Basic Group Theory

Mathew Calkins
mathewpcalkins@gmail.com

October 11, 2018

Abstract

Notes on basic group theory. The original audience was a collection of physics and math majors, most of whom had just finished their freshman or sophomores years of undergraduate study at the University of Maryland. This material was originally presented as part of an intensive course meant to introduce undergraduates to supersymmetry. All errors are my own.

1 Group Theory

1.1 Definitions, basic results, and a first glance at isomorphism

In keeping with some standard practice in textbooks on abstract algebra, we begin by diving into definitions.

Definition of a group A group $(G, *)$ is a set G together with a binary operation $* : G \times G \to G$ which satisfies the following properties:

1. The operation $*$ is associative. That is, for all group elements $x, y, z \in G$,
$$x * (y * z) = (x * y) * z.$$

2. There exists a group element $e \in G$, called the "identity element," with the property that

$$e * x = x * e = x$$

for every group element $x \in G$.

3. For every group element $x \in G$, there exists another group element $y \in G$ (not necessarily distinct from x) such that

$$x * y = e.$$

In that case we call y the "inverse" of x and will frequently write $y = x^{-1}$.

Definition of an abelian group A group $(G, *)$ is called "commutative" or "abelian" if the binary operation $*$ is commutative. That is, if

$$x * y = y * x$$

for all group elements $x, y \in G$.

What follow are some basic properties of groups. As per the focus of this course they are given without proof, but short proofs exist and may be included in an appendix to this section.

The group identity is unique Let $(G, *)$ be a group and suppose that two elements e_1 and e_2 both satisfy the definition of the group identity. That is,

$$e_1 * x = x * e_1 = x \text{ and } e_2 * x = x * e_2 = x$$

for all group elements $x \in G$. Then it must be that e_1 and e_2 are really the same element:

$$e_1 = e_2.$$

Inverses work from both the left and the right Suppose that x is a group element with inverse x^{-1}. That is, $x * x^{-1} = e$. Then $x^{-1} * x = e$ as well.

Proof that inverses work from both the left and the right Assume that the premise

$$x * x^{-1} = e$$

holds. Now multiply both sides of the equality by x^{-1} from the left:

$$x^{-1} * x * x^{-1} = x^{-1}.$$

Since x^{-1} is itself an element of G, it must have an inverse, which we write as $\left(x^{-1}\right)^{-1}$. For the next step, we multiply both sides of the last equality by $\left(x^{-1}\right)^{-1}$ from the right:

$$x^{-1} * x * x^{-1} * \left(x^{-1}\right)^{-1} = x^{-1} * \left(x^{-1}\right)^{-1}.$$

By definition, we know that

$$x^{-1} * \left(x^{-1}\right)^{-1} = e.$$

So this reduces to

$$x^{-1} * x = e.$$

QED

The inverse of the inverse of x is x itself Let x is an element of the group $(G, *)$. Then x has an inverse $y = x^{-1} \in G$. Likewise, y has an inverse $y^{-1} = \left(x^{-1}\right)^{-1} \in G$. That inverse is simply x.

$$\left(x^{-1}\right)^{-1} = x.$$

Some examples of groups

1. Let $G = \mathbb{Z}$ (the integers) and let $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be integer addition. Then $(G, *)$ (often pronounced "the integers unders addition") forms a group. The identity element is the integer 0 and the inverse of $n \in \mathbb{Z}$ is $-n \in \mathbb{Z}$.
2. The non-zero rational numbers form a group under multiplication. The identity element is the rational number 1 and the inverse of $p/q \in \mathbb{Q}$ is $q/p \in \mathbb{Q}$.
3. The non-zero complex numbers form a group under multiplication. The identity element is the complex number 1 and the inverse of $z \in \mathbb{C}$ is $1/z \in \mathbb{C}$.
4. The set of all real invertible 2×2 matrices is a group under matrix multiplication. The identity element is the 2×2 identity matrix and the inverse of the matrix M is M^{-1}.

5. The set $\{+1, -1\}$ is a group under real multiplication. The identity element is $+1$, and both elements are their own inverses. This group is often denoted $GL(n, \mathbb{R})$.
6. The set of all complex number of unit magnitude - $\{e^{i\theta} | \theta \in \mathbb{R}\}$ - is a group under complex multiplication. The identity element is $1 \in \mathbb{C}$ and the inverse of $e^{i\theta}$ is $e^{-i\theta}$. This group is often denoted $U(1)$.

