The contents here are not finalized and are being constantly updated.
Check the website for quicker updates.

Contents

Part I

Mathematical Basics

Chapter 1

Into The Groups

1.1 Introduction

Starting to explain the abstract ideas is always difficult. Since it is hard to pinpoint a single approach or a viewpoint that captures the whole idea of the subject, carrying the first words is challenging. Among these difficult and abstract theories, there lies the group theory.

From what I've seen in group theories' textbooks, books, or lectures, there are usually two different approaches to it. People either start with an easy group theory example, usually talking about symmetries and other similar stuffs (stuffs like Rubik's cube symmetry group), or they start off by simply stating the axioms that defines groups. In here, we're going to do the second one, because I believe the second approach is a lot more straight-forward and is actually much easier to follow.

What is a Group Theory?

Group theory is a theory that studies a special creature in mathematics called **Group**. But what is a group you might say? Group is actually a combination of a set and an operation, with some special rules governing them. These rules are the definition of groups and they are usually called the **axioms** of group. Let's take a look at these axioms:

$$(G, \circ) \qquad \circ : G \times G \to G$$

1. Identity member:

$$\exists e \in G : \forall g \in G : eg = ge = g \tag{1.1}$$

2. Inverse member:

$$\forall g \in G : \exists g^{-1} \to gg^{-1} = g^{-1}g = e \tag{1.2}$$

3. Associativity:

$$\forall g, h, l \in G : g \circ (h \circ l) = (g \circ h) \circ l \tag{1.3}$$

So what does it say?

Let's dig in and see what these axioms say. If we have a set G, and an operation $\circ$, we note our group like $(G, \circ)$. This set and this operation can be any arbitrary set or operation, as long as they satisfy the equations 1.1 to 1.3.

So let's go through them one by one. What do these actually mean? And why after all, these three specific and *strange* rules? Let's talk about that.

First of all, you can see that before our axiom number 1, we have $(G, \circ)$ $\circ : G \times G \to G$. This little rules, that we didn't put a number on, is actually stating that the set G should be closed under $\circ$. Some people count this so called *closure* property as the first axiom of a group, thus they have 4 axioms in total. Here, we didn't count it as one of the main axioms, but a beforehand assumption. This closure property is actually very important, and it means that for every a, b as members of our set G, $a \circ b$ is also inside our G. This property helps us a lot, and is very necessary, since it makes groups some independent creatures that are closed within themselves.

Imagine you have a set $G = \{1, -1\}$ and an operation of common $\times$. Since $1 \times 1 = 1 \in G$, and $1 \times -1 = -1 \in G$, and $-1 \times 1 = -1 \in G$, and $-1 \times -1 = 1 \in G$, the set G is closed under $\times$. First step is checked.

So let's go for the first axiom. All it says is: There should be a single member e in our set G, that when it is combined with any other member g of G, whether from left or right, it returns g itself. This e is called identity member. This identity is something that looks like number 1 for common $\times$. Or maybe 0 for common $+$. It's somehow the neutral member of our group. From now on we are going call this identity member e for all of our groups, unless it is mentioned otherwise.

The second axiom uses this identity member e, in a relation between other members. So what does the second axiom states? It says that for any member, there should be an inverse member. But what is exactly defined as an inverse member? An inverse of g is noted like g^{-1}, and when it is acted with operation $\circ$ on g from any side, it should return the identity member e. These notations are pretty much like the common notations of th same old multiplication $\times$, but be very careful that in here we are talking about the general operation of $\circ$ which could be $\times, +$, or any other different or even strange operations. But anyhow, we still use notations similar to the common $\times$, because it is familiar to our eyes.

So until now group is $(G, \circ)$, which our set G looks something like this:

$$G = \{\cdots, g_3^{-1}, g_2^{-1}, g_1^{-1}, e, g_1, g_2, g_3, \cdots\} \tag{1.4}$$

Note that we have e as an identity member, and for every member of G, we have its' inverse. Also note that inverse of the inverse of a member is the

member itself $(g_1^{-1})^{-1} = g$ (this is pretty easy to prove). What about inverse of e? well inverse of e is e itself, since $e \circ e = e \circ e = e$. We also assumed that G is closed under $\circ$.

Now onto the third axiom. Associativity. This third one seems a little strange and out of place, but believe me, it is a very important characteristic of our operation $\circ$. You have surely heard of associativity before, and all it says is that the order of operation $\circ$ should not matter. Either you do $\circ$ on the first two first, and then on the third, or you do it on the second and the third one first, then on the first one, this should not produce a different result. This is actually a very important rule in group theory. Its' importance is not obvious in here, but you will see that almost every time we are proving something, we are using this property. Without it, this theory and its' Theorems are unprovable.

Before we go on, I should mention that the order of $\circ$ matters in general. so $a \circ b \neq b \circ a$. We didn't assume anything regarding this matter. But if $a \circ b = b \circ a$ is true in a group for any $a, b \in G$, We call that group an **Abelian** group. So an Abelian group is a group which its' members order in an operation is commutable.

