and to help us in this journey.

Definition 9. We define the following subgroups of $SL_2(F)$:

- $B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = 1 \right\} \subset SL_2(F)$ called the Borel subgroup.
- $U := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in F \right\} \subset B$
- $H := \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in F^* \right\} \subset B$

We can easily see that $U \triangleleft B$ and that $B = UH$. The following theorem tells us that

Theorem 3.3. $SL_2(F) = B \cup BwB$, where $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(F)$

Proof. See [Lan02]. □

For $PSL_2(7)$ we need a finite field with 7 elements. So the natural field to take is $\mathbb{Z}_7$. Now, we can see that $U = \left\langle \alpha := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ and $H = \left\langle \beta := \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} \right\rangle$, in $SL_2(7)$. The reader is invited to check that the relations in G are satisfied by α and β and w (α has order 7, β has order 3, and w has order 2) in $PSL_2(7)$. Moreover, as we have in Theorem 3.3, α, β, w generate $SL_2(7)$ and thus, their images generate $PSL_2(7)$. So we have an epimorphism from G onto $PSL_2(7)$, which means that G has order of at least 168.

We now use the TCA with the following definitions of cosets, where taking $\mathfrak{B} := \langle a, b \rangle$ as the subgroup: $1 := \mathfrak{B}$, $2 := 1w$, $3 := 2a$, $4 := 3a$, $5 := 4a$, $6 := 5b$, $7 := 3b$, $8 := 3w$. We get the following deductions:

$$7a = 6,\ 2b = 2,\ 8a = 2,\ 4b = 3,\ 7b = 4,\ 5a = 7,\ 6a = 8,\ 6b = 8,\ 8b = 5,\ 7w = 6,\ 4w = 5,$$

with no coincidences. The coset table we get is

	a	b	w	a^{-1}	b^{-1}
1	1	1	2	1	1
2	3	2	1	8	2
3	4	7	8	2	4
4	5	3	5	3	7
5	7	6	4	4	8
6	8	8	7	7	5
7	6	4	6	5	3
8	2	5	3	6	6

So we get index 8, which yields the upper bound of $8 \cdot 7 \cdot 3 = 168$. So, as in previous examples we get our desired isomorphism; that is,

$$PSL_2(7) \cong \langle a, b, w \mid a^7 = b^3 = w^2 = e, bab^{-1} = a^2, (bw)^2 = e, (aw)^3 = e \rangle.$$

Our last example is quite similar to the previous but contains a bit more detail.

(7) $PSL_2(9) \cong G$

$$G := \langle a, b, c, w \mid a^3 = b^3 = w^2 = c^4 = e, (cw)^2 = e,\ cac^{-1} = b^{-1},\ cbc^{-1} = a, (aw)^3 = e,\ ab = ba,\ wabw = ab^{-1}c^{-1}wab^{-1} \rangle$$

In this case we need a field with nine elements. It is not obvious what is the natural field to choose. We choose the field $\mathbb{Z}_3[i] := \{a + bi \mid a, b \in \mathbb{Z}_3\}$. We again go to the Bruhat decomposition, but this time we get that $U = \left\langle \alpha := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \beta := \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \right\rangle$ and $H = \left\langle \gamma := \begin{pmatrix} 1+i & 0 \\ 0 & i-1 \end{pmatrix} \right\rangle$, in $SL_2(9)$. These elements, together with $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, satisfy the relations in G and generate $SL_2(9)$. Thus, Theorem 2.3 gives us a lower bound of 360. Now let us see what the TCA gives us: define the cosets

$$1 := \mathfrak{B} := \langle a, b, c \rangle,\ 2 := 1w,\ 3 := 2a,\ 4 := 3c,\ 5 := 4c,\ 6 := 5c,\ 7 := 4a,\ 8 := 5b,\ 9 := 3b^{-1},\ 10 := 8w.$$

We get the following deductions:

$$9c = 7,\ 2c = 2,\ 2b = 4,\ 7c = 8,\ 3b = 7,\ 7w = 9,\ 7b = 9,\ 5a = 2,\ 8a = 4,\ 10c = 9,\ 6b = 2,\ 9a = 10$$
$$3w = 5,\ 4w = 4,\ 6a = 9,\ 4b = 6,\ 3a = 5,\ 8b = 10,\ 10a = 6,\ 6w = 6,\ 10b = 5,\ 6c = 3,\ 8c = 10,$$

with no coincidences. The coset table is

	a	b	c	w	a^{-1}	b^{-1}	c^{-1}
1	1	1	1	2	1	1	1
2	3	4	2	1	5	6	2
3	5	7	4	5	2	9	6
4	7	6	5	4	8	2	3
5	2	8	6	3	3	10	4
6	9	2	3	6	10	4	5
7	8	9	8	9	4	3	9
8	4	10	10	10	7	5	7
9	10	3	7	7	6	7	10
10	6	5	9	8	9	8	8

So the index that we get from the process is 10 and $|G| \leq 10 \cdot 3^2 \cdot 4 = 360$. So from both the upper and lower bound we get the desired isomorphism.

