

1 Introduction

The idea of groups is a sort of generalization of addition and multiplication. While this may not initially sound very interesting, it turns out to be very useful, as it allows a number of very different concepts to be studied and understood using some of the familiar properties of addition and multiplication. Although groups are typically introduced in an upper-level course in mathematics, nothing beyond basic high school algebra is required to understand them. This note aims to give a brief, informal outline of what groups are, mostly through definitions and examples, and to show how group representation provide a tool to find relationships between mathematical structures that may seem to be unrelated. The reader is assumed to have a mathematical background up to the pre-calculus level, although further experience may be beneficial in understanding some of the examples and references.

2 Binary Structures

The definition of a group is easier to form given a few other definitions. A natural starting point is the definition of a binary operation.

Definition 1. A **binary operation** on a set S is a function, $*$, mapping an ordered pair of elements S to another element in S . The function acting on the ordered pair (a, b) can be written as either $*(a, b)$ or $a * b$, with the latter the more common.

There are slicker, more precise definitions for a binary operation, but for this informal discussion, the above will suffice. The definitions for *function*, *ordered pair*, and *set* are the typical ones, omitted here for brevity with the assumption the reader is familiar with them.

One point which is worth emphasizing is that a function in the above definition is nothing more than an association of the input variable(s), in this case, the ordered pair of elements from S , with some other element, in this case, from S . So while formulas such as $f(x) = x^2$ are how functions are typically defined in many early math courses, these are just a convenient short-hand for describing a function. Functions can exist without a closed-form algebraic formula to describe them. The only requirement is for each input (or set of inputs for multiple variable functions, like our binary operation) to have a unique element associated with it.

Another important point to note is that in our definition above, a binary operation on a set S can only map to another element within S . That is, the element associated with the ordered pair of elements from S is also in S . This property is summarized by saying the binary operation is *closed* on S .

A set together with a binary operation on that set is called a *binary structure*, repeated below for reference.

Definition 2. A **binary structure** is a set S , together with a binary operation, $*$ acting on that set.

A binary structure is denoted by $\langle S, * \rangle$, where S and $*$ are the set and binary operation, respectively, that the structure refers to.

Here are a few examples of binary structures, to illustrate.

Example 1. Take the set $S = \{0, 1\}$, and define an operation on it by assigning to each pair of elements from S an element from S (either a 1 or a 0). There are 16 such possible operations that can be defined this way, yielding 16 possible binary structures on the set $\{0, 1\}$. Those familiar with digital or Boolean logic may notice that the AND, OR, XOR, NAND, NOR, and XNOR operations make up six of these structures.

The above is an example of a finite binary structure, which is a binary structure whose associated set contains only a finite number of elements. A helpful way of representing a finite binary structure is with a table. A table of one of the binary structures in the previous example is shown below.

*	0	1
0	0	1
1	0	1

The first column and the first row contain each element in the set. The remaining squares contain the output of the binary operation for the ordered pair made up of the element in the first column on the same row as the square, and the element in the first row on the same column as the square. The convention used in this note is that the first column is associated with the first element in the ordered pair, and the first row is associated with the second element in the ordered pair. So we could rewrite the above table as $*(0, 0) = 0$, $*(0, 1) = 1$, $*(1, 0) = 0$, $*(1, 1) = 1$.

Infinite binary structures, as you probably expect are binary structures whose sets contain an infinite number of elements. Although they cannot be totally specified by a table like finite binary structures, it is sometimes helpful to imagine them as a table made up of an infinite number of rows and columns.

Example 2. The set of $m \times n$ matrices, for any particular choice of m and n , under addition is a binary structure, as is the multiplication on the set of $n \times n$ matrices, for any particular choice of n . Note that each choice of m and n yields a distinct binary structure.

Example 3. Addition on the set of integers is a binary structure, as is addition on the set of rational numbers, the set of real numbers, and the set of complex numbers. Likewise, multiplication on the set of integers, the set of rational numbers, the set of real numbers, and the set of complex numbers are all binary structures. Similarly, subtraction on each these sets is a binary structure, as is division (where integer division is the quotient portion of the quotient and remainder, similar to what is seen in many computer programming languages).

It is important to realize that the sets do not have to be made up of familiar mathematical operations, as the following example demonstrates.

Example 4. Let F be the set of all cats in the world. Define an operation on this set by assigning the author's cat, Deuce, to any ordered pair of cats. This operation together with F is a binary structure.

While the previous example seems pretty useless, it does demonstrate how general binary structures can be.

3 Identities and Inverses

The definition of a binary structure is important in defining groups, as groups are binary structures with certain other restrictions. We are not out of the woods yet, however, as these restrictions require a few definitions of their own.