So that's it. You now know what a group is. In summary, **Group** is a set and an operation, usually denoted like $(G, \circ)$, which G is **Closed** under $\circ$, has an **Identity** member e, for any of its' members has an **Inverse** member, and the operation $\circ$ is **Associative** for all members of our set G. Remember and memorize these four characteristics of a group since from these, rises everything else.

But Why These Specific Set Of Rules?

Well, this is not very easy to answer. Historically speaking, many ages ago in the ancient Greece, people were very much interested in geometry, as a main subject of mathematics and logic that they cherished much. People started proposing theorems and proving them from many places. Almost all of these theorems and facts about the geometrical world, were somehow dependent on the other theorems. After a while that the number of these theorems was increased, a concern were risen. What if all of these theorems are connected to each-other in a circular reasoning. This means that if we put all of our reasonings together it will become something like these: A is true because B is true. And B is true because C is true. But why is C true? because A is true. You can see that this is actually a logical fallacy.

So Euclid came to the rescue. He said to avoid this or any other fallacy, we should assume some axioms to be true, and from there, make our way up to prove everything else. Now just assuming something to be true is a little bit out of the spirits of mathematics, so he wanted the list of these postulates to be as short as possible. After-all, he came out with the famous 5 euclidean geometry axioms that we still use today.

Now this method and idea was used again many years after Euclid, in the field of algebra. Algebra was at first, probably mainly developed for its' applications in trading, taxing, and daily applications. It was not formed based

on any axioms, and like the world of geometry before Euclid, there was a huge number of theorems, any of them from a different era and different people, and all of them depending on each other. Many years later mathematicians started axiomatic study of algebra. What was the least amount of axioms required to develop the whole algebra we know?

Now this is a very huge topics and we are not going to talk about that here. People came out with many postulates as axioms, like the rule of associativity that we've already discussed. A great deal of modern algebra is developed because of these endeavors. You've probably heard of basic algebra axioms, for the common operations of $\times$ and $+$. Now these studies became very important at the dawn of the modern mathematics. Mathematicians started assuming different axioms for their algebraic structure and check what will come out of them. They've played with these rules, added or removed some of them and tried to modify these axioms or definitions. People started asking questions like: Okay, what if I had a algebraic system without associativity? And there it came *Non-Associative Algebras*. Many ideas and phenomena were developed like **Fields** and **Rings**. For example, a field is a set with two operations defined on it, usually denoted as $+$ and $\cdot$, with six axioms or definitions pretty similar to the axioms that we had for our groups. For these fields, if the set be $\mathbb{R}$, and we select the two operations to be the common summations and multiplication, we would have a field, and the common algebra that we've learned in high school. So you can see that these ideas are generalizations of the common algebra. A generalizations to any arbitrary set and any arbitrary operations, that they all act the same way.

Some group theory books tend to talk about Fields or Rings, before mentioning the definitions of group, but we are not going to cover them here. Anyway, if you are interested to know them, you can search and check them up, before continuing reading this.

The first mentioning of something named group was done by Evariste Galois in 1830s to the study polynomial equations. Galois tried to find a definitive solution to the fifth order of general polynomial equations, and in his papers he described a algebraic system for his proof. Years later this system was polished, with nice and definite axioms (Which we've just learned), under the name of *group*. After that people realized that this algebraic system has lot's and lot's of applications, and we can actually see and form systems that behave in these four simple characteristics, over many different fields. Hence the group theory was developed and grew. And more than a hundred years later, it's still one of the hot topics of mathematics.

I've told all of this history just to create a general idea that why these certain axioms were formed and why they matter. My attempt certainly didn't answer the main question directly, and I have to say the answer to that question is a little bit hard. But I hope with this general picture and history behind group theory made everything a little bit more clear, and I hope you find the subject more appealing. The more that you learn about group theory, the more you are going to get closer to the answers of these basic questions, and you're going to appreciate group theories' simplicity and its' vast applications. And

it is interesting that sometimes, to answer the very basic and simple questions, ironically, you require lot's of knowledge and experience. So with all of these questions at the back of our head, let's dig in and hope to find our answers in our way.

I think this is enough for an introduction. In the next part we are going to cover some examples of groups, and check if these four characteristics that we've talked about are true about them or not.

1.2 Examples of Groups

The best way to understand the power of groups is to see some of its' examples. So let's examine some of the most famous examples of group theory.

1.2.1 $(\mathbb{Z},+)$

OK, let's check if $\mathbb{Z}$ is a group under the operation common $+$. We already know that sum of two integer is an integer, therefor the set is **closed** under $+$. First let's check for an **identity member** e. We can easily see that our identity member is $e = 0$ here, since $0 + g = g + 0 = g, \forall g \in \mathbb{Z}$.

Do we have an **inverse member** for all of our members inside our set? Yes. For all $g \in \mathbb{Z}$ we have $-g$ as its' inverse, since $g + (-g) = (-g) + g = 0 = e$. Since we already know that common $+$ is **associative**, then the $(\mathbb{Z},+)$ is a group. That easy. The first example of a group.

1.2.2 $(\mathbb{R}^+,\times)$

By $\mathbb{R}^+$ we mean $\{r \in \mathbb{R} | r > 0\}$. So is it **closed**? It is obvious that multiplication of two strictly positive numbers produce a strictly positive number. So yes.