"It is my experience that proofs involving matrices can be shortened by 50 percent if one throws the matrices out."
E. Artin, Geometric Algebra

4 Exceptional Isomorphisms

We have not worked so hard on the TCA just to describe it. We would like to use the results of the presentations to get isomorphisms between groups that at first sight do not seem to be related. We shall show that $A_5 \cong PSL_2(5) \cong SL_2(4)$, $PSL_2(9) \cong A_6$ and that $SL_3(2) \cong PSL_2(7)$.

Let us work on the isomorphism $A_5 \cong SL_2(4)$. We take the field with four elements defined by $\mathbb{F}_4 := \mathbb{Z}_2[x]/(x^2+x+1)$. We denote the elements in $\mathbb{F}_4$ by $\{0, 1, x, x+1\}$. We also note that $x^2 = x+1$. Thus, every element in $SL_2(4)$ has the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{F}_4$ and $ad - bc = 1$. We are going to show now that the matrices $A := \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}$ and $B := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ generates $SL_2(4)$. Indeed, the order of A is 5, the order of B is 3 and the order of AB is 2. Thus, by Lagrange's theorem the order of the group $\langle A, B\rangle$ must be divisible by 5, 3 and 2. Therefore, the order is at least 30. However, from A and B we can produce a Klein-4 subgroup V of G: define the elements $C := A^2BA^{-2}$ and $D := C(AB)C^{-1}$, and the subgroup $\langle AB, D\rangle$ generates V. Thus, the order of $\langle A, B\rangle$ must also be divisible by 4. So the order of $\langle A, B\rangle$ is at least 60. From Equation (2) we get that $|SL_2(4)| = 3 \cdot 4 \cdot 5 = 60$, so $\langle A, B\rangle = SL_2(4)$. As we pointed out already, the orders of A,B and AB are 5,3 and 2, respectively. Therefore, A and B also satisfy the relations of the presentation of A_5, and by Theorem 2.3 we get epimorphism of A_5 onto $SL_2(4)$. However, both are of order 60, so the epimorphism is an isomorphism, and $A_5 \cong SL_2(4)$. The (enthusiastic) reader is invited to verify that the matrices $A := \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$ and $B := \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ generate $PSL_2(5)$ and satisfy the relations appearing in the presentation of A_5. Thus, we get the isomorphisms $A_5 \cong PSL_2(5) \cong SL_2(4)$.

We move on to show that $SL_3(2) \cong PSL_2(7)$. It is left to the reader to check that the matrices $A := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $B := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ and $W := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ have orders 7,3 and 2, respectively (for keeping your sanity, you may want to use Matlab or Maple for that). However, $SL_3(2)$ is a simple group (which means that it does not have a proper normal subgroup). But in $\langle A, B, W\rangle$ the subgroup $\langle AWB\rangle$ is of order 4, so the order must be divisible by 4 as well. Thus, the order of $\langle A, B, W\rangle$ is at least 84. If it is 84, then it means that $\langle A, B, W\rangle$ is a proper normal subgroup of $SL_3(2)$ (as $|SL_3(2) : \langle A, B, W\rangle| = 2$), which cannot happen as $SL_3(2)$ is simple. Every subgroup induces a partition on the group. By Lagrange's theorem every coset has the same number of elements. Therefore, a cell in a partition (which is not the trivial partition) cannot contain more than a half of the elements of the group, so it must be that $\langle A, B, W\rangle = SL_3(2)$. Now, from Theorem 2.3 we get our desired isomorphism, namely, $SL_3(2) \cong PSL_2(7)$.

We are going to show the last exceptional isomorphism; that is, $PSL_2(9) \cong A_6$. As we have done until now, we are going to have elements that satisfy the relations in $PSL_2(9)$ and generate A_6. This will give us the desired isomorphism implied by Theorem 2.3.

