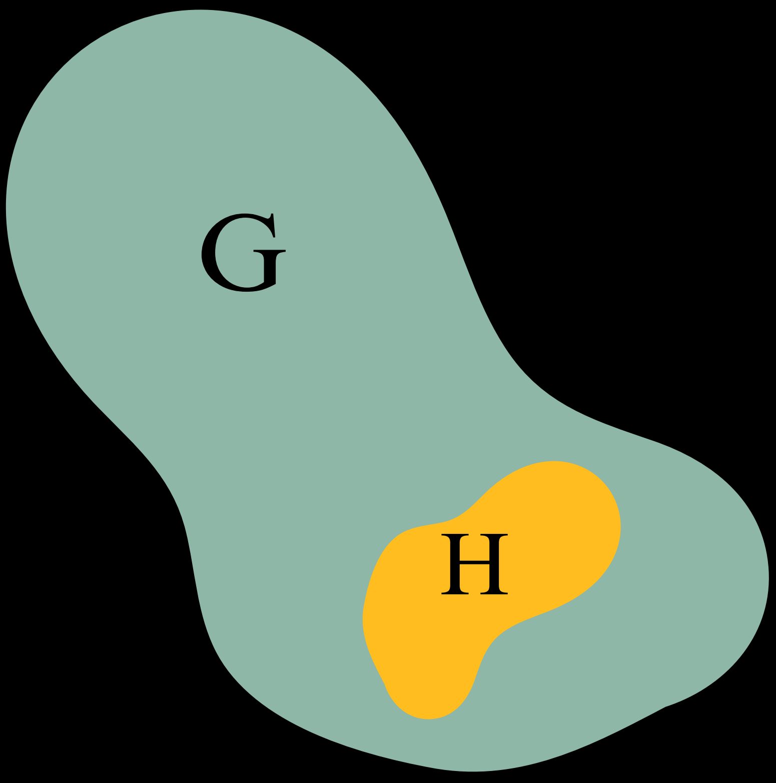
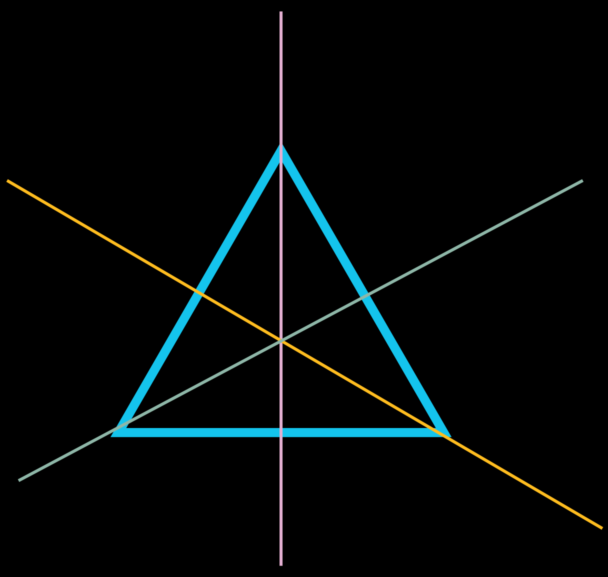
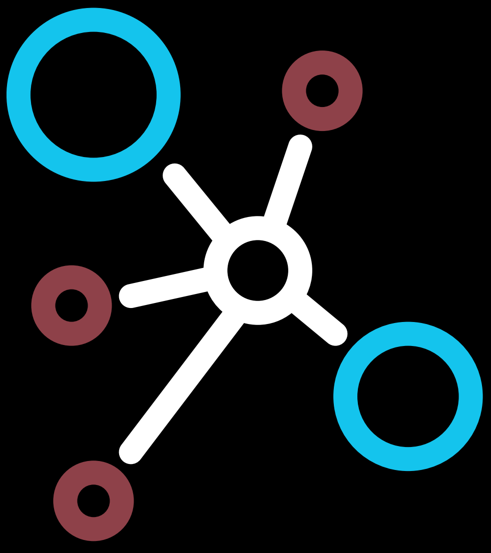
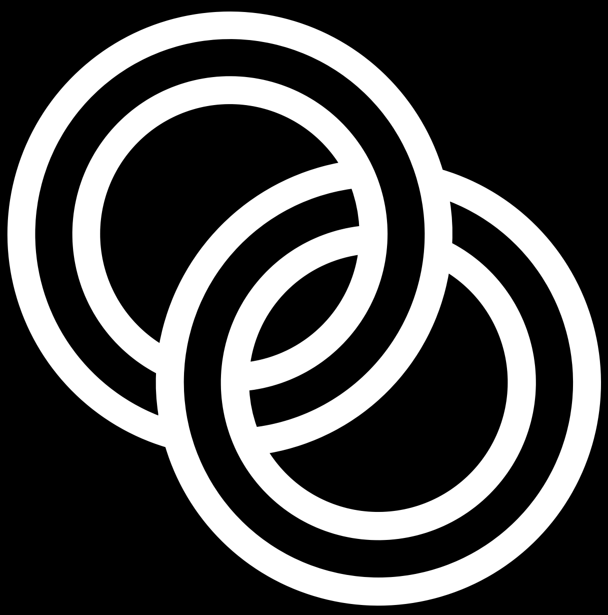
DEMYSTIFYING University Math



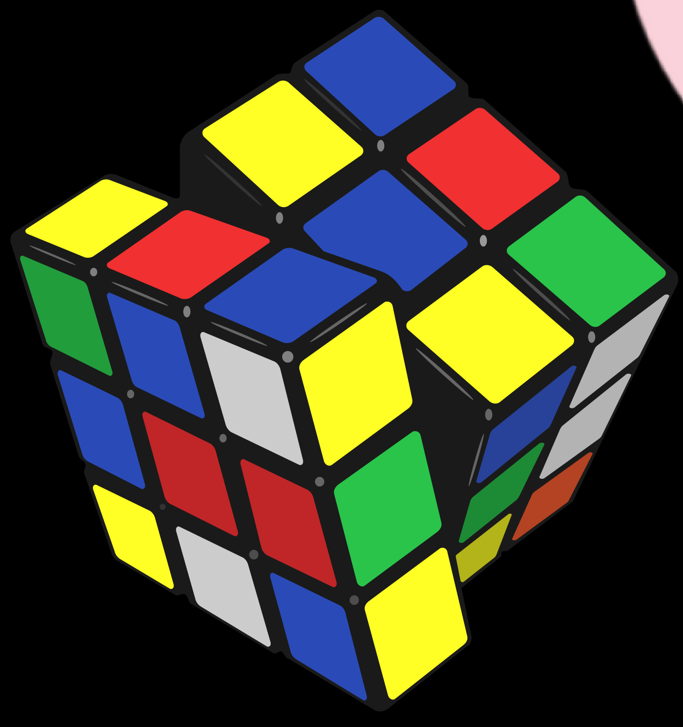




A VERY Informal Intro to GROUP THEORY



Desgined for Curious High-School and College Students!



By Y. Lakhani

A VERY

Informal Intro to

GROUP THEORY

By Y. Lakhani

Table of Contents

About this Book

MATH AFTER HIGH-SCHOOL can be a pain. As someone who has navigated through it (or at least tried to), I can tell you that it often feels like a massive leap from what you learnt in school. One of the most intriguing and fundamental ideas you will encounter in advanced math is group theory, the study of algebraic structures otherwise known as groups. This will provide you with a foundation to study abstract (or "modern") algebra, a key part of any university math education.

Why Group Theory?

Group Theory might seem intimidating at first, if not outright BORING, but it's actually a powerful and really interesting tool that helps us understand patterns, symmetries, and structures in mathematics and beyond.

Take it from someone who was never a fan of math in general, much less "group theory".

It has applications in many fields, from physics and materials science to computer science and cryptography. The elegance of group theory lies in its ability to simplify complex problems and reveal the underlying order in seemingly chaotic systems. Puzzle-solving enthusiasts and codebreakers don't study group theory for no reason!

Interested? Read on.

By Y. Lakhani

Here, you'll gain a fundamental and comprehensive understanding of what groups are and how they work. You'll study the rules (we nerds call them "axioms") that govern groups too. In addition, you'll see how to apply the knowledge you've learnt in various other fields, including solving Rubik's Cubes.

Please note that studying math at a university level is quite different from the math done at middle and high school levels. Whilst you may be used to SOLVING or CALCULATING things, in college, you will be expected to PROVE theorems and concepts rather than simply "plug-and-chug" solutions to problems.

However, we understand that not all students may be familiar with the concept of a proof. We have therefore included it in the Prerequisites section of the book. From that point onwards, proofs will be used to outline certain concepts in group theory. Feel free to skip this if you think you already know it.

Other than proofs, you should be good to go.
You may keep a pen, paper, and a positive attitude
ready by your side (no calculators necessary)
as you work through the problems in
this book. Don't be afraid to take notes
down and read the same page multiple times.
All the best!

PREREQUISITES

Sets

A review exercise for all the prerequisite topics can be found at the end of the chapter!

A set is an *ordered* list of *unique* items called "**elements**". Here are a few examples of valid sets:

Sets are denoted by a pair of **curly braces** and **comma-separated** elements.

$\{-1, 0, 5.6, 7, 4\pi\}$

Sets MUST be **ordered**.

Sets need not necessarily contain numbers only. Variables or letters can be used.

$\{x, y, r, t, u, v\}$

Symbols and shapes too!

{▲, ●, 5, t, ■}

Sets can have elements of different kinds, even if it doesn't make much sense to group them together!

The **empty set** has no elements and is denoted by ∅. Nothing interesting here!

$\{\}$

Three dots means it goes on forever.

$$\mathbf{\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots\}}$$

Sets can be infinitely big. This set is known as the set of **Natural Numbers** (i.e- positive integers or "counting numbers").

Sets can contain sets within them.

$$\mathbf{\{\{4, 5\}, 2, \{1, 2, 3, 4\}, 37\}}$$

The way the elements are arranged here doesn't matter as the set contains mixed element types.

Even though 2 and 4 appear twice, this is still a valid set as *each element* is unique.

Although the following may look like sets, they are actually invalid as certain rules are violated. Always keep an eye out for those!

$$\mathbf{\{5, 6, 4, 7, 8, 2\}}$$

This is not ordered...

...and this has duplicate elements.

$$\mathbf{\{3, 3, 4, 6, 7, 7\}}$$

Prerequisites

Sets are generally represented by a capital letter, whilst its elements are referred to using lowercase letters.

$$S = \{1, 3, 5, 6, 7, 12\}$$

$$s = 3$$

Formally, this is the notation used to show that a particular element *belongs* to a set.

$$3 \in S$$

$$4 \notin S$$

4 is not in S. This is the notation used to indicate that a particular element *does not* belong to a set.

$$7 \in \{-2, 0, 4.5, 7, 81\}$$

$$\blacktriangle \notin \{\{2, 5\}, \bullet, 10, f\}$$

$$22 \in \{0, 2, 4, 6, 8, \ldots\}$$

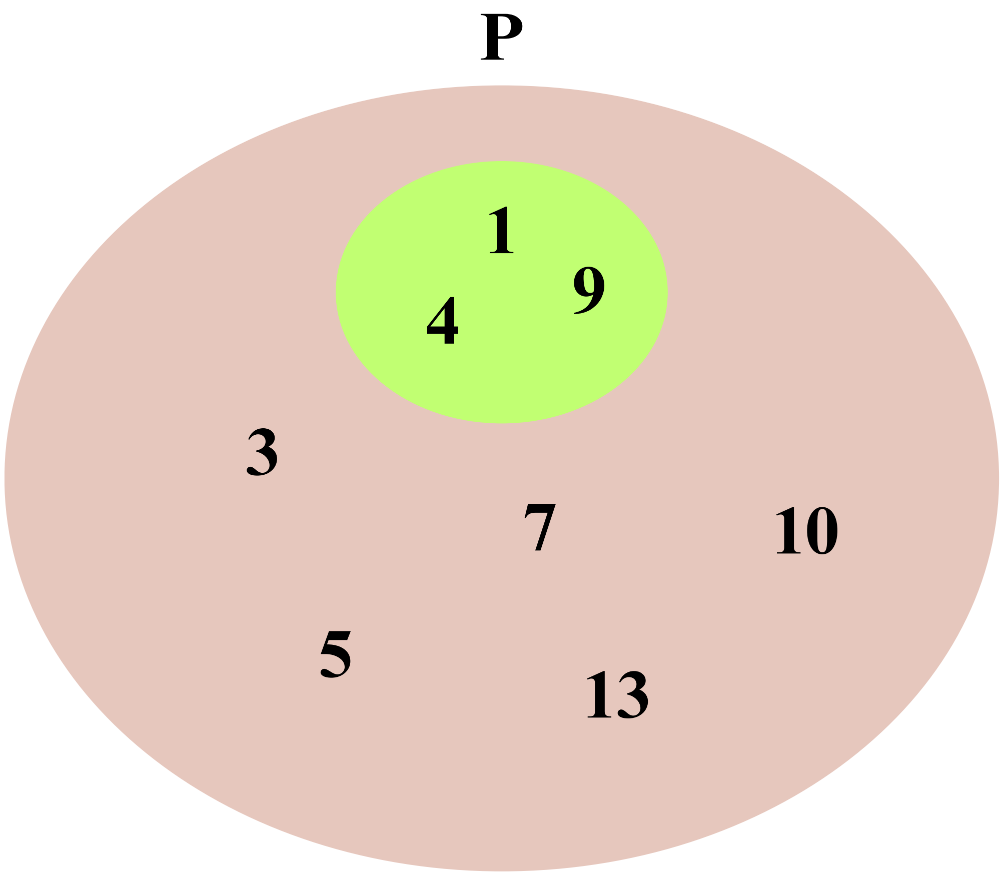
A few more examples.

You must also be aware of subset notation. Subsets of a set "S" are sets that contain the elements that must be found in S. Refer to the following example of the set P.

$$P = \{1, 3, 4, 5, 7, 9, 10, 13\}$$

$$\{1, 4, 9\} \subset P$$

"Is a subset of"



$$\varnothing \subset P$$

The empty set is a subset of all the possible sets in existence.

$$\{1, 3, 4, 5, 7, 9, 10, 13\} \subseteq P$$

All sets have themselves as a subset too, as seen above.