Strictly speaking, all there is to a group is a set together with a rule for pairing up elements of that set to get new elements. For many such sets, we can fully describe the structure of the group using a *group structure table*. If G is the set $\{a, b, c, \ldots\}$, we can write the group structure table of $(G, *)$ as

$*$	a	b	c	$\cdots$
a	$a * a$	$a * b$	$a * c$	$\cdots$
b	$b * a$	$b * b$	$b * c$	$\cdots$
c	$c * a$	$c * b$	$c * c$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

For example, consider the group $(G, *)$ where $*$ is complex multiplication and G is U_4, the set of "4th roots of unity":

$$\begin{aligned} U_4 &= \text{4th roots of unity} \\ &:= \{z \in \mathbb{C} | z^4 = 1\} \\ &= \{1, i, -1, -i\}. \end{aligned}$$

The group multiplication table is then

$*$	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Notice that this table is, in a sense, not unique. It could be layed out differently if we were to list the group elements in a different order. For example, the table

$*$	1	i	-i	-1
1	1	i	-i	-1
i	i	-1	-1	-i
-i	-i	1	-1	i
-1	-1	-i	i	1

describes precisely the same group. More absractly, if we denote $a := 1, b := i, c := -1, d := -i$, then we can fully represent this group in a table without any reference to complex numbers or multiplication or roots of anything:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Above it was noted that these tables could only be constructed for certain sets G. In particular, they can be constructed when G has finitely many elements, or at least the number of elements is only countably infinite so that they can be assembled into a discrete list of the form $(a, b, c, \ldots)$.

Definition of two isomorphic groups Let $(G, *)$ and $\left(\tilde{G}, \tilde{*}\right)$ be two groups. These groups are said to be "isomorphic" if we can pair of each element of G with exactly one element of $\tilde{G}$:

$$\begin{aligned}(x \in G) &\leftrightarrow \left(\tilde{x} \in \tilde{G}\right)\\ (y \in G) &\leftrightarrow \left(\tilde{y} \in \tilde{G}\right)\\ (z \in G) &\leftrightarrow \left(\tilde{z} \in \tilde{G}\right)\\ \vdots &\leftrightarrow \vdots\end{aligned}$$

in a way that is "preserved" or "respected" by the operations $*$ and $\tilde{*}$. More precisely, this pairing up must satisfy the property

$$\text{if } x \leftrightarrow \tilde{x} \text{ and } y \leftrightarrow \tilde{y}, \text{ then } (x * y) \leftrightarrow (\tilde{x} \tilde{*} \tilde{y}). \tag{1.1}$$

One interpretation of this situation is that the groups $(G, *)$ and $(\tilde{G}, \tilde{*})$ are completely equivalent. In the common parlance of abstract algebra, they have the same structure. Another interpretation - perhaps a more powerful one - is that we really only have one group and have merely found two different ways of labeling its elements.

Example Let $G = \mathbb{Z}$ be the set of integers and let $\tilde{G}$ be the set

of even integers:

$$\begin{aligned}\tilde{G} &= \{2n \mid n \in \mathbb{Z}\} \\ &= \{\ldots -4, -2, 0, 2, 4, \ldots\}\end{aligned}$$

and consider the groups $(G, +)$ and $(\tilde{G}, +)$, where in both instances $+$ denotes familiar integer addition. These groups are isomorphic under the pairing given in the following table.

G	$\tilde{G}$
$\vdots$	$\vdots$
-1	-2
0	0
1	2
2	4
$\vdots$	$\vdots$
n	2n
$\vdots$	$\vdots$

1.2 Subgroups, finite groups, and generators

Definition of a subgroup Suppose the set G and the binary operation $* : G \times G \to G$ constitute a group $(G, *)$. Furthermore, suppose that H is a subset of G. If the pair $(H, *)$ also forms a group (i.e., if H is a group under the operation $*$), $(H, *)$ is a subgroup of $(G, *)$.

Protip: If you want to verify that $(H, *)$ is a subgroup, there is no need to go through all of the groups axioms. Just check the $(H, *)$ contains the identify e

We often refer to a group $(G, *)$ by writing G when context makes clear what binary operation is being used (or else when the particular operation is unimportant). For example, we might rewrite the last sentence of the above definition as

> If H is also a group under $*$, then we call H a subgroup of G.