Definition 3. Let $\langle S, * \rangle$ be a binary structure. An element, e , of $\langle S, * \rangle$ with the property $e * a = a * e = a$ for all $a \in \langle S, * \rangle$ is called an **identity** of $\langle S, * \rangle$ (also referred to as an **identity element**).

An example of a binary structure with an identity element is addition of integers, with 0 acting as the identity. Another example is multiplication of real numbers, with 1 as an identity. It may be obvious, but it is worth noting that not all binary structures have an identity element. For instance, the example above involving cats has no identity.

Another important point to note for an identity element is that only one can exist for a particular binary structure. To see this, assume there are two identities, e_1 and e_2 . If we let these operate on each other, we get $e_1 * e_2 = e_2 * e_1 = e_1 = e_2$. Since $e_1 = e_2$, it is not possible to have two distinct identities.

The next definition needed is that of an inverse element.

Definition 4. Let $\langle S, * \rangle$ be a binary structure, and let a be an element of S . An element, a' which has the property $a' * a = a * a' = e$ is called an **inverse** of a .

Outside of the context of a group, an inverse element is not quite as interesting, so further discussion of it will wait until we define a group in the next section.

4 Groups

There is one more definition required before defining the group.

Definition 5. A binary operation is called associative on a set S , if for every $a, b, c \in S$, it is true that $(a * b) * c = a * (b * c)$.

Associativity is probably familiar from earlier subjects. The gist of the property is that it allows a binary operation on more than two elements to be written unambiguously without any parentheses. That is, we can write $a * b * c * d * \dots$, and it only has one result. If the operation is not associative, an operation on more than two elements can have a different result depending on the order in which we evaluate the elements.

Now we are finally able to give the definition of a group.

Definition 6. A group is a binary structure, $\langle G, * \rangle$, that has the following properties.

1. $*$ is associative
2. $\langle G, * \rangle$ has a identity element.
3. Every element in $\langle G, * \rangle$ has an inverse.

For convenience, a group, $\langle G, * \rangle$, will sometimes be referred to as G , and the identity element will be referred to as e .

As mentioned before, this definition sort of abstracts some of the useful properties of addition and multiplication. Any structure which fits the definition of a group will have certain properties in common. One of the more important of these properties is the ability to solve certain types of equations with unknowns in them, such as $a * x = b$, where a and b are known elements of a particular group, and x is the unknown. We can multiply each side of this equation on the left by a' , the inverse of a , giving us $a' * a * x = a' * b$. The associative property lets us write this as $(a' * a) * x = a' * b$. The inverse property lets us know that this can be rewritten as $e * x = a' * b$. Finally, the identity property lets us rewrite this as $x = a' * b$. Thus the group properties have allowed us to cancel out the known element on the left, to find the value of the unknown. It is also possible to cancel out an element on the right (e.g., $x * a = b$), through a similar procedure.

Note that in the above, it is important to note which side the multiplication is done on. That is, had we started our equation as $a * x * a' = b * a'$, we would not necessarily be able to manipulate the equation to cancel out the a . This is because there is nothing in the definition of a group which requires $a * b = b * a$ for the elements of a group. Groups where this property holds for all elements are called *commutative*, and those where it does not hold are called *anticommutative*. Groups with a commutative operation are called *abelian* groups.

One thing you might notice from the above equation is that $x = a' * b$ is still an ambiguous equation, if the element a has more than one inverse. Fortunately, the inverse of each element in a group is unique. This can be seen by letting a'_1 and a'_2 be inverses of the element a . This gives the equation $e = a * a'_1 = a * a'_2$. Taking from this equation, $a * a'_1 = a * a'_2$, we can cancel out the a on the left, as above, using either of the inverses, to give $a'_1 = a'_2$, which shows the two inverses must actually be the same.

At this point, we will give some examples of groups, to try to flesh out the definitions and properties given so far.

Example 5. Addition on integers is a group, with 0 acting as the identity element, and $-a$ acting as the inverse element for a (e.g., $1 + (-1) = 0$). Similarly, addition is also a group on rational numbers, real numbers, and complex numbers.

