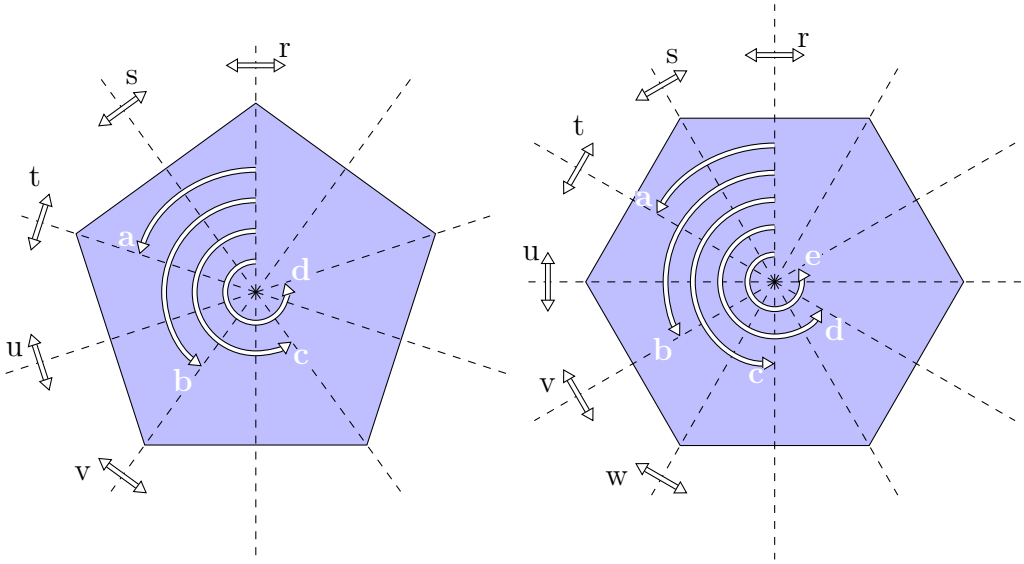
Higher Math Handout

# Group Theory

*Author:*
Emma Cardwell
Matthew Ho

*For:*
AoPS

*Date:*
January 6, 2021




*"We may as well cut out group theory. [It] will never be any use in physics." – James Jeans*

# Contents

# §0 Acknowledgements

This was made for the Art of Problem Solving Community out there! I would like to thank Evan Chen for his evan.sty code. In addition, all problems in the handout were likely from the AoPS Wiki.

Art of Problem Solving Community

Evan Chen's Personal Sty File

And Evan says he would like this here for evan.sty:

```
Boost Software License - Version 1.0 - August 17th, 2003
Copyright (c) 2020 Evan Chen [evan at evanchen.cc]
https://web.evanchen.cc/ || github.com/vEnhance
```

He also helped with the hint formatting. Evan is a LaTeXgod!
And finally, please do not make any copies of this document without referencing this original one. At least cite us when you are using this document.

# §1 Introduction

## §1.1 Group Theory?

You may be wondering what it is. Here's a definition from Wikipedia:

> **Definition 1.1** (Group Theory) — **Group theory** studies the algebraic structures known as groups.

The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces, can all be seen as groups endowed with additional operations and axioms.

## §1.2 Remarks on the Authors

The two authors, **Emma Cardwell** and **Matthew Ho** are actually not a part of Euclid's Orchard. They taught a class on Group Theory back in June, and it was decided that some of their slides could be made into a handout, to boost the popularity of their work. The hope is that through this article you will find that group theory, or more generally, higher level math, is not something to be feared. Dipping your toes into the water of group theory won't hurt you, and through Euclid's Orchard we hope you'll see that. Thank you to both authors!

# §2 Sets

## §2.1 Notation

A **set** is a well defined collection of objects (numbers, functions, colors, shapes, beautifully-designed presentation slides, etc).[1] Sets can have a finite or infinite number of elements, and the order of the elements doesn't matter. One way to define specific sets is by listing the elements in the set:

- $\{\text{red}, \text{orange}, \text{yellow}, \text{green}, \text{blue}, \text{purple}\}$
- $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\{1, 2, 3, 4, 5\}$

Here's some notation that might be helpful to know:
$2 \in X$ means 2 is an element of set X.
$f : X \to Y$ means $f$ is a function from set $X$ to set $Y$. (Its imputs are from set $X$ and its outputs are in set $Y$.)

> **Example 2.1**
> Let set $X = \{1, 2, 4\}$ and set $Y = \{a, b, c, d\}$. We can define a function $f : X \to Y$ as $f(1) = a$, $f(2) = b$, and $f(4) = b$. An example of something that is NOT a function $f : X \to Y$ would be letting $f(1) = a$, $f(2) = b$, and $f(4) = g$, because $g \notin Y$ ($g$ is not an element of set $Y$).

We can also define sets in terms of the properties that their elements satisfy. Some sets even have special names and symbols. $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is the set of integers, and it is commonly denoted as $\mathbb{Z}$. $\{1, 2, 3, 4, 5\}$ can be written as $\{n \in \mathbb{Z} : 0 < n < 6\}$, meaning "elements of the set of integers such that they are greater than 0 and less than 6".

[1] This is an informal definition of a set. There are different types of axiomatic set theory which rely on different sets of axioms to define sets and their properties. One of the most common systems is the Zermelo-Fraenkel axioms, which form the basis of Zermelo-Fraenkel set theory. You can read the Wolfram page about the Zermelo-Frankel Axioms for more information: https://mathworld.wolfram.com/Zermelo-FraenkelAxioms.html.

## §2.2 Direct Product

The **Direct Product** of two sets $A$ and $B$ is the set of all ordered pairs $(a, b)$ where $a \in A$ and $b \in B$. Using set notation,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\} \tag{1}$$

It is important to note that $A \times B$ is NOT equal to $B \times A$, unless $A = B$.

**Example 2.2**

Let set $A = \{1, 2, 4\}$ and set $B = \{7, a, \text{hello}\}$. The direct product of $A$ and $B$ equals:

$$A \times B = \{(1, 7), (1, a), (1, \text{hello}), (2, 7), (2, a), (2, \text{hello}), (4, 7), (4, a), (4, \text{hello})\}$$

## §2.3 Binary Operation

A **Binary Operation** on a nonempty set is a map $f : A \times A \to A$ such that $f(a_1, a_2)$ is defined for every pair of elements $a_1, a_2 \in A$ and $f(a_1, a_2)$ is an element in $A$.

**Example 2.3**

Arithmetic operations such as addition and multiplication are binary operations on the set of integers. Division is not a binary operation on the set of integers because the result of the division of two integers $a, b$ is not always an integer for every pair of $a, b$. Division is a binary operation for the set of rationals excluding 0 because the division of two rational numbers always produces a rational number. (We exclude 0 because dividing by 0 causes problems).

But really, a binary operation can be anything we define it to be, as long as it takes 2 inputs and generates 1 output that is in the same set.[2]

**Example 2.4**

Let's define the binary operation $x \cdot y$. We can let $x \cdot y = a + 2b$, where $x, y \in \mathbb{Z}$ and $a$ is the tens digits of $x$ and $b$ is the sum of the digits in $y$ (and $+$ is addition as we know it). The result will always be an integer, so this function is a binary operation on the set of integers.

# §3 Groups

## §3.1 Definitions

A **group** is a set, $G$, together with a binary operation $(\cdot)$ such that the following are satisfied:

1. Closure: $x \cdot y \in G$ for all $x, y \in G$.
2. Associativity: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$.
3. Identity: For every $x \in G$, there exists an element $e \in G$ such that $e \cdot x = x \cdot e = x$.
4. Inverses: For every $x \in G$, there exists an element $y \in G$ such that $x \cdot y = y \cdot x = e$.

Note: We often denote groups simply by their sets, ex: $G$ instead of $(G, \cdot)$.

[2] About notation: there are many ways to represent a binary operation. One way is similar to defining a function with two inputs: $f(a, b)$, $g(a, b)$, $h(a, b)$, etc. Another way is by defining an operator between two elements: $a \cdot b$, $a \circ b$, $a \star b$, etc.

