0 Sets and Relations

Learning Objectives:

- Identify sets and describe constructions of sets, subsets, products, partitions etc.
- Define relations on sets, describe examples of sets and relations
- Relate equivalence relations on a set to its partitions

Our goal in this class is to do algebra. What is algebra?

In order to formally describe what algebra is and examine its patterns and structures, we need to take a step back and set the stage on which algebra occurs. *"If you wish to make an apple pie from scratch, you must first invent the universe."* - Carl Sagan.

0.1 Sets

This course will likely be very different from the previous mathematics courses you have taken. We will do our mathematics the proper, rigorous way that professional mathematicians do it, which is to say that we will do it □. If you were to write a book that contained all of mathematics, what would you put on page one? Perhaps $1+1=2$? Why is this true? What does 1, or 2 mean for that matter?

Aside: Philosopher and mathematician Bertrand Russel once authored a book on the foundations of mathematics that took roughly 379 pages to prove that $1+1$ does in fact equal 2.

It is impossible to define every single concept, so we will take a few facts, or □ for granted. Specifically, we will not define, but we will make sense of, the concept of a □. Loosely,

We will usually denote sets by capital letters.

Example 1. Here are some examples of sets:

1.

2.

3.

4.

Almost any collection you mention could form a set, however there is some structure to sets. Here are some assumptions we will make:

1. A set S consists of objects called . We use the symbol $\in$ to denote that a set contains an element. for example:

2. There is a set that doesn't contain any objects. It is called the .

3. We can describe a set in several different ways. We can do this in words:

   We can list every element using braces:

   Or we can use set-builder notation which makes use of a property each member of the set satisfies to describe its elements:

4. A set is . Loosely, this means that it can be determined which elements are in the set, and which are not. For example,

Next, we discuss some structure within sets.

Definition 1. (**Subset**)

Remark 1. Note that according to this definition, we get the following two facts:

Definition 2. (**Proper Subset**)

Note that the book uses the notation $\subset$ instead of $\subseteq$, but I will always use the latter.

Exercise 1. List all of the subsets of the set $S = \{a, b, c\}$.

Definition 3. (**Cartesian Product**)
Let A and B be sets.

Exercise 2. Let $A = \{1, 2\}$ and $B = \{2, 3, 4\}$. Find the elements of $A \times B$.

Example 2. We will frequently refer to sets of numbers throughout the course and will use the familiar notation.

-
-
-

- □
- □
- □

Example 3. The set □ is familiar, it is usually written as □, which is the Euclidean plane.

Exercise 3. Decide if the following statements do indeed describe sets (that is, are well-defined). If it is a set, give an alternate description.

1. $\{2n \in \mathbb{Z} \,|\, n \in \mathbb{Z}^+\}$
2. $\{n \in \mathbb{R} \,|\, n \text{ is close to } 0\}$
3. $\{x \in \mathbb{Z} \,|\, n^2 < 0\}$
4. $\{x \in \mathbb{Q} \,|\, x \text{ is almost an integer}\}$
5. $\{x \in \mathbb{Q} \,|\, x \text{ can be written with a denominator greater than } 100\}$

0.2 Relations Between Sets

We can begin to impose a structure on sets and relationships between sets using the idea of a "relation". Very loosely, a relation is some sort of rule that pairs up elements of set A with elements of a set B. Since pairs of elements (a, b) are elements of the Cartesian product, we can explicitly define relationships between sets using subsets of $A \times B$.

Definition 4. (**Relation**)
Let A and B be sets.

Example 4. (**The Equality Relation**)
What does it mean to be equal? Let S be a set.

Note: A relation between a set S and itself is called a **relation on** S.

Example 5. (**Graphs in** $\mathbb{R}^2$)

Definition 5. (**Function**)

Example 6. (**Addition**)
We can think of addition of real numbers as a function:

0.3 Cardinality

Definition 6. (**Cardinality**)

Remark 2. How can we tell if two sets have the same size? If they are finite, we could count them. If they are very large, counting becomes tedious, and if they are infinite then this no longer works. However, there is a method to deal with this.

Definition 7. (One-to-One and Onto)
Let $\varphi : A \to B$ be a function.

Exercise 4. Determine if the following functions are one-to-one and if they are onto. Explain your answers.

1. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^4$.

2. $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = 2x + 1$

3. $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \ln(x)$

4. Can you come up with an example of a function that is one-to-one but not onto?

Remark 3. Suppose $\phi : X \to Y$ is a one-to-one correspondance.

Definition 8. (**Same Cardinality**)

We have outlined an argument above that shows that □ and □ have the same cardinality. It can be shown that □ as well:

Note: It is impossible to construct a one-to-one correspondence between □ and □, and in fact □

Exercise 5. 1. Find the cardinality of the following sets:

(a) $\{x \in \mathbb{Z} : 0 < x \leq 9\}$

(b) $[-10, 2\pi] \cap \mathbb{Z}^+$

2. Let A and B be sets with $|A| = m$ and $|B| = n$. What is the cardinality of $A \times B$? Prove this.

0.4 Partitions and Equivalence Relations

Definition 9. (Disjoint Sets)

Definition 10. (Partition)

Loosely, partitioning a set is simply breaking the set up into a collection of subsets.

Exercise 6. Find all of the partitions of the set $\{1, 2, 3\}$.

Example 7. (**Residue Classes Modulo** n)

Definition 11. (**Equivalence Relation**)
Let S be a set. Then $\sim$ is called an equivalence relation on S if $\sim$ satisfies the following three properties:

1.

2.

3.