Example 6. Multiplication on \mathbf{R}^* , the set of all real numbers excluding 0, is a group, with 1 acting as the identity and a^{-1} or $1/a$ acting as the inverse element of a (e.g., $2 \times \frac{1}{2} = 1$). Multiplication is also a group on the similarly defined sets, \mathbf{Q}^* (rational numbers excluding 0) and \mathbf{C}^* (complex numbers excluding 0)

As this note has advertised groups as abstractions of the properties of addition and multiplication, the previous two examples should come as no surprise. The sets the multiplication examples are defined on may be somewhat unexpected, however. The reason 0 must be excluded is because 0 has no inverse, as $\frac{1}{0}$ is not defined. Also, multiplication on the integers is not mentioned because it is not a group. While it is associative and it does have the same identity element (1), the only elements with inverses are 1 and -1 . This is because $\frac{1}{a}$ is not an integer for any integer, a , other than 1 or -1 , but are generally rational numbers.

It is also worth pointing out the binary operations of subtraction and division are not groups on any of these sets. This is because these operations are not associative (i.e., $(a - b) - c \neq a - (b - c)$ and $(a \div b) \div c \neq a \div (b \div c)$, in general).

Example 7. The binary structure in the following table is a group

*	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

You might recognize this as the bitwise XOR operation on the elements 0 through 3 (this is the \oplus operator in C). As a matter of fact, the bitwise XOR operation is a group on any set of integers 0 through m , where m is one less than a power of 2 (i.e., $m = 2^n - 1$ where n is an integer).

This example reveals a few interesting points about groups written in table form. The first is a property those familiar with the puzzle game Sudoku might recognize. Completed Sudoku puzzles have each of the numbers 1 through 9 written in the table so that each row and each column has a complete list of the numbers, but they only appear once. Groups have a similar property, though without the extra restriction in Sudoku that each 3x3 cube also have a complete list of the elements. In a group table, an element only appears once in each row and column. This relates to the property of each element having a unique inverse. Take the following table, for example:

*	a	b	c
a	a	b	c
b	b	a	a
c	c	a	b

Now assume we wanted to solve the equation $b * x = a$. We know that with a group, we can cancel out the b with its inverse to find the value of x . But with the above table, there are two possible solutions for x , as both $b * b = a$ and $b * c = a$ are true. So b does not have a unique inverse in this table.

Another property we will mention in passing that the above table of a group shows is that of a commutative group. A bitwise XOR operation is a commutative operation, so this is a commutative group, meaning that $a * b = b * a$ for all elements of the group. As you can see in table, this causes a symmetry across the diagonal portion of the group. The reason for this is straightforward - $a * b$ and $b * a$ have a symmetrical relationship in the table, since the left side of the equation is an index into the rows and the right side of the equation is an index into the columns. Since a commutativity implies that $a * b = b * a$, the symmetrical relationship between these equations in the table is mirrored by the arrangement of the elements.

Example 8. The set of n functions representing n evenly spaced rotations around the unit circle, with the operation of function composition is a group. To illustrate this a little more concretely, take $n = 4$. This gives us 4 rotations around the circle, evenly separated by $360/4 = 90$ degrees. So the elements of this set are r_0, r_{90}, r_{180} , and r_{270} , where the subscript denotes the angle of rotation (i.e., r_0 is rotation by 0 degrees, r_{90} is rotation by 90 degrees, etc.). Composition of these functions is just performing one rotation after another, which gives a rotation equal to the sum of the individual rotations. So for example, composing r_{90} with itself gives a rotation by 90 degrees, followed by

another rotation by 90 degrees, resulting in a rotation by a total of 180 degrees, or r_{180} . So the table for these rotations is as follows:

*	r_0	r_{90}	r_{180}	r_{270}
r_0	r_0	r_{90}	r_{180}	r_{270}
r_{90}	r_{90}	r_{180}	r_{270}	r_0
r_{180}	r_{180}	r_{270}	r_0	r_{90}
r_{270}	r_{270}	r_0	r_{90}	r_{180}

Here we write any rotation greater than 360 degrees by in terms of degrees less than 360 degrees, since any angle written as $360n + \theta$ is equal to the angle θ .

You can see from the above table that the operation on this set is closed. Associativity of the operation follows from the fact that the operation results in the addition of angles, and addition is associative. The identity for this set is r_0 , and the inverse for each angle, r_θ is the rotation, $r_{-\theta}$. Thus, this operation is a group, as is any similar group of n rotations starting at 0 degrees and evenly spaced by $360/n$ degrees around the unit circle.

This example shows how groups can apply to a wide range of topics, such as the typically geometric idea of rotations around the unit circle.

5 Isomorphism

The concept of isomorphism allows us to show that two seemingly different groups are actually the same, in the sense that one group can be thought of as a relabeling of the elements of the other group. To demonstrate, compare the following two tables.

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

*'	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Notice in the above, even though we have two different labels for our operations acting on different elements, if you equate the elements as in $a = 0$, $b = 1$, and $c = 2$, we can see that the tables are actually the same. This is what an isomorphism between two groups tells us - that the groups are structurally the same, labeled differently. The elements between each group are synonymous.