Do we have an **identity member** for this group? Well, what is a strictly positive real number, that when it is multiplied by another number, it gives us the same one? Our identity is $e = 1$. What about an **inverse member**? Well the inverse of $g \in \mathbb{R}^+$ is $\frac{1}{g}$, since $\frac{1}{g} \times g = g \times \frac{1}{g} = 1 = e$. And you can check that $\frac{1}{g}$ is also both positive and real, therefor a member of $\mathbb{R}^+$.

The last axiom talks about **associativity**. We know that the common $\times$ is associative for real numbers. Therefor this $(\mathbb{R}^+,\times)$ is also another example for groups.

1.2.3 $(\{1,-1\},\times)$

We have covered the **closure** of this group in the previous section. The **identity member** of this small set is $e = 1$. We can see that aside from the **inverse** of the identity member, which is always itself, the inverse of -1 is also itself, since $-1 \times -1 = 1 = e$. Lastly by knowing that **associativity** is true for this set (groups' sets with less than 3 members are always associative), we've proved that this small set with common $\times$, is actually a group.

Until now we've just shown collection of sets and operations which are groups. Let's see the next two examples which look like groups, but in fact they are not groups.

1.2.4 $(\mathbb{R},\times)$

Well. This seems like a group, but it's not. You can see that $1 = e$, since 1 times any reals number is that number itself. You can also see that this operation is **associative**. The problem we have here is with the **inverse member**. At the first glance $\forall g \in \mathbb{R}$ the $\frac{1}{g}$ seems like a legit inverse member, and we might mistakenly think that this is a group, but our problem is with the inverse of 0. Since $\frac{1}{0}$ is not defined inside real numbers, then 0 is not invertible, and this $(\mathbb{R},\times)$ is **not** a group. Now you can see why we've chosen $\mathbb{R}^+$ to be our set in our previous examples. By removing zero from the set, everything will be fine. So $(\mathbb{R} - \{0\},\times)$ is in fact also a group.

1.2.5 $(\{a, b, c\},*)$

This is an example that I've came up with, and I have a purpose for mentioning this. This $*$ is actually not any common or previously known operation. This operation is defined this way:

$$a * b = b * a = c \tag{1.5}$$

$$b * c = c * b = a \tag{1.6}$$

$$c * a = a * c = b \tag{1.7}$$

$$a * a = b \tag{1.8}$$

$$b * b = c \tag{1.9}$$

$$c * c = a \tag{1.10}$$

So the $*$ of any two members is the other member. So the question is: Is it a group?

Well, even though it is **closed**, we can see that there is no **identity member**. So it is obviously not a group. But let's check the other characteristics of this set and operation.

Well you can see that since we don't have any identity member, we cannot have any **inverse member**, because an inverse member g^{-1} is a member which $g^{-1} * g = e$. Let's check if this operation is **associative**. We'll check an example, using the defining relations of (1.5) to (1.10) for $*$:

$$(a * b) * c \stackrel{?}{=} a * (b * c) \tag{1.11}$$

$$(c) * c \stackrel{?}{=} a * (a)$$

$$a \neq b$$

By this single example we can see that $*$ is not generally an associative operation (note that we had to check every single combination of a, b, c for their associativity, if we'd wanted to prove that). So, even though this seems like a group, it does not fulfill any three of group axioms. I've brought this example to create an insight, that these kinds of structures of closed sets which make a roundabout with an operation within its' members, are not what we deal with in group theory. We have *Cyclic groups*, but they are totally different structures. We are going to talk about them in the future.

So here were some basic examples of group theory. Let's go for some more complicated examples of groups, and from now on, try to check for yourself, if these examples are groups or not, before reading the answers.

1.2.6 2×2 invertible matrices

({ All of 2×2 invertible matrices } , Matrix Multiplication)

OK. As a reminder, the inverse of any matrix A can be calculated as:

$$A^{-1} = \frac{1}{det(A)} adj(A) \tag{1.12}$$

Which $det(A)$ and $adj(A)$ are determinant and adjugate of our arbitarary $n \times n$ matrix A. In case of our 2×2 matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, the inverse is determined like this:

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \tag{1.13}$$

You can see that if the $ad - bc = 0$ or $ad = bc$, the inverse does not exist. Actually, we know from Linear algebra that a matrix is invertible if and only if its' determinant is not equal to zero. Now let's check if 2×2 invertible matrices do form a group or not.

We know that $det(AB) = det(A)det(B)$. By knowing this, we can see that the determinant of two non-zero matrices multiplication is also non-zero, and hence its' matrix is a member of our set. This shows that our set is **closed** under matrix multiplication.

We know that $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is the **neutral member** of matrix multiplication. Since $det(I) = 1 \neq 0$, then I is in fact a member of our set. So the first axiom is checked.

Do we have an **inverse** for all of our members? Well, Obviously yes, since we've selected all of the *invertible* matrices. You can see now why this certain selection was necessary to form a group out of our square matrices.