Example 8. The following are equivalence relations

1. Let S be a nonempty set.

2. **(Congruence Modulo n)**

Exercise 7. Let the relation $\mathscr{R}$ on $\mathbb{Z}$ be defined by $m \mathscr{R} n$ if and only if $mn \geq 0$. Determine whether $\mathscr{R}$ is an equivalence relation by checking the three necessary conditions.

Theorem 1. (Equivalence Relations and Partitions)

Proof.

□

Definition 12. (Equivalence Classes)

Exercise 8. The following are questions about equivalence relations.

1. What are the residue classes of $\mathbb{Z}$ modulo 5? Which one contains the number 123?

2. Is the relation defined by "$x \sim y$ if and only if x divides y" an equivalence relation? Either prove this or explain why not.

3. Show that the following defines an equivalence relation on points in $\mathbb{R}^3$:

   $$P \sim Q \text{ if and only if } P \text{ and } Q \text{ have the same } z\text{-coordinate.}$$

   How would you describe the equivalence classes of this relation geometrically?

1 An Extended Example

Learning Objectives:

- Compute expressions consisting of complex numbers
- Use Euler's formula to represent complex numbers
- Compare algebra on circles to multiplication of complex numbers and roots of unity

The goal of this section is to give a feeling of the nature of "abstract algebra". The goal is to study *structural* properties of the set on which we are algebraically manipulating.

For instance, consider the set $\mathbb{R}$:

We shall later see that the structure of □ under □ behaves in the "same" way as □ under □! (and make sense of what it means to be the "same" in this context).

1.1 Complex Numbers

The set of can be represented as a number line

As we know, the equation $x^2 + 1 = 0$ does not have a solution in $\mathbb{R}$. In the 16th century, Italian mathematicians came up with a way to “fix” this problem that allowed them to solve complex equations. Define the symbol i to be a solution to this equation. That is, $i^2 + 1 = 0$. The number i is (unfortunately) called the imaginary unit.

Definition 13. (**The Complex Numbers**)

One can visualize as the set of points in a plane:

The of complex numbers is easily defined, and resembles vector addition:

The of complex numbers is a bit more involved:

Exercise 9. Compute $(5+3i)(6-2i)$

1.2 Polar Form and Euler's Formula

As you know from precalculus, every point in the plane can be represented in polar form, using distance from the origin and an angle.

Definition 14. **(Absolute Value, Polar Form)**

A famous formula due to Leonhard Euler in the early 1700s states the following.

Theorem 2. **(Euler's Formula)**

Proof.

□

As a consequence of this, we have the following. Set $z_1 = |z_1|e^{i\theta_1}$ and $z_2 = |z_2|e^{i\theta_2}$. Then

Geometrically, this results in the following:

We can use polar forms to solve complex equations.

Example 9. Find all solutions to the equation $z^2 = i$.

Remark 4. Using polar form, you can solve any equation of the form □. You will always find □ unique solutions, as long as □.

1.3 Algebra on Circles

Definition 15. (**The Unit Circle in** $\mathbb{C}$)

Remark 5.

Now, if $\boxed{}$, then $\boxed{}$, so by Euler's formula,

This means every $z \in U$ only depends on a real number $\theta \in \mathbb{R}$ where $0 \leq \theta < 2\pi$. This (half open) interval is usually denoted $[0, 2\pi)$, however, we will denote it by $\mathbb{R}_{2\pi}$. We can define addition on this set as follows:

Definition 16. (**Addition Modulo** 2π)

Example 10. Compute the following:

1. $\frac{3\pi}{4} +_{2\pi} \frac{\pi}{2}$

2. $\frac{7\pi}{6} +_{2\pi} \pi$

Why do we introduce this new version of "adding" things? Because now multiplication on □ is the "same" as addition modulo 2π in □!

More precisely, □ with □ has the same algebraic properties as □ with □!

Remark 6.

Example 11. (Identity Element)

Example 12. (Solving Equations)

Remark 7.

Example 13. Compute the following in $\mathbb{R}_{7.5}$:

1. $5 +_{7.5} 3$

2. $2 +_{7.5} 3.2$

3. $2 +_{7.5} 5.5$

1.4 Roots of Unity

Definition 17. (**Roots of Unity**)

Example 14. What are the elements of U_3?

Remark 8.

For example, if $n = 8$, then we can simplify as in the following computations:

Like with the unit circle, we can relate roots of unity to a more familiar set with a modified addition.

Thus, and have the same algebraic structure!

Exercise 10. Compute the following using modular addition:

1. $4 +_6 5$

2. $\frac{1}{2} +_1 \frac{7}{8}$

3. $\frac{5\pi}{6} +_{2\pi} \frac{13\pi}{10}$

Find *all* solutions to the following equations:

1. $x +_{15} 7 = 3$ in $\mathbb{Z}_{15}$.

2. $x +_7 x +_7 x = 5$ in $\mathbb{Z}_7$.

2 Binary Operations

Learning Objectives:

- Interpret the “usual” operations on real numbers as functions
- Define and compute a variety of binary operations on sets, understand common properties thereof
- Use tables to compute and describe binary operations

2.1 Definition and Examples

We have seen (see Section 0, Example 6 of the notes) that familiar algebraic operations on sets can be interpreted as □. When we first learn about addition and multiplication, we memorize common computations and then learn “rules” for computing more involved combinations. To analyze the underlying structure of addition and multiplication, of the real numbers, ore more generally, algebraic combinations on any set □ we will interpret them as □ on □ of objects from □, that is, on the elements of □.

Definition 18. (**Binary Operation**)

Example 15. We now present examples and non-examples

1.

2.

3.

Definition 19. (**Closure, Induced Operation**)

Example 16. Consider the real numbers $\mathbb{R}$ under addition $+$.

Exercise 11. Consider the set of integers $\mathbb{Z}$.