Let's formally define the ⊆ and ⊂ symbols.

Definition: A set A is a subset of set B (A ⊆ B) if every element of A is also an element of B. This includes the possibility that A is equal to B.

$$A = \{1, 2\}$$

$$B = \{1, 2, 3\}$$

$$C = \{1, 2, 3\}$$

$$A \subseteq B \subseteq C \text{ is True!}$$

Definition: A set A is a ***proper subset*** of set B (A ⊂ B) if every element of A is also an element of B, and A is not equal to B. This means A must be smaller than B.

$$A \subset B \text{ is True,}$$

$$\text{but } B \subset C \text{ is False!}$$

The order (also known as the "cardinality") of a set refers to the number of elements contained within a set.

$$F = \{1, 5, 14.4\}$$

$$n(F) = 3$$

Both of these are valid notations for the order of a set.

$$|F| = 3$$

$$L = \{\{1, 4\}, \{2, 5, 6\}, \{2\}, \{3, 5\}\}$$

Be careful to count the individual elements in the set! In the case of L, its order would not be 8.

$$|L| = 4$$

Prerequisites

There are certain number sets which you must be aware of when studying group theory. These include:

The set of all Natural Numbers.

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, \ldots\}$$

The set of all Integers.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

The set of all Rational Numbers.

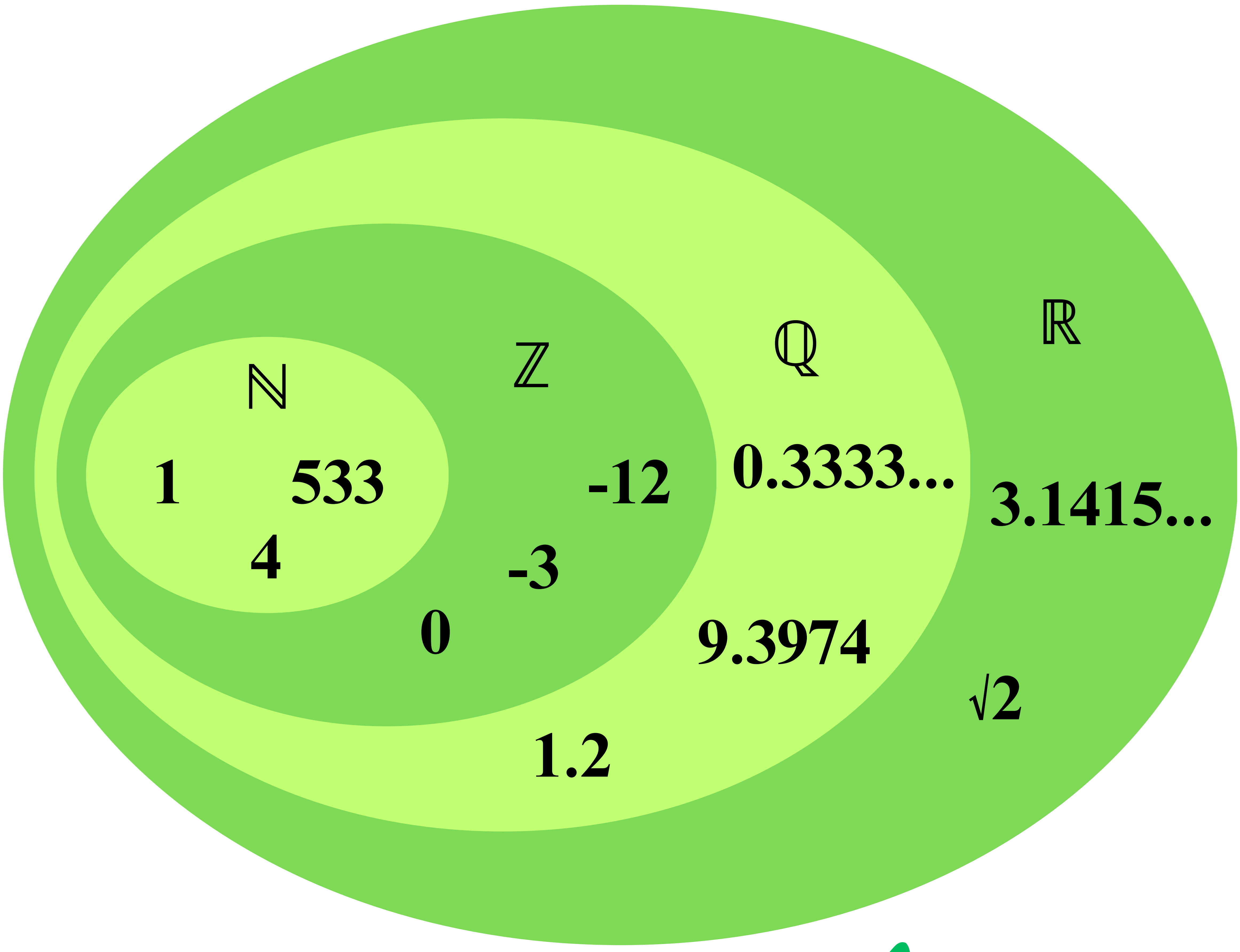
$\mathbb{Q}$ contains all numbers representable in the form p/r for some $p, r \in \mathbb{Z}$

The set of all Real Numbers.

$\mathbb{R}$ contains all possible numbers.

Please refer to the table below.

	-57	π	0	1.1	18	√-1
$\mathbb{N}$	×	×	×	×	✓	×
$\mathbb{Z}$	✓	×	✓	×	✓	×
$\mathbb{Q}$	✓	×	✓	✓	✓	×
$\mathbb{R}$	✓	✓	✓	✓	✓	×



$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

What's the cardinality of the set of natural numbers? Is it the same as that of the set of reals? The answers to those are beyond the scope needed for moving on with the prerequisites, but if you're curious, search it up!

Aaaaaand that's all for sets! Not that bad so far huh? Be sure you're well familiar with set notation before you move on to group theory. If this is your first time, review the notation discussed throughout this chapter so far- a list of symbols and their meaning is provided at the back of the book.

Binary Operations & Cayley Tables

You're likely familiar with the basic binary operations: addition, subtraction, multiplication, and division.

But what exactly is a binary operation?

A binary operation is a function with two inputs (hence the "bi", meaning two) and one output.

The key feature of a binary operation is that it can be applied to any **two elements of a set such that the result of the operation is also a member of that same set.** This is known as the **"Axiom (or rule) of Closure"**

For example, "**+ on the set** ℕ" is a binary operation.

$$4 + 7 = 11$$

4 and 7 are both members of ℕ. 11 is also a member of ℕ. Hence, "**+ on** ℕ" is a binary operation.

Consequently, the binary operation "**÷ on** ℤ" is not a valid binary operation.

$$10 \div -5 = -2$$

Although division on the integers works here, there are cases that show it is not a valid binary operation as it violates the Axiom of Closure...

$$7 \div 0 = ?$$

... as can be seen here.

$$5 \div 2 = 2.5$$

Division by zero is impossible.

$2.5 \notin \mathbb{Z}$

The same way we denote functions as f(x) by default, and "x"as a default variable, this book (and most others) use * to denote a typical binary operation. For example:

$$a * b \text{ on } \mathbb{Z} \text{ is defined as } a + b + 1$$

Watch out! * may look like multiplication, but in group theory, * represents a predefined binary operation - which could be anything! In this case, it means a + b + 1, but it could mean something completely different elsewhere. Remember to think abstractly as you study abstract algebra!

$$6 * 8 = 6 + 8 + 1 = 15$$

$$2 * 2 = 5$$

$$9 * 0 = 10$$

Some examples of this case of *.

Here are some more random examples of valid binary operations. Note that we can use any symbol to represent a binary operation.

$$a * b = a + ab - 1 \text{ (on } \mathbb{N})$$

$$7 * 4 = 34$$

Recall that raising a number to the power of 0.5 means square rooting the number!

$$a \blacktriangledown b = a^b + 1 \text{ (on } \mathbb{R})$$

$$100 \blacktriangledown 0.5 = 11$$

Is the following a valid binary operation?

$$a \boxtimes b = (a + b) \div a \text{ (on } \mathbb{R})$$

$$4 \boxtimes 8 = 3$$

Absolutely not! Keep an eye out for possible cases where the operation would fail. What would happen when a = 0, for example? Recall division by zero is impossible and yields "undefined". "Undefined" ∉ ℝ, violating closure.

Prerequisites

We say a binary operation, *, is **commutative** if it satisfies the following condition:

This means that you could reverse the order of operation, and it wouldn't matter.

$$a * b = b * a$$
$$\forall\ a, b$$

Don't be scared of the ∀! It is a commonly used symbol in higher mathematics meaning "**for all**".

For example, multiplication is commutative. (on ℝ) So is addition. However, subtraction and division aren't.

$$4 + 5 = 5 + 4 = 9$$
$$4 \times 5 = 5 \times 4 = 20$$
$$4 - 5 \neq 5 - 4$$
$$4 \div 5 \neq 5 \div 4$$

Throughout this book, × is used to denote multiplication, and * for contextual binary operations.

We say a binary operation, *, **associative** if it satisfies the following condition:

This means that when more than two numbers are passed through a binary operation, it doesn't matter how they're grouped.

$$(a * b) * c = a * (b * c)$$
$$\forall\ a, b, c$$

Addition and multiplication are associative. Subtraction and division however, are not.

$$6 + (2 + 2) = (6 + 2) + 2 = 10$$
$$6 \times (2 \times 2) = (6 \times 2) \times 2 = 24$$
$$6 - (2 - 2) = 6 \neq (6 - 2) - 2 = 2$$
$$6 \div (2 \div 2) = 6 \neq (6 \div 2) \div 2 = \tfrac{3}{2}$$

Sets sometimes have an **identity** element under a particular binary operation. For example, the identity element of $\mathbb{R}$ under addition is 0 since adding 0 to any member of $\mathbb{R}$ (any real number) will leave the number unchanged. In other words, the following condition must be satisfied.

$$a * e = e * a = a$$
$$\forall a \in S$$

e is the identity element, whilst ***a*** is a member of the set in context, and * is any binary operation. Remember that ***e*** and ***a*** are both in ***S***.

S is the set in question. This second phrase means “for all elements ***a*** in the set ***S***. We mathematicians love to be specific, even if you think it may not be necessary to state such details!

A crucial feature of the identity element of a binary operation is that it is unique (i.e. there is only one of it). We will prove this in the **Proofs** chapter!

Here are a few examples of identity elements:

$$\text{“}\times \text{ on } \mathbb{Q}\text{” has } e = 1$$
$$\text{“}\times \text{ on } \{-1, 1\}\text{” has } e = 1$$
$$\text{“}+ \text{ on } \{-2, 0, 5, 9\} \text{ has } e = 0$$

Trick example! The third example here is NOT a valid binary operation as 5 + 9 = 14, and 14 is not a member of the set.

Prerequisites

Elements in a set sometimes have **inverses** in the set. Let's have a look at **× on** ℝ as an example:

4, a real number, multiplied by its inverse

$$4 \times \frac{1}{4} = 1$$

Notice how 1 is the identity element of **× on** ℝ.

In general, the inverse of an element under an operation * must satisfy the following condition:

Commutativity is a MUST!

$$a \times a^{-1} = a^{-1} \times a = e$$

An element, a, is **self-inverse** if the following is true:

$$a = a^{-1}$$

The inverse of ***a*** is the same as ***a*** itself.

Here are some examples of inverses for a few binary operations:

"+ on ℤ**"**

$$t = 35, t^{-1} = -35$$

$$35 + (-35) = 0$$

The identity element for "+ on ℤ"!

"× on ℚ**"**

$$a = 1, a^{-1} = \frac{1}{1} = 1$$

The identity element is always a self-inverse element for all binary operations.

For any *finite set*, a table showing the result of certain types of binary operation on all possible element pairings can be drawn. This is called a **Cayley table.**

Let's look at an example. Consider the basic case of the binary operation * on the set {a, b, c}.

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

Observe how the convention is to take the first elements from the left side and the second from the top.

Below is the Cayley table for the binary operation of multiplication on the set {-1, 1}.

Here, you can see that the identity element (*e*) is 1. This is because all the elements corresponding to the element 1, are unchanged. Notice how it runs down the diagonal.

×	1	-1
1	1	-1
-1	-1	1

That's not all! Observe how both 1 and -1 are self-inverses since -1×-1 and 1×1 give the identity element 1.

Here’s another example. Try and find the identity element and which elements are self-inverse.

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

The identity element here is ***d***, because any element operated with ***d*** yields the element itself. ***b*** and ***d*** are self-inverse elements as **b * b = d * d = d**.

Another detail to be aware of is that each row and column has exactly one **instance** of each element - no duplicates, and none missed. Kinda like Sudoku.

Always keep an eye out for any interesting **patterns** in abstract algebra! Uniquely coloring in each instance of an element, do you now see any underlying patterns? Notice the how the Cayley table is **symmetric** about the diagonal. The significance of this will be explained later in the book.

That’s a wrap for binary operations and Cayley tables! If you want some more practice, refer to the end of the Prerequisites Chapter for the review questions or search the web for some question banks. Ensure you have at least a decent grasp of these concepts before you continue working through this book.

Modular Arithmetic

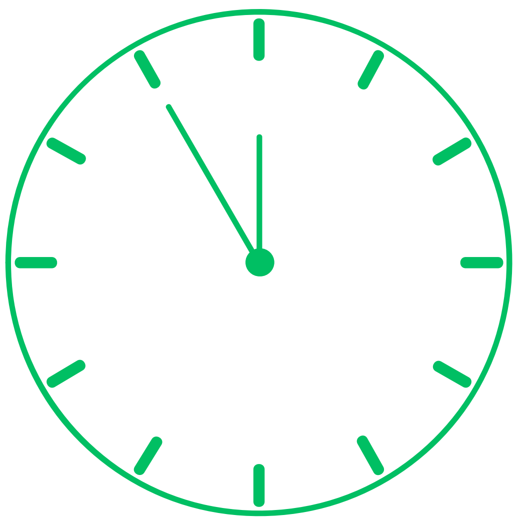
Modular arithmetic is a special kind of arithmetic, but instead of dealing with infinite values, you are constrained to a certain set of numbers, defined by a **modulo**.