And finally, by knowing that the matrix multiplication is an **associative operation**, we prove that this is in fact a group.

Before going to get more serious, let's examine a very fun and interesting example.

1.2.7 Colors

({ All of the Colors } , Color Combination)

Groups are not all about numbers. They talk about any type of set or operation, and they can form in many different forms. Now let's see if this certain set and operation is a group or not.

We know that all of the colors can be created out of three Red, Green and Blue. We can denote each color by their RGB (Red, Green, Blue) colors like (r, g, b). We can formally define the set of all the colors as $\{(r, g, b)|r, g, b \in \mathbb{R}\&0 < r, g, b < 1\}$. So $(1, 0, 0)$ is the color red, $(1, 1, 1)$ is the color white and $(0, 0, 0)$ is black. When we are combining two colors, we are taking a mean out of their values of rgb, so our color combination operation is like $(r_1, g_1, b_1)(r_2, g_2, b_2) = ((r_1 + r_2)/2, (g_1 + g_2)/2, (b_1 + b_2)/2)$.
Based on these definitions, is this a group?

Well, it seems like a group at first, and it is **closed**, but actually it does not fulfill any of the axioms to be a group. At a first glance for an **identity member**, the color black (0,0,0) seems like a good idea. But it is not actually an identity member. Only the the combination of a color with itself returns the same color. But remember, for a group, a **Single global** identity member is required, so the first axiom remains unfulfilled.

You can see that **inverse member** is not also present in this set. What about **associativity**? Let's check it for an example of White(1,1,1), gray(0.5,0.5,0.5), and black(0,0,0).

$$\Big((1,1,1)(0.5,0.5,0.5)\Big)(0,0,0) \stackrel{?}{=} (1,1,1)\Big((0.5,0.5,0.5)(0,0,0)\Big) \tag{1.14}$$

$$\Big((0.75,0.75,0.75)\Big)(0,0,0) \stackrel{?}{=} (1,1,1)\Big((0.25,0.25,0.25)\Big) \tag{1.15}$$

$$(0.375,0.375,0.375) \neq (0.625,0.625,0.625) \tag{1.16}$$

In fact you can check that since $\overline{(\overline{(a,b)},c)} \neq \overline{(a,\overline{(b,c)})}$ shows no associativity, no operation with the form of taking a *mean* can be a legitimate group operation.

This is not the subject of our book, but these structures with only their closures to be true are actually called *Magma*s.

1.2.8 General Linear Groups

$GL_n(\mathbb{R})$ =({ **All of n $\times$ n invertible matrices** } , **MM)**

We have already proven the special case of 2×2, $GL_2(\mathbb{R})$ under MM [1] , is in fact a group. The notation of $\mathbb{R}$ indicates that we are dealing with real matrices. GL stands for **General Linear**.

These invertible $n \times n$ matrices represent linear transformations in a n-dimensional space. Again, by repeating the same argues for 2×2 cases, we can show that since a multiplication of two $n \times n$ matrices produce another $n \times n$ matrix, and since the determinant still remains as a non-zero value, the set is **closed**. The **identity member** is I_n and the **inverse** is also exists for each member, according to (1.12). Since matrix multiplication is **associative**, $GL_n(\mathbb{R})$ is a group, in fact an important group, for each dimension value of n.

If $det(A) = 1$, we call A *special*. We can form another group from the set of all the $n \times n$ invertible matrices, which their determinant is 1. It is a special case of the above group. You can see that since $det(AB) = det(A)det(B)$, if $det(A) = det(B) = 1$, then their product is also a member of this new group, and this assures the **closure**. The other axioms can be checked, the same as before. We call this group *Special Linear Group*, and denote it as $SL_n(\mathbb{R})$.

These special matrices/transformations are important for us because they preserve the volume (length) in $\mathbb{R}^n$ space upon application. For example, $SL_2(\mathbb{R})$, is actually group of rotations in 2D space in the form of $\left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix}\right)$. You know from linear algebra, that this rotation preserve the length in this 2D space.

1.2.9 Orthogonal Groups

O_n =({ **All n-dimensional Orthogonal Matrices**} , **MM)**

Let's have a reminder for the orthogonal matrices:

Imagine you have a n-dimensional vector $\vec{V}$. This vector can be written in matrix form, as a column matrix, in some arbitrary basis. As we know, The absolute value squared of the vector $\vec{V}$ is denoted as $|\vec{V}|^2$ and can be written as $|\vec{V}|^2 = \vec{V}^T\vec{V}$, which $\vec{V}^T$ is the transposed $\vec{V}$. A transpose of a matrix, is the same matrix, with its' rows and columns switched. For instance $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^T = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$. Now imagine we act a $n \times n$ matrix transformation A, on our vector $\vec{V}$, and we want to check what will happen to the size or the absolute value of my vector.

$$|A\vec{V}|^2 = (A\vec{V})^T(A\vec{V}) = \vec{V}^T A^T A\vec{V} \tag{1.17}$$

Which we have used the property $(AB\cdots Z)^T = Z^T \cdots B^T A^T$. Notice that Based on the above equation, if $A^T = A^{-1}$, then the size of my vector is preserved under the application of A. If this is true for any $n \times n$ matrix, we call

[1] Matrix Multiplication

that matrix an *Orthogonal Matrix*.