1. Is the subset of even number closed under addition? Under multiplication?

2. Is the subset of perfect cubes $\{n^3 \,|\, n \in \mathbb{Z}\}$ closed under addition? Under multiplication?

Example 17. Real-valued Functions

Example 18. We now present some non-standard examples of binary operations.

1.

2.

3.

WARNING: THE ORDER OF ELEMENTS IN OPERATIONS MATTERS!!.

In the first example, we have for all . However, in the second example, we have, for instance, .

Definition 20. (Commutativity)

You should never assume a binary operation is commutative unless told otherwise. Another standard example is matrix multiplication:

We next address how to combine *more* than two elements, that is, how to compute the expression

In the first example from the previous page, we have

However, in the third example from the previous page

Definition 21. (Associativity)

Thus if a binary operation □ is □, there is no ambiguity by writing □.
Another example of an operation that is not associative is the □

You should not assume a binary operation is associative unless told otherwise. The most useful and common binary operations are associative. In particular, any operation that can be considered a composition of functions is associative.

Theorem 3. (Associativity of Function Composition)

Proof. □

Corollary 1. (Associativity of Matrix Multiplication)

Proof. □

2.2 Tables

One way that we can analyze a binary operation on a set with a small number of elements is using a table:

Example 19. Consider the table below. Is the operation $*$ commutative?

Exercise 12. Let $S = \{a, b, c, d\}$. Suppose $*$ is a commutative binary operation on S. Fill in the table below.

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

2.3 Words of Warning and Non-examples

In order to define a binary operation $*$ on a set S, we must have

1.

2.

There are three ways these conditions can fail:

- If we only know how to combine certain elements of S but **not every** element of S, we say that

- If for some pairs of elements from S we could assign several elements of S, we say that

- If condition 2 from above is violated, we say that S is

.

Example 20. We now present several examples that seem plausible as binary operations, but fail to meet the criteria.

1.

2.

3.

4.

5.

3 Isomorphic Binary Structures

Learning Objectives:

- Use tables to recognize isomorphic binary structures
- Prove that binary structures are or aren't isomorphic
- Differentiate structural properties from non-structural properties

Definition 22. (**Binary Algebraic Structure**)

Our main focus for this lesson is how to determine when binary structures are structurally the same, or □. We saw in Section One that □ and □ are isomorphic. Can we expand on that strategy and grow our tool set in this regard?

Example 21. Let $Q = \{a, b, c\}$, $R = \{\#, \$, ☺\}$, $S = \{1, 2, 3\}$ and $T = \{x, y, z\}$. Consider the following binary structures on these sets:

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

$\star$	#	\$	☺
#	☺	#	\$
\$	#	\$	☺
☺	\$	☺	#

$\circ$	1	2	3
1	1	1	1
2	1	1	1
3	3	3	3

$\otimes$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

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

$\star$	#	$	☺
#	☺	#	$
$	#	$	☺
☺	$	☺	#

$\circ$	1	2	3
1	1	1	1
2	1	1	1
3	3	3	3

$\otimes$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

Definition 23.

Example 22. We now address the old examples with the new definition and notation.

1.

2.

3.

3.1 How to Show that Binary Structures are Isomorphic

Let $\langle S, *\rangle$ and $\langle T, \star\rangle$ be binary structures. Lets outline a step-by-step process for proving that the two structures are isomorphic, i.e. that $\langle S, *\rangle \cong \langle T, \star\rangle$.

Step 1:

Step 2:

Step 3:

Step 4:

Example 23. Prove that $\langle \mathbb{R}, +\rangle$ is isomorphic to $\langle \mathbb{R}^+, \cdot\rangle$.

Example 24. Let $2\mathbb{Z} = \{2n \,|\, n \in \mathbb{Z}\}$, so that $2\mathbb{Z}$ is the set of even integers. Then $\langle 2\mathbb{Z}, +\rangle$ is a binary structure with the *induced operation* of $+$ from $\mathbb{Z}$. Show that $\langle \mathbb{Z}, +\rangle$ is isomorphic to $\langle 2\mathbb{Z}, +\rangle$.

3.2 How to Prove Binary Structures are Not Isomorphic

Suppose you have two binary structures □ and □ that are **not** □. How can you show this? You would have to show that there is no way to construct a function □ that is simultaneously □, □ and that satisfies the □ property:

There is one case in which this is straightforward.

Example 25. Explain why the binary structures $\langle \mathbb{Q}, +\rangle$ and $\langle \mathbb{R}, +\rangle$ cannot be isomorphic.

Definition 24. (Structural Property)

Intuitively, a □ is a general statement that will be true of any other binary structure that behaves the same way. More loosely, it is a property that can be perfectly "translated" through an isomorphism.

Strategy:

Example 26. Show that $\langle \mathbb{Z}, + \rangle$ is not isomorphic to $\langle \mathbb{Q}, \cdot \rangle$

Here are some possible structural properties of a binary structure $\langle S, * \rangle$:

-
-
-
-

Contrast those with some possible non-structural properties:

-
-
-
-

Definition 25. (**Identity Element**)

Theorem 4. (**Uniqueness of Identity**)

Proof.

□

Theorem 5. **(Identity Elements are Structural)**

Proof.

□

Exercise 13. Show that $\langle \mathbb{Z}, + \rangle$ and $\langle \mathbb{Q}, + \rangle$ are not isomorphic.

Exercise 14. Show that $\langle \mathbb{C}, \cdot \rangle$ and $\langle \mathbb{R}, \cdot \rangle$ are not isomorphic.

Exercise 15. Show that $\langle M_{2\times 2}(\mathbb{R}), \cdot \rangle$ and $\langle \mathbb{R}, \cdot \rangle$ are not isomorphic.