It is easy to find two elements of order 3 in A_6, namely $\alpha := (123)$ and $\beta := (456)$. They are also commutative since they are disjoint. We also want an element that conjugate α to β^{-1} and conjugate β to α. Thus, we can define $\gamma \in S_6$ as $\gamma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (1634)(25)$. By trial and error one finds that $\omega := (13)(25)$ is the missing part of order 2 ($\gamma\omega = (1634)(25)(13)(25) = (14)(36)$ and $\alpha\omega = (123)(13)(25) = (253)$, and the ugly relation can be checked manually by the reader). We can see that the group $G := \langle \alpha, \beta, \gamma, \omega\rangle$ generate the element $\alpha\omega\beta = (253)(456) = (25643)$ of order 5, so the order of the group must be divisible by 5. So the order of G is at least 60. However, $\langle \alpha, \beta\rangle$ generate a group of order 9. So the order of G must be divisible also by 9. The least common multiple

of 9 and 60 is 180, so the order of G is at least 180. But as we claimed in the previous discussion, $|A_6 : G| = 2$ and A_6 is a simple group, which leads to a contradiction (in fact, for every $n \geq 5$, we have A_n is a simple group). Thus, $G = A_6$. So the generators of A_6 satisfy the relations in the presentation of $PSL_2(9)$, and thus we get an epimorphism (by Theorem 2.3) which is actually an isomorphism, so $PSL_2(9) \cong A_6$.

There are two ways to do great mathematics. The first way is to be smarter than everybody else. The second way is to be stupider than everybody else – but persistent.
Raoul Bott

5 Appendix

Here we shall give a short and simple account for building a finite presentation of a group using the software GAP. Let us note that GAP is distributed freely, and installation files are available for Linux, Mac and Windows. It is distributed under the GPL license. We use the GAP manual in order to provide the explanation below. The manual can be found on
https://www.gap-system.org/Manuals/doc/ref/manual.pdf.
More information can be found on the GAP website
https://www.gap-system.org/.

According to Definition 4, we define the presentation of a group using factoring the free group by the relations, namely F/N. To do so, we first need to define the free group F (we shall use lower case letters in the code) by the command `FreeGroup` as follows

```
gap> f:=FreeGroup("a", "b");
<fp group on the generators [ a, b ]>
```

(In order to suppress the output here use double semicolon ;;). We have generated a free group on the letters 'a' and 'b'.

In the definition of the `FreeGroup` we gave the names 'a' and 'b'. Alternatively, it is possible to write the number of generators we want and the software will give them names automatically. For example:

```
gap> f:=FreeGroup(3);
<free group on the generators [ f1, f2, f3 ]>
```

Since our first example in this work is done on S_4, we continue this tradition and remember that the presentation of S_4 given by (1). **Note**: We used equations $\omega = e$ on the relators. However, there is no need to equate the relations to the identity as it is done automatically. We access to our generators of the free group by the position they were defined in the command. For example, 'a' is in position 1, so we access it by typing f.1 and similarly for 'b' and 'c' (It is also possible to use the command `AssignGeneratorVariables(f)` to access 'a', 'b' and 'c'). In order to define the factor group, we use the '/' symbol as follows:

```
gap> f:=FreeGroup("a", "b", "c");;
gap> g:=f/[f.1^2, f.2^2, f.3^2, (f.1*f.2)^3, (f.2*f.3)^3, (f.1*f.3)^2];
<fp group on the generators [ a, b, c ]>
```

Now our presentation of S_4 is complete. We can get the order of the group by typing `Size(g)`, getting the generators and the relations in the group by `GeneratorsOfGroup(g)` and `RelatorsOfFpGroup(g)`, respectively. We can also get a faithful (injective) premutation representation by `IsomorphismPermGroup(g)`.

But this is not why we have chosen to add an appendix on GAP. For finitely presented groups GAP uses the Todd-Coxeter Algorithm for coset enumeration. Obviously, no one would like to do the process for larger groups by hand, so we review here the commands to achieve the coset tables.

First, we need to define which subgroup we would like to operate on. In order to do so we use the command `Subgroup(G,gens)`, where G is the group and *gens* are the generators of the subgroup. Continuing our example of S_4:

```
gap> h:=Subgroup(g, [g.1,g.2]);
```

Note that now we are dealing with the elements of the group 'g' and not of the group 'f', so the generators will be accessed by g.1, g.2 and g.3. To get the coset table we use the command `CosetTable(g,h)`. The value returned is a list of lists, and it appears as

```
gap> CosetTable(g,h);
[ [ 1, 2, 4, 3 ], [ 1, 2, 4, 3 ], [ 1, 3, 2, 4 ], [ 1, 3, 2, 4 ],
[ 2, 1, 3, 4 ], [ 2, 1, 3, 4 ] ]
```