**Example 3.1**

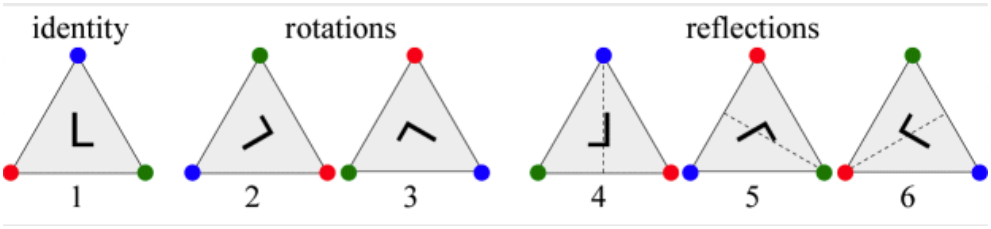
The set of integers under the binary operation of addition form a group. To show this, let's check that the four conditions are satisfied:

1. Closure: The sum of any two integers always produces another integer.
2. Associativity: Addition for integers satisfies the associative property.
3. Identity: 0 is the identity. For any integer $n$, $0 + n = n + 0 = n$.
4. Inverse: The negative version of any integer is its inverse. For an integer $n$, $n + (-n) = (-n) + n = 0$.

An **Abelian group** is a group, $G$, such that, for all $x, y \in G$, $x \cdot y = y \cdot x$. (Where $\cdot$ is the binary operation). Basically, an Abelian group is a group where the binary operation is commutative.

## §3.2 Triangle Transformations Activity

There are 6 symmetries of an equilateral triangle:




We call the first transformation $e$, because we often use $e$ to denote the identity. We can represent the remaining 5 transformations in terms of a counterclockwise rotation by 120 degrees, which we will call $\rho$, and a reflection across the vertical line of symmetry, which we will denote $\tau$. Here are the transformations from the diagram above represented in terms of $e$, $\rho$ and $\tau$:

| Transformation | Alternate representation |
|---|---|
| 1 | $e$ |
| 2 | $\rho$ |
| 3 | $\rho^2$ (this means apply $\rho$ twice) |
| 4 | $\tau$ |
| 5 | $\rho\tau$ |
| 6 | $\rho^2\tau$ |

It turns out that these 6 transformations form a group, with the composition of transformations as the binary operation. Let's check the four conditions:

1. Closure: The composition of two transformations is another transformation.
2. Associativity: A bit harder to check. You can play around with an equilateral triangle of your own to convince yourself[3].
3. Identity: We have an identity element, $e$, which when composed with any other transformation, results in that other transformation.

[3]Technically, it is inherited because the composition of mappings is an associative binary operation, and our composition of transformations is a composition of mappings. Proving that the composition of mappings is associative requires a bit more set theory than we covered, but if you're interested, here's a proof: https://proofwiki.org/wiki/Composition_of_Mappings_is_Associative.

4. Inverses: Intuitively, we must have inverses because we can undo every transformation sequentially. The inverse of $\rho$is $\rho^2$, and the inverse of $\tau$is itself. For a more rigorous justification, check the group multiplication table (below).

This group actually has a name: the Dihedral group of order 3, or $D_3$.

## §3.3 Group Multiplication Tables

These are sometimes known as Cayley tables. A group multiplication table is exactly what it sounds like; a table that shows what the result of each possible binary operation between two elements in the group. When constructing/reading a group multiplication table, the element in the row reference is applied first, then the element in the column reference. Here's the group multiplication table for $D_3$:

| | e | $\rho$ | $\rho^2$ | $\tau$ | $\rho\tau$ | $\rho^2\tau$ |
|---|---|---|---|---|---|---|
| e | e | $\rho$ | $\rho^2$ | $\tau$ | $\rho\tau$ | $\rho^2\tau$ |
| $\rho$ | $\rho$ | $\rho^2$ | e | $\rho\tau$ | $\rho^2\tau$ | $\tau$ |
| $\rho^2$ | $\rho^2$ | e | $\rho$ | $\rho^2\tau$ | $\tau$ | $\rho\tau$ |
| $\tau$ | $\tau$ | $\rho^2\tau$ | $\rho\tau$ | e | $\rho^2$ | $\rho$ |
| $\rho\tau$ | $\rho\tau$ | $\tau$ | $\rho^2\tau$ | $\rho$ | e | $\rho^2$ |
| $\rho^2\tau$ | $\rho^2\tau$ | $\rho\tau$ | $\tau$ | $\rho^2$ | $\rho$ | e |

So, instead of flipping and rotating paper equilateral triangles to figure out the result of a composition of transformations, we can calculate their result instead! For example, to find the result of $tau \circ \rho^2\tau$, see the box that corresponds to the $\rho^2\tau$ row and $\tau$ column in the group multiplication table. Note that we evaluate from right to left. Since each element represents a transformation, we can think of applying the binary operator as the composition of functions here, like how $(f \circ g)(x)$ means $f(g(x))$. For example, $\tau \circ \rho^2\tau$ means apply $\rho^2\tau$ first, then $\tau$.

**Example 3.2**

As a more complicated example, let's find the result for the following sequence of transformations: 5 - 2 - 4 - 3:

Written in terms of $\rho$and $\tau$, we have:

$$\rho^2 \circ \tau \circ \rho \circ \rho\tau$$

Now, let's evaluate!

$$\rho^2 \circ \tau \circ \rho \circ \rho\tau = \rho^2(\tau(\rho(\rho\tau)))$$

*Associativity means that we can ignore the parenthesis, though we still have to evaluate from right to left:*

$$\begin{aligned}\rho^2 \circ \tau \circ \rho \circ \rho\tau &= \rho^2(\tau(\tau)) \\ &= \rho^2(e) \\ &= \rho^2\end{aligned}$$

Thus, the result of the sequence of transformations 5 - 2 - 4 - 3, is equivalent to transformation 2.

# §4 Moduli

We define $a \mod b$ to be the remainder when $a$ is divided by $b$. We also say that $a \equiv x \mod b$ if $a$ divided by $b$ gives the same remainder as when $x$ is divided by b.

**Example 4.1**

$$5 \equiv 2 \mod 3$$
$$7 \equiv 27 \mod 4$$
$$6 \equiv 2 \mod 4$$

Note that moduli add, subtract, and multiply nicely! Namely,

$$(a \mod x) + (b \mod x) \equiv (a+b) \mod x \tag{2}$$
$$(a \mod x) - (b \mod x) \equiv (a-b) \mod x \tag{3}$$
$$(a \mod x) \cdot (b \mod x) \equiv (a \cdot b) \mod x \tag{4}$$

However, they do not divide nicely. Sad.

It turns out that division normally works because we have inverses. For example, division by 0 fails because 0 does not have a multiplicative inverse. If we are careful and make sure the mod we're using is prime (that is, the $n$ in $\mod n$ is prime), we can actually do division! From here forwards, $p$ will denote a prime.

**Theorem 4.2** (Properties of $(\mathbb{Z}/p\mathbb{Z})^*$)
We have unique inverses in $(\mathbb{Z}/p\mathbb{Z})^*$. Moreover, this is a group!

*Proof.* What is $(\mathbb{Z}/p\mathbb{Z})^*$? This is the set $\{1, \ldots, p-1\}$ combined with the binary operation of multiplication modulo $p$.

Let's first try to check if this is a group.

1. Closure: This is closed because $(a \mod x) \cdot (b \mod x) \equiv (a \cdot b) \mod x$.
2. Associativity: This "inherits" associativity from normal multiplication.
3. Identity: 1 is the identity.
4. Inverses: This is harder.

Now, we need to show that every element has an inverse. First, we'll introduce a new theorem:

**Theorem 4.3** (Pigeonhole Principle)
If we put $n+1$ objects into $n$ groups, at least one group must contain multiple objects

We'll give this theorem without proof, you can look up a proof online if you're curious, but the theorem is very intuitive. Basically, because the average number of objects per group is greater than 1, this implies that at least one group must have 2 objects.

Great, let's use that now! Consider any element $x$ in the group, we'll show it has an inverse. First, consider the set $S = \{x, x \cdot 2, \ldots, x \cdot (p-1)\}$. We'll first show that every element inside this set is distinct.