4 Groups

Learning Objectives:

- Determine whether binary structures are groups
- Prove that groups satisfy certain properties, use these to solve equations
- Recognize whether a table represents a group, determine properties of groups from Cayley Tables

Thinking back to the very first day of class, we said that was

Now that we have stripped algebraic manipulation down to its fundamentals, it is time to build up the kind of structures in which it make sense to "do algebra". Consider the following algebraic structures:

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

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

More concretely, consider $\langle \mathbb{Z}, + \rangle$ or $\langle \mathbb{Q}^*, \cdot \rangle$. Then one can solve any equation that resembles those above:

There are only three properties necessary to make this possible –associativity, the existence of an identity element e, and the ability so solve $a * x = e$ for any a.

Definition 26. (Group)

1.

2.

3.

Example 27. We now turn our heads to our motivating examples, namely $\langle U, \cdot \rangle$ and $\langle U_n, \cdot \rangle$.

Remark 9. When speaking about a group $\langle G, * \rangle$, one usually drops the $*$ simply writes G. If we need to explicitly say what the operation is, the usual verbiage is "A group G under $*$". For example, "Consider the group $\mathbb{R}$ under $+$..."

Definition 27. (**Abelian Group**)

Remark 10. This is in honor of Norwegian mathematician Niels Henrik Abel (1802-1829).

Example 28. We now present several examples and non-examples.

1.

2.

3.

4.

5.

6.

Example 29. We now present several examples related to Linear algebra.

1. Let V be a vector space.

2. Let $M_{m\times n}(\mathbb{R})$ be the set of $m \times n$ matrices with real entries.

3. Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices with real entries.

4. Claim: The subset of $M_n(\mathbb{R})$ consisting of all *invertible* matrices forms a group under multiplication.

   Proof.

   □

Definition 28. **(General Linear Group)**

Remark 11.

Exercise 16. Prove that $\mathbb{Q}^+$ under $*$ is a group, where $*$ is defind by $a * b = \dfrac{ab}{3}$.

Proof.

□

4.1 Properties of Groups

We now make precise what it means "cancel" something in algebra.

Theorem 6. (Cancellation Laws)

Proof. □

The next result is related to solutions "linear" equations. For example

Theorem 7.

Proof.

□

Remark 12. Note that in the above theorem, the solutions □ and □ need not be the same unless □.

Theorem 8. (Uniqueness of Identity and Inverse Elements)

Proof.

□

Corollary 2. (Inverse Formula)

Proof.

□

4.2 Finite Groups and Cayley Tables

We will now examine all the possible groups of low cardinality. A general theme of group theory is to *classify* all groups – that is, describe every possible group structure on a given set.

By classify all groups, we mean *up to isomorphism.*. We could always come up with a new group by changing the names of the elements or the symbols used for the operation. In this context, we don't classify U_n and $\mathbb{Z}_n$ as different groups, since they are isomorphic.

Let G be a group with $|G| < \infty$. Let's examine the possible group structures for low values of $|G$—.

$|G| = 0$:

$|G| = 1$:

$|G| = 2$:

$|G| = 3$:

Remark 13. Some things to notice:

-
-
-
-

5 Subgroups

Learning Objectives:

- Use multiplicative and additive notation in abstract groups
- Recognize and verify subsets with group structures
- Compute cyclic subgroups of familiar groups

5.1 Notation and Terminology

Until now, we have been painstakingly making use of symbols such as $*$ or $\star$ or $\circ$ to denote binary operations. In the setting of a group, there are agreed upon standards used by lazy mathematicians to make the notation faster to write down, but certainly more confusing for the initiate. When talking about an **abstract group** G with any sort of possible operation $*$, we will now suppress the symbol $*$ and always use either multiplicative notation, or if we know the group is abelian, additive notation.

Multiplicative Notation:

Additive Notation:

Definition 29. (Order of a Group)

5.2 Subsets and Subgroups

Now that we have seen many examples of groups, we proceed in discussing structural properties of groups. The first of which we will discuss is when one group is contained in another group. For example, consider the group □.

Definition 30. (**Subgroup**)

Summarizing the example above, we have ☐ but ☐, even though ☐.

Definition 31. (**Proper/Improper/Trivial Subgroups**)
Suppose that G is a group.

-
-
-

Example 30. We now examine some familiar examples.

1.

2.

3.

Example 31. Crucial Motivating Example – Groups of order 4

Example 32. Consider the set F of all real-valued functions with domain $\mathbb{R}$, that is

$$F = \{f : \mathbb{R} \to \mathbb{R} \,|\, f \text{ is a function}\}$$

We have discussed previously that F is a group under $+$.

1.

2.

Theorem 9. (**Subgroup Theorem – The "Easy" Way to Determine if a Subset is a Subgroup**)
A subset □ of a group □ is a subgroup if and only if

1. □
2. □
3. □

Proof.

□

Example 33. (**Differentiable Functions**)

Example 34. **(Matrices of Determinant 1)**

5.3 Cyclic Subgroups

Theorem 10.

Proof.

□

Definition 32. (Cyclic Subgroup)

Definition 33. (Generator, Cyclic)

In some sense ______ groups are the easiest to understand, since you can express every element in G as a "power" (or "multiple") of the generator.

Example 35.

Example 36.

Example 37.

Example 38.

Exercise 17. Determine if the given subsets of famiilar groups are subgroups.

(a) The subset $S = \{bi \mid b \in \mathbb{R}\} \subseteq \mathbb{C}$ under addition.

(b) The subset S of $GL_N(\mathbb{R})$ of matrices with determinant 2.

Exercise 18. Come up with two non-isomorphic groups of order 6. [Hint: You should think about possible Cayley Tables ...]