One of the most famous examples of modular arithmetic is the clock. You can use modulo 12 addition to determine what time it will be after a certain number of hours. For example, five hours after 11:00 is 4:00, not 16:00, as 16:00 doesn't exist on a typical circular clock.

Likewise, four hours before 1:00 is not "-3:00" (that's ridiculous), but is actually 9:00.

Mathematically, we write it as the following:

$$\mathbf{11 + 5 = 4 \ (mod\ 12)}$$
$$\mathbf{1 - 4 = 9 \ (mod\ 12)}$$



Essentially, every time we reach 12, we reset from 0. It is said that 12 is **congruent** to 0 in mod 12.

Any modulo can be used for modular arithmetic. For example, using modulo 7, whenever you reach a multiple of 7 you start again from 0.

Therefore, 7 is congruent to 0, 8 to 1, and so on.

For example, 4 + 5 = 2 (mod 7) and 5 × 5 = 4 (mod 7).

Alternatively, one can say that ***h (mod n)*** is the remainder when ***h*** is divided by ***n***.

Keep in mind that modular arithmetic can be used to add, subtract, multiply, and divide.

$$\mathbf{99 \div 11 \ (mod\ 7) = 9 \ (mod\ 7) = 2}$$

$$\mathbf{74 + 19 \ (mod\ 5) = 93 \ (mod\ 5) = 3}$$

As seen in these two examples, compute the binary operation first and then find the appropriate congruent value.

The following notation will be used in the book to represent addition modulo n and multiplication modulo n respectively.

$$+_n \ \textbf{and} \ \times_n$$

Cayley tables are often used to represent binary operations involving modular arithmetic. On *finite sets only* of course, otherwise there wouldn't be enough paper!

For example, let the binary operation * on ℕ = $+_5$ on ℕ

We can use the fact that **a * e = e * a = a** for the identity element ***e*** as we fill out the table starting from the diagonal. In this case, the identity element is **0**.

Notice the symmetry down the diagonal?

*	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The inverse of 4 is 1 and vice versa. The inverse of 2 is 3 and vice versa. 0 and 5, on the other hand, are self-inverse.

4 * 1 = 1 * 4 = 0 (the identity element)
2 * 3 = 3 * 2 = 0
5 * 5 = 0 * 0 = 0

It looks like you've covered modular arithmetic well! Once again, don't forget to soak in everything you've just learnt. You can do this by taking a break, reviewing the practice problems in the review exercise, or both! What's important is that you have a strong foundation of the prerequisite topics before you build up any further.

By the way, modular arithmetic has many applications in the real world, some of which are covered in the **Applications of Group Theory** chapter! Have a look if interested.

Basic Logic & Proof Techniques

In mathematics, **proofs** are crucial for demonstrating that statements are true through **logical reasoning** (a series of coherent steps). There are many ways to carry out a proof, and some methods may be more effective and efficient than others for particular situations.

In this book, we cover 4 important proof techniques:

- **Proof by Deduction** (called "**Direct Proof**" by some)
- **Proof by Exhaustion**
- **Proof by Contradiction**
- **Disproof by Counterexample**

Proof by Deduction is the most basic type of proof, and involves applying a series of steps in order to prove that your statement is true. Here's a simple example:

Claim: The sum of any two odd integers is even.

Proof:

- **Assume m and n are two odd integers.**
- **By definition of the odd integers, let $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b.**
- **This follows that**

$$\begin{aligned} m + n &= 2a + 2b + 2 \\ &= 2(a + b + 1) \\ &= 2k, \text{ where } k = a + b + 1 \text{ is some integer.} \end{aligned}$$

- **Since $2k$ is the definition of an even integer, we can say that $m + n$ is even as $2k = m + n$**
- **$\therefore$ the sum of any two odd integers is, indeed, even.**
- **QED**

□

Make the statment to be proved clear.

Deductive steps, presented one after the other

The $\therefore$ symbol means "therefore"

"**QED**" is latin for "quod erat demonstrandum", meaning "end of demonstration" (or proof).

Here’s another basic example:

Claim: The sum of any three consecutive integers is a multiple of three.

Proof:

- **Let n, n + 1, and n + 2 be three consecutive integers.**
- **Hence, their sum is $n + n + n + 1 + 2$**
  $= 3n + 3$
- **This can be written as $3(n + 1)$**
  $= 3k$, where $k = n + 1 \in \mathbb{Z}$
- **3k is clearly divisible by 3 ⇒ we can say that the sum of the three consecutive integers is a multiple of 3.**
- **∴ the statement has been proven true ∀ integers.**
- **QED**

□

Get used to the symbols!

The arrow means “implies” .

Notice the box at the end of the proof? Like “QED”, it is used to denote the end of a proof. This book uses both “QED” and a box.

Let’s apply the knowledge we learnt from the Binary Operations chapter in this example:

Proofs will be used extensively to verify concepts in Abstract Algebra.

The ∃ symbol means “**there exists**”. It is formally known as an “**existential qualifier**”.

Claim: The identity element for a binary operation is always unique.

Proof:

- **Assume that the binary operation * has two identity elements: e and f in the set S**
- **It follows that, since f is an identity element, $e * f = e$**
- **Likewise, since e is an identity element, $e * f = f$**
- **⇒ $e = f$**
- **∴ ∃ some identity element e and e is always unique**
- **QED**

□

We are essentially proving that the two “different” identity elements are actually the same, hence showing that there is only one identity element.

Proof by Exhaustion is another extensively used proof technique and is very straightforward. It involves verifying your statement for every relevant value (brute force) until your statement is proven true for **every possible case**.

Proof by Exhaustion can get tedious. However, you will see situations where proof by exhaustion would work very well, such as the following:

Claim: For all single digit prime numbers, p, the expression $p^3 + p$ is a multiple of 10.

Proof:

- **List out all single digit primes: 2, 3, 5, 7**
- **Test the claim for each case:**
  For p = 2: $2^3 + 2 = 10 = 10(1)$
  For p = 3: $3^3 + 3 = 30 = 10(3)$
  For p = 5: $5^3 + 5 = 130 = 10(13)$
  For p = 7: $7^3 + 7 = 340 = 10(34)$
- **∴ the claim is true ∀ single-digit primes.**
- **QED**

□

Very simple example here, but it conveys the fundamental idea of proof by exhaustion: try it for EVERYTHING.

Claim: All square numbers are either a multiple of 4 or one more than a multiple of 4.

Proof:

- **Let's verify the claim for two cases: when n is odd, and when n is even**
- **When n is odd:**

$$n = 2k + 1, \quad \text{for some } k \in \mathbb{Z} \quad \text{(by the definition of an odd number)}$$
$$n = (2k + 1)^2 = 4k^2 + 4k + 1$$
$$= 4(k^2 + k) + 1$$

- **Since $k^2 + k \in \mathbb{Z}$, it is clearly visible that n is one more than a multiple of 4 for odd n.**
- **When n is even:**

$$n = 2k, \quad \text{for some } k \in \mathbb{Z} \quad \text{(by the definition of an even number)}$$
$$n = (2k)^2 = 4k^2 = 4(k^2)$$

- **Since $k \in \mathbb{Z}$, it is clearly visible that n is a multiple of 4 for even n**
- **The claim has been verified for both odd and even integers, hence it is true $\forall n \in \mathbb{Z}$**
- **QED**

□

This is also proof by exhaustion, albeit more elegant, as it shows that the claim is true for all possible integers.

"for all integers"...

Proof by Contradiction is essentially a sneaky "swicheroo". You first assume the opposite of what you want to prove is true, and then go through a series of steps, which should lead to a fault in your proof - i.e. the contradiction! This therefore confirms your original statement.

A very famous example would be the proof that the square root of two is irrational (can't be written as a fraction):

Claim: The square root of 2 is irrational.

Proof:

- **Assume that the square root of two is rational.**
- **It follows that $\sqrt{2} = {}^{m}/_{n}$, where m, n $\in \mathbb{Z}$ and the <u>fraction is in its simplest form</u>.**

- **Let's manipulate our equation a little bit:**

$$\sqrt{2} = {}^{m}/_{n}$$
$$2 = {}^{m^2}/_{n^2}$$
$$2n^2 = m^2$$

m^2 is a multiple of 2 $\Rightarrow$ m is a multiple of 2

- **m is a multiple of 2 $\therefore$ $m = 2p \Rightarrow m^2 = 4p^2$**
- **Substituting this back into our older equation, we get:**

$$2n^2 = 4p^2$$
$$n^2 = 2p^2$$

n^2 is a multiple of 2 $\Rightarrow$ n is a multiple of 2

- **$\therefore$ Both m and n have a common factor of 2**
- **This contradicts the fact that ${}^{m}/_{n}$ can no longer be simplified**
- **This contradiction arises from the fact that we incorrectly assumed $\sqrt{2}$ to be rational.**
- **$\therefore$ $\sqrt{2}$ is irrational.**
- **QED**

□

As you can see, a fault has arisen in
the proof, implying that one of our
early assumptions was incorrect.

Prerequisites

Disproof by counterexample is quite simple, and is used to prove that a certain statement is false. It involves finding a case where the statement does not hold. Here's an example:

Claim: The product of two primes is always odd

Proof:

- **Testing the claim for valid prime values such as $3 \times 7 = 21$ and $11 \times 17 = 187$ don't disprove the claim.**
- **Use 2 and 3. $2 \times 3 = 6$, which is clearly not odd.**
- **A counterexample of 2 and 3 shows a fault in the claim.**
- **$\therefore$ the claim is False.**
- **QED**

□

All you need to do is find one fault in the claim and you're set!

We found counterexamples just like this in previous chapters, but now we're proving things more "formally".

Claim: "Subtraction on $\mathbb{N}$" is a valid binary operation.

Proof:

- **Let $a = 4$ and $b = 5$ as $\{4, 5\} \subset \mathbb{N}$**
- **$a - b = 4 - 5 = -1 \notin \mathbb{N}$**
- **This violates the Axiom of Closure as -1 is not natural**
- **$\therefore$ the claim is False.**
- **QED**

□

Claim: The binary operation "Subtraction on $\mathbb{Z}$" is commutative.

Proof:

- **Let $a = 6$ and $b = 8$ as $\{6, 8\} \subset \mathbb{Z}$**
- **$a - b = 6 - 8 = -2$**
- **$b - a = 8 - 6 = 2$**
- **$2 \neq -2$**
- **This violates the rule of commutativity $(a * b = b * a)\ \forall\ a, b \in \mathbb{R}$**
- **$\therefore$ the claim is False.**
- **QED**

□

Don't forget the meaning of important properties such as "commutativity" and "associativity"!

$\mathbb{Z} \subset \mathbb{R}$

You've reached the end of the prerequisites section! I know I repeat this a lot, but you need to GRASP the stuff you've learnt so far. Finish the exercise on the next page, and brace yourself for an informal yet tough intro to Group Theory!

Review Test

The answers can be found in the back!

1

Complete the table below

	6.7	$4/5$	$\sqrt{-7}$	-20	1	0
$\mathbb{N}$						
$\mathbb{Z}$			×			
$\mathbb{Q}$					✓	
$\mathbb{R}$		✓				

2

Which of these are binary operations on the set $\mathbb{Q}$? Explain your answers.

$s \spadesuit p = s^p$ $a \curlywedge v = a/v$

3

Which of these are binary operations on the set $\mathbb{Z}$? Explain your answers.

$a * b = a - b + 1$ $a \curlywedge v = a/v - 1$

$f \lozenge j = f - fj + 9$ $r ⊠ h = r/h + rh^2$

4 **Explain whether or not each of these binary operations are associative and commutative. Identify the identity element for each binary operation.**

$a * b = a - b$ on the set $\mathbb{Q}$

$a * b = a^2 + b$ on the set $\mathbb{R}$

$a * b = a + b$ on the set $\mathbb{Z}$

5 **For each of the following, write down the identity element and explain which of the elements have inverses.**

$a * b = a \times b$ on the set $\{-1, 0, 1\}$

$a * b = a \times b$ on the set of all odd numbers

$a * b = a + b$ on the set of all even numbers

6 **For the following Cayley Tables, find the identity element and the inverse of each of the elements.**

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

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

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

6 **Simplify each number to the form “a (mod n)”, where $0 < a < n$ using the modulo given.**

7 (mod 3)

27 (mod 9)

25 (mod 6)

-5 (mod 8)

46 (mod 13)

134 (mod 12)

7 **Using modular arithmetic, compute the following and write each answer in the form “a (mod n)”, where n is the modulo given.**

22 + 18 (mod 3)

4 + 25 (mod 2)

5 × 13 (mod 6)

29 - 7 (mod 8)

34 × -12 (mod 5)

29 × 4 (mod 6)

8 **Draw the Cayley table for the set of integers modulo 2 under *, where a * b = a - b (mod 2). State the identity element and explain which elements have an inverse.**

9 **Draw the Cayley table for the following binary operations and state the identity element for each.**

$+_3$ on the set {0, 1, 2}

$\times_7$ on the set {1, 2, 3, 4, 5, 6}

$+_4$ on the set {0, 1, 2, 3}

$\times_5$ on the set {1, 2, 3, 4}

10 **Complete the Cayley table for the set {0, 2, 4, 6, 8} under $+_{10}$. State the identity element and the inverse of each of the elements**

*	0	2	4	6	8
0		2			
2				8	
4					
6			0		
8					

11 **Prove the following:**

“The square of any even integer is a multiple of 4” by deduction.

“The sum of any two consecutive squares between 100 and 200 will always be odd” by exhaustion.

“$p = n + 2$ is not a multiple of 4, where $n \in \mathbb{Z}$ and $2 \leq n \leq 7$”, by exhaustion .

12 **Find a counterexample to the following statements:**

“If m is an integer and m^2 is divisible by 4, then m is divisible by 4"

“$a^2 + b^2 \neq c^2 \ \forall \ a, b, c \in \mathbb{N}$”

“The sum of two irrational numbers is always irrational.”

INTRO TO THE GROUP THEORY

What is Group Theory?

Group theory is a branch of mathematics that studies the concept of **symmetry and structure**. Imagine you have a collection of objects, such as numbers or shapes (a **set**), and a way to combine them, such as rotating shapes or adding numbers (a **binary operation**).

Group theory looks at how these objects can be combined and what rules they follow. These rules are formally known as **axioms**, and will be referred to as so from now on.