In order to get a matrix view of the table we use the commands `PrintArray` and `TransposedMat`. The `PrintArray` command prints the array as a matrix. However, this is not the modern view of the coset table we have used in this work. This matrix is transposed. Thus, we need to use the command `TransposedMat` to get the same structure of matrix we used in our work. First we transpose the matrix and then print it in a tabular view. For convenience reasons, it is useful to give the coset table a name. So the code for getting a coset table might look like

```
gap> tab:=CosetTable(g,h);
[ [ 1, 2, 4, 3 ], [ 1, 2, 4, 3 ], [ 1, 3, 2, 4 ], [ 1, 3, 2, 4 ],
[ 2, 1, 3, 4 ], [ 2, 1, 3, 4 ] ]
gap> PrintArray(TransposedMat(tab));
[ [  1,  1,  1,  1,  2,  2 ],
  [  2,  2,  3,  3,  1,  1 ],
  [  4,  4,  2,  2,  3,  3 ],
  [  3,  3,  4,  4,  4,  4 ] ]
```

The columns we get correspond to a, a^{-1}, b, b^{-1} and c, c^{-1} (since in S_4 the generators are of order 2, they are inverses of themselves, so the columns of each generator and its inverse are identical). Moreover, we can get the index of h in g by the command `Index(gr,sub)`. Notice that since there are different ways of defining the cosets in the TCA, we might get different coset tables. However, it does not matter which representative we take from the equivalence class.

Errata

- Page 10, paragraph after Theorem 3.1: the sentence "Indeed, if we take ... then there is no guarantee that the TCA stops." should be "Indeed, if we take... then **the algorithm never stops**."
- In page 11, in the paragraph immediately after , ignore the sentences that start with "This is one of the cases..." and end with "... we must sometime (without knowing) define some redundant cosets.".
- Page 12, the header of the coset table of A_5 should be

	a	b	a^{-1}	b^{-1}

- Page 15, line 9: the field $\mathbb{Z}_3[i] := \{a + bi \mid a, b \in \mathbb{Z}_3\}$ should be defined as $\mathbb{Z}_3[i] := \{a + bi \mid a, b \in \mathbb{Z}_3,\ i = \sqrt{-1}\}$
- Page 16, line 7: the sentence "We are going to show now that ... generates $SL_2(4)$." should be "We are going to show now that ... **generate** $SL_2(4)$."
- Page 16, line 22: reference for simplicity of $SL_3(2)$ is [Lan02].
- Page 17, line 2: reference for simplicity of A_n, $n \geq 5$ is [Rot95].

References

[Coh99] Arjeh Cohen. *Some Tapas of Computer Algebra*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999.

[Dyc82] Walther Dyck. "Gruppentheoretische Studien". In: *Mathematische Annalen* 20.1 (Mar. 1882), pp. 1–44.

[Fra03] John Fraleigh. *A first course in abstract algebra*. Addison-Wesley, 2003.

[Gal13] Joseph Gallian. *Contemporary abstract algebra*. Brooks/Cole Cengage Learning, 2013.

[Gar86] Cyril Gardiner. *Algebraic structures*. E. Horwood Halsted Press, 1986.

[Her64] Israel Herstein. *Topics in algebra*. Xerox College Publ, 1964.

[Hun14] Thomas Hungerford. *Abstract algebra : an introduction*. Brooks/Cole Cengage Learning, 2014.

[Hun80] Thomas Hungerford. *Algebra*. Springer New York, 1980.

[Joh97] D. L. Johnson. *Presentations of Groups*. 2nd ed. London Mathematical Society Student Texts. Cambridge University Press, 1997.

[Lan02] Serge Lang. *Algebra*. Springer, 2002.

[Löh17] Clara Löh. *Geometric group theory : an introduction*. Cham, Switzerland: Springer, 2017.

[MKS04] W. Magnus, A. Karrass, and D. Solitar. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*. Dover books on mathematics. Dover Publications, 2004.

[Neu82] Neubüser. "An elementary introduction to coset table methods in computational group theory". In: *Groups - St Andrews 1981*. Ed. by E.F Robertson C.M Campbell. London Mathematical Society Lecture Notes Series 71. Cambridge University Press, 1982.

[Pei97] David Peifer. "An Introduction to Combinatorial Group Theory and the Word Problem". In: *Mathematics Magazine* 70.1 (1997), pp. 3–10.

[Rot95] Joseph Rotman. *An introduction to the theory of groups*. New York: Springer-Verlag, 1995.

[Ser97] Seress. "An Introduction to Computational Group Theory". In: *Notices of the American Mathematical Society* 44.6 (1997).

[Ste08] Ian Stewart. *Why beauty is truth : the history of symmetry*. New York London: BasicBooks Perseus Running distributor, 2008.

[TC36] J. A. Todd and H. S. M. Coxeter. "A practical method for enumerating cosets of a finite abstract group". In: *Proceedings of the Edinburgh Mathematical Society* 5.1 (1936), pp. 26–34.