6 Cyclic Groups

Learning Objectives:

- Use the division algorithm to find quotients, remainders, and greatest common divisors
- Recognize and prove properties of cyclic groups
- Describe the structure, subgroups and draw subgroup diagrams of finite cyclic groups

In this lesson, we will focus on cyclic groups. Recall the following notation and terminology from the previous lesson:

Definition 34. (**Order of an Element**)
Let G be a group and $a \in G$.

Example 39. Consider the group $\mathbb{Q}^*$ under multiplication.

1.

2.

3.

6.1 Properties of Cyclic Groups

Theorem 11.

Proof.

□

Moving forward, we will frequently invoke a fact about the integers which you learned long ago. We now present it complete with proof.

Theorem 12. (**Division Algorithm for** $\mathbb{Z}$)

Proof.

□

Remark 14.

Example 40. We now present some examples of using the division algorithm.

1. Find the quotient q and remainder r when 54 is divided by 17.

2. Find the quotient q and remainder r when -41 is divided by 11.

The next fact will become useful later on.

Exercise 19. Let n and m be positive integers. Show that the set $H = \{nr + ms \,|\, r, s, \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ under addition.

Theorem 13.

Recall that for $n \in \mathbb{Z}^+$, the set $n\mathbb{Z} = \{mn : m \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ is a group under addition. Then applying the previous theorem to $\mathbb{Z}$ yields the following:

Corollary 3. (Subgroups of $\mathbb{Z}$)

Combining this corollary and the previous exercise allows us to give a more precise algebraic definition of a familiar concept.

Definition 35. (Greatest Common Divisor)

Remark 15. This definition is equivalent to the one you learned in elementary school:

Example 41. Find the greatest common divisor d of $n = 28$ and $m = 70$. Express your answer in the form $d = nr + ms$.

Definition 36. (**Relatively Prime**)

Proposition 1.

Proof. □

Example 42. Use the previous proposition to show that 18 and 25 are relatively prime.

6.2 The Structure of Cyclic Groups

We now have the tools to describe all cyclic groups up to isomorphism.

Theorem 14.

Proof.

□

6.3 Subgroups of Finite Cyclic Groups

Now that we turn our attention to the subgroups of cyclic groups. We have already discussed the infinite case (Corollary 1), so only the finite case remains.

Theorem 15.

Proof.

□

Example 43. Consider the group $\mathbb{Z}_6$.

Corollary 4.

Example 44. Let us describe all subgroups of $\mathbb{Z}_{20}$ and draw its subgroup diagram.

7 Free Groups and Generating Sets

Learning Objectives:

- Compute products and inverses in free groups
- Describe subgroups of familiar groups with generating sets
- Use generators and relations to define groups

We have spent some time describing cyclic groups, that is, groups that are generated by one element. Today we will make sense of what it should mean for a group to be generated by a set of elements.

Suppose that G is a group and let a and b be elements of G.

Example 45. Let us consider some familiar groups

1. Consider the group $\mathbb{Z}_6$ under addition.

2. Conisder the group $\mathbb{Q}^+$ under multiplication.

Remark 16. The next definition will make use of what is called an . This is simply the set which we use to "label" the objects in the set. For example,

We often use as an index set

In general, index sets could be any set, they could even be uncountable:

Definition 37. (**Generators, Finitely Generated**) Let G be a group, and $\{a_i \,|\, i \in I\}$ a subset of G for some index set I (think $I = \{1, \ldots, n\}$, or $I = \mathbb{Z}$).

-
-

Example 46. (**The Gaussian Integers**)

Theorem 16.

Proof.

□

Remark 17. Let $r, s \in \mathbb{Z}$ be positive integers.

7.1 Free Groups and Group Presentations

We can utilize the concept of generation to describe groups succinctly, and cook up new abstract groups.

Definition 38. (**Free Group on n Letters**)

Example 47. Let's take a closer look at a few free groups

1. The free group on a.

2. The free group on a, b.

Remark 18. One way of describing a group is to give it as a set of $\boxed{\qquad\qquad\qquad}$ and $\boxed{\qquad\qquad\qquad}$.

Definition 39. (Group Presentation)

Example 48. Consider the group $G = \langle a, b \,|\, ab = ba \rangle$.

8 Permutation Groups

Learning Objectives:

- Compute multiplication of permutations
- Describe Groups of Symmetries
- Recognize familiar groups as subgroups of permutations

We have seen before that one possible binary operation is composition of functions (provided the codomain and domain are the same). Let's revisit an older example:

Example 49. Recall that $GL_2(\mathbb{R}$ is the set of invertible 2×2 matrices.

Definition 40. (Permutation of a Set)

8.1 Permutation Groups

Notation:

Theorem 17.

Proof.

□

Proposition 2.

Proof.

□

Definition 41. **(Permutation Group on n Letters)**

8.2 Dihedral Groups

Example 50. Symmetric Group on 3 Letters

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0						
ρ_1						
ρ_2						
μ_1						
μ_2						
μ_3						

(Example Continued)

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Example 51.

8.3 Cayley's Theorem

We will prove an important result about groups, that essentially tells us where to "find" examples of groups. First, a definition and a lemma that we will use in the proof of the theorem.

Definition 42.

Lemma 1.

Proof. □

Theorem 18. (**Cayley's Theorem**)

Proof.

□

Example 52.

9 Orbits, Cycles, and Alternating Groups

Learning Objectives:

- Identify orbits of permutations
- Use cycle notation to represent and multiply permutations
- Prove basic facts about permutation groups and their subgroups

9.1 Orbits

A permutation, σ of a set X gives rise to a natural partition of X.

Definition 43. (**Orbits**)

Example 53. We now give three examples.