Orthogonal matrix:

$$A^T = A^{-1} \tag{1.18}$$

So as we've seen, these matrices preserve the length of the vectors under transformation. It is obvious that these kinds of matrices are invertible, with their inverse A^T. It can be proved that $det(A^T) = det(A)$, and based on this we have:

$$A^T A = I \implies$$

$$det(A^T A) = det(A^T) det(A) = 1$$

$$\Big(det(A)\Big)^2 = 1 \implies det(A) = \pm 1 \tag{1.19}$$

So the determinant of an orthogonal matrix is either 1 or -1. Notice that the opposite is not necessarily true.

Now let's check if the set of all the orthogonal matrices under MM is a group. If A and B are orthogonal, then because $AB(AB)^T = ABB^T A^T = ABB^{-1}A^{-1} = 1$, then the set is **closed**. Since $I_n = I_n^T = I_n^{-1}$, this is the **neutral member** of our group. Because the determinant of any orthogonal matrix is either $+1$ or -1 (a non-zero value), then they are **invertible**. And we have already seen than MM is an **associative** operation for a set of $n \times n$ matrices. This is in fact a group.

Just like the case for general linear group, we can make a separate group for the *special* cases of orthogonal matrices with their their determinant equal to 1. We call this group *Special Orthogonal Group*, in n dimensions, and denote it as SO_n. Notice that it is impossible to make any different special case for the case $det(A) = -1$, since our identity member's determinant is 1.

1.2.10 Unitary Groups

U_n =({ All n-dimensional Unitary Matrices} , MM)

This is analogous to the above case of orthogonal matrices, just in this case, unitary matrices are defined for complex matrices of $\mathbb{C}$. We know that the squared absolute value of a complex number is $|z|^2 = z^* z$, which z^* is the complex conjugate of z. because of this difference, the squared absolute value of a complex vector, is defined as $|\vec{V}|^2 = (\vec{V}^*)^T \vec{V}$. We denote $(\vec{V}^*)^T$ as $\vec{V}^\dagger$ [2]. We can follow the same argument as orthogonal matrices, and get the definition for a unitary matrix:

[2] Different people have different notations for this, but physicist usually use this notation, a deformed T called dagger †.

Unitary matrix:

$$U^\dagger = U^{-1} \tag{1.20}$$

Orthogonal matrices are actually the real analogue of these unitary matrices. These matrices preserve norm of our complex vectors. Similarly, we can prove that $|det(U)| = 1$, but this time since U is complex (hence $det(U)$ is also complex), the $det(U) = e^{i\phi}$, with $0 < \phi < 2\pi$ as a phase in our complex plane.

Now is the set of our $n \times n$ unitary matrices a group under MM? Using a similar reasoning to the orthogonal case, we can assure its' **closure**. The **identity member** is the same I_n. Since $det(U) = e^{i\phi} \neq 0$, the **inverse member** exists for each of the unitary matrices. The MM is still an **associative** operation for complex matrices of $\mathbb{C}$. Based on all of these, we can see that our U_n is also a group. Again for the *special* case of $det(U) = 1$, we are having another group called SU_n.

So, we've talked about many forms of $n \times n$ matrices as a linear transformation, that with MM, forms a group. These groups are very important, and we are going to come back to them many times, so try to memorize their notations. The table below summarize these groups that we've talked about, and can assist you to remember everything we've just mentioned.

	General	Special(det=1)
Linear ($det \neq 0$)	$GL_n(\mathbb{R})$	$SL_n(\mathbb{R})$
Orthogonal ($A^T = A^{-1}$)	$O_n(\mathbb{R})$	$SO_n(\mathbb{R})$
Unitary ($U^\dagger = U^{-1}$)	$U_n(\mathbb{C})$	$SU_n(\mathbb{C})$

Table 1.1: Summary of $n \times n$ Matrix Groups

OK, let's continue our examples, but this time, let's change the subject from matrices.

1.2.11 Symmetry and Permutation Groups

Symmetry and Permutation groups are one of the most famous examples for group theory. Regardless of you intentions with group theory, you are going to encounter with them many times in group theory. This is both generally and historically, an important example.

Imagine you have a set of n different objects with a specific position, numbering these positions as $1, 2, \cdots, n$. A permutation of them is any change of their orders, and we can refer it as a function p which changes our position a to b like $p(a) = b$.

As an example, imagine an arbitrary p for $n = 3$ that p(1)=2, p(2)=1, and p(3)=3. The following notation is often used, because of its' simplicity, and it is called *Cauchy's two line notation*.

$$p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{1.21}$$

By comparing the first and the second rows, you can see that 1 goes to 2, 2 goes to 1, and 3 is remained unchanged. Notice that the order of columns does not matter, for example, the following representation is also showing the same function as before:

$$p = \begin{pmatrix} 3 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix} \tag{1.22}$$

Now that we are familiar with the notation, let's define our group. The set of **all** the possible permutations of n positions, along with the operation of **Composition of Permutations** is called *Symmetry Group*, and is denoted as S_n. let's talk about that in detail.