See the next definition for more of this looser vocabulary.

Definition of a finite group If a group G has only finitely many elements, we call it a finite group.

Before we discuss generators, we need further useful vocabulary. If $x \in G$ is a group element of $(G, *)$ and id. is the identity in G, then we define the notation x^n (for positive integers $n \in \mathbb{Z}$) by first defining

$$\begin{aligned} x^1 &:= x, \\ x^2 &:= x * x. \end{aligned}$$

Continuing naturally in this way, we write

$$\begin{aligned} x^3 &:= x^2 * x \\ &= x * x * x \end{aligned}$$

and

$$\begin{aligned} x^4 &:= x^3 * x \\ &= x * x * x * x \end{aligned}$$

and so on. We can even make this meaningful for negative integers n:

$$\begin{aligned} x^{-1} &:= \text{ inverse of } x \text{ (as before)} \\ x^{-2} &:= x^{-1} * x^{-1} \\ x^{-3} &:= x^{-1} * x^{-1} * x^{-1} \\ &\vdots \\ x^{-n} &:= \left(x^{-1}\right)^n. \end{aligned}$$

Observe that this notation was constructed in such a way that it satisfies the familiar rule

$$x^m * x^n = x^{m+n} \text{ for all } m, n \in Z$$

no matter whether m or n are positive integers, negative integers, or 0.

Now suppose we have some finite group $(G, *)$ with $G = \{g_1, g_2, \ldots, g_N\}$ and some group element $x \in G$. If we start combining x with itself repeatedly, producing elements x, x^2, x^3 and so on, what happens? Because G is closed under the binary operation $*$, at most N unique elements can be produced before the sequence begins to repeat. If x is simply the identity e, then this repeat happens immediately. Otherwise, suppose that the sequence contains K elements before it repeats:

$$\text{Repeated operation gives } x^1 = x, x^2, x^3, \ldots, x^{K-1}, x^K, x^{K+1} = x$$

Take a look at that last relation:

$$x^{K+1} = x.$$

Operating on both sides of that equation with x^{-1} gives

$$\begin{aligned} x^{K+1} * x^{-1} &= x * x^{-1} \\ x^{(K+1)-1} &= x^{1-1} \\ x^K &= x^0 \\ \therefore x^K &= e. \end{aligned}$$

This is a very useful result. If one takes an element of a finite group and combines it repeatedly with itself to create a sequence $x, x^2, x^3, \ldots$, then that sequence eventually reaches the identity element. We are often interested in how long it takes for that to happen, and that interest motivates the follow definition.

Definition of the order of a group element Let $(G, *)$ be a group and $x \in G$ a group element. Then there exists some smallest positive integer m such that

$$x^m = \text{id}.$$

We call m the order of the element x and write $m = \mathcal{O}(x)$.

Recall the group structure table that describes the 4th roots of unity under complex multiplication:

*	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Here the identity is id = 1. Examining $i \in U_4$ we find that $i^1 = i$, $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$, so that $\mathcal{O}(i) = 4$. The same analysis shows that $\mathcal{O}(-i) = 4$, $\mathcal{O}(1) = 1$, and $\mathcal{O}(-1) = 2$.

2 Finite Groups

2.1 Modular arithmetic

When we tell time, addition takes on a peculiar property. If we start at 2 o'clock and increment by 3 hours, we reach 5 o'clock. If we

increment by another 6 hours we reach 11 o'clock. 1 more hour makes 12 o'clock. But if we add 1 hour just once more, we can back to 1 o'clock. We typically write this as

$$12 + 1 = 13 \equiv 1$$

where $\equiv$ is pronounced "is equivalent to" and is not the same as the familiar notion of equality of numbers. We might also say that we "identify" 1 with 13. Proceeding forward:

$$\begin{aligned} 14 &\equiv 2 \\ 15 &\equiv 3 \\ &\vdots \\ 24 &\equiv 12 \equiv 0 \end{aligned}$$

In general, two numbers are equivalent not just when they differ by 12. By extension their difference can be any integer multiple of 12. More formally,

$$n \equiv n + 12k \text{ for all integers } n, k \in \mathbb{Z}.$$

When we take G to be the set of all integers wherein n is not distinguished from $n + 12k$, and let $*$ be integer addition, we call the result group $(G, *) := \mathbb{Z}_{12}$. This is pronounced "the integers mod twelve." There exist exactly analogous groups $\mathbb{Z}_1, \mathbb{Z}_2, Z_3$, and so on.