1. Consider the element $\mu_1 \in S_3$.

2. Let X be a set. Consider the identity element $\iota \in S_X$.

3. Consider the following permutation in S_8

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 8 & 2 & 3 & 4 & 7 \end{pmatrix}$$

9.2 Cycles

For the remainder of this section, we will only consider permutations of finite sets, so we may assume that the set is $\{1, 2, \ldots, n\}$. The group of permutations of this set is S_n, the symmetric group on n letters.

Let's look a little bit more closely at the previous permutation $\sigma \in S_8$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 8 & 2 & 3 & 4 & 7 \end{pmatrix}$$

Definition 44. (Cycles, Cyclic Notation)

Example 54. We now present several examples of cylcic notaion.

1. In S_5, consider the element $(1,3,5,2)$.

2. Compute $(1,3,5,2)(4,2,3)$ in S_5

3. In S_8, return to the example

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 8 & 2 & 3 & 4 & 7 \end{pmatrix}$$

Theorem 19.

Proof. □

Remark 19.

Example 55. We illustrate this fact with two examples.

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

2. On the other hand, let $\sigma = (1, 4, 2)$ and $\tau = (1, 3)$

9.3 Even and Odd Permutations

Every permutation of n objects is simply a rearrangement of those objects. You can achieve every such rearrangement by swapping two elements at a time, which we will now make precise

Definition 45. (Transposition)

Example 56. Consider the following examples:

1. $(1, 2)$

2. $(1, 2, 3)$

3. $(1, 2, 3, 4)$

Remark 20.

Corollary 5.

Example 57. In S_8, return to the example

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 1 & 8 & 2 & 3 & 4 & 7 \end{pmatrix}$$

Example 58. Consider the identity element in S_n for $n \geq 2$

Example 59. Although every permutation has a decomposition, the decomposition is not unique. Consider the element $(1, 2, 3)$ in S_3.

Theorem 20.

Proof.

□

Exercise 20. 1. Verify that the six matrices below form a group under multiplication.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Hint: You could do this directly, but that would take a lot of work. Instead, try seeing what the vector $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ is transformed to after multiplying it on the left by each of the matrices.

2. You probably noticed that the matrices permute the elements in the vector. Match up each of the matrices with their counterparts in $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$.

3. Write each of the elments of S_3 as a product of transpositions, and compare these to the determinants of the matrices on the previous page.

Theorem 21. No permutation in S_n can be expressed as both a product of an even number of transpositions and an odd number of transpositions.

Proof.

□

Definition 46. (**Even and Odd Permutations**)

Example 60. Determine if the permutation $(1,4,5,6)(2,1,5)$ is even or odd.

Exercise 21.

1. Draw the orbits of $(1,2,3,4)(5,6,7,8)$ and $(4,5)(1,2,3,4)(5,6,7,8)$ using the circular pictures like in the proof.

2. Draw the orbits of $(1,2,3,4,5)(6,7,8)$ and $(4,5)(1,2,3,4,5)(6,7,8)$ using the circular pictures like in the proof.

3. Decide whether the following permutations are odd or even

   (a) $(2,4,6)(1,3,5,7)$

   (b) $(1,2,3,4,5,6,7)$

   (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 6 & 1 & 3 & 7 \end{pmatrix}$

   (d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 7 & 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 4 & 7 & 1 & 3 \end{pmatrix}$

9.4 The Alternating Groups

We will now proceed in defining an interesting subgroup of S_n for any $n \geq 3$.

Theorem 22.

Definition 47.

Exercise 22. The following exercises will complete a proof of the theorem.

1. Consider the symmetric group on n letters, S_n. Let $A_n \subseteq S_n$ be the set of even permutations and $B_n \subseteq S_n$ be the set of odd permutations. Let $\tau = (1, 2)$ and define the map $\lambda_\tau : A_n \to B_n$ by $\lambda_\tau(\sigma) = \tau\sigma$. Prove that λ_τ is one-to-one and onto. Conclude that $|A_n| = n!/2$

2. Is B_n a subgroup of S_n? Why or why not?

3. Show that A_n is a subgroup of S_n.

10 Cosets and the Theorem of Lagrange

Learning Objectives:

- Find the cosets and the index of a given subgroup
- Apply Lagrange's Theorem to prove results about groups
- Relate Lagrange's Theorem to known groups and subgroups

10.1 Cosets

Theorem 23.

Proof.

□

Let G be a group, $H \leq G$ and $a \in G$. Then $\sim_L$ corresponds to a partition of G. What is the cell containing a?

Definition 48. (Cosets)

Example 61.

Fact 1.

Remark 21.

Example 62. The group $\mathbb{Z}_6$ is belian. Find the partitions of $\mathbb{Z}_6$ into cosets of the subgroup $H = \{0, 3\}$.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

Exercise 23. Here are some exerciese about cosets.

1. Find the cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.

2. Find all cosets of $\langle 2 \rangle$ in $\mathbb{Z}_{12}$.

3. Fnd all cosets of $\langle 4 \rangle$ in $\mathbb{Z}_{12}$.

Example 63. For the group $S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$, find the cosets corresponding the the subgroups $H = \langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ and $K = \langle \mu_1 \rangle = \{\rho_0, \mu_1\}$.

$\cdot$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

$\cdot$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

10.2 The Theorem of Lagrange

Proposition 3.

Proof.

□

Theorem 24. (**Lagrange's Theorem**)

Proof.

□

Corollary 6.

Proof.

□

Theorem 25.

Proof.

□

Definition 49. (Index)

Remark 22.

Theorem 26.

Exercise 24. 1. Find the index of $\langle 9 \rangle$ in $\mathbb{Z}_{36}$.