Assume for the sake of contradiction that two elements, $x \cdot a$ and $x \cdot b$ (with $a < b$, are equal. Then we have that $x \cdot a - x \cdot b = x \cdot (a-b) = 0$. Notice that this means that $p$ must divide $x \cdot (a-b)$. But $p$ is prime! So this means that either $p$ divides $x$, or $p$ divides $a-b$. But $p$ cannot divide $x$, because $x$ belongs

in the set $S$, so $0 < x < p$. Also, $p$ cannot divide $a - b$, because $0 < a < b < p$. Therefore, we have a contradiction.

Now, we can conclude that all elements within $S$ are different. Assume for the sake of contradiction that none of these values are 1, the identity. If this were true, then we would have $p - 1$ "objects" inside the $p - 2$ values, or "groups." But by the Pigeonhole principle, we have a contradiction, because we just proved each of these values are unique! Therefore, exactly one of the values inside $S$ is 1, so we have (unique) inverses for every element inside $(\mathbb{Z}/p\mathbb{Z})^*$.

Now, we've proved all four properties, so we conclude $(\mathbb{Z}/p\mathbb{Z})^*$ is a group! Yay! □

Great, now we'll move onto Wilson's theorem!

**Definition 4.4** (Factorial) — x!, or "$x$ factorial", is $x \cdot (x-1) \cdots 2 \cdot 1$. For example, $3! = 3 \cdot 2 \cdot 1 = 6$.

**Theorem 4.5** (Wilson's Theorem)
$(p-1)! \equiv -1 \mod p$

*Proof.* First, we note that $1! = 1 \equiv -1 \mod 2$. From here, we assume $p$ is an odd prime, since 2 is the only even prime.

**Claim 4.6** — The only two elements which are their own inverse are 1 and $p - 1$.

Why? Because any element $x$ which is its own inverse satisfies $x^2 \equiv 1 \mod p$, so $x^2 - 1 \equiv 0 \mod p$. Because $p$ is a prime, $p$ either divides $x + 1$ or $x - 1$, which immediately implies the claim

Now, take any element $x$ which has an inverse $x^{-1} \neq x$. We proved earlier that inverses in $(\mathbb{Z}/p\mathbb{Z})^*$ are unique (in fact, one of the exercises this week is to prove that in general, inverses are unique in all groups). Therefore, we can divide all elements which are not 1 or $p - 1$ into pairs, such that every element in the pair is the other element's inverse.

Here is the cool part. Consider $(p-1)! = (p-1) \cdot (p-2) \cdots 2 \cdot 1$. Because multiplication is commutative (our group is abelian!) we can rearrange all the numbers here that are not 1 or $p - 1$ into these pairs that we just created, and the product of every pair is just going to be $1 \mod p$! Now, $(p-1)! \equiv 1 \cdot p - 1 \equiv -1 \mod p$! Boom! □

Ok, we're going to finish off this week's material with a couple of definitions.

**Definition 4.7** (Order of a Group) — The **order of a group** $G$ is the number of elements in a group. This is also known as the **cardinality** of a group, and can be denoted as $ord(G)$ or $|G|$.

**Definition 4.8** (Order of an Element in a Finite Group) — The **order of an element $x$ in a finite group $G$** is the minimum exponent $n$ such that $x^n = e$. This can be denoted as $ord(x)$

It turns out the set $\{e, x, x^2, \ldots, x^{ord(x)-1}\}$ is a group, and it's called $\langle x \rangle$ (actually it's a subgroup! We'll talk about that more next week). You can prove this for fun! This actually implies that $ord(x) = | < x > |$.

Wait, but why is it true that the order of an element in a finite group always exists? (Bonus material)

**Theorem 4.9** (Orders in a Finite Group)
Every element in a finite group has an order.

*Proof.* Take an element $x$ in a group $G$. Define $n = |G|$. Consider the set $S = \{e = x^0, x, x^2, \ldots, x^n\}$. Because there are $n+1$ elements inside this set $S$, and only $n$ possible values, two of these elements must be the same by the Pigeonhole Principle. Assume these elements are $x^a$, $x^b$ for $a < b$. Then $x^a = x^b$ implies $\left(x^{-1}\right)^a \cdot x^a = \left(x^{-1}\right)^a \cdot x^b = x^{b-a} = e$. Because $0 < b - a < b < n$, we have that $e$ must be inside $S$, and inside $G$, which finishes! □

# §5 Group Homomorphisms

## §5.1 A Brief Aside for Proofs

Let's try a proof first because it's **important**.

**Theorem 5.1** (Identity is Unique)
Every group has a unique identity element.

*Proof.* Suppose that $e_1, e_2$ are both identity elements of the same group. Then,

$$e_1 = e_1 e_2 = e_2 \tag{5}$$
$$e_1 = e_2 \tag{6}$$

Thus $e_1, e_2$ must be the same element. □

## §5.2 Back to Homomorphisms

**Definition 5.2** (Group Homomorphism) — Let $(G, \diamond)$ and $(H, \star)$ be groups. A **group homomorphism** from $G$ to $H$ is a function $f : G \to H$ such that, for all $g_1, g_2 \in G$, we have $f(g_1 \diamond g_2) = f(g_1) \star f(g_2)$.

**Example 5.3**
The function $p : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ is a group homomorphism, where $p(x) = e^x$ for all $x \in (\mathbb{R}, +)$.

*Solution.* Consider $x, y \in (\mathbb{R}, +)$. To show that $p$ is a homomorphism, we must show that $p(x+y) = p(x) \cdot p(y)$:

$$p(x+y) = e^{(x+y)} \tag{7}$$
$$= e^x \cdot e^y = p(x) \cdot p(y) \tag{8}$$

□

**Example 5.4**
The function $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ is a group homomorphism, where $f(x) = 5x$ for all $x \in (\mathbb{Z}, +)$.

*Solution.* Consider $x, y \in (\mathbb{Z}, +)$. To show that $f$ is a homomorphism, we must show that $f(x+y) = f(x) + f(y)$:

$$f(x+y) = 5(x+y) \tag{9}$$
$$= 5x + 5y = f(x) + f(y) \tag{10}$$

□

# §6 Kernels and Images

## §6.1 Kernels

**Definition 6.1** (Kernel) — Let $f : G \to H$ be a group homomorphism. The **kernel** of $f$ is defined as $\text{Ker}(f) = \{g \in G : f(g) = e_H\}$.

More informally, the kernel is the set of all elements in $G$ that get sent to the identity element in $H$.

**Example 6.2**

Consider the group homomorphism $p : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$, where $p(x) = e^x$ for all $x \in (\mathbb{R}, +)$. What is $\text{Ker}(p)$?

*Solution.* The identity element of $(\mathbb{R}^+, \cdot)$ is 1, so $\text{Ker}(p)$ consists of all $x \in (\mathbb{R}, +)$ such that $p(x) = e^x = 1$. The only solution is $x = 0$, thus $\text{Ker}(p) = \{0\}$. □

Let's use $\mathbb{Z}$ to denote the integers under the binary operation of addition.

**Example 6.3**

Consider the group homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, where $\phi(a, b) = a + b$ for all $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. What is $\text{Ker}(\phi)$?

*Solution.* The identity element of $\mathbb{Z}$ is 0, so $\text{Ker}(\phi)$ consists of all $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ such that $\phi(a, b) = a + b = 0$. This condition is satisfied whenever $a = -b$, thus $\text{Ker}(\phi) = \{(a, -a) \in \mathbb{Z} \times \mathbb{Z}\}$. □

## §6.2 Images

**Definition 6.4** (Image) — Let $f : G \to H$ be a group homomorphism. The **image** of $f$ is defined as $\text{Im}(f) = \{h \in H : f(g) = h \text{ for some } g \in G\}$.

More informally, the image is the set of all elements in $H$ that get mapped to by $f$.

**Example 6.5**

Consider the group homomorphism $f : \mathbb{Z} \to \mathbb{Z}$, where $f(x) = 5x$ for all $x \in \mathbb{Z}$. What is $\text{Im}(f)$?

*Solution.* $\text{Im}(f) = \{n \in \mathbb{Z} : 5 \mid n\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$. □

# §7 Homomorphisms Proofs

## §7.1 Identity

**Theorem 7.1** (Homomorphisms Preserve Identity)

Let $(G, \diamond)$ and $(H, \star)$ be groups, and let $f : G \to H$ be a group homomorphism. Then, $f(e_G) = e_H$, where $e_G$ is the identity in $G$ and $e_H$ is the identity in $H$.