Imagine $n = 2$. From the basic combinatorics, you know that the total amount of possible permutation of n member is $n!$. So for $n = 2$, we have $2! = 2$ members. These member are as below:

$$\{e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\} \tag{1.23}$$

We can say the **Order** of symmetry group S_n is $n!$, and this *order* means the number of members in a group's set.

Now that we know about the set in our group, let's talk about the operation of the group. If α and β are two members of S_n, when we are saying $\alpha\beta$, we mean first apply the permutation β, and then apply *alpha*. This is called *composition of functions* and is defined as below.

$$(\alpha\beta)(x) = \alpha(\beta(x)) \tag{1.24}$$

So our operation in this group, often called *multiplication*, is simply a statement of the order of application. For our example, you can see that if you apply α twice, or $\alpha\alpha(= \alpha^2)$ you will get e. At first, α changes the position of 1 to 2, and 2 to 1. With the second application, the 2 will get back to 1, and 1 to 2. We can write this characteristic this way:

$$\alpha\alpha = e \tag{1.25}$$

Let us examine a more complicated example of S_3. This group's order is $3! = 6$. Here are its' 6 members of all the possible permutations of $n = 3$ positions:

$$\{e = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \alpha = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \beta = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \\ \gamma = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \delta = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \epsilon = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \} \tag{1.26}$$

Now let's talk about the multiplication in this group. As an example, what will happen if you apply ϵ and then α? You should one by one check what will happen to each position after their successive application. For example, by knowing $\epsilon(1) = 3$, and $\alpha(3) = 2$, We'll get $\alpha\epsilon(1) = \alpha(\epsilon(1)) = \alpha(3) = 2$. Doing this for all three positions we will get:

$$\alpha\epsilon = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \gamma \tag{1.27}$$

Now we should do this for all of the possible combinations of our members. Obviously this could take a while. We can show the result of this calculation in a compact way called *Multiplication Table*, or *Cayley Table*. This is similar to the multiplication table of numbers we used way before, and each cell in this table shows the result of (row $\circ$ column). For S_3 we have:

$\circ$	e	α	β	γ	δ	ϵ
e	e	α	β	γ	δ	ϵ
α	α	e	δ	ϵ	β	γ
β	β	ϵ	e	δ	γ	α
γ	γ	δ	ϵ	e	α	β
δ	δ	γ	α	β	ϵ	e
ϵ	ϵ	β	γ	α	e	δ

Table 1.2: Multiplication Table of S_3

As you've probably realized by now, groups can either have **finite** or **infinite** members, and these multiplication tables can be formed for any finite groups, and can carry important information about the group. First of all, any different combination and number of multiplication can be calculated using these tables. You can also check if a group is closed or not by looking at its' multiplication table. For instance, S_3 is closed because every single value in the multiplication table is also a member of our group's set. If you've formed the multiplication table for a structure, and you've encountered a member outside of your set in your table, then that structure cannot be a group because it lacks the closure.

You can easily check if a system is Abelian or not too. If the table is symmetric from its' diagonal line, then it is an Abelian group. You can check that S_3 is in fact not an Abelian group, and if you form the multiplication table for S_2, you can see that group is Abelian. In fact, the only Abelian S_n is S_2.

The other good advantage of multiplication table is that you can easily check for an identity member in it too. There should be one row and column that return the same values of the original members. These row and column usually take place at the first row/column, but generally, the order is arbitrary and it can be anywhere in our multiplication table. If you do not see any of these Identical set of rows and columns, then your structure is not a group.

You can also check if there's an inverse member for each of your group members from multiplication table. For this to be true, there should at least one identity member e, in every column and row. And also check for these es' to be diagonally symmetrical. If these we not true for you multiplication table, then you are not dealing with a group.

The only thing that is not obvious from the multiplication table is the associativity characteristic. To check if the operation is associative or not, you usually need to do some extra work. But still, the table can be useful to check three of the four defining characteristics of groups easily by a few glances, therefor it is pretty useful for finite (and of course low order) structures.

OK, now let's actually prove that S_n is a group. By knowing that S_n consists of all of the possible permutation, and by knowing combination of any two permutation is another permutation, we can be sure of its' **closure**. There's always a permutation which does not change any position, and we call it e, our **identity member**. What about **inverse member**? Again, it's easy to show that because S_n consists of all of the possible permutation, there is always another member (could be itself) that does the opposite of the prior one. For our two line notation, to get inverse member of any permutation, just change the place of the rows, and you'll end up with the inverse member. And it is obvious that this new permutation is also a member of our symmetry group!

What about **associativity**? Well, this is a little bit trickier than the others. Our operation is the function composition for our permutation functions, and for associativity to be true, the following should be true for any three arbitrary α, β, and γ:

$$\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma \rightarrow \alpha(\beta(\gamma)) = (\alpha(\beta))(\gamma) \tag{1.28}$$

But this is true for any function, and because permutations are also functions, we know that associativity is true for S_n, therefor they are groups.