Knowledge on how what **groups** are and how they work is essential to further study in **abstract algebra**, where you will learn about similar **abstract structures** such as **rings, fields, and modules.**

For simplicity sake, this book covers groups, their types, and their real-life applications only.

Groups & The Four Axioms

Here's some good news! Remember the concepts of closure, associativity, and others? If you've been paying good attention to those, you've already finished a solid portion of the fundamental thinking required to understand group theory. Let's cut to the chase:

A group is a collection of mathematical objects (a set) that can be combined subject in some way to the set of axioms.

The set can be any valid ordered list of unique objects, like the set of natural numbers, or the set of all possible rotations a square can do. However, all elements must be able to "combine" (via a particular binary operation) such that the following axioms are satisfied:

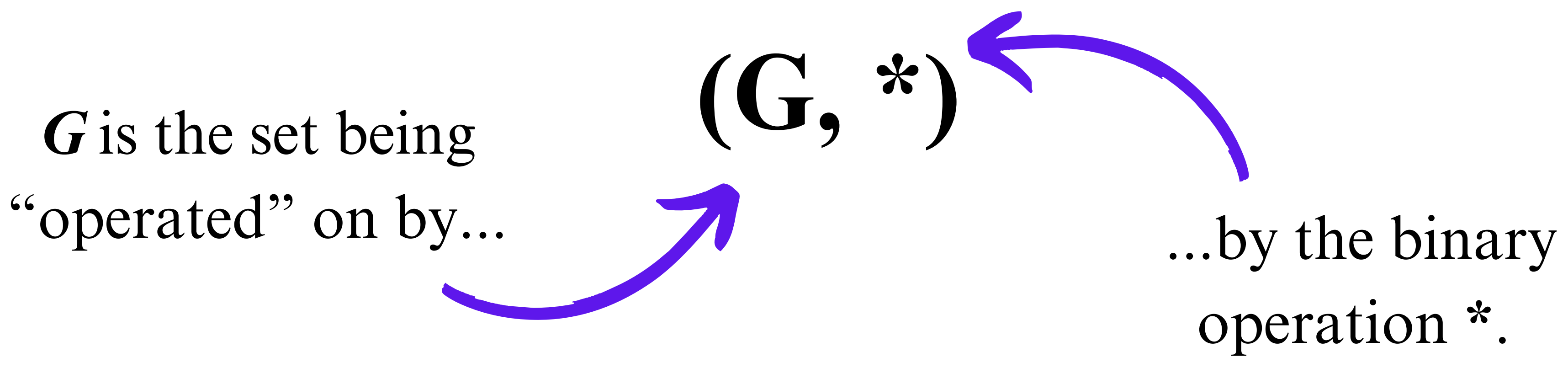
- **The Axiom of Closure**
- **The Axiom of Associativity**
- **The Axiom of Identity**
- **The Axiom of Invertibility**

Important vocab!

Once each of these axioms are satisfied, we say that the set "**forms a group**" under that binary operation. Of course, we don't expect you to instantly understand what each of them means instantly, but we encourage that you try to take a guess for now. We'll start explaining and proving these axioms on the next page.

Group Theory Basics

This is the formal notation of a group :



(G, *)

G is the set being "operated" on by...

...by the binary operation *.

Overall, this group is referred to as " *** on *G*** " (***G* forms a group under** *) or even just ***G*** as a shorthand, even though ***G*** is actually the set alone. In this book, we make clear whether we're referring to the group itself or the set which forms the group.

The first axiom that any valid group must satisfy is the Axiom of Closure. As discussed in the prerequisites section, this axiom states that two elements in the relevant set must combine to yield an element that is also in that set.

Although we will provide proofs for each of the other axioms, there isn't really any need for a proof here. Why? Well, when we discussed binary operations, we established that a valid binary operation must satisfy closure. Therefore, when we declare a group with a valid binary operation *, it **isn't necessary to explicitly restate that the group satisfies closure**, as it is implied that * will follow that axiom itself.

As a result, you'll also often see some textbooks or websites omitting the closure axiom, as they consider it **trivial**. They then say there are only 3 axioms that a group must adhere to, and they obviously aren't wrong. This textbook, however, addresses all four group axioms.

The word "trivial" means insignificant. This word is often used in mathematics to describe self-evident facts that don't always need explicit stating. For example, the **trivial subsets** of any set ***S*** is **Ø** and the set ***S*** itself. This applies to all sets, making them obvious choices.

In order to stay in the Groups-Only Kool Klub, groups must satisfy the second axiom: The Axiom of Associativity. This is outlined in the following:

$$* \text{ on } G \text{ is associative if, } \forall\ a, b, c \in G,$$
$$a * (b * c) = (a * b) * c$$

Ensures the way we group elements doesn't matter

For example, the group formed by the set of integers under additions is associative:

$$5 + (-2 + 4) = 7$$
$$(5 - 2) + 4 = 7$$

Along with associativity, there has to exist a single identity element - known as The Axiom of Identity. This identity element is essentially neutral and does nothing when operated on an element

$$a * e = e * a = a$$
$$e, a \in G$$

As an example, consider the set of positive real numbers under multiplication. Here the identity element is 1 as multiplying any positive real by 1 equals that number itself.

$$4 \times 1 = 1 \times 4 = 4$$
$$324.567 \times 1 = 324.567$$

Remember that 0 is not a part of this group, otherwise it wouldn't be considered one as 0 has no multiplicative inverse; dividing by zero invalid, remember?

Group Theory Basics

This is the proof showing that there is exactly one identity element (no more, no less) for every valid group:

Claim: The identity element for a group is always unique.

Proof:

- **Let (G, *) be a group formed by a set G under ***
- **Assume that * has two identity elements: $e, f \in G$**
- **It follows that, since f is an identity element, $e * f = e$**
- **Likewise, since e is an identity element, $e * f = f$**
- **$\Rightarrow e = f$**
- **$\therefore \ \exists$ an identity element e and e is <u>always unique</u>**
- **QED**

□

A similar proof was done earlier in the book!

Then there's The Axiom of Invertibility, meaning that every element of a group must have an **inverse** in that group such that:

$$a^{-1} * a = e$$
$$\forall a, a^{-1} \in G$$

That's the identity element of the group!

Here's the proof showing that there is exactly one inverse per element (no more, no less) in any valid group:

Claim: For each $a \in G$, a^{-1} is uniquely determined

Proof:

- **Let (G, *) be a group formed by a set G under ***
- **Assume that b and c are two distinct inverses of *a,* and that the identity element is *e***
- ***By* axiom $a * b = e$ and $c * a = e$,**

$$\begin{aligned} c &= c * e && \text{(by identity axiom)} \\ &= c * (a * b) && \text{(by inverse axiom)} \\ &= (c * a) * b && \text{(by associativity axiom)} \\ &= e * b && \text{(by inverse axiom)} \\ &= b && \text{(by identity axiom)} \end{aligned}$$

- **Hence $c = b$, which is a contradiction to our initial statement saying that they are distinct!**
- **$\therefore \ \exists$ an inverse for each $a \in G$ and it is <u>uniquely detemined.</u>**
- **QED**

□

"Distinct" means different

Here's a rather easy proof showing another property of the inverse element:

Trivial, I know, but you can never be sure about something unless you prove it!

Claim: $(a^{-1})^{-1} = a$

Proof:

- **To prove this is exactly the same problem as to showing a^{-1} is the inverse of a. Reading the definition of an inverse, and switching the roles, we can see that a is indeed the inverse of a^{-1}, hence proving our claim.**
- **QED**

□

This property and its proof is quite important. I've seen it pop up in linear algebra a couple times (you'll get it once you learn about matrices):

Claim: $(a * b)^{-1} = b^{-1} * a^{-1} \ \forall \ a, b \in G$

Proof:

- **Let $c = (a * b)^{-1}$, so by definition of c, $(a * b) * c = e$**
- **Multiply both sides by a^{-1}**

$$
\begin{array}{rl}
a^{-1} * (a * b) * c = a^{-1} * e & \\
(a^{-1} * a) * b * c = a^{-1} * e & \text{(associative)} \\
e * b * c = a^{-1} * e & \text{(inverse)} \\
b * c = a^{-1} & \text{(identity)}
\end{array}
$$

- **Multiply both sides by b^{-1}**

$$
\begin{array}{rl}
b^{-1} * (b * c) = b^{-1} * a^{-1} & \\
(b^{-1} * b) * c = b^{-1} * a^{-1} & \text{(associative)} \\
e * c = b^{-1} * a^{-1} & \text{(inverse)} \\
c = b^{-1} * a^{-1} & \text{(identity)} \\
(a * b)^{-1} = b^{-1} * a^{-1} & \text{(definition of } c\text{)}
\end{array}
$$

- **$\therefore$ the claim is true $\forall$ a, b $\in$ G**
- **QED**

□

Notice how the order switched! Never take commutativity for granted!

To conclude, this is a complete, compact definition of a group:

- **Non-empty set of elements**
- **Operation: ***
- **Closed under ***
- **Inverses**
- **Identity: *e***
- **Associative**

A simple example of a group lies below.

Set: G = {..., -4, -2, -, 2, 4, ...}

Operation: +

Group: (G, +)

Closure: Any two elements added yields an element in the set *G* (e.g. -2 + 18 = 16)

Inverses: The inverse of 4 is -4, and 4 + (-4) = 0 (identity)

Identity: The identity element is 0, as

$$a + 0 = 0 + a = a \ \forall \ a \in G$$

Associativity: Addition is associative.

$$(a + b) + c = a + (b + c)\ \forall\ a, b, c \in G$$

All four axioms have been satisfied, hence the set of **even integers forms a group under +**.

If you've been following along so far (or at least, trying to), you may be wondering: what's the point of all this? Why are we defining groups so abstractly? Well, the axioms you've learnt about so far as usually facts that we take for granted in our everyday lives or in math class, but not all mathematical structures same these same properties. In order to gain a sense of **motivation for the definition of a group**, lets look at the following equation:

$$x + 4 = 9$$

Pretty easy right? The answer is clearly 5, but how did you reach that conclusion? You may think it's as easy as subtracting 5 from 9, but subconsciously, you're applying the very axioms listed in previous pages.

$x + 4 = 9$	($\mathbb{Z}$ under +)
$(x + 4) + -4 = 9 + -4$	(inverse of 4 is -4)
$x + (4 + -4) = 9 + -4$	(associative)
$x + (4 + -4) = 5$	($\mathbb{Z}$ closed under +)
$x + 0 = 5$	(identity is 0)
$x = 5$	

As you can see, we've solved the most basic of basic equations using only the four main axioms. This motivates the definition of a group as it must satisfy these four simple axioms in order to solve easy equations like the one above.

Because, you've spent most of your life in school so far, attending math class several times a week and getting used to doing small arithmetic in your head, all these extra steps have been "un-abstracted" for you, meaning you take these small steps for granted. For the sake of doing well in high-school math, this isn't a bad thing!

When studying quadratic equations and the Pythagorean Theorem, such basic (or should I say, trivial) arithmetic is implied while working through problems. As you outgrow this book and (hopefully) study more advanced abstract algebra and other areas of math, you'll see how thinking like a high-school student isn't always the best approach.

Instead, embracing abstraction becomes your ticket to deeper understanding and solving more complex problems. Better get used to it now than later!

Quick note, keep in mind that **finite groups** are those formed by a finite set. $\{1, 3, 4, 5, 9\}$ would be an example of a finite set. An **infinite group** however is formed by an infinite set, such as $\mathbb{Z}$, or $\mathbb{R}$.

Finite groups can be represented using a Cayley table. When used to represent groups, Cayley tables could be called "**Group tables**" interchangeably. Infinite groups, however, obviously can't, unless you have a LOT of paper and time on your hands.

This is the Cayley table for the binary operation **$+_4$ on the set S = {0, 1, 2, 3}**

(S, $+_4$)	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

See the familiar patterns formed by each number?

Just like the prerequisites section! The only difference is that this time it is in the context of a group.

(P, $\times_5$)	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\times_5$ on {0, 1, 2, 3, 4}

Order, Period, & Commutativity

The **order** of a group refers to the number of elements in the group. In other words, how many elements are in the set that forms the group under a particular binary operation. This is denoted by **| G |**.

The **period** of an element of a group is the smallest non-negative integer n such that $x^n = e$, where e is the identity.

An **abelian group** (pronounced “uhh-bee-lee-in”) is a group with the additional property of commutativity between the elements of the group. “**Commutative group**” and “abelian group” are synonymous terms.

Remember that commutativity isn’t a necessary axiom to be considered a group.

As an example, for the two Group Tables on the Page 38, both groups can be considered abelian.

Notice that, a defining feature of abelian groups is that their Group table has a **line of symmetry down the leading diagonal.**

Here's an example to help these points sink in. Consider the group of the set of permutations of the numbers 1, 2, and 3.

Don't be confused! This is the first example of a group in this book so far that doesn't basic or modular arithmetic as an example, but remember to think abstractly!

You can list these permutations: (1 2 3), (2 1 3), (3 2 1), (1 3 2), (3 1 2), (2 3 1). You can also write the permutations using notation which indicates how the original order of the numbers changes under each permutation:

$$e = \begin{matrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{matrix}$$

$$a = \begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix}$$

$$b = \begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix}$$

$$c = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix}$$

$$d = \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix}$$

$$e = \begin{matrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{matrix}$$

Observe that each of these six permutations are the individual elements of the group. The order of this group is 6.

All possible combinations of two permutations can be shown in a Cayley Table:

		First permutation					
		e	**a**	**b**	**c**	**d**	**f**
Second permutation	**e**	e	a	b	c	d	f
	a	a	e	d	f	b	c
	b	b	c	e	a	f	d
	c	c	b	f	d	e	a
	d	d	f	a	e	c	b
	f	f	d	c	b	a	e

Element a has a period of 2 since $a = e$ and Element c has period 3 since $c = c(cc) = cd = e$

Here, $ba \neq ab$; therefore this group is not abelian. Notice that the table is not symmetrical diagonally.

Reread this chapter. Seriously. Reread it. It is *very* important to understand what a group is in order to continue studying group theory and further abstract algebra, so give this chapter a quick skim once again. Do a couple problems here if you feel you need to, or search a few beginner problem sets online.