*Proof.* Since $f(e_G)$ must be an element of $H$ and inverses are unique,

$$f(e_G) \star [f(e_G)]^{-1} = e_H \tag{11}$$
$$f(e_G \diamond e_G) \star [f(e_G)]^{-1} = e_H \tag{12}$$
$$f(e_G) \star f(e_G) \star [f(e_G)]^{-1} = e_H \tag{13}$$
$$f(e_G) = e_H \tag{14}$$

□

**Example 7.2**

Recall the group homomorphism $f : \mathbb{Z} \to \mathbb{Z}$, where $f(x) = 5x$ for all $x \in \mathbb{Z}$.

*Solution.* The identity element in $\mathbb{Z}$ is 0. $f(0) = 5(0) = 0$, which is the identity element in $\mathbb{Z}$. □

**Example 7.3**

Recall the group homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, where $\phi(a, b) = a + b$ for all $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

*Solution.* The identity element in $\mathbb{Z} \times \mathbb{Z}$ is $(0, 0)$. $\phi(0, 0) = 0 + 0 = 0$, which is the identity element in $\mathbb{Z}$. □

**Example 7.4**

Recall the group homomorphism $p : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ , where $p(x) = e^x$ for all $x \in (\mathbb{R}, +)$.

*Solution.* The identity element in $(\mathbb{R}, +)$ is 0. $p(0) = e^0 = 1$, which is the identity element in $(\mathbb{R}^+, \cdot)$. □

## §7.2 Inverses

**Theorem 7.5** (Homomorphisms Preserve Inverses)

Let $(G, \diamond)$ and $(H, \star)$ be groups, and let $f : G \to H$ be a group homomorphism. Then, $f(g^{-1}) = [f(g)]^{-1}$, for all $g \in G$.

*Proof.* Let's mainpulate $e_H$:

$$e_H = f(e_G) \tag{15}$$
$$e_H = f(g \diamond g^{-1}) \tag{16}$$
$$e_H = f(g) \star f(g^{-1}) \tag{17}$$

multiply both sides by $[f(g)]^{-1}$:

$$[f(g)]^{-1} \star e_H = [f(g)]^{-1} \star f(g) \star f(g^{-1}) \tag{18}$$
$$[f(g)]^{-1} = f(g^{-1}) \tag{19}$$

□

**Example 7.6**

Recall the group homomorphism $f : \mathbb{Z} \to \mathbb{Z}$, where $f(x) = 5x$ for all $x \in \mathbb{Z}$.

*Solution.* Let's split it up:

- **Finding the inverse first, then applying the homomorphism**: Consider some element $x \in \mathbb{Z}$. The inverse of $x$ is $-x$. $f(-x) = 5(-x) = -5x$.
- **Applying the homomorphism first, then finding the inverse**: Let's find the inverse of $f(x)$. $f(x) = 5x$, and the inverse is some element $y$ such that $f(x) + y = 0$. $y = 5x$, so $[f(x)]^{-1} = 5x$.

Thus, $f(-x) = -5x = [f(x)]^{-1}$. □

**Example 7.7**

Recall the group homomorphism $p : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ , where $p(x) = e^x$ for all $x \in (\mathbb{R}, +)$.

*Solution.* Let's split it up:

- **Finding the inverse first, then applying the homomorphism**: Consider some $x \in (\mathbb{R}, +)$. The inverse of $x$ is $-x$, as $x + (-x) = 0$. $p(-x) = e^{-x}$.
- **Applying the homomorphism first, then finding the inverse**: $p(x) = e^x$. The inverse of $e^x$ is the element that, when multiplied with $e^x$, equals 1, the identity of $(\mathbb{R}^+, \cdot)$. $[p(x)]^{-1} = e^{-x}$.

Thus, $p(x^{-1}) = e^{-x} = [p(x)]^{-1}$. □

## §8 Subgroups and Cosets

**Definition 8.1** (Subgroup) — A **subgroup** $H$ of a group $G$ is a group that consists of a subset of $G$ combined with the same binary operation (so it has to obey closure, associativity, inverse, and identity properties as well).

**Example 8.2**

The x-axis of $\mathbb{R}^2$ is a subgroup, because it's clearly closed under addition, addition is associative, inverses clearly exist, the origin is the identity.

**Example 8.3**

$\mathbb{Z}/n\mathbb{Z}$ (the integers mod $n$) is a subgroup of $\mathbb{Z}$ (the integers).

**Definition 8.4** (Coset) — Take a subgroup $H$ of an abelian group $G$. Then the **cosets** of $H$ are defined as the sets $gH = \{gh : h \in H\}$ (read: the set of all possible products $gh$, where $h$ is an element of $H$), where $g$ can take any value in $G$.

**Example 8.5**

The set of numbers that are congruent to 1 mod 5 are a coset of the group of the multiples of 5 under addition, when we let $g = 1$ in our definition above.

**Example 8.6**

Each horizontal line would be a coset, if $H$ is the x-axis in the group $G = \mathbb{R}^2$.

## §8.1 Properties of Subgroups

1. The identity of a subgroup is equivalent to the identity of the whole group. This is true because every group has a unique identity.
2. A group is a subgroup of itself.
3. The group consisting only of the identity is also a subgroup of any group.
4. In abelian groups (groups where the binary operation is commutative), there always exists a homomorphism from the group to each subgroup.

We won't rigorously prove the last fact, but we'll talk about it more later. Consider the homomorphism from $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, where $f$ is taking a number mod $n$ to be an example.

## §8.2 Property of Cosets

**Theorem 8.7** (# of Elements of Cosets and Subgroups)

Each coset has the same number of elements as its subgroup, if $H$ is a finite group.

*Proof.* Note that if $gh_1 = gh_2$, then $g^{-1}gh_1 = g^{-1}gh_2$ which implies $h_1 = h_2$, so every element in $H$ creates a different element in the coset. □

## §8.3 Applications

**Example 8.8**

Let's say, I have to multiply two really, really large numbers... and Emma conveniently has a supercomputer! So I want to give Emma my two numbers to multiply, but I don't want her to know my numbers (let's say, one of them is my SSN and the other is my password to all of my accounts). What do I do?

*Solution.* Use homomorphic functions. If I have two positive integers, say $p, q$, then what we need to do is create some homomorphism $f$ from $\mathbb{Z}$ to some other group $G$ such that $f(pq) = f(p)f(q)$, which is invertable.

So I give Emma $f(p)$ and $f(q)$, and tell her to combine these two values in the group $G$ using her supercomputer. She then gives me $f(p)f(q) = f(pq)$, and I invert $f$ to find $pq$. If Emma doesn't know what $f$ is, or doesn't know how to invert it, my inputs are still secret! □

Where is homomorphic encryption used?

1. Storing information online, or in the Cloud
2. Elections
3. Secure data (say, biomedical data or DNA or something that's very personal and private)

# §9 Number Theory

Let's start by thinking of this without group theory.

## §9.1 Fermat's Little Theorem

**Theorem 9.1** (Fermat's Little Theorem)
If $a$ is a positive integer, and $p$ is a prime number, then $a^p \equiv a \mod p$

**Example 9.2**
For any $p$, $0^p \equiv 0 \mod p$

**Example 9.3**
For $a = 2, p = 5$,

$$\begin{aligned} 2^5 &\equiv 32 \mod 5 \\ &\equiv 2 \mod 5 \end{aligned}$$

For the rest of this section, $p$ will denote *primes*.

## §9.2 Combinatorial Proof

**Definition 9.4** (Double Counting) — **Double counting** is the method of counting the same thing in two different ways.

Let's use this trick!

- Consider a circular necklace with 5 beads on it. If we can color each bead one of two colors (R or G, for short), there are $2^5$ possible ways to color the necklace.
- Now, how many ways are there to color this necklace, if we don't allow the possibility of all beads being the same color? $2^5 - 2$.
- Here are all possible colorings (not including single-color necklaces):

  `RRRRG, RRRGR, RRGRR, RGRRR, GRRRR`
  `RRRGG, RRGGR, RGGRR, GGRRR, GRRRG`
  `RRGRG, RGRGR, GRGRR, RGRRG, GRRGR`
  `RRGGG, RGGGR, GGGRR, GGRRG, GRRGG`
  `RGRGG, GRGGR, RGGRG, GGRGR, GRGRG`
  `RGGGG, GGGGR, GGGRG, GGRGG, GRGGG`

  Wow, we can divide the set of possible colorings into groups of 5... coincidence?
- Nope!