To give a formal definition for isomorphism, we need just a few short supporting definitions.

Definition 7. An **injective** (or **one-to-one**) function, $*$, is a function where $*(a) = *(b)$ for any two elements a and b in the domain of $*$, implies $a = b$. An injective function is called an **injection**.

Definition 8. A **surjective** (or **onto**) function, $*$, is a function where for any element, b , in the range of $*$, there exists an element, a in the domain of $*$ such that $*(a) = b$. A surjective function is called a **surjection**.

Definition 9. A **bijective** function, also called a **bijection**, is a function that is both injective and surjective.

The formal sounding definitions maybe obscure the nature of these ideas, which are actually pretty straight-forward. An injection is any function, f , which assigns an element in the range to only one element in the domain, so that for any two elements in the domain, a and b , you will never have $f(a) = f(b)$. An example of an injective function is $f(x) = x$ on the set of real numbers. Evaluating at $x = 1$, we have $f(1) = 1$. For no other value of x will we have $f(x) = 1$. An example of a function which is not injective is $f(x) = x^2$ on the set real numbers. Here, we have $f(2) = f(-2) = 4$. Since 4 is assigned to both 2 and -2 , f can not be injective.

A surjective function, f is one in which each element in the range is assigned by f to at least one element in the range. This will largely depend on how the domain and range are chosen. For example, if we say let f map from real numbers to non-negative real numbers, and say $f(x) = x^2$, then f is surjective, since every non-negative real number can be written as x^2 for some x . However, if we say that f maps from the real numbers to the real numbers, then f is not surjective, because there is no real number for which $x^2 = -1$.

The bijection merely combines these two. It can be thought of as an assignment of each element from one set to exactly one element in the other set, and vice versa.

With these definitions, we can now give the definition of a isomorphic groups.

Definition 10. Two groups, $\langle G, * \rangle$ and $\langle H, *' \rangle$ are **isomorphic** if there exists a function ϕ (called an isomorphism) mapping from G to H which has the following properties:

1. ϕ is a bijection
2. For every $a, b \in G$, $\phi(a * b) = \phi(a) *' \phi(b)$

The property that ϕ is a bijection insures that there is a way to provide a mapping between both groups so that each element of one group can be mapped to exactly one other element of the other group, which is possible for any two sets which have the same number of elements. The second property is a compact way of saying the operation for one group maps each element in that group in the same way as the operation of the group it is isomorphic to.

Some examples of isomorphic groups are helpful to illustrate the idea.

Example 9. Engineers who design radio circuits or other signal processing circuits often have to deal with amplifier circuits made up of different gain stages. Each gain stage multiplies a signal, so the total gain (that is, the factor by which the input signal is multiplied) of the amplifier is equal to the product of the gain of all the individual stages. It is common for the gain of each stage and the total gain of the amplifier to be expressed in decibels, abbreviated dB. To convert a gain value, x , from a scale factor to dB, the formula is $\text{dB} = 20 \log x$. So for example, if an amplifier multiplies a signal by 10, then the gain in dB is $20 \log 10 = 20$.

Using some of the ideas presented above, we can gain some insight as to why this unit is useful. First consider the set of positive real numbers with the operation of multiplication. This forms a binary structure, $\langle \mathbf{R}^+, \times \rangle$. We know the operation is associative, since multiplication of real numbers in general is associative. We also know the set has an identity, since $1x = x$ for any $x \in \mathbf{R}^+$. Finally we know each element in the set has an inverse in the set, since $\frac{1}{x} \in \mathbf{R}^+$ and $\frac{1}{x}x = x\frac{1}{x} = 1$ for all $x \in \mathbf{R}^+$. Thus this binary structure forms a group.

Now take addition on the set of real numbers, $\langle \mathbf{R}, + \rangle$. As we already explained above, this is a group, too. The interesting thing here is that these two groups are isomorphic. The isomorphism from multiplication to addition is $\phi(x) = \log x$ (note that here we are taking $\log x$ to mean the logarithm base 10, not the natural logarithm which is more common in mathematics). To verify this, first notice that if $\log(x) = \log(y)$, then $10^{\log x} = 10^{\log y}$ which implies $x = y$. Thus ϕ is injective. Now notice that for any $y \in \mathbf{R}$, there exists some $x \in \mathbf{R}^+$ such that $\log x = y$, namely, $x = 10^y$. Thus ϕ is surjective. Finally recall that $\log xy = \log x + \log y$. So ϕ meets the last requirement of an isomorphism, proving that $\langle \mathbf{R}^+, \times \rangle$ is isomorphic to $\langle \mathbf{R}, + \rangle$.