2. Find the index of $\langle 6 \rangle$ in $\mathbb{Z}_{36}$.

3. For the group $G = \mathbb{Z}_{40}$, find a subgroup of G that has index 5.

4. Let $\sigma \in S_5$ be the element $\sigma = (1, 2, 5, 3)$. Find the index of $\langle \sigma \rangle$ in S_5.

5. Prove that the relation $\sim_R$ from the first theorem is an equivalence relation.

6. Either prove the following statements or give a counter example:

   (a) If $aH = bH$ then $Ha = Hb$.

   (b) If $Ha = Hb$ then $b \in Ha$.

7. Show that if H is a subgroup of index 2 in a finite group G then every left coset of H is also a right coset of H.

8. Prove the final theorem of the lesson: If H and K are subgroups of G where $K \leq H \leq G$ and $(G : H)$ and $(H : K)$ are both finite then $(G : K)$ is finite and $(G : K) = (G : H)(H : K)$

11 Direct Products and Finitely Generated Abelian Groups

Learning Objectives:

- Compute arithmetic operations and solve equations in direct products of groups
- Find subgroups of direct products of known groups
- Determine all finite abelian groups of a given order

11.1 Direct Products

What are the common examples of groups that we know so far?

We will now describe a method to produce new groups from those we have already studied.

Definition 50. (Cartesian Product of Sets)

Remark 23.

Theorem 27.

Proof.

□

Remark 24.

Example 64. List the elements of the group $\mathbb{Z}_2 \times \mathbb{Z}_3$ and show that it is cyclic.

Example 65. List the elements of the group $\mathbb{Z}_3 \times \mathbb{Z}_3$. Argue that it is NOT cyclic.

Exercise 25. 1. Let $G = \mathbb{Z}_3 \times \mathbb{Z}_5$.

(a) How many element are in G?

(b) Perform the following computations in G:

i. $(1,0) + (2,3)$

ii. $(2,4) + (2,3)$

iii. $3(1,3)$

iv. Find the inverse of $(1,4)$ in G.

(c) Find the cyclic subgroup of G generated by $(2,3)$. What can you conclude about G?

2. Now let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

   (a) What is the order of G?

   (b) Find all cyclic subgroups of G. What can you conclude about G?

   (c) Is $G \cong \mathbb{Z}_4$? Why or why not?

   (d) What familiar group is G isomorphic to?

Theorem 28.

Proof.

□

Corollary 7.

Example 66.

Definition 51. (**Least Common Multiple**)

Theorem 29.

Proof.

□

Example 67. Find the order of the element $(6, 10, 3)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{15} \times \mathbb{Z}_{33}$.

Example 68. Consider the group $\mathbb{Z} \times \mathbb{Z}_3$.

Remark 25. Consider the group $G = G_1 \times G_2 \times \cdots \times G_n$.

Exercise 26. 1. Find the orders of the following elements in the following groups:

(a) $(2, 6)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12}$

(b) $(2, 3)$ in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

(c) $(3, 6, 12, 16)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$.

2. What is the largest possible order among all of the cyclic subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_8$?

3. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic? Why or why not?

4. Let G be an abelian group, and let $H \subseteq G$ be the set consisting of the identity element and all elements of order two in G. Show that H is a subgroup of G.

5. Show by specific that the previous statement is NOT true if G is not abelian.

11.2 FTFGAG

Theorem 30. (**Fundamental Theorem of Finitely-Generated Abelian Groups**)

The proof is a bit beyond the scope of this course.

Example 69. Find all of the abelian groups of order 360 up to isomorphism.

Definition 52. **(Decomposable/Indecomposable)**

Theorem 31.

Proof.

□

Theorem 32.

Proof.

□

Theorem 33.

Proof.

□

Exercise 27.

1. Up to isomorphism, how many abelian groups are there of order 180?

2. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the **torsion subgroup** of G.

3. Let G, H, and K be finitely generated abelian groups, Show that if $G \times K$ is isomorphic to $H \times K$, then G is isomorphic to H.

12 Homomorphisms

Learning Objectives:

- Determine if a function is a homomorphism of groups
- Find the kernel of a homomorphism
- Describe structure preserving maps between groups

Definition 53. (Homomorphism)

Note that there are no requirements that a homomorphism be one-to-one or onto.

Remark 26. There is always at least one homomorphism between any two groups.

Note that the trivial homomorphism doesn't provide any information about the relative structure of the groups. We are aware that a homomorphism □ that is □ and □ is called an □, and in this case the two groups have the exact same structure. However, one need not have an □ to get at least some information.

Proposition 4.

Proof.

□

Example 70. We now present several examples of homomorphisms that are not necessarily isomorphisms.

1. Recall that S_n is the symmetric group on n letters.

2. **Linear Transformations of Real Vector Spaces**

3. Recall that $GL_n(\mathbb{R})$ is the group of $n \times n$ matrices with entries in $\mathbb{R}$ under matrix multiplication.

4. **Multiplication by an Element**

5. Let $G = G_1 \times G_2 \times \cdots \times G_n$.

6. Let F be the additive group of continuous functions with domain $[0, 1]$ and $\mathbb{R}$ be the real numbers under addition.

7. **Reduction Modulo** n

Exercise 28. In the following, several maps between groups are given. Decide if each map is a homomorphism.

1. $\varphi : \mathbb{R}^* \to \mathbb{R}^+$ where $\varphi(x) = |x|$.

2. $\varphi : \mathbb{R} \to \mathbb{Z}$ under addition, where $\varphi(x)$ is the greatest integer $\leq x$

3. Let G be any group, and let $\varphi : G \to G$ be given by $\varphi(g) = g^{-1}$.

4. $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2$ given by $\varphi(x) =$ the remainder of x when divided by 2 according to the division algorithm

5. $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_2$ given by $\varphi(x) =$ the remainder of x when divided by 2 according to the division algorithm

6. Let M_n be the set of $n \times n$ matrices under addition and $\mathbb{R}$ be the additive real numbers. Let $\varphi : M_n \to \mathbb{R}$ be given by $\varphi(A) = \det(A)$.