Notice that each coloring is part of a **class** of colorings, where each "class" has size 5. We can rotate each coloring to produce all the other colorings in the same class, and there are 4 ways to rotate any coloring (shift by 1, shift by 2,... shift by 4), giving that each class has size 5.

Because 5 is prime, there is no way to shift a coloring by less than 5 and obtain the same coloring. If we could, that would be bad, because we would be counting some colorings multiple times (it's why we need 5 to be prime). For example, if we had colorings of length 4, `RGRG` can be shifted twice to form itself.

This shows that we can **partition** all these colorings into classes, so we must have that 5 divides the total number of possible colorings!

- In other words, $5 \mid 2^5 - 2$, or $2^5 \equiv 2 \mod 5$.

  Of course, 2 and 5 are not special! In particular, assume we're trying to color a necklace of length $p$ with $a$ colors. Then there will be $a$ colorings we need to subtract out (because they'll only be one color) and so we'll obtain $a^p \equiv a \mod p$!

### §9.2.1 NT Proof

- Define the set $S := \{1, 2, \ldots, p-1\}$. Remember, this is a group under multiplication!

  Now, take some number $a$. Look at the set $aS = \{a, 2a, \ldots, a(p-1)\}$. Assume that $a \not\equiv 0 \mod p$ (if $a \equiv 0 \mod p$ then trivially $a^p \equiv 0 \mod p \equiv a \mod p$). Then $aS = S$

  **Lemma 9.5**
  $aS = S$

  *Proof.* If we have two elements $ax \equiv ay \mod p$, then $a(x-y) \equiv 0 \mod p$, which is impossible. Then all elements must be distinct, and Pigeonhole implies the conclusion. □

- Now, we multiply all the elements inside $aS$.

$$a \cdot a(2) \cdot a(3) \cdots a(p-1) = 1 \cdot 2 \cdot 3 \cdots (p-1)$$

  because $aS = S$, so the product of all the elements in each set modulo $p$ must also be the same.

  But because $(\mathbb{Z}/p\mathbb{Z})^*$ is an abelian group, we can rearrange this to:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)!$$

  But we can cancel out the $(p-1)!$ (in fact, $(p-1)! \equiv -1 \mod p$ by Wilson's theorem), which gives us $a^{p-1} \equiv 1 \mod p$.

  Multiplying both sides by $a$ gives $a^p \equiv a \mod p$.

### §9.2.2 Euler's Totient Theorem

The natural generalization of FLT is Euler's Totient Theorem.

**Definition 9.6 ($\phi$)** — $\phi(x)$ ("phi of x") is the number of positive integers $n$ smaller than $x$ that are relatively prime to $x$ (so $gcd(x, n) = 1$ for each $n$).

Some examples:

1. $\phi(6) = 2$, because only 1 and 5 are relatively prime to 6.

2. $\phi(32) = 16$, because all odd numbers $1, 3, \ldots, 31$ are relatively prime to 32.
3. $\phi(p) = p - 1$ for any prime $p$, because all numbers $1 \ldots p - 1$ are relatively prime to $p$.

It turns out that we can create a formula to calculate the totient function. We're not going to prove this, but if you're curious, you can Google it online. It uses something called the Chinese Remainder Theorem.

**Theorem 9.7** (Totient Formula)
If $x = p_1^{q_1} p_2^{q_2} \cdots p_n^{q_n}$ for primes $p_1, \ldots p_n$, then $\phi(x) = x \cdot \prod_{i=1}^{n} (1 - \frac{1}{p_i})$

Some examples:

1. $6 = 2^1 \cdot 3^1$, so $\phi(6) = 6 \cdot \frac{1}{2} \cdot \frac{2}{3} = 2$.
2. $p = p^1$, so $\phi(p) = p \cdot \frac{p-1}{p} = p - 1$.
3. $1000 = 2^3 \cdot 5^3$, so $\phi(1000) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400$.

Now for what everyone's been waiting for:

**Theorem 9.8** (Euler's Totient Theorem)
If $a$ and $n$ are relatively prime, $a^{\phi(n)} \equiv 1 \mod n$.

You can try proving it as a problem, using a method very similar to the Number Theory proof presented earlier for Fermat's Little Theorem.

## §9.3 Lagrange's Theorem

**Theorem 9.9** (Lagrange)
Let $G$ be a finite group and let $H$ be a subgroup of $G$. Then the order of $H$ divides the order of $G$.

**Example 9.10**
Consider the symmetries of a triangle $D_3 = \{e, \rho, \rho^2, \tau, \rho\tau, \rho^2\tau\}$.
The subgroups of $D_3$ are: $\{e\}, \{e, \tau\}, \{e, \rho\tau\}, \{e, \rho^2\tau\}, \{e, \rho, \rho^2\}, \{e, \rho, \rho^2, \tau, \rho\tau, \rho^2\tau\}$

We need three lemmas to prove Lagrange. Let's start:

**Lemma 9.11** (First Lemma)
Let $G$ be a group and $H$ be a subgroup of $G$. For any two cosets $g_1H$ and $g_2H$ (where $g_1, g_2 \in G$), either $g_1H = g_2H$, or $g_1H \cap g_2H = \emptyset$.

In other words, any two cosets of $H$ are either equal or disjoint (two sets are said to be disjoint sets if they have no element in common).

*Proof.* Suppose the cosets $g_1H$ and $g_2H$ are not disjoint. Then there is some element $x$ that belongs to both cosets, so $x = g_1 \circ h_1 = g_2 \circ h_2$ for some $h_1, h_2 \in H$ ($g_1h_1$ is an element of $g_1H$ and $g_2h_2$ is an element of $g_2H$). We can write $g_1$ in terms of $g_2$: $g_1 = g_2h_2h_1^{-1}$. Now, let's show that every element in $g_1H$ is also an element of $g_2H$. Consider $g_1h \in g_1H$.

$$g_1h = (g_2h_2h_1^{-1})h = g_2(h_2h_1^{-1}h) \tag{20}$$

Since we can represent $g_1h$ in the form $g_2h'$ (for $h' \in H$), we know that $g_1h$ must be an element of $g_2H$. As we can repeat this for any element $g_1h \in g_1H$, we know that $g_1H \subseteq g_2H$.

But, there's really no difference between $g_1H$ and $g_2H$, so our argument still holds if we swap $g_1$ and $g_2$ and repeat the proof above. This tells us that $g_2H \subseteq g_1H$. Putting this together, we conclude that if $g_1H$ and $g_2H$ are not disjoint, then they are equal. □

**Lemma 9.12** (Second Lemma)

Let $G$ be a group and $H$ be a subgroup of $G$. Then any two cosets of $H$ contain the same number of elements.

*Proof.* Bijection – each element of one set is paired with exactly one element of the other set, and each element of the other set is paired with exactly one element of the first set.

We know that no element $g_1h \in g_1H$ can have multiple representations. That is, $g_1h \neq g_1h'$ for any $h \neq h' \in H$.

To show that any two cosets $g_1H$ and $g_2H$ have the same number of elements, we will set up a bijection between them. We can define a function $f : g_1H \to g_2H$ by $f(g_1h) = g_2h$ for $h \in H$. Since every element in $g_1H$ only appears once in $g_1H$, we know that $f$ pairs every element in $g_1H$ with one element in $g_2H$.

This same reasoning still applies if we set up a function $g : g_2H \to g_1H$, so $g$ pairs every element in $g_2H$ with one element in $g_1H$. Thus, we've set up a bijection between $g_1H$ and $g_2H$, so we've shown that any two cosets of $H$ have the same size. □

**Lemma 9.13** (Third Lemma)

Consider a group $G$ with a subgroup $H$. $G$ is the union of the cosets of $H$.

*Proof.* Since $H$ is a subgroup of $G$, we know that $e \in H$. It follows that $g \circ e = g \in gH$, so every element $g \in G$ is contained within some coset of $H$.