Review Test

1

Draw a Cayley table for the binary operation multiplication modulo 5 ($\times_5$) on the set L = {0, 1, 2, 3, 4}

Is the set closed under $\times_5$?

State the element that is the identity element.

For each element, write down its inverse.

Is L a group? Why or why not?

2

Draw a Cayley table for the binary operation multiplication modulo 6 ($+_6$) on the set B = {0, 1, 2, 3, 4, 5}

Is the set closed under $+_6$?

State the element that is the identity element.

Show that B forms a group under $+_6$

Is the group formed an abelian group? Why?

3

Consider the group G, formed by {0, 1, 2, 3, 4, 5, 6} under $\times_7$
State the order of G.

Determine the period of the element 6 in the group G.

4

Show that $\mathbb{Z}$ forms a group under the binary operation *, where $x * y = x + y - 2$

Dihedral & Cyclic Groups

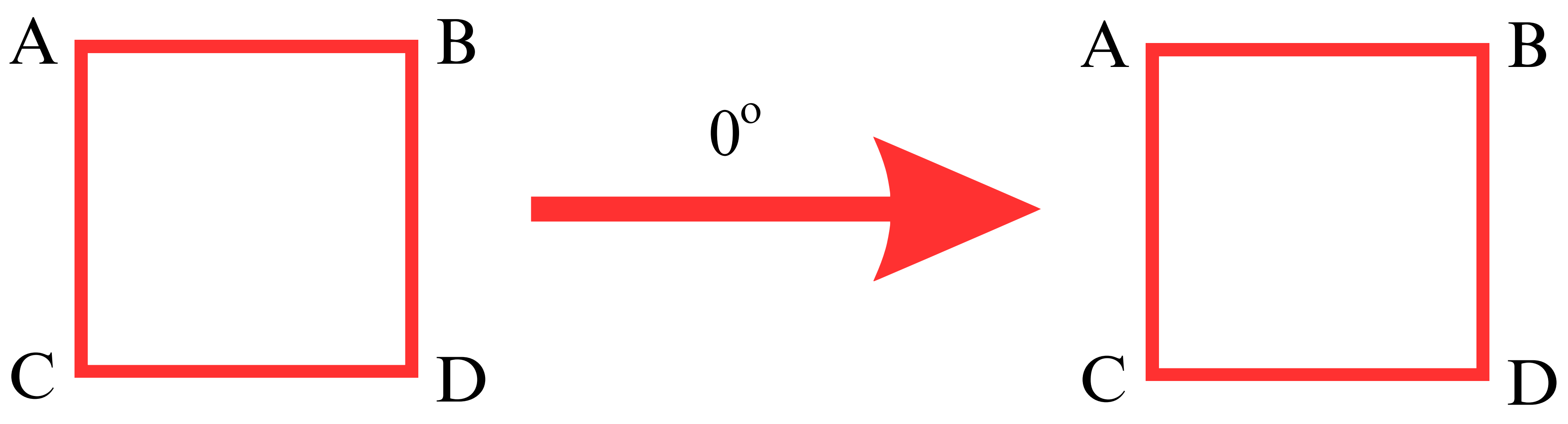
The set of all symmetries of a regular polygon also form a group. These symmetries include rotations and reflections that map the polygon onto itself.

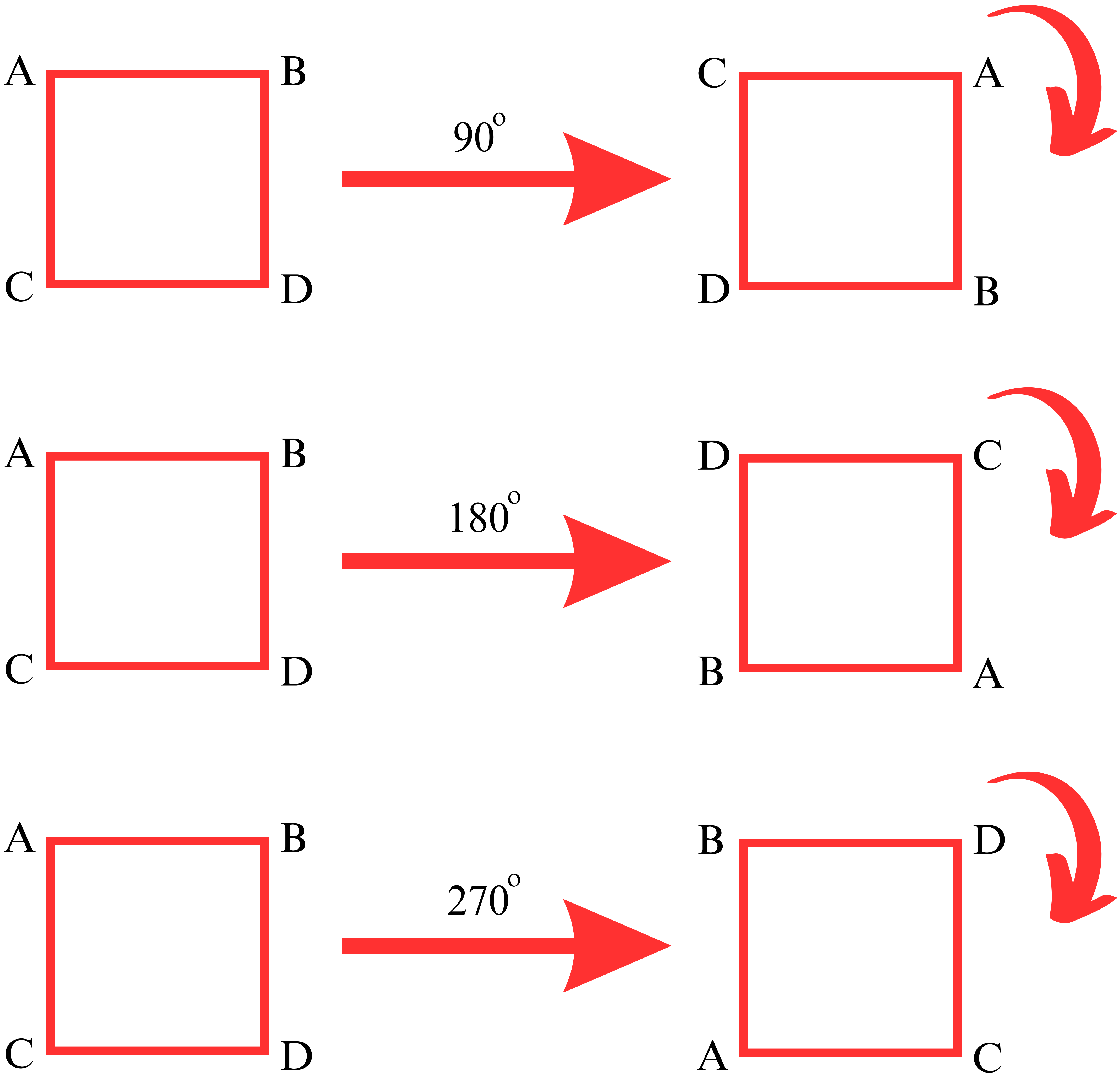
Such groups are called **dihedral groups** (denoted by D_n, where n is the number of sides in the regular n-gon).

A simple example would be D_4, the dihedral group of all symmetries of a regular square.

The order of this group is 8: 4 clockwise rotations (0^o, 90^o, 180^o and 270^o), and 4 reflections (over the four axis of symmetry).

Here's a visualization of each element of D_4, using letters on each vertex to follow along with the transformations.



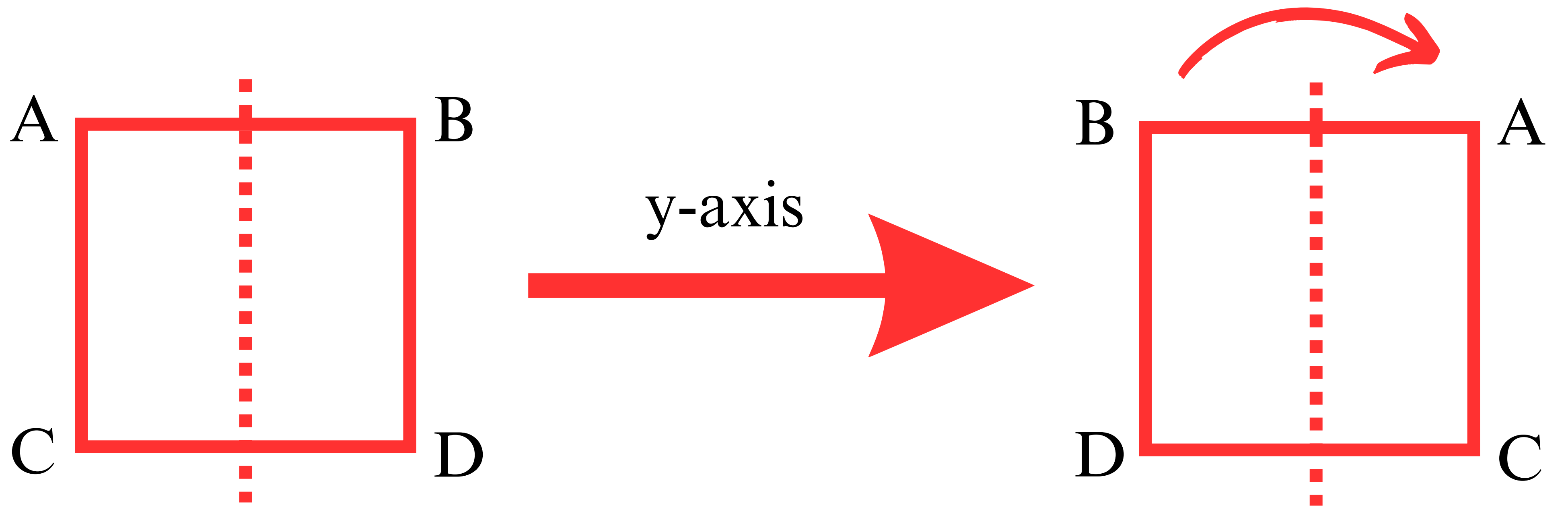


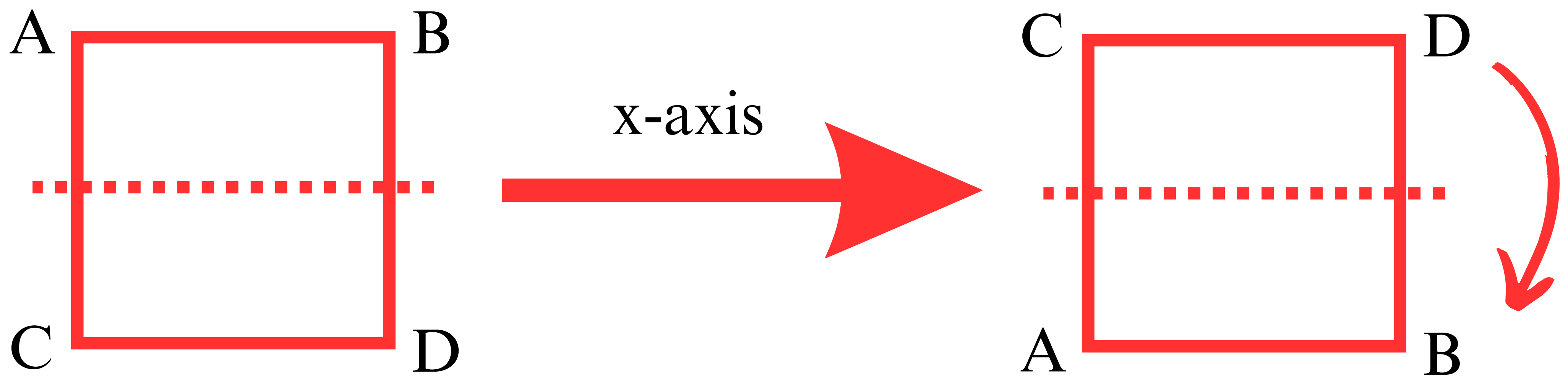
Out of these four elements, which do you think is the identity? It would most definitely be the first one, 0°, as it leaves the square unchanged.

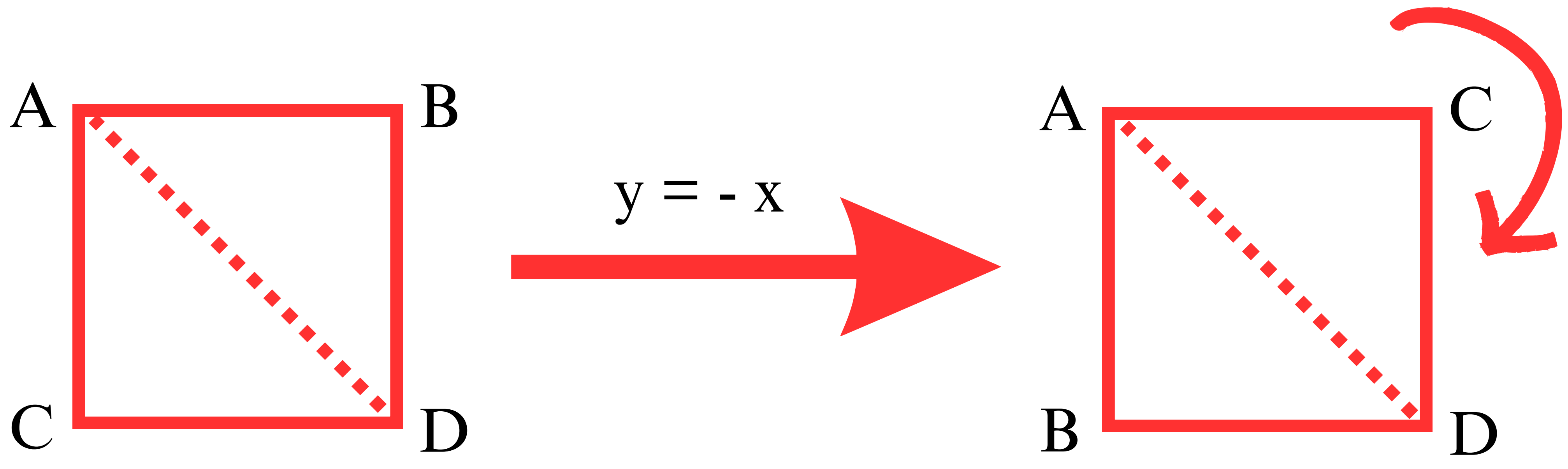
Notice how the 180° and 270° rotations are repeated operations of the 90° rotation. If the 90° turn was denoted by a, and the 180° by b, we would say that $b = a^2$. Keep this concept in mind when studying cyclic groups!