7. Let M_n be the set of $n \times n$ matrices under addition and $\mathbb{R}$ be the additive real numbers. Let $\varphi(A) = \text{tr}(A)$, the **trace** of A, which is calculated by taking the sum of the entries on the main diagonal of A. So, for example $\varphi\left(\begin{bmatrix} -1 & 6 \\ 3 & 2 \end{bmatrix}\right) = -1 + 2 = 1$.

12.1 Properties of Homomorphisms

Definition 54. (Image, Range, Inverse Image)

Theorem 34. Let $\phi : G \to G'$ be a homomorphism of groups.

1.

2.

3.

4.

Loosely speaking, homomorphisms preserve the identity element, inverses, and subgroups.

Proof.

□

Remark 27.

Definition 55. (Kernel)

Remark 28.

Let $\phi : G \to G'$ be a homomorphism, and set $H = \ker \phi$.

Theorem 35.

Proof.

□

Example 71. We present two examples of homomorphisms with nontrivial kernels.

1.

2.

Corollary 8.

Proof. □

How to Show a Function $\phi : G \to G'$ is an Isomorphism:

1.

2.

3.

Definition 56. (Normal Subgroup)

Corollary 9.

Proof. □

Exercise 29. Note: A homomorphism $\varphi : G \to G'$ where G is cyclic is completely described by where the generator for G goes, since every element is of the form a^n for some n, and $\varphi(a^n) = \varphi(a)^n$. Keep this fact in mind and complete the following:

1. There is a homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_7$ where $\varphi(1) = 4$. Find $\varphi(25)$, then find $\ker(\varphi)$.

2. There is a homomorphism $\varphi : \mathbb{Z} \to S_8$ where $\varphi(1) = (1, 4, 2, 6)(2, 5, 7)$. Find $\varphi(20)$, then find $\ker(\varphi)$.

3. There is a homomorphism $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\varphi(1, 0) = (2, -3)$ and $\varphi(0, 1) = (-1, 5)$. Find $\varphi(4, 6)$, then find $\ker(\varphi)$.

4. Let $\varphi : G \to G'$ be a group homomorphism. Show that if $|G|$ is finite then $|\varphi[G]|$ is finite and is a divisor of $|G|$.

5. Show that if G, G', and G'' are groups and $\varphi : G \to G'$ and $\gamma : G' \to G''$ then the composite map $\gamma\varphi : G \to G''$ is a homomorphism.

13 Factor Groups

Learning Objectives:

- Compute factor groups from homomorphisms
- Compute factor groups from normal subgroups
- Determine if a subgroup is normal using inner automorphisms

This section discusses situations where the cosets of a subgroup H of a group G form a group.

13.1 Factor Groups from Homomorphisms

We will show that the cosets of the kernel of a homomorphism form a group. To do so, we first need to discuss how one defines a binary operation on a set of sets.

Remark 29. Suppose a set S has the same cardinality as a group G.

Theorem 36.

Proof.

□

Example 72. Consider the map $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ where $\gamma(m)$ is the remainder when m is divided by n in accordance withe the division algorithm.

Remark 30.

13.2 Factor Groups from Normal Subgroups

So far, we have shown that G/H is a group if H is the kernel of some homomorphism. You may be wondering if this works for any subgroup H. The answer is no, however there is a large class of subgroups for which we can construct factor groups. Recall that a subgroup $H \leq G$ is called **normal** if $aH = Ha$ for every $a \in G$.

Theorem 37.

Proof.

□

Corollary 10.

Proof.

□

Definition 57. (Factor Group)

Example 73.

Example 74.

13.3 The Fundamental Homomorphism Theorem

In Theorem 1, we showed that ever homomorphism $\phi : G. \to G'$ gives rise to a factor group $G/\ker\phi$. We now prove the converse.

Theorem 38.

Proof. □

Theorem 39. (The Fundamental Homomorphism Theorem)

Proof. □

Example 75. Classify the following factor groups according to FTFGAG.

1. $(\mathbb{Z}_4 \times \mathbb{Z}_3)/(\{0\} \times \mathbb{Z}_3)$

2. $(\mathbb{Z} \times \mathbb{Z})/(\langle(1,0),(0,5)\rangle)$.

13.4 Normal Subgroups and Inner Automorphisms

Theorem 40. The following are three equivalent conditions for a subgroup H of a group G to be a **normal** subgroup.

1.

2.

3.

Proof.

□

Remark 31. Let G be an abelian group.

Remark 32.

Definition 58.

Remark 33.

14 Rings and Fields

Learning Objectives:

- Differentiate between groups, rings, and fields
- Prove results about basic properties of groups
- Provide examples of commutative and non-commutative rings.

Until now, we have only looked at algebraic structures with one binary operation. Today we will explore structures with two operations and list their axiomatic definition and properties.

14.1 Definition and Basic Examples

Definition 59. (Ring)

$\mathscr{R}_1$:

$\mathscr{R}_2$:

$\mathscr{R}_3$:

Example 76.

Example 77. We now present several examples of rings.

1.

2.

3.

4.

5.

6.

Theorem 41.

Proof.

□

14.2 Homomorphisms and Isomorphisms

Definition 60.

Example 78. We now present two examples.

1.

2.

14.3 Fields

Definition 61. (Commutative, Unity)

Remark 34.

Definition 62. (Unit, Field, Division Ring)

Example 79. We present some examples and non-examples:

1.

2.

3.

4.

Definition 63. (Subring, Subfield)