Just to make sure, let's verify that the cosets don't contain any additional elements:

Every element $h \in H$ is also an element of $G$ (by definition of subgroup). From our definition of group, $g_1 \circ g_2 \in G$ for any $g_1, g_2 \in G$. Since all of the elements we're composing to generate cosets are all elements of $G$, we know that we can't generate an element that isn't in $G$. □

**Example 9.14**

Consider the group $(\mathbb{Z}/8\mathbb{Z}, +) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and the subgroup $H = \{0, 2, 4, 6\}$. Let's find the cosets of $H$:

$$0 + H = \{0, 2, 4, 6\} \tag{21}$$
$$1 + H = \{1, 3, 5, 7\} \tag{22}$$
$$2 + H = \{2, 4, 6, 0\} \tag{23}$$
$$3 + H = \{3, 5, 7, 1\} \tag{24}$$
$$4 + H = \{4, 6, 0, 2\} \tag{25}$$
$$5 + H = \{5, 7, 1, 3\} \tag{26}$$
$$6 + H = \{6, 0, 2, 4\} \tag{27}$$
$$7 + H = \{7, 1, 3, 5\} \tag{28}$$

As you can see, there are 2 distinct cosets of $H$, and the union of the elements in all of the cosets is precisely the elements of $G$.

And now we can prove Lagrange.

*Proof.* By the First Lemma, cosets are disjoint. By the Second Lemma, all cosets have the same size. By the Third Lemma we can think of $G$ as the union of all cosets $gH$. So, the total number of elements in the union of all cosets equals the number of elements in each coset multiplied by the number of cosets. The number of elements in each coset is equal to the order of $H$, thus $|H|$ times the number of cosets (an integer) equals the total number of elements in $G$. □

**Corollary 9.15**

The order of any element of $G$ divides the order of $G$.

*Proof.* Recall that we can generate a subgroup using any element $g \in G$. This subgroup is of the form $\{e, g, g^2, \ldots, g^{\text{ord}\,(g)-1}\}$. The number of elements in the subgroup is $\text{ord}(g)$, so the order of the subgroup is equal to $\text{ord}(g)$. So, by Lagrange's Theorem, $\text{ord}(g)$ must divide the order of $G$. □

## §9.4 Back to FLT

With a bit of NT group theory under our belt, let's finally prove Fermat's Little Theorem with group theory.

*Proof.* Recall the group $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, (p-1)\}$. We can represent $a$ as some element of $(\mathbb{Z}/p\mathbb{Z})^\times$: $a \equiv b \mod p$. By the corollary above, $\text{ord}\,(b)$ divides $|(\mathbb{Z}/p\mathbb{Z})| = p - 1$, so $b^{p-1} = e$.

This means $a^{p-1} \equiv 1 \mod p$. Multiplying both sides by $a$, we get $a^p \equiv a \mod p$. □

## §9.5 Back to Euler's

Let's try Euler's Totient Theorem as well.

**Proposition 9.16**

An integer $a$ has an inverse modulo $n$ if and only if $\gcd(a, n) = 1$.

*Proof.* This is more of a sketch, fill in the details on your own:

- $\gcd(a,n) = 1$ **implies inverses**: If $\gcd(a,n) = 1$, then we can find some integers $b$ and $c$ such that $ab - cn = 1$ (this is a consequence of Bézout's identity). Since $cn + 1 \equiv 1 \mod n$, we have $ab \equiv 1 \mod n$.
- **inverses imply** $\gcd(a,n) = 1$: If $a$ has an inverse, then there exists some number $b$ such that $ab \equiv 1 \mod n$. This means $ab = 1 + cn$ for some integer $c$. Rearranging, we find $ab - cn = 1$. Bézout's identity implies that $\gcd(a,n) = 1$.

□

**Proposition 9.17**

Consider the set of all integers less than $n$ which have inverses modulo $n$. This forms a group under multiplication.

This group is commonly denoted as $(\mathbb{Z}/n\mathbb{Z})^\times$.

*Proof.* We must prove four things:

1. **closure**: The product of two numbers that are relatively prime to $n$ will result in another number that is also relatively prime to $n$.
2. **associativity**: The binary operation is multiplication modulo $n$, which is associative.
3. **identity**: 1 is the identity because $1 \cdot n = n \cdot 1 = n$ for any number $n$. (we know that 1 1 must be in the set because 1 is relatively prime to every number).
4. **inverses**: We defined our group as the set of all integers that have inverses modulo $n$.

□

Alright, we're reading to prove Euler's Totient Theorem.

*Proof.* Recall the above corollary from our proof of Lagrange's Theorem: the order of any element of $G$ divides the order of $G$.

- Let's consider the group $(\mathbb{Z}/n\mathbb{Z})^\times$. By this corollary , $\operatorname{ord} g$ divides $|(\mathbb{Z}/n\mathbb{Z})^\times|$ for any element $g \in (\mathbb{Z}/n\mathbb{Z})^\times$.
- Since $g^{\operatorname{ord} g} \equiv 1 \mod n$ and $\operatorname{ord} g$ is a factor of $|(\mathbb{Z}/n\mathbb{Z})^\times|$, we know that $g^{|(\mathbb{Z}/n\mathbb{Z})^\times|} \equiv 1 \mod n$.
- But we know that $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, so we have $g^{\phi(n)} \equiv 1 \mod n$.

We can represent any integer that is relatively prime to $n$ as an element of $(\mathbb{Z}/n\mathbb{Z})^\times$ simply by considering its value modulo $n$, so Euler's Totient Theorem works for any integer $a$. □

## §9.6 More on FLT

Sometimes, $a^p \equiv a \mod p$ works even when $p$ is not prime!

**Theorem 9.18** (Fermat Primality Test)

$a^p \equiv a \mod p$ is unlikely to hold for a random $a$ if $p$ is composite.

**Definition 9.19** (Fermat Liar) — A **Fermat liar** is any $a$ such that $a^{n-1} \equiv 1 \mod n$ where $n$ is composite.

**Definition 9.20** (Fermat Witness) — A **Fermat witness** is any $a$ such that $a^{n-1} \not\equiv 1 \mod n$ where $n$ is composite.

**Definition 9.21** (Carmichael Number) — A **Carmichael number** is any composite number $n$ which satisfies $b^n \equiv b \mod n$ for all integers $b$ which are relatively prime to $n$.

The smallest Carmichael number is 561. We won't use this much – it is just for the interested reader.

# §10 Non-Abelian Groups

**Definition 10.1** (Abelian Group) — An **abelian group** $G$ is a group where the binary operation is commutative. That is, for all $a, b \in G$, we have

$$ab = ba$$

**Example 10.2**

The set of integers under addition is abelian, because addition is commutative.

Everyone can see non-abelian groups coming:

**Definition 10.3** (Non-Abelian Groups) — An **nonabelian group** $G$ is a group where the binary operation is *not* commutative. That is, there exist some $a, b \in G$, such that

$$ab \neq ba$$

**Example 10.4**

The group of transformations of an equilateral triangle, or $D_3$, is nonabelian.

| | e | $\rho$ | $\rho^2$ | $\tau$ | $\rho\tau$ | $\rho^2\tau$ |
|---|---|---|---|---|---|---|
| e | e | $\rho$ | $\rho^2$ | $\tau$ | $\rho\tau$ | $\rho^2\tau$ |
| $\rho$ | $\rho$ | $\rho^2$ | e | $\rho\tau$ | $\rho^2\tau$ | $\tau$ |
| $\rho^2$ | $\rho^2$ | e | $\rho$ | $\rho^2\tau$ | $\tau$ | $\rho\tau$ |
| $\tau$ | $\tau$ | $\rho^2\tau$ | $\rho\tau$ | e | $\rho^2$ | $\rho$ |
| $\rho\tau$ | $\rho\tau$ | $\tau$ | $\rho^2\tau$ | $\rho$ | e | $\rho^2$ |
| $\rho^2\tau$ | $\rho^2\tau$ | $\rho\tau$ | $\tau$ | $\rho^2$ | $\rho$ | e |

Remember, **the multiplication tables of abelian groups are symmetric about the main diagonal, while the multiplication tables of nonabelian groups are not**!

## §10.1 A Difference Between Abelian and Non-abelian

We've already defined cosets for abelian groups. In particular, left and right multiplication are the same. But for nonabelian groups, right and left multiplication are different! So now, we have right and left cosets.