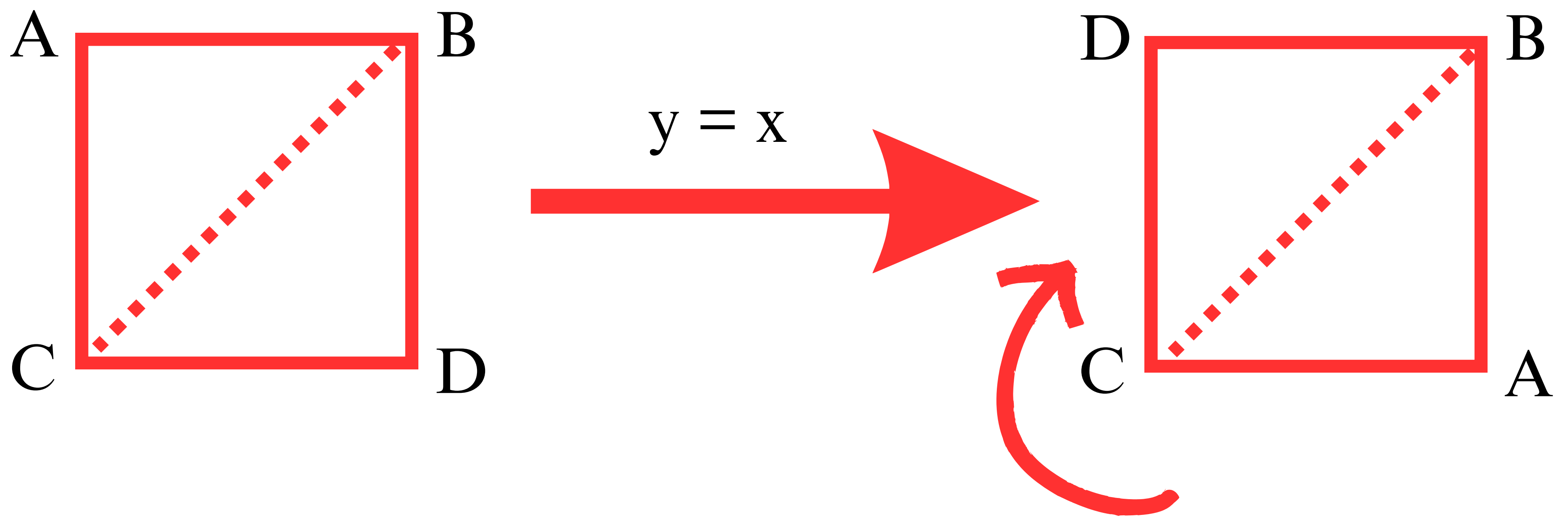
A 360° rotation exists, but is essentially the same as the 0° turn, so we don’t count it as a unique element. Same for 450°, and so on.

As for the other four elements...









Each of these 8 visualizations represents an element of the dihedral group D_4. These rotations and reflections, when combined, will map the square onto itself, demonstrating the symmetry properties of the group.

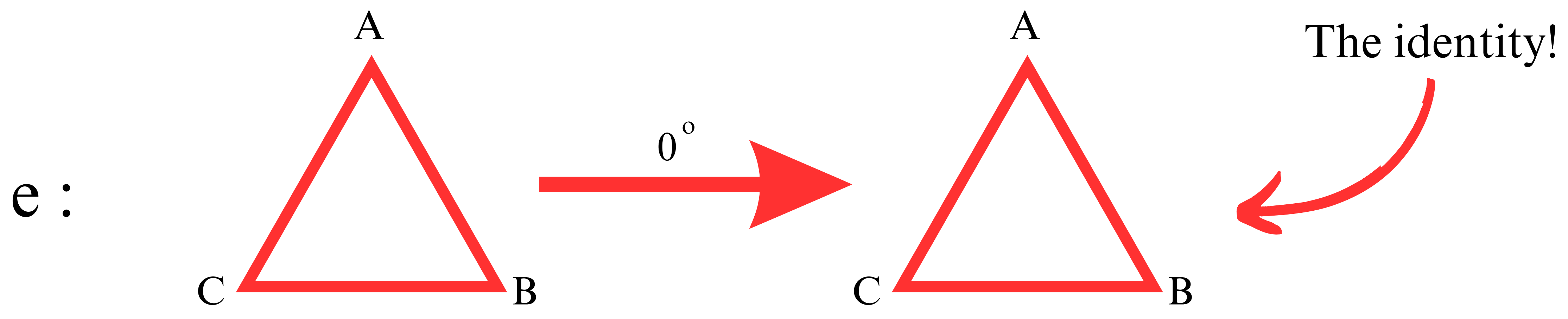
Since this is a group, you would be right in assuming that each element has an inverse. For reflections, they are self-inverse. A 90° rotation, on the other hand, could be undone with a 270° rotation.

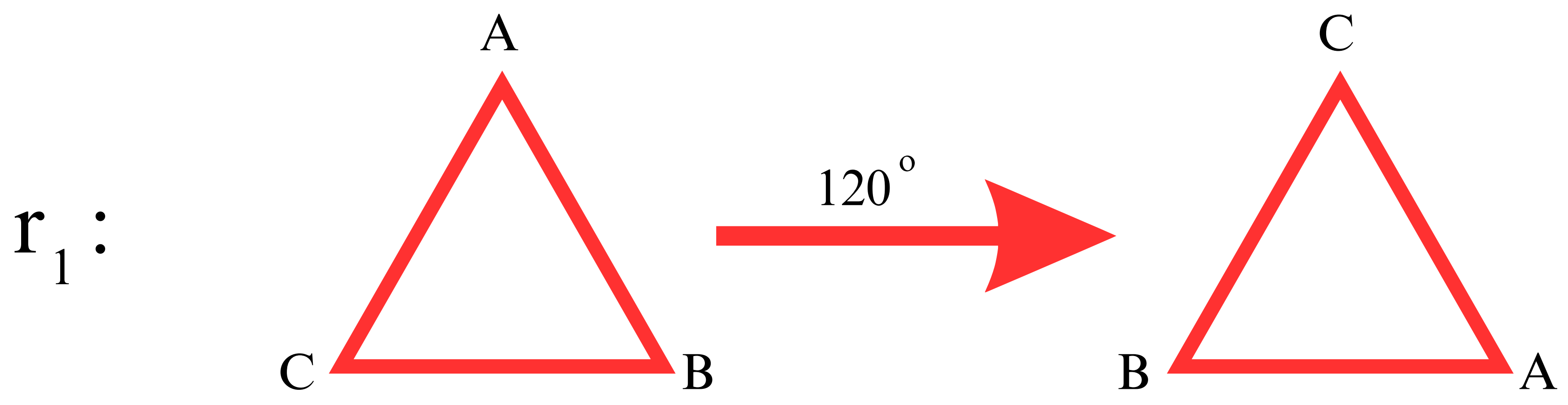
The process of identifying symmetries and finding an appropriate dihedral group can be extending to any polygon. Triangles, pentagons, tricontakaiheptagons, you name it!

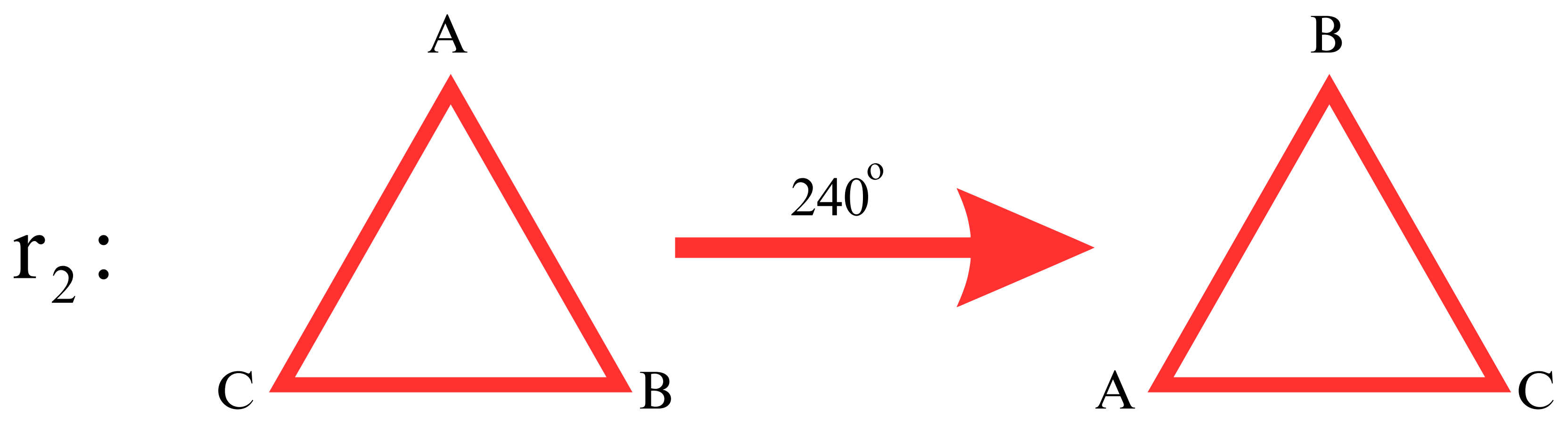
One important piece of information to be aware of is that the **order of a dihedral group is twice that of the number of sides** of the group's respective polygon. For the D_4 example earlier, the order is 8: twice of 4. For D_3 , the order will be 6.

Cyclic groups (pronounced "sick-lick") is a group that can be "generated" by a single element, called a **generator**. This means that every group element can be obtained by repeatedly applying the binary operation to this generator.

An example of a cyclic group would be the set of rotational (not reflectional) symmetries of an equilateral triangle:







Here's the respective Cayley table

	e	**r_1**	**r_2**
e	e	r_1	r_2
r_1	r_1	r_2	e
r_2	r_2	e	r_1

In this group, the generator is r_1, as each element can be acquired from repeated applications of r_1.

We denote this by $\langle \mathbf{r}_1 \rangle$

Note that there can be more than one generator! In this case, r_2, is also a generator.

A numerical, not geometrical, example of a cyclic group would be the integers under addition **G = (ℤ, +)**

Claim: $\mathbb{Z} = \langle 1 \rangle$

$$\langle 1 \rangle = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

Additive inverses

0 is the identity

Each number is generated from adding (or subtracting!) another "1".

Hence, "ℤ under +" is a cyclic group.

Let’s prove the fact that every cyclic group must be abelian.

Claim: For a cyclic group *G*, generated by an element *g*, meaning that $G = \{g^n \mid n \in \mathbb{Z}\}$, *G* is abelian (i.e. for any *a*, *b* ∈ *G*, *ab* = *ba*)

Proof:

- **Consider any two elements *a* and *b* in *G*. Since *G* is cyclic, we can write $a = g^m$, $b = g^n$ for some integers *m* and *n*.**
- **Compute the product *ab*:**

$$\begin{aligned} a \times b &= g^m \times g^n \\ &= g^{m+n} \qquad \text{(by law of indices)} \end{aligned}$$

- **Compute the product *ba*:**

$$\begin{aligned} b \times a &= g^n \times g^m \\ &= g^{n+m} \end{aligned}$$

- **Observe that, since addition is commutative, it follows that:**

$$ab = g^{m+n} = g^{n+m} = ba$$

- **Hence, ab = ba ∴ all cyclic groups are abelian.**
- **QED**

□

The notation for a cyclic group is typically ⟨**g**⟩, where *g* is a generator of the group. This represents the cyclic group generated by *g*. If the group is finite, it can also be denoted as $\mathbf{C_n}$, where *n* is the order (number of elements) of the group.

Subgroups & Lagrange's Theorem

Imagine you have a group *G*, which consists of certain elements and an operation that combines them. A **subgroup** is just a smaller group within *G* that still satisfies all the properties of a group.

In other words, if you take some of the elements from *G* and those elements can form a group on their own (under the same operation), then this smaller collection of elements is called a subgroup of *G*.

This is the notation for a subgroup *H* of *G*:

$$\mathbf{H \leq G}$$

(not the "less than or equal to" sign!)

The **trivial subgroup** is the simplest subgroup: the group containing only the identity element. Keep in mind that the trivial (sub)group is cyclic as it only needs itself (and *is* itself) to be generated.

Non-trivial subgroups are any other subgroups that contain more than just the identity. This includes the group itself.

Proper subgroups are those that are subgroups of *G* but are not equal to *G* itself.

Proper subgroups
are denoted like this

$$H < G$$

In order to show that a group *H* is a subgroup of another group *G*, you need to check the following four conditions:

- ***H*** **is non-empty**
- **The identity element of** ***G*** **is in** ***H***
- ***H*** **is closed under the binary operation for** ***G***
- **The inverse of each element of** ***H*** **belongs to** ***H***

As an example, let's prove the following

Claim: $H = (\mathbb{Q}, +) \leq G = (\mathbb{R}, +)$

Proof:

- **H is non-empty since there exist (an infinite number of) elements in H**
- **The identity element of G under the binary operation addition is 0 and $0 \in \mathbb{Q}$**
- **H is closed since if $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$**
- **The inverse of an element x is x^{-1}, which is $-x$ under addition. $x, -x \in \mathbb{Q}$**
- **We have confirmed the four necessary properties, $\therefore H \leq G$**
- **QED**

□

You should be able to find subgroups for a given group.

Let’s look at an example by finding all the non-trivial subgroups of a group *G* formed by the set *S* = {a, b, c, d} under the binary operation *

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

Ignoring {a}, the trivial subgroup, we see our options are {a, b}, {a, c}, {a, d}, {a, b, c}, {a, b, d}, {a, c, d}, and {a, b, c, d}.