So what does that have to do with engineers using decibels? Well, multiplication is typically more difficult to do in your head than addition. So converting from a multiplicative scale factor to dB allows the total gain of an amplifier made up of several stages of amplifiers to be computed quickly without a calculator. It also lets the engineers consider their problems in smaller numbers which are a little easier to work with mentally. While there is still the issue of computing the logarithm, engineers typically memorize a few factors between 0 and 20 to make the process of converting back and forth a little easier.

This is not to say that this relationship is why decibels are used so widely in engineering. Often the source of that choice has to do with changes occurring linearly on a logarithmic scale, and thus being easier to conceptualize when using such a scale. Groups, however, give us insight as to why the conversion is possible and another way of looking at it. The idea that multiplication and addition are the same operations, merely with different labels, is fascinating, considering how different the operations seem to be on the surface.

Example 10. Let S be the set of the n complex solutions to the equation $z^n = 1$, where n is an integer. The binary structure $\langle S, \times \rangle$, where \times is complex multiplication is a group. To illustrate this, look at a specific example, say $n = 4$. In general, if we write the n complex solutions in polar form, then the elements in our set will be $e^0, e^{\frac{2\pi}{n}}, e^{2\frac{2\pi}{n}}, \dots, e^{(n-2)\frac{2\pi}{n}}, e^{(n-1)2\frac{2\pi}{n}}$. So for $n = 4$ this gives $e^0, e^{\frac{\pi}{2}}, e^\pi$, and $e^{\frac{3\pi}{2}}$. You can verify this set is closed by multiplying each element by each other element. Associativity of the set follows from associativity of complex multiplication. The set has an identity, which is e^0 , which is the same as 1. Each element has an inverse as you can again verify by multiplying the elements by each other. The table below will make it easier to verify the operations. This verifies that the structure is a group, and a similar approach can be used to verify that any choice of n will yield a group.

\times	e^0	$e^{\frac{\pi}{2}}$	e^π	$e^{\frac{3\pi}{2}}$
e^0	e^0	$e^{\frac{\pi}{2}}$	e^π	$e^{\frac{3\pi}{2}}$
$e^{\frac{\pi}{2}}$	$e^{\frac{\pi}{2}}$	e^π	$e^{\frac{3\pi}{2}}$	e^0
e^π	e^π	$e^{\frac{3\pi}{2}}$	e^0	$e^{\frac{\pi}{2}}$
$e^{\frac{3\pi}{2}}$	$e^{\frac{3\pi}{2}}$	e^0	$e^{\frac{\pi}{2}}$	e^π

Look at the table above and look back at the table for the group of rotations in one of the previous examples, to see if you can spot any similarities. You may notice that the group here has the same structure, with different labels, meaning the two groups are isomorphic. This is the case, and as a matter of fact, when rewriting the table for the complex numbers, the author simply used

a search and replace function on a copy of the previous table. To give a formal isomorphism between the two sets, let $\phi(r_\theta) = e^{\frac{\pi i \theta}{180}}$. It should be clear that this is both injective and surjective (try following the previous example to show this formally). We also have $\phi(r_{\theta_1} * r_{\theta_2}) = \phi(r_{\theta_1})\phi(r_{\theta_2})$ since function composition in the first set corresponds to multiplication in the second set, which in polar form is the same as adding the arguments and multiplying the magnitudes (which are always 1 for these sets).

The solutions of the equation $z^n = 1$ can be thought of as the complex numbers lying on the unit circle. The isomorphism between these solutions and the group of rotations above shows that multiplication between these numbers can be used to represent rotations. This fact can actually be used to derive formulas for rotation of vectors around the origin.

6 Conclusion

While this note has only touched on some of the basic definitions involved, hopefully it has provided some idea of the power of group theory, and prompted the reader to learn more. There is much more to learn beyond the definitions given above, and applications to areas such as number theory, error correcting codes, encryption, etc. The materials in the bibliography are a good place to start learning more. There is also plenty of information available online on groups and related subjects. Try searching for "modern algebra", "abstract algebra", "group theory", "algebraic field theory", and "algebraic field theory" to find a lot of relevant material.

References

- [1] John B. Fraleigh *Abstract Algebra* 1998: Addison-Wesley, Reading, MA.
- [2] J. F. Humphreys and M. Y. Prest *Numbers, Groups, and Codes* 2004: Cambridge University Press, Cambridge.
- [3] Allan Clark *Elements of Abstract Algebra* 1971: Dover Publications Inc, NY.