There's another term called *Permutation Group*, and it is often misused instead of symmetry group. There lies a little bit of ambiguity between these two notions, and it is good to know that they are in fact different. Permutation group is any group that can be formed with the permutation functions, but the symmetry group is the group consisting of **all** of the permutations possible for n positions. You can see that symmetry group is actually a special case of permutation group, and it is much more well know.

Permutation groups are usually denoted in many particular ways, but we are not going to go through them one by one. As an example, take ϵ, δ, and e from S_3, and you can see that this set also forms a group, a permutation group (this group is actually called $A3$), and you can see its' multiplication table in

the following Table 1.3.

$\circ$	e	δ	ϵ
e	e	δ	ϵ
δ	δ	ϵ	e
ϵ	ϵ	e	δ

Table 1.3: Multiplication Table of an Example of a Permutation Group

Before ending this section, it is good to mention another very well-known notation for permutations, other than our two line notation. This is called *cyclic notation* and it is used in many books. Instead of writing our permutation function in two lines, we will use only one line and we will write any two positions related to each other, successively. It can be best understood and explained with an example. For instance:

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)(3) \tag{1.29}$$

To see how it works, you should start with a number. For example 1. The next number to 1 is 2. so $\gamma(1) = 2$, or 1 goes to 2. There is no number next to 2, and there's only a closed parenthesis. When there is a closed parenthesis, go back to the start of that block's opened parenthesis, and the first number is what 2 goes to. for our example, 2 goes to 1 or $\gamma(2) = 1$. For three, you can see it is in a separate parenthesis by itself, it means that 3 goes to itself or $\gamma(3) = 3$. Let's check a more complicated case:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix} &= (1\ 5\ 2)(6\ 4)(3) = (3)(6\ 4)(1\ 5\ 2) \\ &= (2\ 1\ 5)(4\ 6)(3) = (2\ 1\ 5)(4\ 6) \end{aligned} \tag{1.30}$$

All of the written cyclic permutations are actually equivalent. let's check that. For the first cyclic example we read it like (you can check their equivalent two line notation whilst reading): 1 goes to 5. 5 goes to 2. we've reached a closed parenthesis, then 2 goes all the way back to 1. Next block. 6 goes to 4, And 4 goes to back to start, 6. At the end, 3 goes to 3. This is how it works.

You can see that you can change the position of different blocks, it does not matter. You can also shift the members inside any blocks, it's still the same. Another thing is that people usually don't write the single membered blocks like (3), so it is up to you to mention them, or not. Each number is only mentioned once, so if you don't see a number in this notation, that number returns to itself.

And that's it for this cyclic notation, a notation that is very commonly used for symmetric and permutation groups' members.

1.2.12 Symmetry Groups for Different Shapes

These groups are probably the most famous examples of groups, but we are covering them lastly. Some of the texts covering group theory tend to start the idea of groups by introducing the shapes and the set of all of their symmetrical transformations. We've followed another path, but anyway, these groups are in fact one of the important applications and examples of group theory, therefor, they must be covered at some point. They are also one of those groups that we are going to get back at them many times.

To start, let's take a look at the following shape. It is called *Snoldelev Interlaced Horns*, a symbol that was found on a rune-stone named *Snoldelev Stone* found in Denmark, believed to be created back at the 9th century, at the age of Vikings.

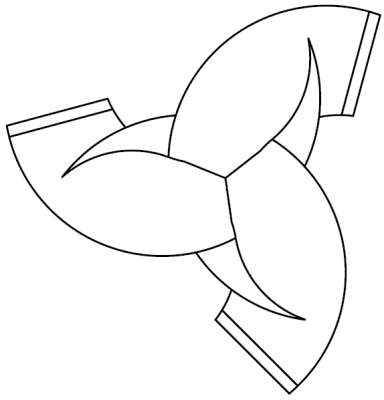


Figure 1.1: Snoldelev Interlaced Horns.

Now let's talk about this beautiful sign's symmetries. What do we mean by symmetries? Let's have a definition of symmetry here. Symmetry is a *transformation* that under which the shape remains unchanged. These transformations can be any functions like displacement, rotations, mirroring, etc. Now, let's take a look at Snoldelev interlaced horns, and try to find these transformations.

Well, we can rotate it by 120 °from its' middlepoint and we will get the same shape. Also it is possible to rotate it 240°, and we'll still get the same shape. What about 360°? Well yes, and this transformation is the same as doing nothing or rotating by 0°. This is in fact our identity member. We can go on and add more 120°s to get like 480°, but we know that a rotation by 480°(or any others similarly), is the same as a rotation by 120°.

So here are 3 symmetrical transformations, are there any else? The answer is no. At first you might think that mirroring is also possible, but if you pay a closer attention, you'll see that by mirroring, you will change the orientations of the horns. The horns are now facing clockwise, but upon mirroring, they'll become counter-clockwise, therefor they are not symmetric operation for this shape. As an opposite example, take a look the following one:

Figure 1.2: Mitsu Ichō Symbol (3 ginkgo leaves).

This symbol of 3-leaves is a common Japanese emblem called *Mitsu Ichō* that it is believed that the *Tokugawa* clan used to bear in the 17th century. You can see that for this symbol, other than rotations by 0°,120°,240°, you have mirroring by the lines such as the orange line shown in Figure 1.2.12.