To see more concretely how these groups work, study the group structure table for $\mathbb{Z}_3$:

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

The group structure table for $\mathbb{Z}_4$ should look somewhat familiar:

*	0	1	2	3
0	a	1	c	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

By denoting $a := 0, b := 1, c := 2, d := 3$, this takes the abstract form

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

This is precisely the same as the group structure table for U_4. In a sense which will be explained more deeply with time, we conclude therefore that $\mathbb{Z}_4$ and U_4 are really the same group.

Definition of a group generator Let $(G, *)$ be a group. A group element $x \in G$ is said to be a generator of G if every element of G can be written in the form x^m for some integer m. In that case, we say that x generates G.

There is another way to think about a group generator. Recall that every group $(G, *)$ must be closed under the operation $*$. When we demand that our group at least contains x and then add all of the elements necessary for closure - but none that are not - the result is the group generated by x. This prompts the following alternative definition.

Alternative definition of a group generator Let x be some object and let $*$ be a binary operation that can be used to produce new objects from x of the form x, x^2, x^3, and so on. Then the group generated by x is the smallest group $(G, *)$ such that G contains x.

This alternative definition allows for generalization to more than one generator. We could just as well take two elements x and y and build up a group by combining them in all possible ways. Three elements would work just as well, or four, or five. So we establish an even more general definition.

Definition of a generating subset Let $(G, *)$ be a group and let $x_1, \ldots, x_n \in G$ be group elements. If G can be built up purely by combining those group elements, we say that $x_1, \ldots, x_n$ generate G. Denoting that subset by $H := \{x_1, \ldots, x_n\}$, we call H a generating subset of G.

2.2 Permutation groups

The mapping p which rearranges five ordered elements as

$$(a\ b\ c\ d\ e) \mapsto (a\ c\ d\ b\ e)$$

can be written as

$$\big((1\ 2\ 3\ 4\ 5) \in \mathbb{Z}^5\big) \overset{p}{\mapsto} ((1\ 3\ 4\ 2\ 5))$$

or as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}.$$

We can describe p by showing what it does to the original ordered quintuple (1 2 3 4 5):

$$p = (1\ 3\ 4\ 2\ 5).$$

We can even represent p as a matrix M_p whose entries are 0's and 1's that acts by permuting the elements of the column vector $v = (1\ 2\ 3\ 4\ 5)^T$:

$$M_p = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Indeed, this acts the way we want:

$$M_p v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 4 \\ 2 \\ 5 \end{pmatrix}.$$

Transpositions generate S_nd

Definition of permutation parity

3 Group Homomorphisms and Group Isomorphisms

3.1 Definitions

To start off, consider the sets

$$A = (p, q, r),$$
$$B = (x, y, z)$$

and a function $f : A \to B$ defined by

$$f(p) = x,$$
$$f(q) = x,$$
$$f(r) = z.$$

Definition of a 1-1 function A function $f : A \to B$ is 1-1 if no two domain elements $p, q \in A$ are mapped to the same codomain element. That is,

$$\text{if } p, q \in A \text{ and } p \neq q, \text{ then } f(p) \neq f(q)$$

or equivalently

$$\text{If } f(p), f(q) \in B \text{ and } f(p) = f(q), \text{ then } p = q.$$

Definition of an onto function A function $f : A \to B$ is onto if every codomain element $x \in B$ is the image of some domain element $p \in A$. That is,

$$\text{for every } x \in B, \text{ then there exists some } p \in A \text{ such that } f(p) = x.$$

Definition of a bijective function

Definition of a group homomorphism Let $(G, *)$ and $(\tilde{G}, \tilde{*})$ be groups and let $f : G \to \tilde{G}$ be a mapping which respects the group structure. That is,

$$f(x)\tilde{*}f(y) = f(x * y) \text{ for all group elements } x, y \in G.$$

Then f is said to be a homomorphism from $(G, *)$ to $(\tilde{G}, \tilde{*})$.

New (but equivalent) definition of a group isomorphism Let $(G, *)$ and $(\tilde{G}, \tilde{*})$ be groups. A group isomorphism is a function $f : G \to \tilde{G}$ which is both invertible and a homomorphism.

3.2 Examples