**Definition 10.5** (Left/Right Cosets) — Take a subgroup $H$ of an nonabelian group $G$.

1. The **left cosets** of $H$ are defined as the sets $gH = \{gh : h \in H\}$ (read: the set of all possible products $gh$, where $h$ is an element of $H$), where $g$ can take any value in $G$.
2. The **right cosets** of $H$ are defined as the sets $Hg = \{hg : h \in H\}$.

## §10.2 Normal Subgroups

**Definition 10.6** (Normal Subgroup) — Here are three definitions of what a **normal subgroup** $H$ of $G$ is:

1. The sets of right and left cosets of $H$ are the same
2. Consider a group $G$ with normal subgroup $N$. For any element $g \in G, n \in N$ we have $gng^{-1} \in N$.
3. A group is a normal subgroup if and only if it is the kernel of a homomorphism from $G \to G'$, for some $G'$.

**Example 10.7**

All subgroups of abelian groups are normal. (Why?)

**Example 10.8**

The whole group $G$ and the trivial subgroup $\{e\}$ are both normal subgroups of $G$.

**Example 10.9**

The subgroup $\{e, \rho, \rho^2\}$ of $D_3$ is normal. (Why?)

Let's try to see why these definitions are the same.

First, let's assume the second definition, and try to see why the first definition holds. If we always have $gng^{-1} \in N$ for all $g \in G, n \in N$ then what does this mean?

Rewriting this, we have $gng^{-1} = n'$, for some $n' \in N$. Then $gn = n'g$. So consider the set of elements "outputted" on the left side... it's the left coset $gN$! Similarly, the right hand side is the right coset $Ng$!

Now, let's assume the first definition, and try to see why the second definition holds. We assume the set of right and left cosets are the same.

Every element only belongs to one left coset, and one right coset (remember, cosets partition the group.) So what this means is that, for any element $g$, we have $gn = n'g$, for some $n, n' \in N$. Multiplying by $g^{-1}$ on the right, we have $gng^{-1} = n'$. That's exactly what the second definition says!

## §10.3 Quotient Groups

**Definition 10.10** (Quotient Group) — Let $G$ be a group and let $N$ be a normal subgroup of $G$. Then $G/N = \{gN : g \in G\}$ is called the **quotient group** of $N$ in $G$.

In essence, the quotient group is the set of all of the (left) cosets of $H$.

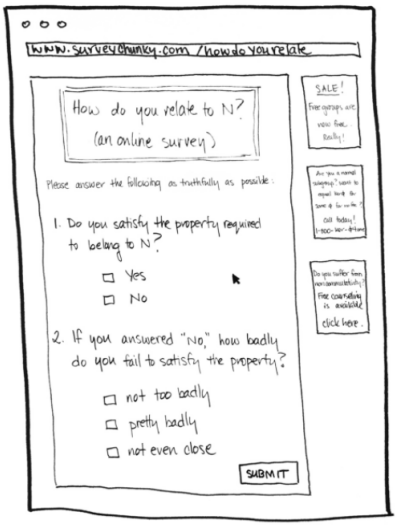
Okay, we have a set, but we also need a binary operation that can be performed between the cosets: consider two cosets $aN$ and $bN$ in $G/N$. We define the composition of $aN$ and $bN$ as $(aN)(bN) = (ab)N$, where $(ab)N = \{abn : n \in N\}$.

$G/N$ satisfies the group axioms:

1. Closure: $(aN)(bN) = (ab)N$, and $(ab)N$ is also a coset of $N$.
2. Associativity: $\big((aN)(bN)\big)(cN) = (abc)N = (aN)\big((bN)(cN)\big)$.
3. Identity: $eN$ (or just $N$) is the identity.
4. Inverses: every element $g \in G$ has an inverse, so for every coset $gN$, there exists a coset $g^{-1}N$ such that $(gN)(g^{-1}N) = (gg^{-1})N = eN$.

## §10.4 A More Intuitive Explanation of Quotient Groups

In other words, **storytime**. The following are copied from a blog post by Tai-Danae Bradley on her blog Math3ma.




**Mathematician enters room full of elements of $G$ chatting quietly amongst themselves** Hi folks. How are we today? Doin' well? Great. Listen, would those of you who answered "yes" to question #1 please raise your hand? Fantastic, hi there. Thank you. Now, if you would, please huddle together in a single pile. Yes, just like that. You're doin' fine, folks, just fine. Alright, from now on we will refer to you collectively as "$N$" or - on a good day - we might also call you "the trivial coset." But we no longer care about y'all as individuals. Sorry. You'll get used to it.

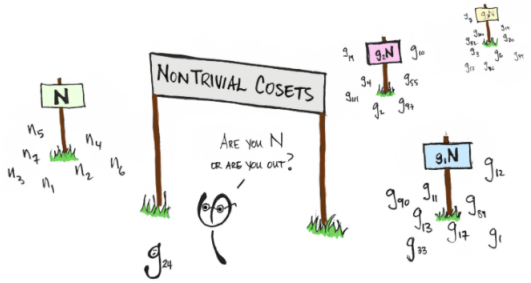
**Mathematician turns her attention to the folks not in $N$** Hey there, everyone. Would you please raise your hand if you selected "not too badly" for question #2? Great, how you folks doin'? Good. Look, although none of you satisfy the property to belong to $N$, you do satisfy a different property: You all fail not too badly ($ntb$). Congrats! Now please form your own huddle over in that corner. Quickly now, folks. Okay perfect. Listen, we no longer care about you individually - y'all are all indistinuishable to us. For this reason, we'll refer to you as "$(ntb)N$" or sometimes "the coset ntb."

**Mathematician addresses remaining elements in the room** Hi there, y'all, thanks for waiting. Would those of you who fail to belong to $N$ "pretty badly" (pb) please form your own pile? Sure, you can stand in that

corner. That's right, go ahead. Now because you all possess the special property of 'failing pretty badly,' you're all the same to us, and so we'll just call all of you "(pb)N" or "the coset pb."

Alright now, I see y'all who are "not even close" (nec) to meeting the requirements of belonging to $N$ have already huddled together. Thanks so much, folks. Now now, stop all that crying! It's not such a bad thing. You, too, satisfy a very special property: you all fail really badly. Isn't that great? It sure is. So we'll collectively refer to you all as "(nec)N" or "the coset nec."

**Mathematician happily exits the room**




## §10.5 Examples of Quotient Groups

**Example 10.11** (Wikipedia)

Consider the group of integers $\mathbb{Z}$ (under addition) and the subgroup $2\mathbb{Z}$ consisting of all even integers. This is a normal subgroup, because $\mathbb{Z}$ is abelian. There are only two cosets: the set of even integers and the set of odd integers, and therefore the quotient group $\mathbb{Z}/2\mathbb{Z}$ is the cyclic group with two elements. The two cosets are $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

**Example 10.12**

Consider the group $\mathbb{Z}$ and the subgroup $6\mathbb{Z}$. The distinct cosets are

$$6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, \text{ and } 5 + 6\mathbb{Z}.$$

**Example 10.13**

Consider the set of reals under addition and the (normal) subgroup, the $x$-axis. The cosets are all of the horizontal lines. (Addition is defined by adding their $y$-components).

**Theorem 10.14** (Normal Subgroup Criterion)

A subgroup $N$ of $G$ is normal if and only if there is a homomorphism from $f : G \to G'$ such that $ker(f) = N$.

*Proof.* One way is easy: If we define $f$ to be the map from $G$ to $G/N$, then clearly $N$ is mapped to the subgroup.

In the other direction, we already know $ker(f) = N$ is a subgroup from previous classes. Now, $f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \circ e_{G'} \circ f(g^{-1}) = e_{G'}$, so $gng^{-1}$ is inside the kernel of $f$. In particular, this implies $gng^{-1} \in N$, so we have $N$ is normal. □

# §11 Rings and Fields

## §11.1 Rings

**Definition 11.1** (Ring) — We define a **ring** $R$ to be a set with the following properties:

1. It's an abelian group under "addition" (one binary operation), and the additive identity is called "0"
2. We have a second binary operation $\cdot$ (multiplication) that's commutative (no inverse needed)
3. There is a multiplicative identity (called "1")
4. $a \cdot (b + c) = a \cdot b + a \cdot c$

In other words, rings are basically a set that's a group in 2 ways, satisfying the distributive property but not needing an inverse for one of the binary operations.

**Example 11.2**

$\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$ are all rings under normal addition and multiplication.