Checking each one:

- {a, b} is non-empty, closed, and since *a* and *b* are self-inverse, {a, b} is a subgroup of *G*
- {a, c} is non-empty, but c^2= b, it is not closed
- {a, d} is non-empty, but d^2= b, it is not closed
- {a, b, c} is non-empty, but bc = d, it is not closed
- {a, b, d} is non-empty, but bd = c, it is not closed
- {a, b, d} is non-empty, but cd = b, it is not closed
- {a, b, c, d} is the group itself, so by definition, it is a non-trivial subgroup of *G*

Hence the non-trivial subgroups are {a, b} and {a, b, c, d}.

An important concept to be aware of is that **every subgroup of a cyclic group is always also cyclic.**

Claim: Every subgroup of a cyclic group is also cyclic.

Proof:

- Let $G = \langle g \rangle$ be a cyclic group generated by an element g, and let H be a subgroup of G
- If $H = \{e\}$, where e is the identity element, then H is trivially cyclic, generated by e
- If H contains elements other than e, choose the element of H with the smallest positive integer exponent, say g^m, such that $g^m \in H$ and $m > 0$
- Take any element $g^k \in H$. Since g^k generates the smallest positive power in H, k must be a multiple of m
- Therefore, $g^k = (g^m)^n$ for some integer n, implying that g^k can be written as a power of g^m
- This shows that $H = \langle g^m \rangle$ ∴ H is cyclic
- Hence, every subgroup of a cyclic group is also cyclic.
- QED

□

On the Page 51, we identified subgroups by checking each and every possible combination of elements. If the order of a group is large though, this becomes quite an annoying task.

Imagine the group of all symmetries of an octagon (order of 16). You would have to check a substantial number of cases.

Lagrange's theorem allows you to reduce the number of cases significantly.

Lagrange's theorem states that for any finite group *G*, the order of every subgroup of *G* divides the order of *G*.

Also, by Lagrange's theorem, **the period of any element in the group *G* is a factor of the order of *G*.**

The consequence of this is that, for our octagon as an example, you would only need to look for subgroups of order 1 (the trivial subgroup containing the identity), order 16 (the group itself), 2, 4, and 8. This is still a lot of work, but it's nice that you don't also have to check for subgroups of order 3, 5, 7, 9, etc.

Here's Lagrange's theorem in action. Consider the group $G = (\{0, 1, 2, 3, 4, 5, 6\}, +_6)$. Say we want to find all possible *proper non-trivial* subgroups of *G*.

Instead of blindly checking each possible subgroup to see if it's valid, let's determine the order of possible subgroups of *G*. Clearly, they are 1, 2, 3, and 6. Now we don't need to check subgroups of order 4 and 5.

List all the possibilities.

$\{0\}$ -- this is the trivial subgroup of order 1. Discard this.

$\{0, 1, 2, 3, 4, 5, 6\}$ -- this is the group itself; not a proper subgroup. Discard this too.

Other possibilities: $\{0, 1\}$, $\{0, 2\}$, $\{0, 3\}$, $\{0, 4\}$, $\{0, 5\}$, $\{0, 1, 2\}$, $\{0, 1, 3\}$, $\{0, 1, 4\}$, $\{0, 1, 5\}$, $\{0, 2, 3\}$, $\{0, 2, 4\}$, $\{0, 2, 5\}$, $\{0, 3, 4\}$, $\{0, 3, 5\}$, and $\{0, 4, 5\}$

For the two-element options, the element other than the identity must be self-inverse.

$2 + 2 \neq 0 \pmod 6$, $3 + 3 = 0 \pmod 6$, $4 + 4 \neq 0 \pmod 6$, $5 + 5 \neq 0 \pmod 6$

Hence $\{0, 3\}$ is the only valid two-element subgroup

For the three-element options, both elements other than the identity must be self-inverse, or they must be inverse pairs.

Since 3 is the only self-inverse element other than the identity, $\{0, 1, 3\}$, $\{0, 2, 3\}$, $\{0, 3, 4\}$, and $\{0, 3, 5\}$ can be discarded.

$2 + 4 = 0 \pmod 6$ and $1 + 5 = 0 \pmod 6$, so $\{0, 1, 5\}$ and $\{0, 2, 4\}$ are also subgroups

Our final list is $\{0, 3\}$, $\{0, 1, 5\}$, and $\{0, 2, 4\}$

The proof for Lagrange's theorem is beyond the scope of this book, so, just this once, you'll have to take our word for it. Feel free to search up on it, but be sure to find out what a "**coset**" is!

Isomorphisms

An **isomorphism** is an important concept in group theory. Let's say that you've proved results for a certain group of order 5. If you encounter another group of order 5, your first instinct would be to repeat the proofs for this different group.

However, if you can show that the two groups are **isomorphic**, then the results proved for the first group applies to the second one too.

(The word "isomorphism" can be broken up into "iso", meaning "same", and "morph", meaning "shape")

We say two groups are isomorphic if there is a "**one-to-one mapping**" (i.e. an isomorphism) which associates each of the elements of one group with that of the other group, such that:

If p maps to a and q maps to b, then the results of combining p and q under the binary operation of the first set maps to the result of combining a and b under the binary operation of the other set.

Oversimplified, an isomorphism occurs when two groups have a "**similar structure.**"

"H is isomorphic to G"

$$\mathbf{H} \cong \mathbf{G}$$

You may recognise this symbol from geometry to mean "is congruent to." See the link?

Alright, let's look at an example: consider two groups, G_1 ({0, 1, 2} under $+_3$) and G_2 (set of rotations of an equilateral triangle).

G_1 : {0, 1, 2} with addition modulo 3:

- The operation is a + b (mod 3)
- For example, $1 + 2 \equiv 0 \pmod{3}$

G_2 : The set of rotations of an equilateral triangle by 0°, 120°, and 240°.

- R_0 corresponds to a 0° rotation.
- R_{120} corresponds to a 120° rotation.
- R_{240} corresponds to a 240° rotation.

$$0 \leftrightarrow R_0 \ , 1 \leftrightarrow R_{120} , 2 \leftrightarrow R_{240}$$

These are the mappings (links) between each element from both groups.

We can see that each number in G_1 is uniquely matched to a rotation in G_2.

Since the result of combining 1 and 2 in G_1 (which gives 0) matches the result of combining R_{120} and R_{240} in G_2 (which gives R_0), the operation is preserved.

Since every element is paired uniquely and the operations match up, we can say that the two groups G_1 and G_2 are isomorphic.

Here's another example, a bit more abstract this time.

Take groups *G* and *H* with the following Cayley tables:

G

	a	**b**	**c**	**d**	**e**	**f**
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

H

	P	**Q**	**R**	**S**	**T**	**U**
P	S	U	T	P	R	Q
Q	T	R	S	Q	U	P
R	U	S	Q	R	P	T
S	P	Q	R	S	T	U
T	Q	P	U	T	S	R
U	R	T	P	U	Q	S

Let’s prove that G ≅ H:

Claim: G ≅ H for the above two Cayley tables.

Proof:

- **The identity elements for *G* and *H* is *a* and *S* respectively.**
- **The self-inverse elements in *G* are *d*, *e*, and *f*, whilst for *H*, they are *P*, *T*, and *U*.**
- **In *G*, *b* and *c* are not self-inverse, while in *H*, *Q* and *R* aren’t.**
- **Choose an arbitrary mapping, say *b* ↔ *Q***
- **∴ *c* ↔ *R***
- **Let *d* ↔ *P* ∴ *e* ↔ *U* & *f* ↔ *T***
- **Hence, a possible mapping is**

  [b, c, d, e, f] ↔ [Q, R, P, U , T]
- **The Cayley table for *H* can now be represented as:**

	S	**Q**	**R**	**P**	**U**	**T**
S	S	Q	R	P	U	T
Q	Q	R	S	T	P	U
R	R	S	Q	U	T	P
P	P	U	T	S	Q	R
U	U	T	P	R	S	Q
T	T	P	U	Q	R	S

- **The patterns in this table for H matches that of G ∴ G ≅ H**
- **QED □**

Similar to proof by counterexample, in order to prove that two groups aren’t isomorphic, we need to establish just one of the following:

- That there are a different number of self-inverse elements in the two groups.
- That some elements in one group don’t have the same period as the other.
- That one group is cyclic and the other isn’t.

Let’s prove that the following Group *S* is not isomorphic to groups *G* and *H* from the previous page.

	1	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	2
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

You could also show that *S* has elements of period 6, whereas *G* and *H* do not.

Claim: *S* is not isomorphic to *G* and *H*.

Proof:

- **The identity elements for *S* is 1**
- **The only self-inverse element in *S* is 6**
- **However, *G* and *H* each have three self-inverse elements**
- **1 ≠ 3 ∴ *S* is not isomorphic to *G* and *H***
- **QED**

□

Review Test

1 Show that the set of all symmetries of a hexagon form a group and state the order of the group.

Is C_6 abelian? Why?

2 Give a geometric interpretation of the group D_5.

Why is the order of this group 10?

3 The group G is defined as $G = (\langle 5 \rangle, \times_7)$. Find the set of all elements contained within G.

Is G abelian?

4 The group F is defined as $F = (\langle 3 \rangle, +_7)$. Draw a Cayley table for F.

What's the order of F?

Bob claims 3 is not the unique generator of F. Assess the claim.

5 Determine the only possible orders of the subgroups of a group which has an order of 120. Fully justify your answer.

6 Can group A, order 12, be a subgroup of group G, order 30?

7

Prove by deduction that no subgroups of order 8 exist for a group of order 92.

8

Find the one non-trivial proper subgroup of G, where $G = (\{0, 1, 2, 3, 4, 5, 6, 7, 8\}, +_9)$

9

Show that the group formed by the set of rotational symmetries of an equilateral triangle is isomorphic to the group $R = (\langle 4 \rangle, \times_7\ )$

10

Explain why all groups of order 2 are isomorphic to each other.

11

Explain (and prove if you feel you can) why it is impossible for an abelian group to be isomorphic to a non-abelian group.

12

Find the identity element a generator of the following Cayley table:

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

APPLICATIONS OF GROUP THEORY

You may be wondering: “How is anything learnt so far even remotely useful in the real world?”

And you’d be right in asking.

The content throughout this book may seem abstract at first, but its applications are surprisingly vast and deeply integrated into many areas of science, engineering, and beyond. From solving puzzles like the Rubik's Cube to enabling secure communication over the internet, group theory provides the mathematical framework that underpins many of the technologies and concepts we rely on today.

In this chapter, we'll explore some of these fascinating applications, showing how the principles you've learned are used in the real world.

Keep in mind that most of it really takes some complicated understanding of abstract algebra, and the math in this book isn’t nearly as advanced to do justice to these topics. Further reading on group theory concepts and applications is encouraged.

Cryptography

Cryptography is the science of securing information so that only intended recipients can read or understand it. In today's digital world, cryptography is essential for protecting sensitive data, such as your passwords, credit card information, and private messages. Group theory is a key mathematical tool used in cryptography.

One of the most famous cryptographic algorithms is the RSA algorithm, named after its inventors Rivest, Shamir, and Adleman. RSA is widely used for secure communication, including things like online shopping, secure emails, and even virtual private networks (VPNs).

At the heart of the RSA algorithm is the concept of modular arithmetic, which is closely related to group theory. RSA relies on the difficulty of certain mathematical problems within a group to create a secure system for encrypting and decrypting messages. Here's how it works:

Key Generation:

- RSA starts by selecting two large prime numbers, say p and q.
- These primes are multiplied together to get a product $n = p \times q$, which is used as part of the public key.
- The group involved here is the set of integers modulo n, often denoted $\mathbb{Z}_{\text{n}}$, which consists of all integers from 0 to $n - 1$.

Public & Private Keys:

- The public key, which is shared with everyone, includes n and a number e (where e is chosen such that it is relatively prime to $(p - 1) \times (q - 1)$.
- The private key, which is kept secret, includes a number d calculated based on e, p, and q. The private key allows the intended recipient to decrypt messages.

Encryption:

- To encrypt a message M, you first convert M into a number (let's call it m) that is smaller than n. Then, you compute the ciphertext c using the public key:

$$c = m^e \pmod{n}$$

- The group operation here is exponentiation, and because e and n are public, anyone can compute c from m.

Decryption:

- The recipient, who knows the private key d, can decrypt the ciphertext c by computing:

$$m = c^d \pmod{n}$$

- The math behind this ensures that m (original message) is recovered accurately, thanks to properties of the group $\mathbb{Z}_n$ and the unique relationship between e and d.

The security of RSA is based on the group properties of the integers modulo n. Specifically, it's very easy to compute $c = m^e \pmod{n}$, but difficult to reverse the process (i.e., to figure out m given c and e) without knowing the private key. This difficulty comes from the challenge of factoring large numbers into primes, a problem that is deeply connected to group theory.

Applications of Group Theory

Imagine you want to send a secret message to your friend. You both agree on a public key:

- $p = 5$
- $q = 11$
- $n = 5 \times 11 = 55$
- $e = 3$

Your private key is d, calculated such that:

$$(e \times d) \pmod{(p-1)(q-1)} = 1$$

To send the message "7", you encrypt it:

$$c = 73 \pmod{55} = 343 \pmod{55} = 13$$

Your friend, using the private key d, can then decrypt it:

$$m^d = 13 \pmod{55}$$

This will give them back the original message "7"!

In reality, RSA uses much larger prime numbers, making the group $\mathbb{Z}_n$ extremely large and the factoring problem incredibly difficult.

This is why RSA remains a cornerstone of secure communication today. Every time you access a secure website (https://), make a secure payment, or send encrypted emails, group theory is working in the background to keep your data safe from prying eyes.

Group theory provides the mathematical framework that makes modern cryptography possible, ensuring that our digital world can operate securely and privately!

Rubik’s Cubes

The Rubik's Cube is a 3×3×3 puzzle with 6 faces, each composed of 9 smaller squares. The goal is to scramble the cube and then return it to its original state, where each face of the cube has a uniform color. The Rubik's Cube is a perfect playground for group theory because it involves a series of moves (**rotations**) that can be analyzed mathematically.

Each possible move of the Rubik's Cube (rotating a face 90°, 180°, or 270° clockwise or counterclockwise) can be thought of as an element of a group. In this context, a "group" refers to the set of all possible states of the Rubik's Cube, along with the operations (moves) that transform one state into another.

Group Elements: A single element in the group might represent the cube after, say, one clockwise rotation of the front face.

Group Operations: The operation is the sequence of moves. If you perform one move and then another, the combination of those two moves is itself a group operation.