So for our Snoldelev interlaced horns, if we note rotations from the middle-point by 0°as e, by 120°as v, and 240°as w, The set of all of the symmetric transformations in the 2D plane of the shape are:

$$G_1 = \{e, v, w\} \tag{1.31}$$

If we add composition of functions as our operation (just as before), the (G_1,composition) is the **Symmetry Group** of our Snoldelev interlaced horns.

You can see that the **inverse** of v is w, and inverse of w is v, since vw (their multiplication) means a rotation by 240°followed by another rotation of 120°, which sums up to a rotation by 360°= 0°which is our **identity member** e. It is obviously **closed**, and since we are dealing with function compositions, our operation is **associative**. The following is the multiplication table of our Snoldelev interlaced horns:

∘	e	v	w
e	e	v	w
v	v	w	e
w	w	e	v

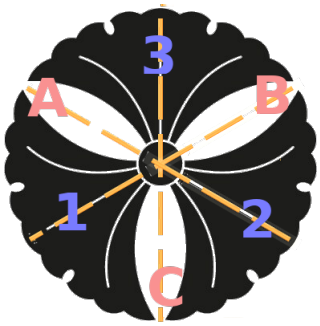
Table 1.4: Multiplication Table of the Symmetry Group of Snoldelev Interlaced Horns Shape.

You can see that this group is Abelian. And also compare this table to Table 1.3 of our permutation group, and see how similar they look. This similarity is a very important phenomena in group theory that we are going to come back in the future to talk about it.

Now let's check out the symmetries of our Mitsu Ichō. We've noticed that other that e, v, w, this shape has 3 other mirroring transformations too. The orange line in 1.2.12 is showing one of these mirroring symmetric lines, and the other two can be spotted easily. We call these three mirroring or reflection transformations A, B, and C. So the set of all the symmetry transformations of Mitsu Ichō sign is:

$$G_2 = \{e, v, w, A, B, C\} \tag{1.32}$$

Now we should make a multiplication table for the symmetry group of Mitsu Ichō label. But before that, let's number each leaf of Mitsu Ichō so we can visualize each transformation a little better (we've actually numbered the area between the leaves, but we are going to call them leaves anyway). Notice that we have 3 leaves, each numbered in a specific way, and each of the members of G_2 changes the order of our numberings in a different way. Look at the figure below:



For example, reflection through A exchanges the places of 1 and 3, but 2 will stay unchanged. Or with transformation v, 2 goes to 3, 3 goes to 1 and 1 goes to 2. Remember that both v and w are chosen to be counter-clockwise. Now based on this figure, try to check the following multiplication table for our Mitsu Ichō label's symmetry group.

You have probably noticed that this group looks pretty much like S_3. You can compare their multiplication tables and see that they actually act like each other. You can actually do a little trick and rearrange the leaves' numbers in a row, and then see that this set of *symmetric transformations* are nothing but our old permutations of our leaves' numbers (you can go now and check which permutation is associated with each Mitsu Ichō's symmetry group's members). By this analogy, it is now obvious why their multiplication tables looks so much like each other, and you can now see why we've called S_n, the *Symmetry Groups*.

These two examples are not the only pairs of groups that look like each other. We will talk about these groups that *look like* each others in details in the future.

Any geometric shape in the world has a symmetry group associated with them. Even the most asymmetric shapes has the trivial group of $(\{e\}, composition)$

$\circ$	e	A	B	C	w	v
e	e	A	B	C	w	v
A	A	e	w	v	B	C
B	B	v	e	w	C	A
C	C	w	v	e	A	B
w	w	C	A	B	v	e
v	v	B	C	A	e	w

Table 1.5: Multiplication Table of Mitsu Ichō's Symmetry Group

as their symmetric group. The order of the symmetry group for many shapes can exceed much more than what we've covered. For example, a simple cube has 24 members in its' symmetry group, or some other highly symmetrical shapes in different dimensions contain even more members. And their transformations can be either transformations, reflections from a point or a line, rotations, and many other things.

I believe these example are quite enough at the start of the study of group theory. I hope these examples have created an idea about groups and what they are all about. You might have noticed that group theory is actually introducing another level of abstraction, because we are dealing with operations and transformations themselves inside our algebraic system. We are talking about the relations and algebra between the rotations and reflections themselves, and we do not talk about the points of any specific shape that undergoes these functions. Now this abstraction created by the groups can helps us in many ways, and it is one of the biggest powers that groups can offer.

There are many other examples of groups, like the Rubic cube group (which has more or less became the symbol of group theory), many puzzle games' groups, Knot theory in in topology, many groups defined in physics such as gauge group, and many more, but I believe these examples here are enough. Try to remember General linear matrices and Table 1.1, Permutation groups, and S_n. We are going to get back to them many times, so try to memorize their notation before continuing.

Before ending this chapter, let us go through another last concept called *Cyclic Groups*, and then move on from the basics and start to learn some important relations between groups and some famous theorems in group theory.

1.3 Cyclic Groups