**Example 11.3**

$\mathbb{R}[x]$, (read: "the real numbers adjoint x") or the polynomials with real coefficients, form a ring. In general, $R[x]$ for any ring $R$ forms a (polynomial) ring.

## §11.2 Fields

**Definition 11.4** (Field)**.** A **field** is a ring with the property that every nonzero element is a unit (or, all elements which are not the multiplicative identity have an inverse).

**Example 11.5**

$\mathbb{R}$, $\mathbb{Q}$ are both fields under normal addition, multiplication. $\mathbb{Z}$ is not.

# §12 Problems

## §12.1 Sets

**Problem 12.1.** Let set $A = \{3, 2, 4\}$ and set $B = \{a, b, c, d\}$. Find the direct product, $A \times B$.

**Problem 12.2.** Under what conditions does $A \times B = B \times A$ for sets $A$ and $B$?

## §12.2 Geometry

**Problem 12.3.** Try to find all of the symmetries of a square and represent them in terms of $\rho$, a counterclockwise rotation by 90°, and $\tau$, a reflection about the vertical axis. Convince yourself that this set of symmetries forms a group.

**Problem 12.4.** A *Platonic solid* is a convex polyhedron whose faces are all congruent regular polygons, with the same number of faces meeting at each vertex. How many symmetries do each of the Platonic solids have?

## §12.3 Homomorphisms

**Problem 12.5** (Math 412)**.** Consider the group $G = \{e, a\}$, where $e$ is the identity element and $a \circ a = e$ and a function $f : (\mathbb{R}\backslash\{0\}, \cdot) \to G$ , where $f$ sends all positive numbers to $e$ and all negative numbers to $a$.[4]

a. Show that $f$ is a homomorphism.

b. Find $\text{Ker}(f)$.

c. Find $\text{Im}(f)$.

**Problem 12.6.** Consider a function $f : G \to H$ between groups $G$ and $H$, where $f(g) = e_H$ for all elements $g \in G$ (where $e_H$ is the identity element of $H$).

a. Show that $f$ is a homomorphism.

b. Find $\text{Ker}(f)$.

c. Find $\text{Im}(f)$.

**Problem 12.7.** Let $f : G \to H$ be a homomorphism between groups $G$ and $H$. Prove that the kernel of $f$ is a group.

- For positive numbers $a, b$:
$$f(ab) = e = e \cdot e = f(a) \cdot f(b)$$
- For a positive number $c$ and a negative number $d$:
$$f(cd) = a = e \cdot a = f(c) \cdot f(d)$$
- For two negative numbers $g, h$:
$$f(gh) = e = a \cdot a = f(g) \cdot f(h)$$

**Problem 12.8.** Let $f : G \to H$ be a homomorphism between groups $G$ and $H$. Prove that the image of $f$ is a group.

**Problem 12.9** (Judson's Abstract Algebra)**.** Let $f : G \to H$ be a homomorphism between groups $G$ and $H$. Prove that, if $G$ is abelian, then the image of $f$ is also abelian.

## §12.4 Number Theory

**Problem 12.10.** What is $5^{2004} \mod 2003$? (Hint: 2003 is prime!)

## §12.5 Groups and Group Theory

Here are some problems that either pertain to **groups** or **group theory** at large (abelian groups and quotient groups and such).

**Problem 12.11.** Is $\mathbb{Z}$ a group under multiplication? Prove or disprove.

**Problem 12.12.** Is $\mathbb{Q}\backslash\{0\}$ (the set of rationals, excluding 0) a group under multiplication? Prove or disprove.

**Problem 12.13.** Is the set of fractions with odd numerators and denominators a group under addition?

**Problem 12.14.** Show that the direct product of two groups is also a group.

[4] $(\mathbb{R}\backslash\{0\}, \cdot)$ is the group of all real numbers, excluding 0, under multiplication.

**Problem 12.15.** Let $G$ be a group. Show that if $g^2 = e$ for all $g \in G$, then $G$ is abelian (the binary operator is commutative).

**Problem 12.16.** Show that every group of order 4 is abelian.

**Problem 12.17** (Challenging)**.** Extend Wilson's theorem to show that the product of all elements of an abelian group is either the identity or an element of order 2.

**Problem 12.18.** Is $\mathbb{Z}$ a group under multiplication? Prove or disprove.

**Problem 12.19.** Is $\mathbb{Q}\backslash\{0\}$ (the set of rationals, excluding 0) a group under multiplication? Prove or disprove.

**Problem 12.20.** Is the set of fractions with odd numerators and denominators a group under addition?

**Problem 12.21.** Consider the group $D_3 = \{e, \rho, \rho^2, \tau, \rho\tau, \rho^2\tau$ and the subgroup $H = \{e, \rho, \rho^2\}$.

a. Find the elements of the coset $\tau H$.

b. Find the elements of the coset $\rho H$.

**Problem 12.22.** Consider the group $\mathbb{Z}$ (integers under addition) and the subgroup $7\mathbb{Z}$ (all multiples of 7). Find the cosets of $7\mathbb{Z}$.

**Problem 12.23.** Consider a group $G$ and a subset $H$. Under what conditions is a coset $gH$ also a subgroup of $G$?

**Problem 12.24.** Prove your answer to the previous problem!

**Problem 12.25** (Challenging)**.** A cyclic group is a group that can be generated from one element in the group. For cyclic groups of finite order, we can represent them as $G = \{e, g, g^2, \ldots, g^{|G|-1}\}$. Prove that every group with prime order is cyclic.

**Problem 12.26** (Challenging)**.** Show that there exists a bijection (a way to map elements from one set to another) from elements of any coset to elements of any other coset, given a subgroup in an infinite group.

**Problem 12.27.** Prove that the center of a group $G$ (the set of all elements $g \in G$ that satisfy $gx = xg$ for all other elements $x \in G$) is a normal subgroup.

**Problem 12.28.** What is the center of any abelian group?

**Problem 12.29.** What are the elements of the quotient group $\mathbb{Z}/n\mathbb{Z}$?

**Problem 12.30.** What are the elements of the quotient group $\mathbb{Z}/(\mathbb{Z}/n\mathbb{Z})$?

# §A Appendix A: List of Theorems and Definitions

## List of Theorems



## List of Definitions

# §B Appendix B: Applications

## §B.1 Math

A few questions:

1. Let's say we have a cube that's already built for us. Can we use a straightedge and a compass to construct another cube that's double the volume?
2. Can we construct a pentagon using ruler and compass? What about a regular $n$-gon?
3. Can we trisect an angle (into three equal parts) only using straightedge and compass?
4. Can we find the roots of a quintic equation with integer coefficients only using addition, subtraction, multiplication, division, and radicals?

The answer to all of these are *no*. For the quintic problem, this has to do with a group called $A_5$ not having any normal subgroups.

## §B.2 Science

Some other applications:

1. Error detecting with hamming code
2. (Discrete Log Problem) Let's say we have a modulus $n$, and elements $a, b$.

> **Definition B.1** (Primitive Root) — $x$ is a **primitive root** modulo $n$ if every number that is relatively prime to $x$ can be written as $x^k \mod n$, for some value $k$.

   If $b$ is a primitive root modulo $n$, then what's the minimum exponent $x$ such that $b^x = a$?

3. Diffie-Hellman (cryptography)

4. (Conservation Laws) It turns out that symmetries in our physical world lead to conservation laws by something called Noether's Theorem. This has many applications, including particle physics. Examples: conservation of momentum, conservation of energy, conservation of angular momentum, etc.

5. (Chemistry) In general, an action which leaves the object looking the same after a transformation is called a symmetry operation. Typical symmetry operations include rotations, reflections, and inversions. There is a corresponding symmetry element for each symmetry operation, which is the point, line, or plane with respect to which the symmetry operation is performed. For instance, a rotation is carried out around an axis, a reflection is carried out in a plane, while an inversion is carried our in a point.

   We shall see that we can classify molecules that possess the same set of symmetry elements, and grouping together molecules that possess the same set of symmetry elements. This classification is very important, because it allows to make some general conclusions about molecular properties without calculation. Particularly, we will be able to decide if a molecule has a dipole moment, or not and to know in advance the degeneracy of molecular states. We also will be able to identify overlap, or dipole moment integrals which necessary vanish and obtain selection rules for transitions in polyatomic molecules.