Identity Element: The identity element in the Rubik’s Cube group is the solved state, where no moves have been made, or equivalently, after performing a sequence of moves that returns the cube to its original solved state.

Inverses: The inverse of any move is simply the move that undoes it. For example, if you rotate the front face 90° clockwise, its inverse is a 90° counterclockwise rotation of the same face.

In order to properly apply group theory here, we need to have a sold understanding of **algorithms**. Algorithms on a Rubik's Cube are sequences of moves that, when performed in a specific order, lead to a desired outcome, such as solving a part of the cube or setting up the cube for another algorithm. Each move corresponds to a rotation of one of the cube's faces (denoted by letters like *R* for right, *L* for left, *U* for up, etc.). The goal is to manipulate the cube systematically, using algorithms to control the outcome of each step in the solving process.

Note that L^{-1} is not the same as *R*. In general:

- *L* rotates the left face of the cube 90 degrees clockwise.
- L^{-1} rotates the left face 90 degrees counterclockwise.
- *R* rotates the right face 90 degrees clockwise.
- R^{-1} rotates the right face 90 degrees counterclockwise.

Each face of the Rubik's Cube has its own corresponding move and inverse move. The above applies to *U* and *D* too.

In the context of Rubik's Cube, a **conjugate** is a sequence of moves designed to bring a particular piece or set of pieces into position, perform an operation on it, and then undo the initial setup moves to restore the rest of the cube. Mathematically, if A and B are sequences of moves, a conjugate is expressed as $B^{-1}AB$. Here, B^{-1}sets up the cube, A performs the operation, and B undoes the setup.

A **commutator** involves two sequences of moves, A and B, performed in the sequence $ABA^{-1}B^{-1}$. The commutator is powerful because it allows you to swap or cycle specific pieces on the cube while leaving the rest of the cube relatively untouched. It's particularly useful in advanced solving techniques where you need to make minor adjustments without disturbing the solved parts of the cube.

Overall, these conjugates and commutators can be combined to form strong algorithms for certain cases of Rubik’s Cubes, such as the “Edge-3 Cycle” & “Corner Twist.” The exact specifics of these algorithms are quite complicated and beyond the scope of this book.

Materials Science

Group theory's applications in materials science, particularly in chemistry, delve into how the symmetrical properties of molecules influence their chemical behavior and physical properties.

At its core, symmetry in chemistry is tied to how a molecule’s structure remains invariant under certain operations, like rotations or reflections. For instance, in crystallography, group theory helps categorize crystals based on their symmetrical patterns, leading to the classification of crystal systems like cubic, tetragonal, or hexagonal. This classification is crucial because the symmetry of a crystal directly affects its physical properties, such as its ability to conduct electricity or its optical properties.

Molecular symmetry, described by point groups, is another area where group theory is essential. A point group is a set of symmetry operations that, when applied to a molecule, leave its overall shape unchanged. These operations can include rotations, reflections, and inversions. For example, the water molecule (H_2O) has a specific symmetry because if you rotate it 180 degrees around its central axis, it looks the same. This symmetry is crucial in predicting how the molecule will interact with light, which in turn affects its infrared and Raman spectra. These are spectroscopic methods are essential tools in identifying molecules and understanding their structures.

Moreover, group theory is vital in quantum chemistry. The electronic structure of molecules, which determines how they bond and react, can be studied using group theory. By understanding the symmetry of a molecule, chemists can simplify complex equations that describe the behavior of electrons. This simplification helps in predicting chemical reactions and understanding why certain reactions occur while others do not. For instance, group theory can predict which molecular orbitals will combine to form bonds in a molecule, aiding in the design of new materials with desired properties.

In materials science, group theory is used to understand the properties of solids, particularly in the study of phase transitions. When a material changes phase, such as from solid to liquid, its symmetry often changes. Group theory helps in understanding these changes, which is critical in fields like metallurgy, where controlling the phase of a material can influence its hardness, ductility, or strength. For example, the phase transition in steel, which affects its strength, can be analyzed using group theory to optimize its properties for construction or manufacturing.

Thus, group theory serves as a powerful tool in understanding and manipulating the properties of materials at a molecular level, with broad applications in chemistry and materials science, from the design of new drugs and materials to the development of advanced technologies.

Music Theory

Music and mathematics have always shared a deep connection, often in ways that are not immediately obvious. One of the most fascinating intersections between these two fields lies in the application of group theory to analyze musical compositions, scales, and symmetries. Group theory provides a framework to understand and formalize the patterns and structures in music, making it an essential tool for music theorists and composers alike.

At the most basic level, a musical scale can be seen as a set of notes. For example, the C major scale consists of the notes C, D, E, F, G, A, and B. These notes can be arranged in various ways to create melodies and harmonies. Group theory enters the picture when we start to consider the operations we can perform on these notes, such as transposing a piece of music to a different key or inverting a melody.

One of the most straightforward applications of group theory in music is through the concept of transposition. Transposing a piece of music involves shifting every note in the piece by the same interval, effectively moving it up or down the scale. Mathematically, this can be understood using modular arithmetic.

Consider the set of notes in a chromatic scale, which includes all twelve distinct pitches: C, C#, D, D#, E, F, F#, G, G#, A, A#, B. If we assign a number to each note (C = 0, C# = 1, ..., B = 11), transposing a note by a certain number of steps can be thought of as adding a number to the corresponding integer. For example, transposing the note C (0) by 5 steps gives us G (7).

This operation is similar to addition modulo 12, where the set of integers {0, 1, 2, ..., 11} forms a cyclic group under addition modulo 12. The operation of transposing notes is analogous to adding elements in this group. For example, transposing C (0) by 7 steps gives G (7), and transposing G (7) by 7 steps gives D (2), which corresponds to the same interval relationship in the music.

Another fundamental musical operation is inversion, where each interval in a melody is mirrored, creating a melody that moves in the opposite direction. For example, if a melody moves up by a perfect fifth (7 semitones), its inversion will move down by a perfect fifth.

In mathematical terms, this is akin to reflecting elements in a group. If we think of the notes in a scale as elements in a set, inversion corresponds to a symmetry operation that maps each element to another element according to a specific rule. In group theory, this is similar to considering the symmetries of an object, where each symmetry is an operation that leaves the object unchanged in some way.

For example, in the group of symmetries of an equilateral triangle, each rotation and reflection corresponds to a different symmetry operation. Similarly, in music, each transposition and inversion corresponds to a different transformation of the original melody.

Beyond pitch and harmony, group theory also finds applications in rhythm. Rhythmic patterns can be analyzed using the concept of cyclic groups, where each beat in a measure can be thought of as an element in a set. Rotating a rhythmic pattern by a certain number of beats is akin to performing a cyclic permutation, which is a basic operation in group theory.

For example, consider a simple 4/4 rhythm with beats on the first and third beats. This pattern can be represented as the sequence (1, 0, 1, 0). Rotating this pattern by one beat gives (0, 1, 0, 1), which corresponds to shifting the rhythm forward by one beat. The set of all possible rotations forms a cyclic group, and exploring this group allows musicians and composers to understand the relationships between different rhythmic patterns.

As you can see, group theory provides a powerful and elegant framework for understanding the mathematical structures underlying music. Whether through the analysis of scales, the exploration of symmetries in melodies, or the systematic transformation of tone rows, group theory offers deep insights into the patterns and principles that govern musical composition. By understanding these connections, both mathematicians and musicians can gain a richer appreciation of the art and science of music.

End-of-Chapter Answers

Prerequisites

EXERCISES

1 Use Lagrange's Theorem to explain why there is no subgroup of order 7 in a group of order 20.

2 The group $G = (\{0, 1, 2, 3, 4, 5\}, +_6)$
The group H consists of the set of rotational symmetries of a regular hexagon. Prove that $G \cong H$

3 $F = (\{1, 2, 4, 5, 7, 8\}, \times_9)$

State the order of F

Draw a Cayley table for F

State the period of the element ‘5’. Explain why this means F is cyclic.

Is F abelian? Why?

4 Draw a Group table for the group K, where
$K = (\{1, 5, 7, 11\}, \times_{12})$

Write down the identity element

Show that every element in K has an inverse

Give at least two examples of the axiom of associativity holding for K.

Exercises

5 Show that the groups $G = (\{1, 3, 7, 9\}, \times_{10})$ and $H = (\{0, 1, 2, 3\}, +_6)$ are isomorphic and write down a possible mapping

Are the groups cyclic? Why?

Are the groups abelian? Why?

6 The group S is formed by the set of all symmetries of an equilateral triangle.

d	**r_0**	**r_1**	**r_2**	**m_1**	**m_2**	**m_3**
r_0	r_0	r_1	r_2	m_1	m_2	m_3
r_1	r_1	r_2	r_0	m_2	m_3	m_1
r_2	r_2	r_0	r_1	m_3	m_1	m_2
m_1	m_1	m_3	m_2	r_0	r_2	r_1
m_2	m_2	m_1	m_3	r_1	r_0	r_2
m_3	m_3	m_2	m_1	r_2	r_1	r_0

State the order of possible subgroups of S

Write down the trivial subgroup of S

Find all proper subgroups of S

7 Prove by contradiction that in any group, the identity element is unique (this was done earlier!)

8 If a and b are elements in a group G, does $(ab)^{-1} = a^{-1}b^{-1}$? Prove or disprove.

9 Explain why all groups of order 3 are isomorphic to each other.

10 Prove that the set of all rotations in the Dihedral group D_n forms a cyclic subgroup.

11 Find all non-trivial cyclic subgroups of ({0, 1, 2, 3, 4, 5}, $+_6$)

12 Why is every dihedral group D_n non-abelian when n > 2 ?

13 How does symmetry in chemistry relate to group theory, particularly in identifying molecular structures?

14 Show that if two groups G and H are isomorphic, then their corresponding element orders match.

15 Explain why no subgroup of a Dihedral group D_n can contain exactly one reflection.

16 Is ({0, 1, 2, 3, 4, 5, 6, 7, 8, 9}, $+_{10}$) cyclic?

List its generators.

17 If G is a cyclic group of order 15, what are the possible orders of elements in G?

18 In D_6 , determine the subgroup generated by a 120° rotation.

Exercises

19 Determine if a set consisting of the identity and two reflections in D_6 forms a subgroup.

20 Do you think understanding dihedral groups can be useful in computer graphics for rendering reflections and rotations. Why do you think so?

21 Verify whether $\mathbb{Z}$ under addition modulo 7 forms a cyclic group and identify its generators.

22 Given the cyclic group $G = \langle g \rangle$ of order 8, list all subgroups of G.

23 Explain why the group of all integers under multiplication is not cyclic.

End-of-book Exercise Answers

1

20 is not divisible by 7. Hence, no subgroup of order 7 exists in a group of order 20.

3

Order of $F = 6$

Cayley Table of F:

$\times_9$	**1**	**2**	**4**	**5**	**7**	**8**
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Period of 5 is 6. Order of F = Period of 5 $\therefore$ F is cyclic

F is abelian because $a \times_9 b = b \times_9 a$ where $a, b \in F$
Also, the Cayley table is symmetric about the diagonal.

4 Group Table of K:

$\times_{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	5	1
11	11	7	1	5

The identity element is 1

By exhaustion:
1: 1 is the identity $\therefore$ the inverse of 1 is 1
5: $5 \times 5 \pmod{12} = 1$ $\therefore$ the inverse of 5 is 5
7: $7 \times 7 \pmod{12} = 1$ $\therefore$ the inverse of 7 is 7
11: $11 \times 11 \pmod{12} = 1$ $\therefore$ the inverse of 11 is 11
$\therefore$ Every element of K has an inverse

Associativity:
Ex1: $(5 \times 7) \times 11 \pmod{12} = 5 \times (7 \times 11) \pmod{12} = 1$
Ex2: $(7 \times 11) \times 5 \pmod{12} = 7 \times (11 \times 5) \pmod{12} = 1$

Notation & Glossary

Here's a list of important notation to be aware of:

{a, b, c}	**A set**
Ø or {}	**The empty set**
$\in$	**Is an element of**
$\notin$	**Is not an element of**
$\subseteq$	**Is a subset of**
$\subset$	**Is a proper subset of**
$\not\subset$	**Is not a subset of**
| S | or n(S)	**Order (cardinality) of a set**
$\mathbb{N}$	**Set of natural numbers**
$\mathbb{Z}$, $\mathbb{Z}^+$	**Set of integers, positive integers**
$\mathbb{Q}$	**Set of rational numbers**
$\mathbb{R}$	**Set of real numbers**
***, փ, ❤, ÷, ⬙, etc...**	**A binary operation**
y (mod n)	**Remainder of *y* ÷ *n***
$+_n$	**Addition modulo *n***
$\times_n$	**Multiplication modulo *n***

$\forall$	"For all"
$\exists$	"There exists"
$\therefore$	"Therefore"
□ and/or "QED"	End of proof
$p \Rightarrow q$	*p* "Implies" *q*
$(G, *)$	Group *G* (set *G* under *)
$\| G \|$	Order of a group *G*
D_n	Dihedral group (*n*-gon)
$(\langle g \rangle, *)$	Cyclic group generated by *g*
C_n	Finite cyclic group of order *n*
$H \leq G$	*H* is a subgroup of *G*
$H < G$	*H* is a proper subgroup of *G*
$H \cong G$	*H* is isomorphic to *G*
↔	"is mapped to"

The Notorious Topic of Group Theory made Simple, Straightforward, and Understandable by All.

$\forall a \in G, e * a = a * e = a$

Written by a math-obsessed high-schooler, this book delivers the elementary concept of group theory in a digestable manner for others to understand. Whether it be Cayley tables or Isomorphisms, this book will ensure that students have a sold grasp on the fundamentals.

After comprehending the concepts and rules of groups, we will explore its real-life applications, including how it is used in algorithms for solving Rubik's Cubes (yes, that shocked me too).

Note that knowledge of elementary algebra, permutations, and basic mathematical thinking/arithmetic is assumed. A prerequisites section for sets, proof methods, and others is included in the book.

> "Beautifully explained bite-sized chunks of abstract algebra.
> A must-read for those interested in learning more about math."
> - Aerith Blacksburg

Authored &
Illustrated by
Yaniv Lakhani

Published by

ISBN Num & Barcode